Hubert B. Keller
Wolf-Dieter Pilz
Bernd Schulz-Forberg
Christian Langenbach

Technical Safety – An Attribute of Quality

An Interdisciplinary Approach and Guideline

Springer

Technical Safety – An Attribute of Quality

Hubert B. Keller · Wolf-Dieter Pilz
Bernd Schulz-Forberg · Christian Langenbach

Technical Safety – An Attribute of Quality

An Interdisciplinary Approach and Guideline

Springer

Hubert B. Keller
Institute of Applied Computer Science
Karlsruhe Institute of Technology
Karlsruhe
Germany

Wolf-Dieter Pilz
Former Airbus Defence and Space
Gerolsbach
Germany

Bernd Schulz-Forberg
Former Federal Institute for Materials
Research and Testing (BAM)
Berlin
Germany

Christian Langenbach
Program Directorate Space Research
and Technology
German Aerospace Centre (DLR)
Cologne
Germany

ISBN 978-3-319-68624-0 ISBN 978-3-319-68625-7 (eBook)
https://doi.org/10.1007/978-3-319-68625-7

Library of Congress Control Number: 2017954286

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Supporting Organizations and People

The authors would like to express their gratitude to people and organizations who support this book.

The following persons contributed own textual and editorial inputs for the VDI (Association of German Engineers) committee “Technical Safety”:

Eschenfelder, Dieter, Dipl.-Ing., Düsseldorf
Gelfort, Eicke, Dr. rer. nat., Köln
Graßmuck, Jochem, Dipl.-Ing., Berlin
Grünberg, Jürgen, Prof., Dr.-Ing., Hannover
Hansen, Michael, PD Dr.-Ing. habil., Hannover
Keller, Hubert B., Dr.-Ing., Karlsruhe
Kunde, Michael, Berlin
Langenbach, Christian, Dr.-Ing., München
Lemiesz, Dieter, Dr.-Ing., Ratingen
Pilz, Wolf Dieter, Dipl.-Ing., Gerolsbach (Chairman)
Rath, Robert, Dr. iur., Berlin
Schulz-Forberg, Bernd, Dr.-Ing., Dir. u. Prof. a.D., Berlin (Deputy Chairman)
Wanduch, Volker, Dipl.-Ing., Düsseldorf
Wilpert, Bernhard, Prof. Dr. phil. Dr. h.c. †
Wingender, Hans-Jörg, Dr. phil. nat., Mömbris

These corresponding companies, institutions and authorities supplied valuable contributions to the VDI committee “Technical Safety”:

Bayerische Motoren Werke AG (BMW), München
Brandenburgische Technische Universität (BTU), Cottbus/Senftenberg
Bundesanstalt für Materialforschung und -prüfung (BAM), Berlin
Bundesministerium für Wirtschaft und Energie (BMWi), Berlin
Eisenbahn-Bundesamt (EBA), Bonn
Gesamtverband der Deutschen Versicherungswirtschaft e.V., Berlin
Katholische Universität Eichstätt-Ingolstadt (KU), Eichstätt
Öko-Institut e.V., Freiburg / Darmstadt/Berlin
Universität Stuttgart, Stuttgart

We would also like to express our gratitude for supporting us to:
Mrs. Jennifer Sweety Johnson, Mr. Thomas Ditzinger and Mr. Dieter Merkle (all Springer Verlag Berlin Heidelberg)
Dr. Martin Wesson (Berlin), Mr. Karl-Heinz Höppner (Dipl.-Grafik-Designer AGD) and Mrs. Sabine Scheer (KIT-IAI, Karlsruhe)

Without the support of the following companies and institutions, we would not had been able to realize this book:

Ada Deutschland e.V., Karlsruhe

Bundesanstalt für Materialforschung und -prüfung (BAM), Berlin

German Aerospace Center (DLR e.V.), Köln

Karlsruhe Institute of Technology, Karlsruhe

The VDI committee “Technical Safety” was initiated in 1985 by
Reinhard Menger, Dr.-Ing., Director of VDI, Düsseldorf
Gustav Wagner, Dr. rer. nat., Curator of VDI (and member of the Supervisory Board of Robert Bosch GmbH), Stuttgart
after the unanimous decision of a high-ranking staffed ad hoc committee, which was charged to develop a promising and forward-looking interdisciplinary mission for the VDI.

Contents

1 Preamble 1

2 Development of Technical Safety 5

3 Interdisciplinary Approach 9

3.1 Need for a Safety Methodically Concept 9

3.1.1 The Need for Action in Safety Engineering 9

3.1.2 Introduction to the Application Area Safety Engineering 11

3.1.3 Reasons for this Publication 12

3.1.4 The General Framework for Technical Safety 14

3.1.5 Legal Basis of Technical Safety 15

3.1.6 Ethical Principles 17

3.2 Generating Safety 18

3.2.1 Principles of Safety Engineering 18

3.2.2 Procedures for an Interdisciplinary Safety-Methodical Concept 25

3.2.3 Implications of a Safety Methodically Concept 43

3.3 Limits of Safety 46

3.3.1 Socially Accepted and State-Defined Limits 47

3.3.2 Unattainability of Absolute Safety 49

3.3.3 The Understanding of Risk 50

3.3.4 Factual Relationship Between Risk, Safety Engineering and Technical Safety 51

3.3.5 Safety-Engineering Feasibility 52

3.4 Verifiability of Safety 57

3.4.1 Limits of Verifiability 57

3.4.2 Learning as a Continuous Task 59

3.4.3 Controlling Technical Safety in the Product Life Cycle . . . 64

3.5 Social Considerations 82
3.5.1 Prevention of Safety-Critical Failures 82
3.5.2 Communication with the Public About Technical Safety 86
3.6 Recommendations 89
3.6.1 The Research Landscape 90
3.6.2 Education and Training Options of the Universities 91
3.6.3 Thematic Focuses 92
3.6.4 Emergency Planning 95
3.6.5 Internationalization 96

4 Interdisciplinary Safety Guideline 97
4.1 Understanding of the Term Safety 97
4.1.1 Safety as a Legal Term 97
4.1.2 The Term "Technical Safety" 98
4.1.3 Technical Safety as a Requirement for Product Design and Implementation 99
4.2 Introduction to Interdisciplinary Safety Engineering 102
4.2.1 Organization and Management 102
4.2.2 Systematics 107
4.3 Generating Safety 119
4.3.1 Safety Methodology 119
4.3.2 Implementation of the Safety Concept 127
4.3.3 Software-Based Functionality and Human Factors 149
4.3.4 Supportive Management 154
4.4 Safety-Compliant Design in Civil Engineering and Process Plant Engineering 170
4.4.1 Notes to the Flow Chart 172
4.4.2 Definitions with Regard to the Flow Chart 175

5 Proposal of the VDI "Technical Safety" Committee 177

6 Summary—Lessons Learned 179

VDI "Technical Safety" Committee 181

References 183

Chapter 1
Preamble

Characteristic of our history as human beings is our development and use of tools and systems which function reliably and are controllable as regards "technical safety"—ranging from simple devices such as hammers and shovels to complex systems such as aircraft and mainframe computers. "technical safety" is to be regarded as an integrated part of the stipulated function (target function). This calls for a holistic way of thinking and a systematic approach over the complete life cycle of products and systems. Here, we must go back to the established structures: "generally accepted rules of technology", the "state of the art" and the "state of science and technology". "technical safety" is an inherent quality attribute whose characteristics must be created systematically.

At the present time every technical field, be it civil engineering, transportation systems, chemical engineering, energy technology, aeronautical engineering, plant construction, mechanical or electrical engineering, has its own system of rules for technical safety. Application-specific safety concepts are developed for conception, definition, development and engineering, production and integration. They contain detailed building regulations, operating procedures, operating regulations and maintenance instructions, as well as requirements relating to retrofitting and disposal. Even the supervision of the operation by the operating company itself and the appropriate supervisory authority is prescribed in application-specific rules and standards. This means that there is no safety concept which covers all fields of application, i.e. interdisciplinary validity. Furthermore, new technologies require and have to be provided with additional rules and standards. In the light of this situation and its previous involvement in the creation of the modern standard of technical rules and safety supervision, the Association of German Engineers (Verein Deutscher Ingenieure—VDI) has seen the need to take action.

The beginning of the 1970s saw the emergence of sociopolitical visions which appeared to make a "risk-free" life possible for the population. The common focus of this development was public discussion of large-scale and technologically innovative facilities, whose safety or safety capability above all was presented as questionable. Particularly in the case of technological innovations, there was more

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_1

talk about potential risks and—in some cases only ostensibly—undesirable side effects than about the actual benefits to the population or economic and social opportunities. As a result, it was no longer the technical assessment alone which was important in making decisions about the safety of such installations but, increasingly, a political and legal assessment as well. The reports of technical experts consulted also revealed the detrimental situation in modern safety engineering, which provides concepts whose particular form depends on the field of application. Even the standards produced by DIN, the German Institute for Standardization, provide a remarkable number of different definitions for "safety" and "technical safety".

About thirty years ago, the European Union (EU) commenced its efforts aimed at implementing the free trade of consumer and capital goods. Bound up with this was the question as to how safety could be ensured for the people using the goods. The set of instruments for safety supervision and approval, whose character at this time was mostly nationally oriented, tended to place obstacles in the way of trade rather than prevent them. With its "New Approach" and "Global Approach", the European Commission, therefore, created a catalogue of measures by which a high degree of independence from national bodies could be achieved on the operative level. The instrument for this was the Declaration of Conformity which, according to the resolution of the European Council, could be issued by either the manufacturer itself or so-called notified bodies. The level of safety itself is laid down here in the European directives and predominantly specified in detail in mandated technical standards. Opinions vary as to the effectiveness of this catalogue of measures. It has clearly already been recognized that both the "New Approach" and the "Global Approach" have considerable weaknesses and are partly a long way behind the effectiveness of the system they replaced. These weaknesses, which at the time of introduction were already known to the experts dealing with safety issues, are diverse and being tackled by the European Commission, and the extent to which these shortcomings can be comprehensively remedied remains to be seen. Over and above the product-related directives, there is the "General Product Safety Directive" 2001/95/EG dated 03.12.2001, which requires all products being put on the market within the European Economic Area to be safe. Precisely how this is to be ensured does, however, call for further regulation.

In both aeronautical engineering and space technology, the New Approach system is still supplemented by mandatory international or European airworthiness certification schemes or final system tests. Similarly, the European Interoperability Directives introduced in the railways sector stipulate that, when the national safety authority grants authorization for putting into service, the new concept system should be supplemented by a final system inspection. The same applies in the process plant sector and, indeed, in other fields as well.

This fragmentation into a large number of "safeties" is increasingly becoming a problem since only a few users are able to look beyond their own area of application to recognize commonalities as a whole. In addition, different interpretations of what is required in technical safety are more and more frequently being settled legally, which in turn can lead to extraneous interference in the technical field.

In 1987, the VDI convened a committee to tackle this problem. This committee of experts agreed in favour of developing a safety concept which could be used on an interdisciplinary basis. In 1999, following a resolution of the Scientific Advisory Board, the VDI "technical safety" Committee was established. The committee was given the task of working out the **hidden commonalities** of the safety concepts in the various specialist technical fields and presenting a standardized practical guide applicable to all technical fields. On 27.09.2013, the draft was intensively discussed in a technical meeting with recognized safety experts from the most varied specialist fields. The results of this discussion have been incorporated in this publication.

It consists of:

- the preamble,
- the development of technical safety,
- the interdisciplinary approach,
- interdisciplinary safety guideline,
- proposal of the VDI 'Technical Safety' Committee and
- summery-lessons learned

Chapter 2
Development of Technical Safety

Technology in the sense of tool developments as aids for humanity has played a central role for millennia and permanently advanced social development. In this process, technical failure was fatalistically tolerated for a long time. Nevertheless, already in 1810, Napoleon issued a decree stating that state officials were to carry out the safety inspection of boilers: this introduced and codified a turning away from the acceptance of accidents and catastrophes as twists of fate.

The markedly rapid progress of industrialization in the nineteenth century called for a comprehensive adaptation of the organizational structures of the technology used in many different ways in society and the economic system. The roots of this are to be found in the Royal Commercial Institute of Berlin, amongst others, and go back as far as 1846. Members of the Academic Association Hütte [Akademischer Vereins Hütte] in Berlin founded the Association of German Engineers (VDI) on 12 May 1856, in Alexisbad (Harz Mountains). Ten years later, in 1866, the VDI prompted the foundation of pressure vessel (steam boiler) supervisory associations as forerunners of today's Technical Supervisory Associations (Technischer Überwachungsvereine–TÜV). In addition, parallel developments, such as those from Mannheim and Bavaria, were taken up and incorporated.

A glimpse into the Bavarian economy of that time makes clear the extent of this development: not a single one of the 1301 pressure vessels in the meantime suffered damage following the introduction of supervisory measures. In the USA, on the other hand, no fewer than 906 of the 2000 or so pressure vessels in Boston alone exploded during a ten-year period (1867–1877).

In May 1917, the VDI appeared again as co-founder of the "Standardization Committee for Mechanical Engineering" (today, DIN). Since then, DIN standards have also served as the measure of flawless technical performance and are, therefore, also important within the legal system. These achievements are also of particular importance to the quality characteristic "technical safety". Nevertheless, it should never be forgotten that the safety level of technical products which has become so taken for granted today is based on the wealth of experience which has

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_2

systematically documented the progressive development of technology over the past centuries. It is common knowledge amongst engineers that:

- 100% safety is unrealizable,
- the quality characteristic "technical safety"—like every other quality characteristic—must be "designed into", "developed into" and "built into" the technical product in question via an engineering process,
- the quality characteristic "technical safety" requires a topic-oriented technical management system (the more complex the structure, the greater the demands on management),
- technical safety constitutes a legal claim whose fulfilment requires a mandatory proof and
- the specification of vague legal terms such as "state of the art" does not suffice in itself to guarantee safety. It is necessary but not sufficient.

Developments in law and technology move in different spheres and at different speeds. In order to create a dependable connection here, vague legal concepts are used in laws and other statutory regulations. When technical safety (the safety of technical products and equipment) is mentioned in laws and legal regulations it is always by "indirect reference" to so-called "general clauses" and "vague legal concepts". These vague legal concepts are then: "generally accepted sound engineering practice", the "state of the art" and the "state of scientific and technical knowledge", together with other special forms such as "recognized good engineering practice" and the "state of safety technology". According to the prevalent legal opinion, which the leading technology lawyers Prof. Dr. Fritz Nicklisch (mainly civil law) and Prof. Dr. Peter Marburger (mainly public law) represent and which has been and will be published widely, legislators and competent authorities employ these "vague legal concepts". In case of need (regarding technology), experts with the relevant qualifications must render these concepts in specific terms, provided the standards to which reference is made can be interpreted or are inadequate on their own. In this case, these vague legal concepts are made so concrete that they become accessible for the application of the law (see [1]). It is part of the standard practice of appointed and sworn experts in this regard that, when making the vague legal concepts of "good engineering practice" and the like concrete, they refer first of all to the rules of technology, in other words to technical rules such as DIN standards, VDI regulations and, increasingly nowadays, standards issued by CEN and ISO. These standards are prepared by experts from manufacturers, consumer organizations, commercial enterprises, universities, insurance companies, public authorities and testing institutes which have an interest in the specific subject of standardization, in other words, the so-called "interested circles". They send their experts to a relevant committee, DIN for example. Standards, like other technical rules, are created by consensus: the delegated experts agree on the contents with the aim of achieving a common understanding regarding the subject of standardization. Technical rules are one of the principal items of reference for ensuring technical products and equipment are **safe** when they are put on the market and use is made of their function. This procedure is standard for existing products and systems.

Should there be major expansions of what is technically available and even further to fundamental innovations, reference to product standards alone will not suffice to ensure technical safety. In this case, the relevant state of the art or state of scientific and technical knowledge must be determined and applied. Guidance in the form of standards is becoming increasingly available even for these processes.

Once again it was the VDI which, at the beginning of the 1970s, took up the technical application of probabilistic parameters and prepared them for engineering use. The VDI handbook on reliability [2], first published nearly twenty years ago, together with its standards VDI 4001 ff., provides a comprehensive introduction to modern reliability engineering and also renders it practicable. It thus contributes to making sufficiently manageable the technical problems, costs and risks which can arise from the failures in the functions of technical products and systems that can never be entirely ruled out. Its application extends to all those areas of engineering in which problems of environmental resistance (resistance to environmental influences), lifetime and service life, functional reliability, maintainability and maintenance, availability and also **safety** are to be expected, have already occurred and need to be rendered manageable. They are areas in which technically sensible, appropriate precautionary measures are required in project planning, design and construction, manufacturing and system integration, etc. The globally recognized achievements of modern aerospace technology are proof of the exceptionally high level of performance of these probabilistic methods in engineering.

However, even today it may be observed that probabilistic approaches are being simplified in a way which is scientifically impermissible. Examples of this are taking redundancies alone into consideration (but ignoring the corresponding failure probabilities) and equating the (stochastic) "mean time between failures (MTBF)" with the (deterministic) "lifetime". In the latter case, it is suggested that function failure can be excluded by redundant functions or even that spontaneous failure can be prevented by "diversitary function elements". In this context, it is worrying that such simplifications can even be brought to application when technical safety is supposed to be the objective.

In engineering, the indispensable basis of any probabilistic method is the systematic determination of **all** failure modes of functions and function elements. However, behavioural analyses of this kind (e.g., FMEA: Failure mode and effect analysis and also FMECA: Failure mode, effect and criticality analysis) are also suitable ways of determining (failure) **risks**. Nevertheless, it is increasingly the case nowadays that the successful and centuries-old routine practice of making calculated risks manageable is now all too readily dispensed with. To an ever greater extent, the generation of technical safety is being replaced more and more by risk analyses or risk assessments. In such cases, an engineering-based procedure is terminated prematurely or even entirely neglected. This enables the creation of scenarios in which technical innovations—often involving an incredibly high outlay in the media and political spheres—are prematurely disqualified for safety-related reasons without there being the remotest reason for casting doubt from the start on, or denying completely, the safety to be achieved in the future.

At the beginning of the twenty-first century, deliberation at the VDI resulted in the approach presented in this publication and in a guideline showing how the **hidden commonalities** in the safety-related knowledge available can be made useful for technological changes and innovations. This concept enables the use of all safety-related knowledge and good engineering practice not only for time-tested but also for innovative technologies. This, above all, includes the realization that the demand for 100% safety—unfortunately still even today—counts as one of the most persistent misconceptions in the history of technology. Engineering and, in particular, safety technology must take this realization into consideration. In our world, there is neither an "absence of danger" nor any "risk-free areas". However, well-founded knowledge relating to technical safety need no longer remain confined to separate application in individual fields of technology but is now available even for comprehensive interdisciplinary use. With the publication of DIN 31004-1 "Terminology in Safety Technology—Basic Terminology"[1] the term "safety" is defined in a technical regulation on the basis of the concept of "risk", which is a probabilistic parameter. Probabilistic concepts thus made their first entry into classic safety technology, which until that time was chiefly characterized by legally motivated causal considerations (if-then relationships). At the time of publication of this standard, safety concepts based on probability considerations had for several decades already proved their value in the field of aerospace engineering, which resulted in a much higher level of safety there.

Every technical field of application now has its own code of practice for technical safety and this is, following an accident, often very specifically expanded. This large number of "safeties" is increasingly becoming a problem as only a few safety experts can see the whole picture beyond the limits of their own sphere of application. In addition, different interpretations of what is required regarding technical safety are leading more and more often to legal disputes, which in turn may result in conclusions that are inappropriate in the field of technology. The debate which started on the occasion of the annual politicians' conference organized by the VDI main group "The Engineer in Profession and Society" in Trier on 10th and 11th september 1984 has been continued in many ways without any solution being arrived at yet.

[1]The provisions of this standard are now to be found in DIN 820-12:2014-06 "Standardization work; Part 12: Guideline for the inclusion of safety aspects in standards".

Chapter 3
Interdisciplinary Approach

3.1 Need for a Safety Methodically Concept

3.1.1 The Need for Action in Safety Engineering

The last century was marked by epoch-making technological achievements. The two world wars caused devastating destruction, but reconstruction also accelerated the technical progress which, above all, characterized the years of rebuilding after the Second World War. New technologies were developed and are being constantly further developed. Worldwide air travel has long become a reality; space technology has become a productive branch of the economy, and microelectronics and computer technology are now an indispensable part of private life. However, as a result of this technological progress, the number of engineering fields has grown—technical subjects are now taught in the technical universities and colleges whose existence half a century ago was not even imaginable. Of course, safety technology has also kept developing continuously parallel to technological progress although specifically for the individual fields of engineering. One of the key reasons for this application-oriented safety technology structured according to individual fields of engineering is to be found in the German legal system since the legal basis for safety technology is also structured according to engineering fields: construction law, railways legislation, air traffic legislation, atomic energy legislation and test facilities legislation, to name just a few.

To date, the number of technical specialist fields has already increased to such an extent that the total field of technical knowledge would have become immense and poorly manageable had not interdisciplinary management methods and system-technical working procedures been introduced. Planning, tracking (monitoring) and verification are carried out with these methods in the various technical specialist fields by following a holistic procedural concept. Over the last forty years, these interdisciplinary management methods and system-technical working procedures, grouped together under the term “interdisciplinary teamwork”, have found ever

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_3

greater application. No major project, which today could cover many years, is now undertaken without the input of a central project management system. With increasing globalization, there is also a greater necessity for internationalized project management with a multilingual capability and operating over national borders. The world of technology does not seem to recognize borders any more. However, these borders do exist, namely in the field of safety engineering. Apart from already existing European regulations (which are, however, principally supposed to ensure the free movement of goods), the provisions of different national legislation still apply here. What they all have in common is their assumption that safety technology is structured on the basis of application-specific fields of engineering.

As has already been mentioned, new sociopolitical ideas arose at the beginning of the 1970s which appeared to make a "risk-free" life possible for citizens (see Sect. 3.1) Thus, public debate was increasingly more concerned with conceivably possible side effects than with the technical facility whose implementation process needed to be managed in the best possible way. Ultimately, it was no longer a technical but increasingly a legal body which had the final say on the safety of the affected facilities. It is problematic that the very exemplary standards issued by DIN show a remarkable variety of different term definitions for "safety" and "technical safety".

Around twenty years ago, the European Union (EU) commenced its efforts aimed at implementing the free movement of consumer and capital goods. Bound up with this was the question as to how safety could be ensured for the people using the goods. The instruments for safety monitoring and approval, whose character at this time was mostly nationally oriented, tended to place obstacles in the way of trade rather than preventing them. Therefore, the European Commission created with its New Approach and Global Approach a catalogue of measures by which a high degree of independence from national bodies was supposed to be achieved on the operative level. The instrument for this was the Declaration of Conformity which, according to the resolution of the European Union Council, could be issued by either the manufacturer itself or a so-called Notified Body. The level of safety itself is laid down in the European directives and generally partly specified in detail in mandated technical standards. Opinions vary as to the ultimate effectiveness of this catalogue of measures. It has clearly already been recognized that both the New Approach and the Global Approach have considerable weaknesses and to some extent are a long way behind the effectiveness of the system they replaced. These weaknesses, which at the time of introduction were already known to the experts dealing with safety issues, are diverse, and improvements are currently being made by the European Commission. The "General Product Safety Directive" 2001/95/EG applies over and above the product-related directives. This regulates that all products being put on the market within the European Economic Area have to be safe. Precisely how this is to be ensured does, however, call for further regulation.

In both aeronautical engineering and space technology, the New Approach system is still supplemented, as before, by mandatory international or European airworthiness tests or final system tests. The European Interoperability Directives

introduced in the railways sector also stipulate in this way that, when the national safety authority grants authorization for putting into service, the New Approach system be supplemented by a final system test.

There is, therefore, sufficient need for a safety methodically holistic concept in which the hidden commonalities of existing safety concepts (admittedly limited by being application-specific) are joined together into an interdisciplinarily applicable overall concept. The VDI has the interdisciplinary technical expertise to elaborate and present such a safety methodically holistic concept.

3.1.2 Introduction to the Application Area Safety Engineering

In their performance of public services, state bodies and institutions—in Germany at least—had up to this point carried out safety-related verification analyses and, in this way, actively participated in the control of technical risks. The relevant EU directives in the meantime envisage these safety-related verifications being increasingly left to the free market and only monitored by the state. The expertise required for this in the field of technical safety, which was previously mostly the concern of governmental agencies, must now be obtained on the free market. The approach outlined in this VDI publication is intended to maintain and spread this safety-related expertise by encouraging a safety methodically concept which, by extensively referring to generally accepted technical regulations and defined objectives, offers a firm basis for engineering practice in the field of safety engineering. This safety methodically concept is equally applicable to the maintenance and further development of existing fields of technology (e.g. civil engineering, transportation systems, chemical process engineering, energy technology, aviation, plant engineering and construction, mechanical engineering or electrical engineering) as to the conceptual design of innovative technologies and their controlled safety-related development.

The term “technical safety” is understood as meaning that a technical system, technical facility or product will fulfil its intended functions over a planned period of time (if applicable, its planned lifetime) and, provided it is operated according to regulations, will not injure or damage any objects of legal protection. This means that neither persons nor property is injured or damaged in as far as the system, the technical facility or the product can be responsible for this. Reliability of function over the envisaged lifetime is not a necessary component of safety, provided loss of function does not lead to an unsafe state.

In the context of discussing technology, safety means more than just technical safety. In everyday speech, a person feels “safe” when he/she does not feel threatened. This threat need not be existential in nature in any way. An impending loss in the quality of life can already trigger a prejudice against technology. In a liberal and affluent society, a situation in which one’s own way of living is

determined by others and the associated feeling of being dependent on conditions not freely chosen (loss of autonomy) can result in aversive reactions in individual groups when the subject of the limits of safety is raised.

On the one hand, the bases for decisions are more weakly developed here in some of the engineering sciences, but also in the life sciences. On the other hand, the public's notions of safety are so broad that adequate acceptance can only be achieved on the basis of a risk-minimization imperative—a limitation with an accepted limiting risk. The expectations of the consumer are manifestly expressed in the idea behind the purity regulations, which at least cover the immediate necessities of life such as food, drinking water and air. Technologies, such as those concerning preservation and processability, which infringe the purity regulations while still offering clear benefits, are only tolerated for as long as they do not infringe legally stipulated contamination levels, provided these technologies are being correctly employed (one example is "good farming practice"). The gap between these levels and the higher health tolerance threshold can however be several orders of magnitude. The rule applies to set permissible limit values as low as necessary but as high as possible.

From this point of view, safety-related technical considerations must, in the broader sense, also apply to the safeguarding of consumer expectations. Incidents which result in threshold values being violated are perceived by the public in most cases as an imminent threat to their physical integrity. Experience shows that the reaction of state supervisory bodies strengthens this impression, especially when there is insufficient latitude for assessing the proportionality of the means for hazard prevention.

In the main features of a general safety methodically concept, the particular form of dealing with "residual uncertainty" (which is a standard concept or special characteristic of the life sciences) cannot be ignored in discussions about the uses and harms in risk management, but it is not examined in greater detail. Clarification is needed that this is an interdisciplinary, scientifically based safety guideline. In the interests of precise statements, the lines of argument and the terms used in this publication have been borrowed from the engineering sciences.

3.1.3 Reasons for this Publication

Spectacular incidents and accidents with a great public impact repeatedly raise the question of adequate safety in technical facilities. In such cases, there is a tendency for some of the media to respond only to the event itself in their news reports but also, at the same time, to rush to assign blame. There is a very common attitude of quickly pointing the finger at a culprit responsible for the failure. Accordingly, there will always be technical experts who support these assumptions as far as possible. In the next step, the question is then immediately asked as to whether the laws, statutory orders, monitoring requirements and sets of regulations are adequate to ensure the expected level of safety.

This typical approach disregards the fact that

- there is no such thing as 100% safety, even though the limits of safety are always to be observed,
- safety must be generated—in other words, developed and produced—before it can be maintained and monitored during utilization, and
- complex circumstances do not in most cases allow the identification of a monocausal connection in incidents and accidents. Instead, there are often in the implementation events, which are not taken into consideration, unknown influences or previously unidentified chains of multiple influences which result in damage.

Safety is, in most cases, created by applying relevant standards and codes of practice and existing legal provisions. Safety concepts are developed with mathematical models and analytical methods. Years of empirical experience gained specifically in the most diverse application areas (civil engineering, transportation systems, chemical process engineering, energy technology, aviation, plant construction, mechanical engineering, electrical engineering, etc.) are also integrated in these concepts. This is one of the reasons why no uniform safety concept as yet exists which spans all application areas.

The development, construction, design and manufacture of a particular technical facility are thus determined by different safety concepts. Detailed operating instructions, operating regulations and maintenance instructions are drawn up for its operation and requirements formulated for retrofitting. Monitoring of operations by the owner and the other bodies entrusted with monitoring is clearly regulated.

The conceptual design, development, manufacture, operation, decommissioning and monitoring of technical facilities require in a particular way the skills of engineers. The VDI addresses these issues with this publication firstly by presenting to the specialist community the current situation regarding the safety of technical facilities. In addition, problem areas are identified such as:

- legal appraisals, assessments and judgments which have a bearing on safety,
- unforeseeable events and chains of events leading to disturbances and failures of technical facilities and
- the individual person as a developer, manufacturer, user, operator and monitoring agent who, although not working free of error himself/herself, nevertheless has a decisive influence on safety.

Recommendations for an interdisciplinary safety concept are derived from this as to how the most diverse safety concepts must be designed and further developed in the future and how the cooperation of all participants must be organized for this purpose.

3.1.4 The General Framework for Technical Safety

Insight into and understanding of the limits of technical safety derive from a number of aspects, e.g. the probability of occurrence and expectation of damage, failure, perception and risk, whose importance requires fundamental and binding clarification. Technical safety is limited by the probability of damage occurring or, depending on the case, the failure of a technical facility. The circumstances are usually subsumed under the term "risk". This is, however, a complex concept (see Sect. 3.3.3) because it is modified by a very different and constantly changing perception.

Dealing with risks which are insufficiently known or are not manageable poses a problem, and difficulties also arise when markedly diverse opinions prevail regarding the assessment of a risk. In such cases, the necessary precautions are essentially a sociopolitical decision. Primarily taken into consideration are dangers emerging from nature, the natural environment, the technical environment, human inadequacy and mistakes:

- hazards from the natural environment may arise, for example, due to:
  - climatic influences in all possible forms at the location (wind, snow, ice, temperatures, etc.),
  - physical influences (e.g. lightning strikes, earthquakes) and
  - reduction in the resistances of construction components due to corrosion, fatigue and ageing;
- hazards from the technical environment may arise, for example, due to:
  - exceeding specified unladen weights and actual loads,
  - influences from the technical environment (nearby buildings, vehicle collisions, physical exposure, chemical exposure),
  - reduction in electrical resistance due to corrosion, fatigue and ageing,
  - production-related failure to reach the calculated requirements for construction components and supporting structures and
  - exceptional influences arising from use (fire, explosions).

Human inadequacies and mistakes can be the causative source of a hazard or impede a successful prevention of hazards. This includes all decisions, actions and omissions in planning, execution and utilization which a series of factors may be the basis of, e.g.

- subjectively unrecognized or objectively unknown hazards,
- insufficient knowledge,
- information gaps, misunderstandings,
- incorrect decisions due to political pressure or misconceived thriftiness and
- negligence.

Hazards may also arise through intentional but unfathomable human actions.

Table 3.1 Hazard categories

Possible consequences of hazards affecting primarily		
Properties	Usability	Hazard category
Large importance of the technical system or facility for the general public; manifold threat to life and limb	Large commercial consequences, large detriment to use; cascade effects	3
Threat to life and limb and/or respectable commercial consequences	Extensive commercial consequences, noticeable detriment to use	2
No jeopardy for life and limb and marginal commercial consequences	Marginal commercial consequences, marginal detriment to use	1

With regard to the possible consequences, the frequency and duration of hazards and the type of preventive measures necessary, a distinction can be drawn between:

- permanent situations whose duration is of the same order of magnitude as the useful life of the system or facility concerned (intended course of operation),
- temporary situations of short duration and with a high probability of occurrence (possibly a rectifiable disturbance of intended operation) and
- exceptional situations arising from exceptional influences or, in the case of local failures, of short duration and with a low probability of occurrence, with long recurrence intervals and a great potential for danger (see also Table 3.1 in Sect. 3.2.1.1).

3.1.5 Legal Basis of Technical Safety

Technical safety is very largely based on the engineering and natural sciences and is administrated by the relevant regulatory legislation. The safety of technical facilities is created by methods which provide systematically hierarchized safety precautions (see Table 3.1). These are formed by both technical measures and organizational arrangements. Detailed regulations often exist for technical measures and regulate the requirements for measures such as safety margins, the degree of redundancy, the diversity to be provided and testing. Limiting values, test specifications and management systems are required and implemented in the form of laws and often as sub-statutory regulations as regards technical and organizational measures. Public technical safety for the citizen thus generally requires that the utilization of technology does not

- unacceptably affect the individual in his/her right to life and physical integrity,
- unacceptably, impermissibly—due to hazardous substances, for example—or irreversibly damage the environment or
- damage other objects of legal protection (property of third parties).

The guarantee of public technical safety thus falls within the responsibility of the individual nation state and, in some fields increasingly, within the responsibility of the EU and even, if applicable, of the United Nations. Public-technical safety is the part of safety which is characterized by the systematic individual risk and the collective risk emerging from the active and, in particular, the passive utilization of technical products, facilities and systems as well as the associated processes for whose regulation the state is responsible. All in all, the state has responsibility for ensuring the safety of its citizens against risks arising from scientific and engineering research and development especially as regards application of the results obtained and forms of technical implementation. It is referred to here as "public-technical safety" and also so understood in general.

Guaranteeing public-technical safety in a constantly changing technological and industrial environment can in its current significance and complexity only be regarded as the state's provision for its internal and external safety. Technical facilities must therefore comply with the objective legal system. It is implemented by legislation in the field of technology, for example, by means of special legal regulations, provisions, guidelines and technical rules. A danger to public safety or order exists when circumstances or an event will probably damage an asset under legal protection if the occurrence objectively expected is permitted to continue unobstructed (Second Senate of the Federal Constitutional Court in its decision of 08.08.78, File no.: 2 BvL 8/77, the so-called Kalkar judgement).

In principle, a distinction is to be drawn between a concrete, tangible hazard and an abstract hazard, which is only conceivable. As to the expected occurrence of damage, the two types of hazard have the same requirements regarding probability. The distinction between "concrete" and "abstract" hazards lies in the point of view. Concrete hazards relate to the individual case, whereby the time at which damage possibly occurs need not be imminent. This time is, however, not so far off that it is no longer manageable.

A hazard is deemed to exist when observation of certain types of behaviour or conditions leads to the conclusion that there is sufficient probability that damage will occur in an individual case. There must therefore be grounds for preventing such hazards even with general-abstract means, e.g. in technology law itself or by technical rules. Verification of the probability of occurrence can then be dispensed with in the individual case. Hazards which are detected when generally accepted threshold values are exceeded are clearly of a concrete nature.

The necessarily vaguely formulated legal requirements regarding the technical safety of technical systems and facilities must be made concrete with technical rules drawn up, not by legally competent committees but experts from the relevant technical fields.

The necessary governmental measures comply primarily with the inherent potential for damage of the respective technical products, processes, facilities and systems, including their subsequent effects. They range from legislative frameworks covering approval and supervisory functions to direct state intervention.

In its duty of care, the state has an obligation to do its utmost to prevent or, by all means, limit injury not only to society as a whole but also to individual humans. In this matter, however, it is not only the safety requirements of the objects of legal protection under consideration—humanity and the environment, for example—which can be determined. It requires, rather, a balancing of their usefulness and/or necessity for society on the one hand and the risks of technology on the other. This results in a risk management system.

3.1.6 Ethical Principles

Technical safety is essentially developed by engineers and natural scientists even though the humanities are becoming increasingly influential. In their responsibility for this, they not only comply with the provisions of the applicable legal system but also, above all, follow the ethical and moral principles which have evolved over the millennia of Western history. The engineer's responsibility is thus anchored in basic ethical standards and the moral obligations developing from them.

In recognizing the engineer's responsibility, the VDI has committed itself to the following ethical principles for the profession of engineer (Düsseldorf, March 2002):

"Engineers

- are individually or jointly responsible for the consequences of their professional work as well as for the diligent discharge of their specific duties,
- acknowledge their obligation to deliver sensible technical inventions and sustainable solutions,
- are aware of the interrelationships of technical, social, economic and ecological systems and their effects in the future,
- avoid deeds which result in constraints on and restriction of independent action,
- orientate themselves on the basic principles of general moral responsibility and respect labour, environmental and technology legislation,
- discuss conflicting values on an interdisciplinary and cross-cultural basis,
- seek institutional support when profession-related moral conflicts arise,
- participate in the formulation and updating of legal and political guidelines,
- commit themselves to constant further training and
- involve themselves in technological mentoring in basic and further education programmes in schools, universities, companies and associations".

In everyday life, however, the distinction between ethics and morality is blurred, whereas in philosophy a clear line is drawn between ethics and morality. Ethics is accordingly the scientific examination of the various aspects of morality, and the subject of ethics is morality. Ethics deals not only with basic questions relating to the nature of morality and the possible rationale for moral standards ("meta-ethics") but also with questions relating to the content of moral values and standards ("normative ethics")—in other words, with good and bad. Among the most

important questions in normative ethics is the question to which extent consideration of consequences may or must play a role in the moral evaluation of human actions. There is no case when moral standards alone suffice to justify certain actions and strategies. If damage is to be prevented and benefits created, goodwill must always be supplemented by expertise and a prognosis capability.

The concept of morality includes both objective and subjective components. Objective components include the standards, principles and moral concepts which society lays down for the individual and are partly reflected in the legal system. Included in this are the institutions (family, media, politics, courts) which set, endorse or enforce these standards (see also [3; 4]). Corresponding on the subjective side to objectively prescribed standards are personal principles, guiding principles and ideals on the one hand and the moral attitudes, motives, feelings and willingness to act of the individual on the other. In practice, the borderline between ethics and morality is blurred. A person who acts morally usually also has an idea of the sense and function of the moral standards he/she follows and advocates and how these standards are justified. Consciously expressed to a greater or lesser extent, this also of course applies to the responsibility of engineers in their daily work and the confidence placed in their work.

Longer-term planning must arise from communication processes dealing with values and strategies for implementing them—they must not be dictated "from the top down". One such strategy is already advisable for pragmatic reasons (risk management). A diktat almost inevitably leads to credibility, trust and legitimacy crises in industry, politics and bureaucracy and contributes significantly to the polarization of positions. A stealthy introduction of new technologies by administration with a later assurance of acceptance through suitable public relations measures does not make sense here.

Rather, acceptance should be secured right from the start by means of a discursively conducted yet technically and strictly orientated approach in safety-engineering procedure. It sets an essential, maybe even mandatory, requirement of the acceptability of a democratically legitimized industrial policy. Many discussions in industrial societies are unsatisfactory since they are based on preconceived notions and one-sided presentations of the incompleteness of the current situation and assume indifferent ethical values.

3.2 Generating Safety

3.2.1 Principles of Safety Engineering

3.2.1.1 Safety—An Interdisciplinary Task

With the aid of the technical resources they have created, human beings seek to expand and perfect continuously their possibilities. This fact, which is verifiable in

our cultural history, represents a well-grounded challenge in itself for every engineer. It consists of regarding one of his/her primary tasks in implementing future engineering tasks as doing justice to the constant striving of human society to perfect the safety of technical products. The actual task here is for the human to adopt technology as a supportive function by creating the connection in the so-called human–machine systems or socio-technical systems. This challenge becomes all the more important when engineers are forced to watch an increasing lack of knowledge in the general public as regards scientific and technological correlations, which has resulted in an often frightening distrust of technology. Engineers should therefore strive to make their technical skills in the safety field generally comprehensible and understandable even for non-technicians and the layperson. In this way, the unease felt by the public towards technical facilities will be removed or at least limited to the point where no unthinking technophobia arises.

Accidents and incidents repeatedly give reason to investigate and eliminate their causes. In this matter, the effectiveness of proven and generally accepted safety-engineering precautionary measures needs to be examined. The VDI once again clearly stresses the engineers' duty of constantly developing further the field of "technical safety", simplifying its applicability and making it comprehensible to non-technicians.

In this context, however, questions do arise such as:

- Is insufficient importance being attributed today to the safety of modern, complex socio-technical systems?
- Is profitability increasingly being given priority over safety?
- Are the relevant technical standards no longer being sufficiently observed?
- Are the relevant technical standards no longer sufficiently productive?
- Are laws and statutory orders being flouted?
- Is there a lack of surveillance by governmental agencies and supervisory bodies?
- What importance does the human being have on the various operating levels?
- Are the understanding and assessment of technical laws underdeveloped (e.g. due to deficiencies in imparting knowledge in schools)?

With regard to the possible consequences of hazards, it seems appropriate to distinguish three hazard categories in technical systems or facilities within the normal range of experience (see Table 3.1). In this respect, both the public's need for safety (danger to life and limb as well as environmental hazards and the importance of the system or facility) and the commercial aspects (possible economic consequences, utilization requirements) must be provided for, whereby priority is given to the first criterion. The overall effort required in the individual hazard categories to determine countermeasures varies depending on the possible consequences of the hazards.

As a basic rule, plant components and assembly parts must be classified differently according to their importance for the nature and serviceability of a technical facility or product. In a simplified form, all important components of a system or technical facility within the scope of individual measures can be assigned to one of these hazard categories. Every safety concept should be orientated with its measures towards these hazard categories.

Achievements in safety engineering have up until now always been adequate for the underlying technological innovation achievements. However, it does seem that safety engineering and safety legislation are gradually being deprived of an ordered applicability. Particularly in modern, technologically innovative and complex systems, the following aspects are currently making it more difficult to find the most effective solution in safety engineering:

- the plethora of technical rules and standards, which often exhibit technical- and application-specific differences,
- legal regulations which apply in a purely application-specific way and the spheres of responsibility of supervisory institutions,
- the wide diversity of opinions among experts in technical and custom-designed matters and
- the specialist terminology cultivated in every technical discipline.

Even in the sphere of classical engineering, which has been manageable until now, signs of adverse effects are now emerging because

- experienced specialist personnel are either no longer available themselves or have not had sufficient opportunity to pass on their own knowledge of basic principles and contexts to subsequent generations of engineers,
- knowledge concerning aspects of safety-engineering methodology in technical rules and standards is gradually becoming swamped by the ever-increasing volume of engineering knowledge, and
- in the course of rationalizing projects, changes in technical concepts may also have been implemented but without any methodological adaption of the corresponding safety-engineering precautionary measures.

Although our legal system lays down legal requirements for safety engineering, there is no uniform concept covering all applications. This makes it more difficult for the operating engineers to pursue interdisciplinary cooperation in the field of safety engineering. Political opponents of the expansion and modernization of the technical–industrial infrastructure now tend to have courts check technical safety concepts rather than expert engineers as before. This often leads to compromise in whose politically orientated decision even safety-engineering shortcomings are accepted.

Can the looming over-regulation and bureaucratization of safety engineering and safety legislation still be averted and steered down more appropriate paths? Does the state not even have the duty, during the process of deregulation and liberalization, of compensating for the disappearance of regulations by establishing other safety principles, such as, for example, a drastic market surveillance in a similar way?

The VDI also seeks to give answers to these questions. In doing so, the following central aspects are examined:

- increasing pressure towards interdisciplinary cooperation of all concerned fields and in all fields of technology,
- generalization across all technical fields of the various safety-engineering concepts by finding the "hidden commonalities",
- subsequent feedback and application of the discovered generalization across all technical fields to individual technical fields,
- consideration of the entire life cycle of a product—from the initial idea to final disposal (see Sect. 3.2.1.2) and
- interplay between safety and the limits of feasibility on the one hand and commercial viability on the other.

As innovative technologies are developed, the corresponding safety-engineering concepts must also be worked out. For this purpose, already existing safety concepts should be investigated for hidden commonalities and merged into a safety methodically concept. A concept of this kind should include the tried and tested findings of safety engineering, which extend from the primarily empirically expanding area of application, e.g. railway technology, to the analytically shaped field of application, such as aviation and space technology. The spectrum ranges from the deterministic concept, which is based on classic if-then relationships with a directly verifiable causality in the occurrence of events (see Sect. 3.2.2.4), to the probabilistic concept of reliability, which is based on both probability observations of possible events and consideration of their possible occurrence (see Sect. 3.2.2.4). The full safety-engineering standardization in the fields of construction and electrical engineering should just as much be taken into consideration here as safety engineering based on failure analysis in the fields of aviation and space technology.

It is a matter here of how concepts in safety engineering and legislation which are practised in different custom-designed ways and have developed differently over time can be merged into a single, interdisciplinary safety methodically concept. Recourse to the methodology presented here for an interdisciplinary concept in the field of safety engineering (see Sect. 3.2.3) facilitates not only communication capabilities but also interdisciplinary cooperation between the different technical specialist fields as well as between engineers, representatives of business, politics and the judiciary and fellow citizens. This in turn will have an equally beneficial effect on technological innovation projects, which is beneficial for the understanding of safety-engineering concepts. In this way, safety-engineering concerns which are already properly respected are prevented from being pushed out of the engineer's consciousness as soon as improvements or other changes are made to technical equipment, facilities or systems.

The highly complex technologies with a great potential for utilization, which were brought to a respectable level of maturity in the latter half of the twentieth century, proved for the first time that even wide-ranging engineering tasks could be unerringly mastered with working methods on a system-technical basis. The methodology of working system technically is presented in this publication (see Sect. 3.2.3). This concept with consistent application enables the implementation of the frequently non-superimposable objectives of safety, reliability and availability

cost-effectively in one system. This is an engineering task whose universally applicable solution needs to be found in interdisciplinary cooperation between safety and cost-effectiveness as an optimization task not only in the creation of safety concepts but also in engineering practice.

3.2.1.2 Application of the System-Technical Phase Concept

In order to maintain always sufficient transparency of the technological and organizational content of complexly structured, technologically innovative and/or high-standard safety-engineering systems, facilities or products, their complete life cycle is subdivided into time segments, which hereinafter will be referred to as "phases". Such a subdivision into content and time segments allows the setting of instructions at the beginning of each of these clearly created phases clear objectives, basic conditions to be observed and other requirements and procedural instructions. At the end of each individual phase, the results obtained can be checked with regard to fulfilment of the set objectives and requirements. On the basis of the results determined, the objectives, basic conditions to be observed and other requirements and procedural instructions are set for each following phase. A phase concept of this kind not only facilitates technical management but also secures notably the organizational management measures required and, ultimately, results in it being possible for the first time to track and monitor properly the specified objectives.

The phases in the product life cycle as shown below will run in chronological order although it does remain possible, in the event of possible inconsistencies, that individual phases run recursively (as indicated by the blue recursion arrows in Fig. 3.1).

Due to the indispensable transparency of these specialist interrelations, the analysis in this publication is geared towards the phase approach presented previously. The topic of "technical safety" should be integrated into this phase concept. This applies not only to the generation of safety in every single phase of the life cycle but also to its verifiability.

Technical safety is one of the outstanding attributes of a technical system, facility or product. Creating technical safety is a task for engineers and scientists if necessary, which cannot be accomplished by itself or incidentally. Even more than any other technical specialist field, the generation and verification of technical safety requires not only the specialist knowledge of the engineers and scientists involved but also special attention and care with the technical–industrial management. Therefore, the safety-engineering process requires the same care and attention as the rest of the project over the entire life cycle of a system, facility or product—including any possible refitting or measures to extend the service life of the project. Thus, all aspects and features of technical safety in every single phase of this life cycle require proper and competent planning, proper tracking and complete verification. Such a process of planning, tracking and verification extending over the entire life cycle of a system, facility or product is commonly referred to as "controlling". Since this case is concerned with controlling in the field of "technical safety", the appropriate term here is "safety controlling" for this subject.

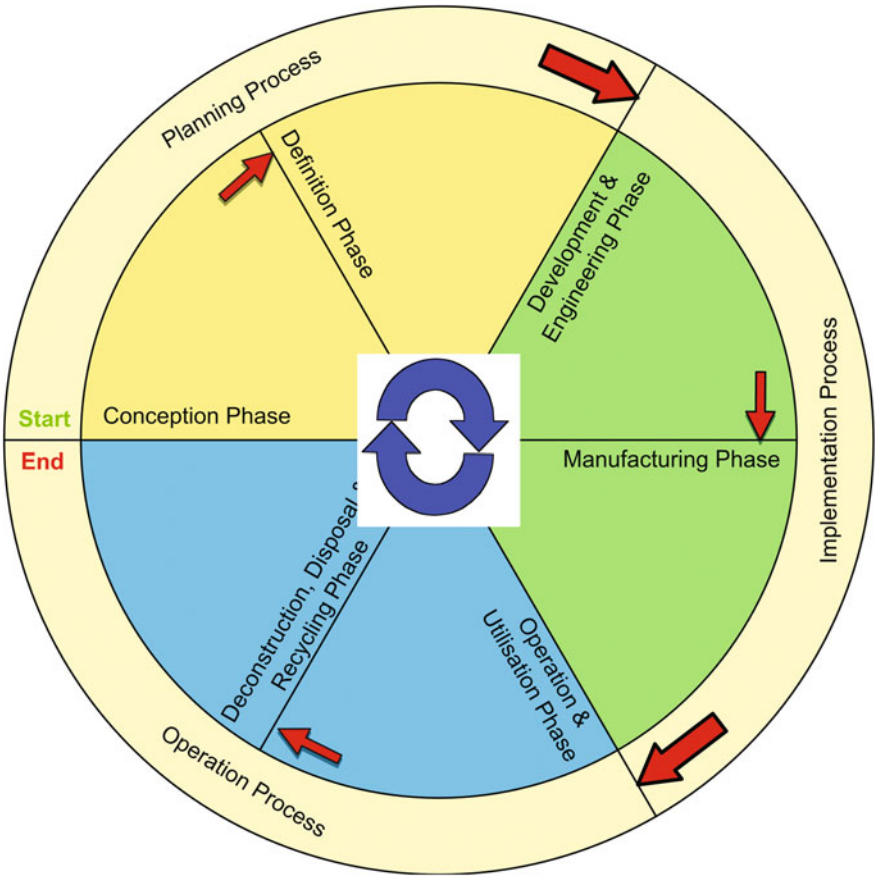

Fig. 3.1 Phases of the product life cycle

3.2.1.3 The Role of the Individual in the Safety of Complex Socio-technical Systems

Incidents and accidents in recent years have made one thing ever clearer in some fields: in view of decades of improvements in this field, the possible beneficial effect of additional improvements in technical system components in highly complex facilities with a high hazard potential is constantly decreasing. In connection with this fact, the relative importance of human actions in triggering accidents and incidents is increasing. However, it would be an unacceptable simplification to focus always solely on the operator acting directly at the human–machine interface. It follows logically from the principle of deeply hierarchized system protection, which is always implemented in complex technical systems, that an individual single error must not lead to a serious incident or accident—various technical or organizational barriers should prevent this. Only where weaknesses lie dormant and

unrecognized in the system and an unfortunate, often stochastically caused constellation of aversive conditions occurs can an incident or accident path be opened up and followed on account of individual single errors at the human–machine interface (MMI). This leads to the events assessed as negative.

The so-called phase concept (see Sect. 3.2.1.2) makes it possible to consider the entire product life cycle of technical facilities comprehensively and in detail. This applies from conception over definition, development and construction, manufacture, operation and use up to dismantling including disposal and recycling. In all phases of this chain, human action makes a significant contribution to the (lack of) reliability and the (lack of) safety of technical systems. Therefore, it is important to provide quality assurance in all phases of the life cycle of a product or service. Furthermore, analysis of serious events indicates that extreme importance is also attached to the control potential of human activity in reducing the possibly adverse or devastating consequences of accidents. The field of "human factors" (HF) is becoming an ever more intrusive complex of problems which requires specific answers. As such, the human contribution to the safety and reliability of socio-technical systems has a high relative importance.

"Human factors" are therefore to be understood as all those factors over the entire product life cycle which affect individuals in their interaction with a technical system or are caused by individuals. In this respect, the unconsidered and frequently encountered synonymous use of "human factors" and "human error" or even "human failure" is impermissible just as is the traditional restriction of the ergonomic aspect of the MMI. Organizational factors, division of labour, prior management decisions and even inter-organizational relations are relevant here in terms of a comprehensive, holistic understanding of "human factors".

The human contribution to the reliability and safety of socio-technical systems is made under general conditions which provide both indispensable potential and unalterable limitations. Both must be taken into account in the design of the system since "the human with his/her natural abilities and limitations must take centre stage in all systems built up by humans for humans" ("Declaration of Saarbrücken" on the occasion of the "World Congress on the Safety of Modern Technical Systems", Saarbrücken, 2001). This ability basically makes the human superior to the machine —the ability to learn compensates for the susceptibility to error and is an important component in safety-oriented action.

Operation mistakes are defined as the failure to achieve an operation. It would therefore be a contradiction in itself to assume that someone could deliberately make a mistake. Whether a mistake in operation was made can therefore only be determined with hindsight and following clarification of the possibility of a "correct" target-oriented act. Seen in this way, the very common kneejerk reaction of assigning blame ("human error") for a mistake contradicts the "human right of error" which safety researchers call for. A reasonable mistake culture recognizes a mistake as a learning opportunity and does not ask: "How could you have done such a thing?", but rather "How could it have come to this?"

Operation mistakes originate from many conditions, especially from

- an overtaxed mental capacity for processing information,
- unreasonable attentiveness demands, monotonous work,
- inherent or learnt (inappropriate for the tasks on hand) behaviour stereotypes or
- limited knowledge.

All of these are possibly stresses and strains which exceed the human capacity for action. In the interest of preventing injury to people and the environment, system design should take into account both the natural human potential and human limitations. This can be achieved, for example, by fault-tolerant constructions and design.

The automation of socio-technical systems has particular significance here. From a technical point of view, it often seeks a maximum to rule out the "error-prone" human as far as possible. In actual fact, the more complex systems become the more necessary the human contribution becomes. Bainbridge speaks here of the "ironies of automation" (in [5]). In the first place, the developer of a system is, as a rule, a human, who is also susceptible to making mistakes and can thus have a negative effect on the correct use of the developed system. In the end, the developer leaves the operator only tasks which are no longer automatable after his/her maximum automation strategy. The result is comparable with what psychologists have called "learned helplessness": the lack of use of motor or cognitive skills becomes a problem when an unforeseen event occurs and new behaviour patterns are required of the inexperienced operator. In a similar way, the purely supervisory function of a technical facility remaining due to comprehensive automation is negatively affected due to the proven human weakness in remaining attentive for long periods.

Furthermore, complex situations requiring a decision can become a problem. Provided all necessary elements of a decision in the production process can be specified, the automated, computer-aided decision can occur faster and more multidimensionally than a decision by the operator. However, the operator is possibly left with judging the result of a decision on a meta-level whose algorithm he/she does not or only insufficiently understand. Automation can thus mask system failure and evade carrying out the correct diagnosis and rectification. What is therefore required would be not maximum but rather appropriate automation which grants the human learning and operational capability so that optimally designed safety measures are created.

3.2.2 Procedures for an Interdisciplinary Safety Methodically Concept

3.2.2.1 General Outline

In what follows, a general overview is given of the basic valid procedure in the required system-related work on safety engineering, especially with regard to public

safety. The interdisciplinary "safety methodically concept" referred to here is presented in Sect. 3.4. The following basic principles listed form the basis for its composition.

3.2.2.1.1 General Agreements on Safety Engineering

As a fundamental rule, technical systems must be designed safety-compliantly such that they meet the current state of public safety. However, this fundamental requirement does not apply when, during testing of the system and its components, safety—according to the needs of a test operation—is temporarily assured by means of specific measures.

In designing a technical system which complies with safety requirements, the following safety-engineering design criteria are to be agreed on:

- The human with his/her natural abilities and disabilities must stand in focus. Among other considerations, this requires design of technical systems as user-friendly.
- A single failure must not cause or encourage a safety-critical failure in the complete system.

Should a technical design meeting these criteria not be possible:

- combinations of failure cases in structural units (failure mechanisms, causal chains)—including human operating errors—which could lead to a safety-critical failure within the entire system must be made recognisable by active or passive self-inspection.

If a technical design which satisfies this requirement is not possible here either (e.g. because this would impair reliability), the following also applies:

- The probability of multiple failures (e.g. a simultaneous single failure of different structural units) which could lead to a safety-critical failure within the complete system must not exceed a specific limiting value relating to the particular type of operation in each case.
- The definition of such limiting values is dependent on stochastic conditions of the failure behaviour of the structural units concerned in each case and the **specified** limiting value considered appropriate for the complete system.

A safety methodically procedural concept for the safety-engineering design of products and technical facilities assumes that the following basic principles are also observed in all activities required for safety-engineering reasons:

- The "safe state" or "safe functional behaviour" must be clearly defined and recorded in the relative specification for every structural unit. This may possibly assume that exact functional and requirement analyses are carried out for operation activities in due consideration of their feasibility.

- The technical design should be such that, in the event of multiple failure interactions in the failure mechanism, the possibility of the function loss of a sub-system or the entire system is ruled out.
- Limiting values of failure probabilities, which are required for the respective structural units, must be set so that fulfilling the safety requirements applicable to the entire system is not put into question.

As regards the time response of the failure rates applying to safety-critical failure events, the requirements relating to service life as laid down in the specifications of the particular structural unit will apply.

3.2.2.1.2 Requirements of the Procedure for Safety-Compliant Design

For all safety-engineering activities—including the appropriate verification—the following sequence of methodically appropriate measures applies with respect to conceivable hazards (see Table 3.1):

1. exclusion of safety-critical failure events (failure exclusion due to natural or technical integrity),
2. exclusion of the consequences of safety-critical failure events (exclusion of failure consequences) and
3. limitation of the probability of safety-critical failure events or mistakes by application of reliability engineering.

This sequence applies to the safety-engineering process and does not represent a priority ranking for a safety-engineering quality rating of the measures referred to.

The methodical approach, which is determined by the defined sequence above, assumes that all structural units in the system are verifiably in flawless and trouble-free condition at the beginning of every stage of use and that mistakes, which can arise not only during the production process and operation but also during maintenance work, are prevented by the appropriate precautions.

3.2.2.1.3 Safety Methodically Work Steps in Project Management

The safety methodically concept must be applied in project management. In this matter, the following work steps must always be carried out:

- transfer of the methodically prepared “safety-engineering catalogue of requirements” into project or system specifications covering the entire “product life cycle”,
- safety-related requirements of the design of the system and its structural units, which requires the involvement of various safety-engineering-relevant specialist fields,

- planned setting of the implementation steps in terms of human factor engineering,
- determination of the safety requirements which are subject to verification (public safety),
- determination of the safety requirements necessary to obtain the operation permit and
- compilation of safety-critical failure modes and preparation of the plan for safety controlling (goal: "lessons learned" for experience feedback).

3.2.2.2 Modules of the Safety Methodically Concept

The basic principles of safety-engineering design are to be systematically coordinated so as to establish an interdisciplinary procedure. This should be uniformly applicable not only to the project in question, the new technology thereby created and the conventional technology employed in practice, but also to the assessment by the responsible supervisory body. A further, general possibility of application is offered to damage inspections of technical facilities.

A valid work and evaluation methodology is thus established for the entire scope of a project. This brings the safety-engineering design criteria essential for getting authorization into a quantitatively assessable relationship with those design criteria which are important for cost-effective utilization and, thus, technical reliability.

Disturbances caused by failures originate mostly in the individual component or in structural units with a low level of integration. However, the safety-critical effects often become evident only on the basis of the functional interaction, which arises from the technical design of the overall complete system. The access required here can only be obtained by means of a suitable information management system.

One basic deficiency is, for example, the ambiguity of technical terms as defined in different technical fields. Since creating new technologies always requires an integration of knowledge from several specialized fields, terms which are not clearly defined in the technical standards and a universally applicable form should be systematically avoided. This is because they either can be interpreted differently depending on the specialist field (such as the term "fail-safe") or are intended only for use in deliberately restricted areas of application (e.g. the term "signal-technical safety" in DIN VDE 0831). This is especially true when common language use already has unambiguous terms in this regard (such as the term "safety"). However, words such as "safe" or "safety" should not be used as a basic principle in the designations of structural units, not even when safety verification already supposedly exists for the structural unit.

The term "maintenance" is used here specifically for all measures to preserve and restore the nominal state of constructions unless a modification is involved. Therefore, this includes terms such as preventive maintenance, inspection and repair, although a distinction can definitely be made between maintenance and repair in terms of content. In everyday speech, "maintenance" includes the

maintenance and modernization work which in the prevailing public understanding is necessary to preserve the nominal condition. On the other hand, "repair" means measures required to restore the nominal condition of a construction after losing it due to unforeseen events, e.g. a fire or a lack of correct maintenance work. Maintenance must be correct. This applies to not only the frequency and accuracy of measures (e.g. maintenance) but also, especially, the form of their implementation. If special expertise or specific technical equipment is required, maintenance can, under certain circumstances, only be correct if the work is carried out by a tradesman, expert or specialist company.

An appropriate information management system is an indispensable requirement for the interdisciplinary procedures of a safety methodically holistic concept.

3.2.2.3 Human Factors Engineering

Discussion of the design and engineering of new technical facilities almost exclusively focuses on technical problems, while aspects of the human factor engineering (HFE) only play a subordinate role, if any. Of course, basic technical design criteria must be given priority in the first stages of a technical concept. This is already advised on account of the cost dimensions thus activated.

However, all technical systems and, in particular, complex facilities consist, without exception, of technical and human components—in other words, they are socio-technical systems. HFE principles for designing socio-technical systems require development and design processes in which optimization of human–machine interfaces as a common optimization of both technical and human components starts determining the concept at the earliest opportunity.

Different areas are addressed here which are to be tackled on an interdisciplinary basis:

(a) Draft of an overall HFE plan
The plan should clarify how and in which phases of the overall design and construction process of future facilities HFE aspects should be systematically taken into consideration.
(b) Evaluation of operational experience
As a first step, it makes sense from the HFE point of view to carry out an evaluation of the experiences identified in already installed, comparable systems in order to avoid problems encountered there and to incorporate positive experiences into future drafts.
(c) Functional requirement analysis and task assignment
The objective is to analyse the requirements of the system in its different functional areas, identify performance requirements and explore the limits and possibilities of the design for options in the task sharing of the human and machine. In this matter, particular attention should be paid to the important principle of the "active operator" gained from HFE experience. Questions also fall into this category concerning possible new requirements of the operating

team and the resulting requirements of the qualification mix and functional reallocation of tasks within the team, as well as the development of appropriate criteria for the design of workplaces. Furthermore, this planning covers the assignment of tasks between the human and machine, including planning for automation measures.

(d) Centralization/decentralization of monitoring and control stations
Closely bound up with the problem of functional requirement analyses is the question of the extent to which decentralized monitoring and control stations are established, whose personnel in turn require appropriate qualifications.

(e) Organizational aspects
The mutual assignment and interaction conditions of different required personnel categories should be analysed together with the dynamic changes in responsibility for tasks in regular operation, incidents and accidents. There is also the question of how, for example, the European directives on work and environment protection require consideration of ergonomics and are relevant to the work organization of facilities.

(f) Determination of qualification requirements
Depending on the division of functions, qualification requirements plans would need to be developed and proposals for their implementation worked out.

(g) Decision support systems (DSS)
Computer-aided DSSs could be used for checking task fulfilment on the part of the personnel and for identifying appropriate procedures in case of need. In this context, the extent to which the use of computer-aided DSSs would entail changes in the interaction modes of personnel should be investigated.

(h) Design of control equipment (e.g. control rooms, control centres)
This includes, among other things, questions regarding the role of analogue and digital signal systems, their redundancy, the use of adaptive displays, transparency of reports and feedback loops for the effects of operator actions. Another point of investigation would be to examine how the team character of the work can be consistently taken into account.

(i) Participatory ergonomics
Ways and possibilities of involving experienced operators in the design process should be investigated. In the interests of an iterative optimization strategy, an analysis should be made of the possibilities and consequences of implementing the principle of "first the simulator, then the facility". Likewise, possibilities of using "rapid prototyping" should be investigated.
The term "rapid prototyping" in this context denotes the rapid creation of prototypes on the basis of design data. Rapid prototyping processes are thus manufacturing processes whose aim is to convert existing CAD data directly and rapidly into work pieces—if possible, without manual detours. These procedures, known as "rapid prototyping" since the 1980s, are usually moulding processes which build up the work piece layer by layer from shapeless or shape-neutral material by using physical and/or chemical effects.

(j) Internal facility incident and emergency measures
This concerns the implementation of HFE principles when developing technically correct, comprehensive, explicit and easy-to-handle procedures in the event of disturbances, incidents and emergencies.
(k) Prevention of operating errors by

- instructions and prohibitions as well as appropriate training and
- built-in interlock devices which, following an operating error, automatically switch to a safe state or safe functional sequence.

All in all, three models can be distinguished of how HFE experts can be involved in the process of designing and constructing complex socio-technical installations. These models are applied differently depending on the need in question:

(a) Integrated model
In this case, the HFE expert (work scientist, psychologist, medical scientist) is integrated from the outset in the design team so as to participate in the design of planned workplaces and the functions of personnel working there with regard to safety and reliability, occupational safety, health aspects and humane design.
(b) Intermittent involvement model
In this case, the HFE expert is consulted in critical design phases to evaluate, for example, a prototype. In this way, experienced operators (pilots, control room staff, etc.) can be involved.
(c) Post hoc involvement model
Only in rare cases will all design flaws be detected before the system goes into operation. It is then necessary to install technical or organizational barriers to prevent dysfunctional use of the system or hazardous system conditions. Under no circumstances, however, should post hoc involvement of HFE experts be chosen for a standard form of participation in the sense of a repair service.

If an event cannot be controlled within the system and system limits are exceeded, steps must be implemented to deal with the interface. In this case too, the knowledge of HFE must be deployed in order to incorporate unconditionally the HFE elements into emergency management planning as well.

3.2.2.4 Evaluation of Failure Prevention from the Interdisciplinary Perspective

Proven concepts with a systems engineering orientation make it possible to examine the potential failure behaviour of technical products and both complex installations and simple devices. In this case, it must always be assumed that a failure of technical products can just as little be excluded as the assumption might be accepted that the human working with this technology is infallible. The findings of such failure analyses, which count as standard tools of any project and development engineer, make it possible to detect systematically the crucial failure possibilities of structural units already in the design or planning stage. This, in turn, creates the

requirement for preventive measures with which undesirable or unacceptable failures should be prevented.

For a better understanding of further explanations, the two terms "deterministic approach" and "probabilistic approach" should first of all be clarified here:

- Deterministic approach
  The deterministic approach in the engineering sciences corresponds to the historically developed, monocausal plot. It is based on both unequivocal if-then relationships and the situation when a specific event occurs at a predetermined time. In addition, it even still shapes in modern technology the classic procedure in the conception, design and testing of technical facilities.
  This approach was also adopted for safety engineering when it was (or is) a matter of devising measures as precautions against a safety-critical failure. The "if" here stands for the safety-critical failure and the "then" for the safety-engineering precaution. In classical engineering, both conditions represent a logically unambiguous (in forwardly oriented logic) or even one-to-one (in forwardly and backwardly oriented logic) connection and relate to monocausal active structures.
  The deterministic approach to engineering is in line with the equally classical conceptual and decision structures in the legal system.

- Probabilistic approach
  The probabilistic approach is based on theoretical or statistical probability principles. In contrast to the deterministic approach, the probabilistic approach is based not on certainty but on the possibility that a specific event occurs with a certain probability. The time when the event occurs is not predetermined and cannot be determined in advance either.
  Modern technology (such as plant engineering, civil engineering, energy supply engineering, information and communication technology, automotive engineering, aerospace engineering) has come to involve highly networked functions and computer-aided facilities. It is also increasingly seeing service in aggressive environments (such as space, open and deep seas, deserts, jungle). This inevitably leads to complex and highly integrated structures which are, as far as safety engineering is concerned, no longer manageable solely by the deterministic approach. They must be supplemented or completed by probabilistic approaches (such as reliability engineering, for example).
  The use of reliability engineering has proven its value for decades now in the conception, design and testing of such complex technical facilities. Without using reliability, the achievements of modern global aviation, scientific and commercial space travel and even modern automotive engineering would not have been possible.
  The application of reliability engineering has become indispensable for aviation and (manned) space travel in the safety-engineering design of highly integrated, complex technical facilities. Nevertheless, its adaption in other technical fields of application is only proceeding very slowly on account of established traditions.

The failure behaviour of technical products can only be fully determined from the systematics and made usable for engineering-related selective precautionary measures if its stochastic manifestations are also taken into account in a probabilistic approach. In addition, it must be taken into account here that the failure behaviour of systems (e.g. supporting structures, supporting devices, mechanical interlocks, fire insulation) which are still transparent and equipped mainly with "captive" attributes ("passive" safety attributes) can usually still be fully determined even with an exclusively deterministic approach. On the other hand, the failure behaviour of complex systems equipped mainly with "losable" attributes ("active" safety attributes)—systems such as energy supply systems, power units, control systems, cooling equipment, extinguishers—is essentially characterized by its stochastic manifestations.

If engineers are to work under these conditions focused with probabilistic approaches as well, they must in all cases have access to probability-related limiting values. As already mentioned, since the first publication of the DIN 31004 safety standard (see Chap. 2), risk assessment as a probabilistic analysis of the stochastic failure modes of technical products has come to be regarded as the generally accepted state of the art.

Consideration of limiting values for a risk assumes that they are also accepted by the general public (see Sect. 3.3.1). Every limiting value so considered must orient itself to acceptance by the impartial "public" (public safety). Attempts to determine the degree of acceptance by public-opinion polls are doomed to failure. At best, they will reveal the polarization always present in the public between, on the one hand, admiration of technology and, on the other hand, a sceptical attitude to technology based in most cases on ignorance but also—due to the unavoidable occurrence of verifiable failings of humans and machines—on justifiable doubts. In this case, the danger cannot be ruled out of this polarization being politically misconstrued when the results of such surveys are presented to the public.

A different, already taken path should be followed purposefully against this. The degree of public acceptance should be measured by the stochastic attributes of technologies which have already been accepted by the public. These are technological attributes which present themselves in shipping, civil engineering, rail traffic, aviation, road traffic, power engineering, chemical engineering, process plants or even in power stations of conventional technology. Acceptance can also be measured by natural risks, which are, for example, characterized by human life expectancy. However, the success of this approach assumes that the relevant institutions make their databases available for general use.

However, defining limiting values of this kind would not lead to a definitive solution. It is ultimately essential that the requisite level of safety be integrated into the technical system. Consequently, it must be proven to the supervisory body to what extent this has actually succeeded. However, instruments with which this evidence can truly be supplied efficiently are only partially available at present and would need further development.

This fact in conjunction with the probabilistic approach required results in a quantitative problem. The numerical values (data) with which safety is to be

calculated must be very low since safety-critical events may only very rarely be possible. If numerical values of this kind are to be proven by stochastic methods, one quickly meets limits which cannot be crossed on account of the necessary effort involved. Therefore, reference in this context is made to the well-proven databank-based concepts as they are presented, for example, in the formerly internationally used US-American standards MIL-HDBK 217F, Notice 2, "Reliability Prediction of Electronic Equipment and NPRD 95, Non-electronic Parts Reliability Data".

The probabilistic consideration of stochastic failure modes as a complement to the deterministic concept of classical safety engineering was developed to make complex systems, which are predominantly characterized by their multiplicity of "losable" attributes, also meaningfully controllable by safety engineering. Attempts are constantly being made to replace the classical deterministic approach so comprehensively proven in safety-engineering practice with a probabilistic approach. This attempt frequently fails due to a lack of suitable, reliable data.

In this interface between deterministic and probabilistic approaches, a lack of relevant knowledge cannot be entirely ruled out. Deterministic safety measures are thus based on the idea that, when a safety-critical failure occurs, technical products must be immediately converted into a safe state. This often consists of blocking a function (e.g. in the deliberately induced shutdown of an installation)—in other words, in an unconditionally commanded failure (the definition of this term is based on DIN 25424 "Fault Tree Analysis", 3.8, c). However, in the case of complex technical systems with their many sub-components, the safety-controlled "switching off" of individual sub-systems leads to reliability problems which, once a technical development is completed or a facility built, are almost incapable of solution.

This behaviour led to the realization that safety and reliability engineering must remain connected in inseparable logic. Both fields deal with failure modes of a stochastic nature, which is why failure behaviour can only be fully determined by stochastic methodology. Thus, the proposed deterministic support measures should also be determined stochastically in their effects on reliability.

3.2.2.5 Criteria for an Interdisciplinary Holistic Safety Concept

In the derivation of criteria for a concept usable on an interdisciplinary basis (on the occasion of a technological innovation project), a deliberate attempt was made to avoid creating again only a safety concept which applied solely to one particular area of application. The criteria prepared are therefore universally valid and can accordingly be used in any field or technology. This also applies to the fundamental principles of the interdisciplinary safety methodically concept presented below (see Sect. 3.2.3), in which these individual criteria are recorded in their logical connections. Their universal validity offers the following advantages for application:

- Institutions which in the overall process exercise the specific governmental responsibility for public technical safety and conduct tests, approvals, declarations of conformity and tolerances and also carry out surveillance and control can work according to the same criteria of the same concept. They thus use the same elements from the perspective of state responsibility, regardless whether they are practised directly, applied in public commissioning procedures or used on the basis of structural criteria by recognized (accredited) private bodies.
- In a uniform introduction of the safety concept, application-independent and clear communication is made possible between the different specialist fields involved. This occurs since one of the essential basic principles of the holistic and interdisciplinary concept from systems engineering has been universalized for all technical fields.
- A precondition for a purposive safety-oriented concept is, however, that
  - sufficiently suitable measures (generating safety, safety management, quality management, safety-related verification) are taken during planning, development and manufacturing, and
  - during the operational phase as well as disposal and dismantling, further measures (safety management, safety-related verification) are taken which are appropriate and by means of which the manufactured product truly has a safety-compliant technical design.
- As with any other interdisciplinary working method, the safety-oriented approach requires appropriate organizational conditions to make an effective application possible. In this matter, the following aspects should be taken into consideration:
  - Only a central control facility, responsible for the entirety of the system in question and equipped with sufficient powers, is practically capable of taking into account appropriately system comprehensive criteria in safety-related activities. However, the precondition is that safety can be verified for all components of the system under consideration itself.
  - This safety-oriented approach guarantees cost-effective usability just as a safety-compliant technical design does. Therefore, in view of this comprehensive objective, overall responsibility can only lie with the design engineer who is comprehensively familiar with the safety-related characteristic since he/she was the one who created it for the product in question (typical example of a matrix organization).
  - The engineer working as an expert only has to assess the safety-related appropriateness of this technical design. Depending on the complexity and scope of the concept, this requires the appropriate cascade-like activation of the expert opinion (principle, dimensioning, execution). The principle must take into consideration the limited nature of consequences, manageability, accessability of negative effects and reversibility.

- Observation of the applicable "good engineering practice" and/or legally qualified regulations is in itself alone a mandatory if not necessarily sufficient precondition for conclusive proof of safety.
- In addition, of course, due regard must be paid to the state of the art and, if required, also to the state of scientific and technical knowledge. (For more detailed information, see Sect. 3.3.5).

With regard to the nature and serviceability of technical facilities, certain qualities of the materials, components, systems, facilities, products and implementation form the basis for their design, dimensioning and construction.

It is crucial that the planning specifications themselves, their calculative and experimental verifications and construction plans be tested as to whether the product with these specifications—as well as with the testing and approval measures planned during implementation—can be put into execution in accordance with these requirements (testing and approval of the planning specifications).

Suitable testing and verification measures must be provided in all major phases of implementation (tracking and testing of the implementation) to prevent implementation deviating impermissibly from the underlying requirements. Deviations can occur, for example, due to the variability of material and component properties, uncertainties in installation and construction or mistakes and errors during the various production steps.

If qualities are expected to change adversely during service life, periodic inspections and special maintenance measures may be necessary (final inspection and verification before going into service).

Requirements relating to the organization of verification

It is only by an appropriate coordination of the designated tests that testing measures can rationally complement each other, unintended gaps in verification be avoided and the necessary information passed on.

In the appraisal of testing measures, it is important not only to record their immediate function but also adverse deviations and their indirect effect, namely their positive or negative impact on important aspects of performance and quality.

Responsibilities for all testing measures, especially for implementing measures in the event of insufficient test results, need to be regulated clearly and unambiguously.

All major test results must be recorded.

Establishing a test plan is then necessary if a large number of contractors and subcontractors are involved in the project and incorrect decisions and gaps in verification can have serious consequences.

Elements of verification

With regard to the nature and scope of verification, a distinction can be drawn between:

- manufacturer testing which is regulated only internally or externally,
- third-party testing by an independent third party carried out either independently of manufacturer testing or relating exclusively to inspecting the correct performance of manufacturer testing and
- acceptance tests on the part of the purchaser or customer which are used for assessing and verifying the quality of goods or services at the transfer of responsibility or ownership.

Manufacturer tests are, in principle, carried out in an office or in-house and can, depending on the importance of verification, occur in the form of self-testing or be conducted by persons not directly involved in the manufacturing process.

Manufacturer tests regulated in an office or in-house special measures for controlling production fall within the sole responsibility of the manufacturer.

Planning tests include a clear definition of rules for assessing quality or a service and also measures for negative test results.

The importance of the individual elements of verification differs depending on whether it concerns tests on planning specifications, constructional execution or tests before the start of operation.

Grading of tests

The grading of test measures for safety-related verification depends on:

- the intensity of testing (frequency and extent of tests or inspections),
- the assessment criteria and measures in the event of negative test results,
- the degree of independence of testing the process in question and
- the use of multiple independent tests whereby, depending on quality assurance requirements, the following gradation is possible:
  - only manufacturer tests,
  - externally regulated manufacturer tests together with third-party tests or acceptance tests and
  - externally regulated manufacturer tests together with third-party tests and acceptance tests or a second independent third-party test.

On the basis of this context, the determination of quality assurance levels and their classification in the hazard categories (see Table 3.1) can be deduced. Individual sub-systems or structural units can be subject to different distinct quality assurance levels.

Inspection and approval of the planning specifications

- Inspection of draft design, dimensioning and structural design
  It is important to test whether all decisive hazards have been identified and appropriate measures provided for their prevention. This concerns, in particular, the appropriate choice of the system, the materials and method of production, the processes and tools used in construction, and also the design of the system or facility (function testing, accessibility). Among other things, a check should be made whether all essential organizational requirements, e.g. special trade and operational qualifications, can be fulfilled, all tests required for implementation have been provided, and all conditions of use and necessary maintenance measures have been defined.
  The design inspection can be carried out in different ways with different degrees of effort, e.g. by tests, calculations or analogy observations. Among other things, it should be checked whether:

  – the calculation includes the relevant requirements and actual influences, basic conditions and conditions of use,
  – verifications are maintained for all major components,
  – the appropriate mathematical models are used,
  – the calculation in itself is consistent, and
  – all effects are borne correctly by the system.

Whether modifications of components cause unacceptable malfunctions should also be checked.
As regards the type of inspection, a distinction can be drawn between:

  – a complete recalculation by an independent third party,
  – simulation tests and
  – prototype tests.

- Inspection and approval of final planning documents.
  A check must be made whether the final planning documents contain all the information required for implementation, such as, for example, tolerance limits or instructions regarding the manufacturing procedure. In this case, it is, among other things, important whether dimensioning results have been communicated correctly, instructions or drawings correspond to the specified requirements, and other basic conditions have been taken into consideration.
  Since all information and requirements on the part of planning are mostly conveyed via implementation plans for production, assembly and integration, special importance is granted to checking clarity and completeness.
- Inspections of constructional implementation (acceptance inspection)

  – Series production—single-item production
    As regards the type and importance of tests, a distinction should be drawn between

- series production with the objective of consistent quality and
- single-item production with the objective of complying with planning specifications.

Preventive measures have priority in single-item production.
The construction of complex technical systems or large technical facilities is generally a matter of single-item production in which only individual components or materials are subject to series production. Therefore, quality assurance systems, e.g. according to DIN 55350 "Concepts in Quality-Management and Statistics", which are oriented towards series production, are not directly applicable to all phases of the construction work.

– Assessment procedures and criteria
Every production unit is tested in the complete assessment. A unit is either accepted as "good" or rejected as "bad". If the assessment is carried out according to quantitative criteria, these generally comply with specified tolerances.
– Periodic testing
Time-staggered periodic tests serve to ascertain that a technical product conforms over its entire service life to the valid configuration according to which it was planned, developed, constructed, put into service and operated.

3.2.2.6 Passive and Active Safety Measures

The following basic classification can be made: when a component, part of a technical facility or an entire facility is developed to fulfil different functions, a distinction is drawn between active and passive functions.

- Passive functions basically involve "captive or inherent attributes". These functions cannot become "lost" in the normal case/operation. No actuator is operated. Passive functions can carry out holding, supporting and locking functions, for example. Specific examples include the floor of a building storey or the static properties of an entire structure. Consideration of both the properties of the hardware and the requirements of the construction components is necessary to maintain these functions. Tests, care and maintenance also play a part in this.
- Active functions, on the other hand, can basically become "lost". They are characterized by the use of an actively operating construction component. Examples include lighting equipment or a regulator. In the event of loss of these functions, safeguards are necessary which must be suitably implemented for the relative possible failure performance.
- Wherever possible, priority must be given to passive safety measures. In the case of application, active safety measures must be proven to be at least equally effective for the hazard category concerned (see Table 3.1).

3.2.2.7 Controlling Failure Mechanisms

If a construction component supporting a passive function fails, the failure is sought in the first approximation in the design or the constructional implementation. If an active function fails, the important construction components may be in order. In this case, individual characteristics of a device might have failed because it has been damaged. Alternatively, the control or the interaction of function elements may have failed—for example due to an instruction or operator error.

Failure mechanisms can be divided into categories. Seven different types of failure in total can be categorized and divided into three fields:

- Failure when installing a function:
  - A system lacks the intended function.
  - The intended function only partially materializes.
  - The function materializes at the wrong point of time.
- Failure in an already existing function:
  - There is a total failure of the existing function.
  - There is a degradation of a function element, and this element can fulfil its function only partially.
- Failure when terminating a function:
  - The function is terminated in an unqualified way.
  - The function is terminated at the wrong time.

In order to generate technical safety, the failure of functions must be weighted. Different approaches can be taken to reduce the probability of the occurrence of a possible failure to an acceptable level:

- A function fails, and the technical state of the system or facility still remains safe. Despite the intended function becoming inoperative no damage results. This "fallback state" is called "fail-safe". In this case, the system is switched off towards a safe state despite the failure of a system component with care being taken that the final state arrived at in the fallback is safe. No injury to persons or damage to property occurs, but the function is no longer available—not even with limitations. The system "comes to a standstill", so to speak.
  The triggering of emergency braking in a railway train is given here as an example of the "fail-safe" approach.
- However, if a function of a system or technical facility should be maintained or must stay at least partially maintained despite the failure of a component supporting that function, this state is called "fail-operational". In this case, restrictions are applied by emergency programmes (automatically or selected by humans) which maintain particularly important functions. Catastrophic behaviour can hardly occur with implementation of this strategy. A systematic approach to establishing appropriate strategies is particularly important here.

The technical and organizational precautionary concepts in a flying plane are given here as an example of the "fail-operational" approach.

- If neither "fail-safe" nor "fail-operational" strategies can be applied, the application of reliability engineering offers the possibility of reducing the risk, although only for Hazard Category 1 (see Table 3.1). This term means the application of probability considerations which examine the possibility of a failure by using empirical values, expert reports, theoretical studies, failure observations and other methods. If the probability of damage is low enough, the system or technical facility can be put into operation.
  The safety-related reliability concept as used in attitude control systems for vertical take-off aircraft or in the landing computer for the lunar module is given here as an example.

3.2.2.8 Generating Safety According to the Phase Approach

Achieving appropriate safety conditions requires different provisions and steps in the various phases of the life cycle of a system, technical facility or product by the individuals involved (see Sect. 3.2.1.2).

Designers and developers of the hardware and software, suppliers, operators, personnel for installation, operation, maintenance, repair and disposal, and the competent supervisory institutions (authorities) must therefore develop and discuss appropriate and realistic measures and ways and discuss what can prevent the failure of functions or changes in properties to the greatest possible extent. The development of international solutions is worth pursuing since many products are developed and used not only on a national level. Worldwide acceptance of good safety solutions, which can differ quite considerably, is helpful.

It is wise to develop suitable and adapted processes for the development of safety-relevant systems and functions in order to achieve the different requirements of safety properties. Such processes may include the following topics, which can or must be adapted to the function and purpose of the systems:

- system definition,
- hazard analysis,
- risk disclosure statement,
- derivation of safety requirements,
- implementation phase,
- documentation,
- management tasks,
- interdisciplinary processes,
- support processes and
- supplier relations.

Due to the rapid further development and innovation of technologies, there must be parallel work which tests and implements the necessity of extensions,

specializations and changes of existing regulations and standards. Innovations result in technical fields being entered which, in many cases, could not be taken into account in previous concepts. The use of electronics, in particular, for putting innovative functions into practice needs such new basic conditions which cannot always be adopted from the past. The utilization of functions depends decisively on legal security for the manufacturer, and this is described by, among other things, the state of the art.

A so-called safety case (safety report) is required for complex systems and technical facilities. The same applies when public-technical safety is concerned. In addition, the safety case should be a selectable option for all cases but, in the fields listed above, must be part of the safety culture practised. Based on the procedures in aerospace engineering, chemical engineering or comparably complex installations in the energy sector, it must be demanded that a factually appropriate safety management system be devised, presented and applied. This means that the documentation for a "safety-engineering requirements catalogue" must be initiated from the very beginning—in other words, with the ideas and first considerations of design. Updating must be continuous and all changes and modifications documented in revised editions. It applies to all technical fields that a system description forms part of the safety case. It also contains the safety management and/or safety plan, a risk assessment, an emergency plan and documentation instructions too. Depending on the specific case, more component- and phase-related parts can be added in high division of labour production—for example, so-called production and test sequence plans. The safety case starts with the product idea and grows over time and with the phases of the life cycle.

In principle, similar requirements apply to the phases of the life cycle of a system (a technical facility or product). Suitable procedures, processes and instructions are worked out during operation, maintenance, repair, decommissioning and disposal which generate and maintain safety. Careful formulation of such procedures ensures optimal results and high safety standards in this field too. However, a guaranteed high level of safety in the long term depends on operators and users complying with the methods and processes established. Understanding and sensitivity are to be solicited here too by means of suitable communication. The human being stands here in a key position in the process for generating safety.

Technical safety is one of those attributes of a technical system, facility or product which is not only to be specifically generated by a controlled process but which also always requires verification. It is not important whether this occurs by testing or inspection at the manufacturer's own responsibility (first party), by possible clients/customers (second party) or independent third parties. The nature of the parties involved here plays an important part in the validity of the tests or inspections.

When life phases are considered in Sect. 3.2.1.2, the role played by tests and inspections is therefore presented. A critical assessment should be made here whether the verifications can be regulated solely by market participants or to what extent testing and inspection must be carried out by independent third parties since the market does not offer a sufficiently suitable regulatory framework. As regards

independent third parties, it must be examined to what extent the monitoring function can be privatized (e.g. in the form of private-sector auditing systems) and which responsibility is better assumed by the state itself. It should be taken into consideration here that the higher the hazard category according to Table 3.1, the more emphatically the responsibility must be observed by the state. It must be considered with this view that an absolute responsibility of guarantee on the part of the state should only be permitted with Hazard Category 1 (see Table 3.1).

3.2.3 Implications of a Safety Methodically Concept

The obligation to design technical facilities that are safe results from both ethical–moral reasons and legal requirements. This working method, which essentially is still practised today, is based on a wealth of experience that has built up in the course of technical development to a considerable extent. This happened, however, mainly under the pressure of damaging events that occurred.

Engineers who design, develop and build technical facilities also have the duty in the framework of their overall responsibility to design these technical facilities safety-compliantly. However, the residual safety risk, which can never be completely ruled out when dealing with technical facilities, always remains for factual reasons with the operator and/or user. From this situation, which is characterized by a polarization arising from the factual circumstances, the problem inevitably emerges: "What and how much is safe enough?" Even in the application of new technologies, this problem ought to be made amenable to a holistic solution. Therefore, the technical design and required verification should be undertaken methodically so that the damage-preventing, risk-minimizing character of safety-related precautionary measures is taken into account by a correspondingly oriented approach which is predominantly analytical preventative.

A precondition of effective safety-engineering activities is a correctly engineered structural design which offers a guarantee that the technical facility will not expect any damaging event if it is operated or used as intended under real-life environmental influences. In this context, special mention should be made of the design principles commonly applied in aerospace engineering in particular. Lifetime concepts on freedom from damage, redundant design, fail-safe design and damage-tolerant design have, despite their sometimes ambiguous word interpretation and partially overlapping modes of action, made a significant contribution to constructive design regarding safety not only in aircraft construction. A further precondition is the structural completion of a technical facility in faultless condition. "Fail-safe design" means fail-safe engineering—in other words, conscious dealing with design principles which make technical safety an integral component of the product composition and behaviour.

Mistakes, disturbances and failures in technical facilities cannot be ruled out in principle—whether because they occur at random times, unpredictable influences cannot be adequately controlled (e.g. lightning strikes) or unintentional operating

errors cannot be unconditionally avoided. A safety-compliant technical design must therefore include not only the correct structural design but also precautionary measures by which such mistakes can be effectively dealt with. An example of this is safety interlock devices which can reliably prevent every kind of operating error. These fault possibilities, which can by no means be presupposed in new technologies, must be analysed systematically in order to be able to determine cause and effect of fault possibilities as far as possible.

The complexity of technologically innovative systems makes it necessary to determine analytically stochastic failure behaviour too so as to be able to test and verify the effectiveness of safety-oriented precautions. The tried and tested methods of reliability engineering are available for this purpose. It definitely conforms with the currently existing "State of Scientific and Technical Knowledge" (Atomic Energy Act Art. 7 II No. 3) when preference is given to the verification of appropriate and adequate reliability as regards safety; the possible effort here can yield statistically verified results, and no coherent result can be expected of an alternative safety-oriented verification. Even such findings of reliability engineering which are not exclusively based on its numerical methods can be usefully included in safety engineering. They are applicable to determine those basic conditions for redundant facilities required from the safety-engineering point of view.

The state of safety engineering was traditionally shaped by learning from experience (see Sect. 3.4.2.2). This means that it is comparably easy to transfer safety-engineering experience to products and technical facilities which are technologically comparable with previous and current products and facilities. However, it always proves to be problematic when "safety based on past experience" should be transferred to products and facilities which have been further developed technologically or are entirely new. In this case, forward-looking approaches in risk assessment become necessary which identify the possible failure modes with probabilistic methods and implement the appropriate precautionary measures in the design ("feed-forward control"). In many cases, a combination of both approaches will be necessary. This will be described in more detail below.

3.2.3.1 Transfer of the Safety Standard to Technologically Comparable Products

If the development and manufacture of a product or technical facility are limited to the existing state of the art, the product in question will neither contain any serious technological innovations nor constitute as a whole a technological innovation. The existing legal and technical regulations will then suffice to be able to guarantee safety for this product. Either

- the relevant and valid statutory orders include a general reference to the technical rules and standards or an undefined reference to the state of the art, or
- the building and executory ordinances already include a direct reference to the relevant applicable technical rules and standards.

In engineering, the possibilities used here are described by two focus points:

- on the one hand, safety through full standardization (as in electrical and civil engineering) and
- on the other hand, safety engineering based on failure analysis (as in aerospace engineering).

Hybrid forms of both focus points are also increasingly being used.

- Different assignments of safety responsibility are also common in the application of law: manufacturer, owner (registered keeper), operator and government agency.
- The potential for modification is primarily limited to the technical rules and standards or, depending on the circumstances, to the state of the art.

3.2.3.2 Transfer of the Safety Standard to Technologically Further Developed Products

In the case of technologically further developed products, safety engineering takes this form:

- Legal bases can be assigned unambiguously here as well.
- Supervisory bodies or institutions are also determined for the application in question.
- Application of the state of the art turns out to be problematic here to a certain extent:
  - Statutory orders (with reference to the state of the art) remain valid.
  - The safety-engineering applicability of the standards is nevertheless questionable and requires in each individual case clarification by safety engineering based on failure analysis, which is always possible.
  - There is no legal obligation to clarify the safety-engineering applicability of the standards.
  - There is the problem of the always present diversity of opinion in the execution of supervision.
- Different allocations of safety responsibility in the application of law: manufacturer, owner, registered keeper, operator, registered keeper and government agency.

3.2.3.3 Transfer of the Safety Standard to Technologically Innovative Products

With technological innovation projects, virgin territory must also be entered in connection with safety engineering (e.g. in the development of magnetic levitation

train technology) since the existing state of the art cannot cover the new, previously unknown technology. The use of forward-looking probabilistic methods of risk assessment is required here:

- Legal bases are not readily assignable:
  - Stopgap solutions arise, such as the German legislation on the construction and operation of test facilities testing the engineering for track-guided transportation systems (Test Facility Act), without which a test facility testing this innovative technology is not legally permitted.
  - Supervisory bodies or institutions do not exist as yet and are to be determined separately for the individual application. In the case of the magnetic levitation train, responsibility lays with the Ministry for Economics and Transportation of Lower Saxony.
- Application of the state of the art is not possible here:
  - Neither exhaustive legal regulations exist (the sole reference to the state of the art is dubious here from the safety-engineering point of view),
  - nor does any standardization exist from which a necessity for safety engineering based on failure analysis arises.
  - The problem is that, when experts are brought into provide assistance, a diversity of opinions arises since there are no rules for an orderly, interdisciplinarily coordinated approach (see Sect. 3.2.2.1.1).
- The assignment of responsibility for safety here almost always remains with the developer or manufacturer since the legal system does not as a rule provide for other bodies which would assume or even only share such a safety responsibility.

3.3 Limits of Safety

The limits of safety are blurred. They are determined, on the one hand, by the basic conditions of development, production, and utilization processes and also by costs. On the other hand, they result from the progressive state of scientific and technical knowledge. Setting limits is necessary. This means profit. As an ethical obligation sensible renunciation is neither a weakness nor a deficiency. At the same time, tendencies towards extreme relocations of limits are observed. The following threatening scenarios emerge from this:

- endangerment of the foundations of nutrition (“purity” of food, animal feed and drinking water),
- specific disturbances caused by criminal activity (sabotage, assassinations, terrorist acts),
- war damage, acts of God, natural disasters,

- hazard from medicaments (deterrent warning of unexpected side effects) as well as consumer goods, household chemicals and cosmetics and
- dangers of new technologies, e.g. pest control, use of genetic engineering and nuclear energy technology.

From the ethical point of view (see Sect. 3.1.6), we should also add the fact that humanity is not only responsible for preserving the foundations of its own existence and that of subsequent generations but also the preserver and protector of all forms of life (animal protection, preservation of biodiversity and protection of the biosphere). On the other hand, a people on the subsistence level will and must fight exclusively for its self-preservation. Therefore, a refined feeling for the effects of technology may be regarded as a characteristic of a satisfied society. Views on the drawbacks and benefits of technology and its safety standards are therefore inhomogeneous.

If the limits of safety are to be understood in the converse argument as a measure of the threat to individual freedom, only a rational balance of protection of the individual and protection of the community in a democratic process can define a limit of safety. It must always be made clear in the process that this is a balancing of interests between the intended and indisputably created benefits and the damage which is conceivable within the context of residual risk. Whatever the case, the beneficiary is the solidarity community, which profits as a whole.

In every case, the following basic ideas apply in defining a safety concept:

- Absolute safety in the sense of zero risk cannot be demanded of the legislator or regulation provider (risk ban) because it is not possible in principle.
- However, all possibilities should be used from this point of view so that there is a well-balanced relationship between the risk of conceivable damage and the benefits created for the legal interests to be protected with different technical products, processes, facilities and systems (risk equivalence).
- The measure for the largest damage still acceptable is determined not only by the need for protection of the legal interests under consideration but also by the intention to satisfy social needs (benefits). In this process, a trade-off in the social consensus is generally needed (risk management).

3.3.1 Socially Accepted and State-Defined Limits

In a state governed by the rule of law the citizen may reliably expect that decisions affecting life and health are publicly legitimized. This is not possible without communication. The aim of this process cannot be to convince the other party that a borderline risk is acceptable or unacceptable. The citizen should much more be put in the position of implementing the right of co-determination in a “risk awareness” as it were. This addresses the ability to make a personal judgement on the basis of knowledge of the factually verifiable consequences of events or activities resulting

in damage, the residual uncertainties and other factors relevant to risk. This ability should or will on the whole correspond to both the values for shaping the individual life and the personal criteria for judging the acceptability of these risks for society.

In recognizing the co-determination of the individual citizen, it is the duty of political institutions to set up and care for the communication basis required for this. Risk communication calls for all forms of communication, from the simple documentation of results to specific information offers followed by dialogue and participation in decision-making.

In a society in which pluralistic values prevail and political actions are always under high pressure to justify themselves, setting limits and risk assessment often meet with scepticism or suspicion. Statements about risks therefore rely on plausibility and confidence in the so-called regulatory bodies. The more individuals and groups have the opportunity of active participation in risk assessment, the greater the chance of them developing trust in political institutions and also taking on responsibility themselves.

Participation, however, cannot and may not be a substitute for effective risk management, and participation is solely a decision-making aid. Above all, the responsibility of the legal decision-makers should not be obscured or softened by this. Participation should be understood as

- a two-way flow of information (as an indispensable precondition of proper decision-making),
- early involvement of the parties involved and relevant social groups (if applicable with a—justifiable—veto right) and
- co-decision.

The postulate "practical thinking" as a measure of the decision-makers requires that the occurrence of a damaging event can "practically" be ruled out in accordance with the state of scientific and technical knowledge. Unlike "theoretical thinking", "practical thinking" does not, however, aim at a mere awareness of ideas but simultaneously provides feasible orientations for action which are based on the realization that there will always be a residual risk.

In view of the theoretically infinite number of possibilities of damage precaution, a corrective is seen in the form of "factual" and "rational" criteria and limits. In terms of content, absolute exclusion of damage is not required. Rather, it is sufficient that the damaging event seems to be ruled out in practice according to the state of knowledge of scientists and engineers including human discretion. Applied to technical safety law, the demand for safety systems, for example, with reduced failure probability presents such orientations for action. All design-engineering precautions against multiple failures, especially simultaneous ones, are part of this.

What scientists and engineers often regard as incomprehensible is nevertheless rational from the viewpoint of different social groups. The rationality of social decisions in a highly complex system means serious challenges because all democracies secure their legitimacy by close correspondence with public opinion. Where under special circumstances the will towards practical rationality is, for example, lacking because sociopolitical requirements are in the foreground, the

instruments of practical rationality are either not being used at all or not in accordance with their inherent possibilities.

In general, the limiting risk cannot be determined quantitatively. It is usually described indirectly by safety-engineering stipulations. This specification or determination of the limiting risk assumes that the probability of a damaging event occurring and the extent of damage associated with particular technical products, processes, facilities and systems are adequately known and qualitatively describable. Describing and evaluating technical risks are thus also among the duties of regulatory bodies or the state, which evaluates and includes the contributions of affected parties (see Sect. 3.3.5.4).

3.3.2 Unattainability of Absolute Safety

Absolute safety cannot exist for several reasons:

- Technical processes never run with 100% reliability, in other words without any incident, and therefore, the technical facilities concerned also cannot be immune in themselves to every failure (safety devices such as "fail-safe" and "fail-operational").
- Material properties cannot be comprehended 100% and are therefore not entirely reliable. (This awareness is taken into account in engineering by, for example, worst-case scenarios and so-called safety factors.)
- The current state of knowledge is never completely and exhaustively comprehensible.
- Economic feasibility sets limits to efforts for maximum safety.
- Human action is always subject to the possibility of error and mistakes.

Ignorance and the imperfection of technical safety can, however, be restricted. However, the effects of safety-oriented measures compared to absolute safety can only be described as an asymptotic approach. A damaging event can then only be ruled out with absolute certainty if it is impossible by the laws of nature. Therefore, the possibility of failure is basically inherent in every technical safety system. Absolute safety can be achieved by no technical facility. There is always a residual risk, although this must be lower than a specific limiting risk. Thus, a demand for absolute safety or faultless solutions in complex technical systems leads in the wrong direction.

Behind the classic question in safety engineering—"How safe is safe enough?"—are hidden conflicting objectives: technical safety and practicability on the one hand and financial feasibility and social notions of safety on the other. Where there is orientation solely towards a maximum in technical safety, it can even be harmful to the user in cases of doubt. An excessively high level of technical safety sometimes leads to a loss in practical manageability. Thus, increased complexity in safety systems even brings with it the danger of an increase in risk.

Accordingly, from both the safety-engineering and the environmental, economic and legal point of view, it is essential to generate optimized (in other words, relative) safety. In this respect, the residual limiting risks of technical facilities, products and operating modes should be determined and compared with the risks of proven safety engineering, alternative products, other human environmental impacts and the natural risks in life. The result should be guided by communications management towards extensive acceptance.

It is only by such comparative risk assessments that it is possible to identify the scientific, technical and legal importance of the optimal safety of a technical facility, product or operating mode. Protection of humans and their environment by technical safety can and must be very well optimized but will always remain relative.

3.3.3 The Understanding of Risk

The term "risk" is understood and used in different ways and is a frequently used word nowadays. Therefore, it will be clarified and defined here in the context of this publication on technical safety.

Risk is both the quantitative and the qualitative characterizations of damage with regard to the possibility of its occurrence and the consequences of the damage effect.

According to W. Bons [6], "risks are a typical modern way of dealing with uncertainties". A look at the historical origin of the risk concept shows that it originated in mediaeval Italian cities in the context of long-distance trading. Long-distance trading was just as much a tactical as an uncertain issue. These uncertainties were not called dangers but rather seen as threats against which nothing could be done but which were identified as risks (the Italian verb *rischiare* means to risk being challenged). The merchant did not bow down to the uncertainties but calculated on them and gambled on success. However, he no longer regarded the uncertainties he encountered as fate-dependent threats but rather as calculable risks—in other words, as problems which only manifested themselves negatively when he had erred in his calculations and taken no precautionary measures.

The complementary terms "risk—opportunity" describe the risk that an action, activity or event will result in harm or benefit, loss or gain, disadvantage or advantage. The concept of risk has been discussed in more detail in connection with the Atomic Energy Act, the legislation dealing with the peaceful use of atomic energy and protection against its hazards. In this matter, the Atomic Energy Act, with reference to the state of scientific and technical knowledge, assumes a separation between the dangers to be repelled and the probability of damage. The probability of occurrence, the extent of certain damage and the associated

evaluation have a decisive influence on the classification in the category-based framework of hazard prevention, risk provisioning and limiting risk. Beyond hazard prevention and risk provisioning the field of so-called limiting risk begins, which can at best be reduced to a "residual risk" and is borne by all citizens as a reasonable social burden. The limiting risk implicitly derives from the sum of technical regulations and responsible action in accordance with these regulations while making use of the accumulated body of knowledge.

Accountability for the limits of safety lies in the readiness of the parties involved to deal appropriately with risks following consideration of the technical, economic, ecological and ethical aspects, to assess and evaluate the risks and to accept or reject them when there is an overall result. Safety, rendered precisely here as technical safety and defined by a limiting risk, must be seen in a series of interactions—from the aim and then over implementation and usefulness up to monitoring—and be taken into account in risk perception.

Scientifically based risk analyses are useful and necessary tools in a rational approach. Risks can only be understood with their help and options selected with the lowest damage expectancy values. The public, however, perceives risk much less scientifically than emotionally. If their feelings are to be listened to, it is entirely rational to open scientifically logical risk analyses to these feelings. However, in such a case, risk analysis could no longer be regarded as scientifically logical. Analysis therefore remains in the field of specialists. The general public should, however, be involved in risk communication by which the results of analysis can be made accessible to interested groups in society.

3.3.4 Factual Relationship Between Risk, Safety Engineering and Technical Safety

Global events in our world are usually linked randomly and multi-causally and therefore are neither foreseeable with mathematical accuracy nor determinable beforehand. The complexity of these natural events offers the human very few, if any, possibilities for influencing them. Locally limited interventions in nature are possible to a very restricted extent, but the consequences resulting from them can often not be estimated at all or only insufficiently. The human remains largely exposed to natural events whereby a nature-related life hazard occurs. Natural risks appear to be matters of fate.

The human has learnt to create technical devices ranging from the prehistoric hand axe to the modern industrial complex and from the simple hearth to modern energy supply. Unlike natural risks, the human can very well and even largely manage the risks involved with the technical equipment he/she has created for his/her own service. The whole arsenal of methods in safety engineering is at the disposal of the human to control these technical risks. When these methods are used

competently and correctly, an extremely high level of technical safety can be achieved. Technical equipment is deemed "technically safe" when the risk associated with the presence and utilization of this technical equipment can be demonstrably controlled so that a specific limiting risk is not exceeded (see Sect. 3.3). The attributes of technical equipment which has been proven to be technically safe are meant by the term "technical safety".

This factual relationship can be summarized as follows:

- Natural risks can only be controlled to a limited extent, while technical risks can be controlled just as the technology itself can.
- Safety engineering is the body of methods for controlling technical risks.
- Technical safety is generated and verified by application of safety engineering.

3.3.5 Safety-Engineering Feasibility

Technical safety is generated and maintained. The state must respond administratively to the possibility of damage and technical risks in order to prevent harm to its citizens. Technical safety legislation is used for this which reacts as a whole to the special characteristics of technology and engineering in the form of the following attributes:

- The time necessarily elapsing between the completed development of a new technology and its legal regulation, which is only subsequently implemented, has resulted in application-specific legal provisions. Technology legislation is fragmented and applies in every case only to specific technical fields of application (engineering fields).
- Putting into concrete terms the demand for technical safety, which for good reasons is vaguely formulated, is shifted by the legislator to the legal users level of the experts, authorities and courts.
- Legal demands for technical safety are defined by vague legal terms such as "generally accepted sound engineering practice", "state of the art" or "state of scientific and technical knowledge". In this way, safety-engineering conditions and behaviour requirements are formulated.

Technical products may only be put on the market if the technical facilities made of them and properly maintained satisfy the safety objective of all relevant legal regulations over an adequate, reasonable period. They must also be utilizable. Technical safety is based, on the one hand, on the relevant knowledge of the active individuals and those organizations directly involved in the field of safety. On the other hand, it is largely based on technical rules and standards, legal regulations and load limits which differ according to the application orientation for historical reasons and are often characterized by different technical languages.

3.3.5.1 Generally Accepted Sound Engineering Practice

The term "generally accepted sound engineering practice" is a legal term which has long been used in criminal law as well. For example, under Article 323 of the Criminal Code (Constructional Hazard), one is prosecuted who violates generally accepted sound engineering practice and thereby endangers life and limb of another person when planning, managing, executing or discontinuing construction work. Generally accepted sound engineering practice is not only achieved when a rule is regarded as correct according to scientific findings but must also be generally recognized—in other words, by being consistently applied by the engineers concerned and recognized in practice as correct.

This means that it is neither a question of whether science has recognized and taught a rule nor, in addition, whether it has been recognized in the relevant specialist literature. Rather, the architecture involved, engineering and building industry, system (facilities, products) and process design—in other words, practice—must be convinced of the necessity. This conviction must have established itself in such a way that for the purpose of the law it is possible to speak of general acceptance.

According to the prevailing view, there is a factual assumption that a standard reflects the "state of the art" at the time of its publication. Very frequently, however, there is still a lack of practical application at the time of publication, especially when the implementation of new technologies is concerned. In the case of very lengthy standardization procedures for complex matters, it can also not be ruled out that the standard at the time of publication no longer conforms with the general opinion and the rules it sets and, therefore, no longer corresponds to the state of the art. Nevertheless, there is a real presumption, which can be disproved at any time, that the relevant standards reflect the "good engineering practice", which is generally recognized.

"Generally accepted sound engineering practice" has been developed by experts in consensus. It can be in written form or not but is, as a general rule, codified. A standard can be generally accepted sound engineering practice but does not have to. The prevailing opinion is that there is only a factual supposition that a standard is generally accepted sound engineering practice at the time of publication, especially when it was produced in the process according to DIN 820 "Standardization". Technology legislation shapes its demands with vague legal terms in order to form technical developments efficiently within the legal framework. In order to make it more concrete, it is, therefore, based on generally accepted sound engineering practice, these rules also being grouped under the term "sub-statutory regulations". The corresponding legislation expresses, for example, the entirely refutable fiction that all technical rules which are generally introduced and made known in legislation are regarded as generally accepted sound engineering practice.

3.3.5.2 State of the Art

The "state of the art" is a vague legal term and represents the technical possibilities at a certain point in time based on the established findings of science and technology. It is found in many regulations and contracts and is precisely defined by the regulations relating to legal formalization. The term is used to designate measures which fall between generally accepted sound engineering practice and the state of scientific and technical knowledge as regards their requirements of content.

The state of the art is the state of development of advanced processes, facilities or operating modes which demonstrates that the practical suitability of the measure for attaining a high standard in the desired objectives is safeguarded on the whole (e.g. occupational health and safety, environmental protection, safety for third parties, cost-effectiveness). It has, however, not yet been tested enough over a sufficient time period and is mostly only known to specialists. Therefore, in building and plant engineering, for example, compliance with generally accepted sound engineering practice is usually contractually required.

3.3.5.3 State of Scientific and Technical Knowledge

In contrast to the "state of the art", the "state of scientific and technical knowledge" refers to a technical state of development in which processes and facilities are tested in test and pilot facilities but have not yet been put into service (see Fig. 3.2).

Linking legal terms to the concept of the "state of scientific and technical knowledge" relieves the legislator of detailed safety regulation for which it is competent neither in the allocation of duties in the separation of powers nor in its

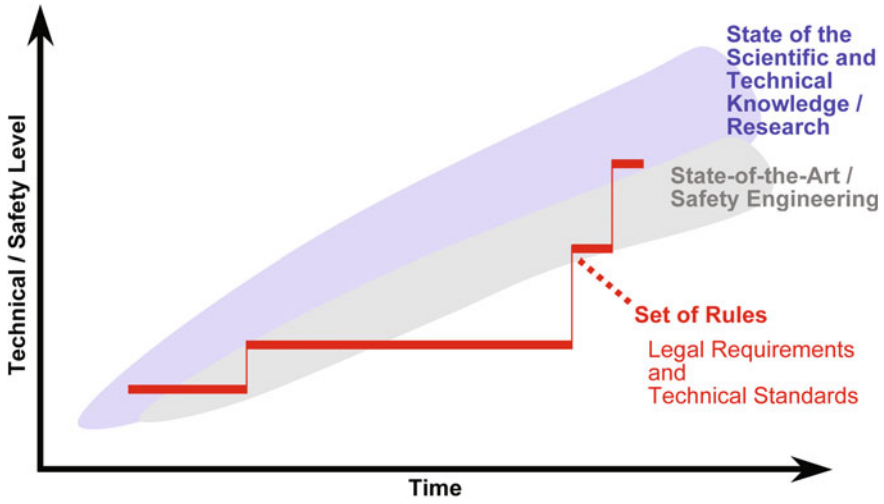

Fig. 3.2 State of the art-code of practice

expertise. By making reference to the "state of scientific and technical knowledge" (e.g. in Article 7 Sect. 2.3 of the Atomic Energy Act), the legislator thus requires observance of scientific and technical development against the background of legal regulation. Precaution for the minimization of technical risk must be taken, which is regarded as essential according to the latest scientific findings.

In both fields of hazard assessment and hazard control, determination and evaluation of the "state of scientific and technical knowledge" must take into consideration the scientific and technical principle of "balance". A risk can be ignored if it:

- occurs in isolation,
- is assessed as only minor,
- does not add up with other similar risks to a noteworthy risk contribution and
- would not, however, cause other greater risks under certain circumstances in the case of its consideration.

The state of scientific and technical knowledge is, however, used widely in technical regulations drawn up by different committees. The current state of research and development within a specific scientific discipline is intended by the term "state of scientific and technical knowledge". It must be based on conclusive evidence which will bear up against verification by third parties. Specialists first come to agreement in this matter in scientific discussions in order then to make it accessible to an expert public.

3.3.5.4 Methodology for Determining the Limits of Safety

The transference of limiting values for large-scale industrial facilities into sub-statutory rules and regulations poses various problems. To begin with, there is the question of legitimization of committee work, its membership and the procedure for the knowledge acquired. Following this, it is often difficult to get an overview of the entire set of rules due to the large number of such committees and regulations, and there are also overlaps and, in some cases, even contradictions. It is not uniform in structure, systematics and wording and thus makes orientation difficult in application of the law. This happens to be dangerous in a field where there is heavy investment on the one hand and considerable risks for possible affected third parties, including the burden of litigation, on the other hand.

An additional problem arises from the mixture of the objective findings of research into truth and their evaluation. The aforementioned committees are regularly qualified and legitimized for the truth-finding process and consequences derived from this but not for the sociopolitical assessment of risks (see Sect. 3.3.3).

The safety-engineering feasibility in its step sequence and processing passes more or less clearly through the phases of the product life cycle as described in Sect. 3.1.5 (see also Fig. 3.2). This phase-based approach not only facilitates

technical management but also notably secures the necessary organizational measures and finally results in risk management.

The following two phases are assigned to the **planning process in the product life cycle**:

- Conception phase
- Definition phase

The following two phases of the product life cycle are assigned to the **implementation process**:

- Development and engineering phase
- Production phase

Finally, the **operation process** comprises these two phases:

- Operation and utilization phase and
- Dismantling, disposal and recycling phase.

If new legislation and stricter regulations are required to tighten limiting values in safety and environmental protection, this will not go unwelcomed in many countries throughout the world. In reality, noticeable improvements are already being achieved at best in the medium and long term due to the time needed for the legislative process and, consequently, transition periods. In this process, the effect remains completely disregarded that every additional complication of the already confusing body of legislation and rules increases the risk of the legal application being impaired due to excessive demands and lack of knowledge. It would be preferable to make today´s applicable laws and regulations relating to safety and environmental protection considerably more transparent. This alone would make for a significant improvement in the standard of safety and environmental protection without a new law needing to be passed.

Reducing the complexity of technical installations, uncertainties and risks is always pursued in technical, economic or environmental problem cases. Compromises are therefore already inevitable here since the resources for implementation are limited and available information incomplete. By its very nature, a compromise cannot represent an optimum but only what is feasible under the circumstances and, therefore, does not claim absolute truth.

Risks must be minimized in a socially acceptable way and a balance always found between individual and social benefits. Compromises are unavoidable here that are nevertheless ethically justifiable. It can be stated that determination of the limits of safety is based on responsibility, acceptance, compromises, the measure of practical thinking, political feasibility, economic opportunities and, ultimately, on ethical standards. The definition of technical safety calls for practical feasibility and cost awareness and is committed to progress in research and development. It is determined by the current state of knowledge and social acceptance.

3.4 Verifiability of Safety

Safety can only be assured to the extent that it can be verified. It is shown here how limits of verifiability are set, which methodical approaches exist for its improvement, and which instruments have proven their worth for verifying the technical safety of a technical product or system over the various phases of its life cycle.

3.4.1 Limits of Verifiability

3.4.1.1 Responsibility

3.4.1.1.1 Types of Responsibility

Technical processes, especially verification of their safety, take place under the responsibility of humans. The individual can take responsibility for verification of safety when it is manageable for him/her. However, more complex forms of responsibility often occur in technology. Institutions or corporations have a specific duty with respect to their customers, members, shareholders or society in comprehending this responsibility.

> The responsibility of the individual arises, on the one hand, from the responsibility of his/her role as a duty to the optimal fulfilment of assigned tasks. Therefore, everyone is firstly responsible for the result and direct consequences of their own actions. This also includes the results and consequences of neglected acts. One special case of role responsibility is prevention responsibility, which obligates a test engineer, for example, to search a facility systematically for weaknesses and thus proactively prevent accidents and malfunctions. On the other hand, everyone has the quite general obligation beyond assigned obligations to respect and comply with basic rights, such as the right to life, the right to private property.

Institutions themselves cannot bear responsibility in their legal function as juristic persons. Responsibility must therefore be transferred to the persons acting in each case who represent these institutions. The complexity of the tasks does, however, call for a clear division of overall responsibility into fields whose scope should be adapted to the possibilities of the individual.

3.4.1.1.2 Conflict Between Economic Constraints and Technical Necessity

A frequent case of conflict is between the responsibility of the institution management for invested funds and the responsibility for safety. The starting point is the idea that the quantity and quality of goods and services are obviously better controlled by the regulatory mechanisms of the market than by state control. Optimization processes are encouraged by the inherent principle of competition which, if not implemented, would lead to displacement from the market. In the case of the usual goods and services, the regulating effect of the market provides for a balance between the quantity and quality of a product and customer satisfaction. As long as the customer is in a position to assess, check or experience the quality, he/she can intervene in the market.

Should the market, however, be disrupted by external effects (outside influences) or an uneven distribution of knowledge on the part of market participants, the state must intervene in the free market by laying down target specifications for the quality of products. In most cases, higher levels of quality are stipulated than would arise in the free play of the market. The state thus takes precautions in the general public interest. It enforces the constitutional principle of physical integrity for technical safety. In addition, it fends off the high consequential costs for the public sector which would be expected in the case of non-regulation.

Due to a number of reasons, the market principle can only be applied to a limited extent to the field of public-technical safety. In addition, the interesting main factors here should be individually checked by the experts before a technical product is put on the market.

Only a limited number of products have solely a safety function (e.g. fire extinguishers, safety valves, safety belts). The purchaser cannot always assess their properties. It is important how frequently and in what situations the products in question must prove their function: in routine use, normal use including common incidents, accident situations or emergencies.

The customer cannot judge the quality of a fire extinguisher which, in the ideal case, never needs to be used. However, if the quality of a safety-relevant product cannot be assessed, the regulating influence on the market is lost. Unsuitable products threaten to survive on the market or, if there are price advantages, even to dominate it.

It is much more common for goods to have a safety function in addition to their utilitarian feature (e.g. process/transport containers, pipelines, truck brakes). In these cases, the selling interest is overlaid by the safety function. If the selling interest and the public safety interest move in the same direction, the market supports the implementation of safe goods.

As experience shows, however, this principle fails in the case of shared or unclear responsibilities. Negative customer experiences do not then make an impact on the manufacturer of the goods. Safety deficiencies typically also occur when the economic benefits of a product or service decline in relation to duties or obligations. Therefore, dangerous goods transports with high-quality products must definitely be regulated differently from waste transportation.

3.4.1.1.3 Priorities in Deciding Responsibility Conflicts

There can be an optimum balance between economic expenditure and the safety achieved, but this must be with the moral reservation of adequate safety. According to Lenk and Maring [7], the following priorities arise in deciding conflicts of responsibility and roles:

(a) Weighing the moral rights of every affected individual (see Sect. 3.1.6).
(b) Seeking a compromise which takes everyone equally into consideration in the event of an irresolvable conflict between basic rights of equal value.
(c) Voting for a solution which results in the least harm to all parties may and should occur only after weighing up the moral rights of every party.
(d) Only when points (a)–(c) have been applied are benefits weighed against drawbacks.
(e) In the event of practically irresolvable conflicts between the parties involved fair compromises should be sought for the various parties with regard to harm and benefits ("Fair compromises" are, for example, an approximately evenly distributed or justifiably apportioned distribution of burdens and benefits).
(f) Universal moral responsibility usually has priority over task and role responsibility.
(g) The public greater good and common welfare should precede all other specific and minority non-ethical interests.
(h) Priority principles are also formulated in technical rules and standards. According to DIN 31004-1:1982-11 (see Chap. 2), for example, in the case of the term "safety" the following rule can be formulated with the aid of the probabilistic parameter "risk": "In safety-compliant design, preference should be given to the solution with which the safety objective is best achieved in a technically meaningful and cost-effective manner. In case of doubt, it should first be assumed that safety-related requirements take priority over economic considerations". On the other hand, it has been demonstrated, particularly in civil aeronautical engineering, that such safety-related solutions are also usually possible which are not necessarily in conflict with economic solutions.
(i) In the case of "urgency", ecological compatibility overrides economic application.
(j) Concrete humanity takes precedence over abstract requirements and universal principles (precise human and socially acceptable weighing of goods).

3.4.2 Learning as a Continuous Task

Disturbances or accidents, even near-accidents (including negligently caused deviations from intended operation), are unintentional, unexpected system states. Since they are unexpected, there is also no possibility of their verifiability. It could be shown in many event analyses that, although the action of the operator may have

triggered the disturbance, this alone does not suffice for an "explanation". Design, construction, maintenance and management errors are frequently a long time before the single action which triggered the disturbance and are also to be regarded as necessary preconditions. These errors must be avoided or eliminated by systematic experience feedback. In principle, there are three strategies for this objective.

3.4.2.1 Feed-Forward Control of Safety and Reliability

Probabilistic approaches to risk assessment, which also cover the actions of personnel in terms of a human reliability analysis (HRA), have long been systematically applied in diverse industrial sectors (among others, in the nuclear industry, civil aviation and engineering). However, these methods leave something to be desired. Although the necessary statistical data about failures in technical components are comparatively good, the same is not true of the underlying statistical information and the quality of the selected model concepts of human action. It must be borne in mind that these methods only permit partial statements and thus have certain weaknesses. Statistically sound databases are lacking, and these methods thus largely work with expert opinions ("informed guesses"). However, this does not have to detract from the possibilities of probabilistic methods. During the design and engineering of technical facilities, these methods are useful in gaining hypotheses and increasing awareness of human factor aspects (HF aspects) and should be developed further. Nevertheless, they are not sufficient on their own for a resilient statement on safety.

3.4.2.2 Feedback Control of Safety and Reliability

People learn from experience, mainly from mistakes, and organizations learn from events, including near-occurrences, which need to be analysed systematically. An event-related reporting system with a direct relationship to systematic root-cause analysis must be installed. The very few industries with a high risk potential have an efficient reporting system for incidents and accidents. Wherever supervisory authorities prescribe a system of this kind and enforce a reporting obligation, it on the basis of criteria is often felt to be burdensome. Incident reports beyond a prescribed reporting threshold are even more rarely gathered, documented and analysed, although exactly these reports would enable especially instructive learning. Thought should be given to how such reporting systems are to be designed and implemented below and beyond the reporting obligation so as to enable the emerging maximum yield of knowledge demanded. This calls for a reorientation of the error culture in Germany which culminates ultimately in communicating the error occurring for the first time and only punishing its recurrence.

3.4.2.3 System of Organizational Learning

The learning process must be institutionalized in the sense of organizational learning. Both forms of safety control ("feed-forward" and "feedback") can be mutually enriching when brought into a systematic relationship. Such a relationship must be created by setting up analysis and reporting databases. The following should be taken into account here:

- standardized category systems,
- periodic analyses of several events,
- derivation of appropriate prevention concepts and
- up-to-date ascertained feedback of results to persons affected.

3.4.2.4 Determination of the State of the Art as Learning Scheme

Determining the state of the art is often the precondition for acting in conformity with the law. Due to this prominent importance, various attempts were made to systematize this (learning) process for determination of the requirements. It begins with specifying for what the state of the art is to be determined, why and by whom. In individual cases, this means the following:

- For what (for what object):
  It can deal with a particular type of technical facility, specific facility, part of a facility or facility component of safety-related importance.
- Why (for what purpose, from which cause):
  The reason (context, background) is enquired into here, e.g. the implementation of an approval procedure for a new facility, change (expansion, increase in capacity, reduction in pollution emissions) or upgrading of an existing facility.
- By whom (person/ institution):
  The type of business should be stated here (e.g. small-/medium-sized enterprise or large company), which internal organizational units and external bodies are involved and, in particular, who the decision-making is established with.

To determine whether a technical facility is state of the art, the following insights can be used:

- comparable procedures, installations and operating methods,
- combination or linking of different safety measures and
- safety precautions in other types of technical facility which, in regard to their technology and materials used, are comparable with the facility under consideration.

Perception of the safety obligation should be implemented in three stages. These steps make it clear that certain safety-related measures can be applied in determining the state of the art without an obligation already being derived from this.

These particular measures do not have to be implemented in the technical facility being assessed since it is only a question of correspondence with the reference parameter.

- In the first stage, the state of the art is to be determined for a specific safety-related assignment of tasks (e.g. in the context of a pilot or demonstration installation) in order to serve as a reference parameter for the specific facility under assessment.
- In the second stage, an evaluative consideration is carried out as to whether the specific technical facility corresponds to the state of the art as determined. A check is made to see whether the safety objectives are attained with the designated measures for the specific technical facility (correspondence check).
- In the third stage, a decision is made—on the basis of the results of the aforementioned stages—regarding the approval or supervisory procedures (legal consequence).

3.4.2.4.1 Conditions for the Determination Process

Determination of the state of the art must take into account what has proved itself in other comparable technical facilities in normal or test operation, or what the general engineering stage of development demonstrates as practically suitable. If none of these three criteria applies, a determination process should be initiated. In this case, the following five conditions must be satisfied:

- All of the steps in the determination process must be completed, some steps being repeated if necessary (iteration loops).
- The persons involved must be suitable.
- The sources of knowledge consulted must cover the subject area thoroughly.
- The methods and investigations applied must be suitable and sufficient.
- The decisions must meet the legal standard of the state of the art.

Compliance with the state of the art is an obligation of the technical facility operator. Failure to meet or comply with this obligation can have serious consequences. Therefore, it is necessary to design the determination process methodologically and transparently and perform it with due diligence.

In certain cases, it is possible to determine the state of the art for a technical facility on the basis of technical rules, administrative regulations or guidelines. Such cases can occur when the boundaries of the technical facility, existing materials and purpose of operation largely correspond to a technical facility described in a technical rule, etc. The rules, guidelines or administrative regulations consulted must be up-to-date and the necessary safety measures sufficiently described. Special technical facility related or environmental hazard sources must be excluded.

In general, the state of the art results from the basis of technical rules and the results of discussions among experts.

3.4.2.4.2 Steps in the Determination Process

To determine the state of the art, the following seven process steps must be completed (corresponding to the first stage in Sect. 3.4.2.4):

(a) definition of the task,
(b) gathering the safety-relevant documents and data of the technical facility/process,
(c) determining the safety-relevant fields (process steps and technical facility components),
(d) analysing possible hazard sources,
(e) determining and selecting knowledge sources,
(f) evaluating the knowledge sources collected and
(g) decision-making.

In this matter, the order of process steps (b) to (f) can vary depending on the particular application case.

The process steps should be run in iteration loops until sufficient certainty about the state of the art is available. Iteration loops can comprise single or several process steps.

Determining the state of the art is only to be regarded as one step in developing a safety-engineering view. The following points are to be added:

- implementation of the state of the art with regard to the particular task,
- documentation of its implementation,
- investigation into and description of the residual risks and
- emergency planning.

3.4.2.4.3 Decision-Making

As a rule, different possibilities will arise as to how the state of the art can be implemented in a specific technical facility. The design option finally selected must be justified and explained in a comprehensible way.

By definition, processes, equipment and operating modes must

- have proved themselves in operation,
- have been successfully tested or
- have provided proof of their practical suitability

so that they can comply with the state of the art. Furthermore, the processes, equipment and operating modes must correspond to the advanced state of development. In this matter, a careful balancing of the effectiveness and

reliability of a safety measure with respect to the specific hazard source is a basic requirement for preventing errors which could increase the likelihood of hazardous incidents.

3.4.3 Controlling Technical Safety in the Product Life Cycle

It is known from quality management that the later a fault is discovered in the planning or production process, the more it costs to eliminate it. This is certainly also applicable to safety-related errors. To achieve optimum cost-effectiveness, one must therefore demand to carry out the safety-related observation from the very first phase of development. This evaluation function can be integrated into the development team or, whenever milestones are reached, take the form of an external check by, for example, a central department (safety/quality) and, if necessary, a third party.

The safety-related information collected and decisions made should be kept available at all times in the subsequent phases of the product life cycle for target/performance comparisons in terms of technical safety controlling. There is an opportunity to structure this controlling information for the continuous installation of the "safety case" in a hierarchy with safety objectives.

3.4.3.1 Phase-Based Pursuance of Technical Safety

A comprehensive hazard analysis should be performed for the entire object (system, technical facility, product) in interdisciplinary collaboration (see Sects. 3.2.1 and 3.2.2). This should take into account technical facility-based and environmental hazard sources, including natural conditions and events and interference by unauthorized persons.

The hazards and their causes should be analysed by means of a recognized, proven test method. In this way, a sufficient measure of thoroughness and depth of testing can be assured. The object under investigation should therefore be limited to manageable fields.

The criteria for terminating the hazard analysis should be recorded. Termination criteria can concern, for example, the depth of testing, exclusion of particular individual hazard sources, material properties and process parameters.

Both the collected documents and data and information from facility and site inspections serve as a basis for the work. Should hazard analysis cover one or more hazard sources, it should be determined which measures should be taken according to the state of the art. Independently of this, the possible consequences of nevertheless conceivable disturbances should be determined, their risk assessed and protective measures taken.

3.4.3.2 Organization of Verification

In the organization of verification, a distinction should be drawn between internal and external inspections. External inspections can be organized under private law or carried out on basic legal principles as required by the state (governmental agencies or bodies authorized by the state).

Only by coordination of a body endowed with adequate authority can inspection measures be reasonably augmented, unintentional gaps in verification prevented and the required information passed on. Its immediate task is to identify not only adverse deviations important for the evaluation of inspection measures but also their indirect effect of exerting a positive or negative influence on performance and/or quality.

3.4.3.2.1 Elements of Verification

With regard to the nature and scope of verification, a distinction can be drawn between:

- manufacturer inspection or testing, whether regulated only internally or also externally,
- third-party inspections by an independent third party carried out either independently of manufacturer inspections or relating exclusively to verifying the correct performance of manufacturer inspections and
- acceptance inspections by the purchaser which are used for assessing and verifying the quality of goods or services at the transfer of responsibility or ownership.

Manufacturer inspections are always carried out in-house. Depending on the importance of the verification, they can take the form of a self-check or be carried out by persons not directly involved in the manufacturing process.

Internally regulated manufacturer inspections—like special measures for checking production—fall within the sole responsibility of the manufacturer.

Planning verifications include both the clear definition of rules for the assessment and corrective and/or preventive measures in the case of negative inspection results. The importance of the individual elements of the verification requires documentation.

3.4.3.2.2 Grading of Verification

The effectiveness of verification measures depends on the following factors:

- degree of independence of inspection from the process concerned,
- qualification of the inspection personnel,
- intensity of checks (frequency and scope of inspections),

- evaluation criteria and action taken in the event of negative inspection results and
- use of multiple independent inspections.

Quality assurance stages and their assignment to hazard categories can be defined based on these factors, and individual items can come under different quality assurance stages.

3.4.3.3 The Modular Concept of the European Union

There is strong pressure to privatize the inspection and monitoring functions performed up to now by the state. This is often justified by the potential to increase efficiency or the responsibility of the manufacturer. Another reason is to be found in the process of European integration: the EU member states are acting on the assumption that barriers to free trade in the internal market can be dismantled more quickly by a private approval body. In the early 1990s, in particular, these tendencies to shift risk to the private sector (in conjunction with the transference of responsibility) have resulted in a real explosion of formal quality management systems and the associated auditing. For this reason, the costs and benefits of quality management systems and their audits have become a central point of discussion in the verification of technical safety.

The EU's New Approach[1] and the Global Approach for conformity assessment[2]—including subsequent module decisions[3]—are a prime example of the privatization and grading of control procedures in technical safety law. The Global Approach and the module decisions of the EU describe control procedures to be used in the EU's legislative proposals for the free movement of goods. The modules constitute a graded system which ranges from the manufacturer's declaration (Module A) to the individual approval of the product by an independent third party (Module G) and comprehensive quality assurance (Module H). The EU directives and the national legislation derived from these contain a selection of modules which take into account the risk of the regulated product. To qualify their product for the

[1]Resolution of the Council 90/C10/010 dated 07.05.85 regarding a "new approach" in the field of technical harmonization and standardization, Official Journal of the European Community, No. C 136 dated 04.06.85, pages 1–9.

[2]Resolution of the Council 90/C10/010 dated 21.12.89 regarding a "global approach " for conformity assessment, Official Journal of the European Community, No. C 010 dated 16.01.90, pages 1–2.

[3]Decision of the Council 90/683/EEC dated 13.12.90 regarding the modules to be used in the technical harmonization directives for the various phases of conformity assessment procedures, Official Journal of the European Community, No. L 380 dated 31.12.90, page and the Decision of the Council 93/465/EEC dated 22.07.93 regarding the modules to be used in the technical harmonization directives for the various phases of conformity assessment procedures and the rules for affixing and using the CE conformity marking, Official Journal of the European Community, No. L 220 dated 30.08.93 pages 23–39.

EU internal market, the manufacturer can select from these modules the one which best meets their production needs unless otherwise specified by a product-specific directive.

With the creation of the EU internal market, the previous limits of national security structures have been shifted to the borders of Europe itself. In the case of global activities, there must be mutual adjustment of the various safety structures (compatibility clauses or reconciliation).

Germany has, until now, actively participated in risk minimization by governmental agencies or bodies authorized by the state to carry out, in their sovereign function, safety verifications or participate in them (implementation responsibility of the state). The relevant EU directives, on the other hand, want even these state-conducted verifications to be left to the free market and only monitored by the state (pure guarantee responsibility of the state). Although it used to be possible for safety-related professional expertise to remain linked with state agencies, it must now be procured on the open market. A safety methodically concept is presented with this VDI publication (see Chap. 4) which makes it possible, in any technological field of application, to systematically generate, verify and maintain technical safety for technical systems, facilities, processes and products. In this matter, due regard is to be paid to the risk-controlling function of the state—in other words, the necessary contribution to implementation responsibility and the possible share of guarantee responsibility are to be specified.

3.4.3.4 Control Directive of the European Union

The European Union (EU) is committed to promoting within its territory the free market through the free movement of goods, capital, services and individuals. On the one hand, it has laid down quality requirements for the marketing of products with safety- or health-related attributes and has intervened in the market to this extent. On the other hand, it has opened up the market for services in connection with the conformity certificate. Testing, certification and monitoring are in principle—subject to national restrictions—open to anyone and are thus open to free competition.

To secure the aims of the EU, instruments have been created in the form of independent conformity certificates. With its New Approach, the EU is increasingly replacing existing responsible authorities and officially recognized experts with "notified bodies" with rights and obligations in testing and certification. This new concept assumes that the services of these notified bodies are subject to the free market (liberalization).

3.4.3.5 Planning Process

The planning process includes the conception phase and the definition phase (see Sect. 3.3.5.4). The following objectives and purposes are pursued in these two phases.

3.4.3.5.1 Objective and Purpose

Objectives are characterized by the fact that they are uniquely qualified and quantified by content, time and scope. Individual objectives for the responsible employees are derived and developed in a process of agreement about objectives and are appropriate for the level concerned. Depending on the employees' fields of responsibility, these might be objectives relating to profit contribution, costs or performance. By combining them, consistent target systems can be developed which are suitable with regard to both responsibilities and decision-making. Guidance by agreement about objectives is clearly superior to simply specifying objectives since employees are included in the process of identifying objectives.

The safety-related part of the design phase is the collection and analysis of available information about safety. The programme in which it is basically possible, from the safety-engineering point of view, to develop new products (and also systems and technical facilities) is defined by external requirements. These requirements derive from sales markets, society, legislation, technological development, supplier and raw materials markets as well as from the internal capabilities of the company, such as the workforce and their qualifications, the existing product range and production resources.

An agreed quality requirement must be reflected in the result of the product life cycle. It consists of the totality of relevant individual requirements relating to the quality of the product. The most important aspect for the requirements which determine quality is for them to be measurably included in test plans and provided with tolerances (see Sect. Fehler! Verweisquelle konnte nicht gefunden werden).

As regards safety, the focus of the design phase is on the following activities:

- organization of safety-related activities taking into account the state of scientific and technical knowledge,
- definition of responsibilities and competences in the field of safety,
- gathering together all technical requirements relevant to safety from, for example, technical standards, relevant legislation and other rules and regulations,
- evaluation of the "lessons learned" from previous events,
- determination of hazard potentials,
- definition of the higher-level "safety requirements catalogue" for the entire system or entire technical facility
- statement of safety requirements,
- definition of a rough structure for performing the safety task and
- verification that this higher-level safety requirements catalogue is coherent in itself and satisfies the relevant regulations and that the safety requirements stipulated in this catalogue can always be tested and verified.

In the definition phase, the same activities are basically included for safety as in the conception phase—but, in many cases, in a more concrete form and with the addition of traceable archiving:

- assessment of the organization of safety-relevant work and likewise, where appropriate, its adaptation to alterations in the definition phase,
- confirmation or redefinition of responsibilities or competences in the field of safety where changes in responsibilities and competences emerged for the definition phase,
- continuation in the collection of all technical requirements relevant to safety from, for example, technical standards, relevant legislation and other rules and regulations,
- continuation of the "lessons learned" aspect and evaluation of every structural unit to be defined here,
- hazard analysis, determination of limiting risks and risk equivalents,
- definition and release of the safety requirements catalogue and the corresponding safety-related limiting values,
- definition of the subordinate safety requirements catalogue for each structural unit to be defined here in a logical continuation of the higher-level safety requirements catalogue for the entire system or entire technical facility,
- application of the safety methodically concept for every structural unit to be defined here,
- traceable archiving of the documentation which has been created and
- verification that the safety requirements catalogues defined here for the subordinate structural units are coherent in themselves, do not conflict with the higher-level safety requirements catalogue and satisfy the relevant regulations.

The safety requirements laid down in these catalogues must also be demonstrably verifiable.

3.4.3.5.2 Materials and Sampling Procedures

In order to evaluate the homogeneity of the materials to be used, the manufacturer must make a statistically random selection from an internally homogenous totality (from a production batch, for example)—in other words, a random sample. It must come from a representative number of samples from a batch of reference materials in question. This evaluation procedure should be implemented and documented in compliance with recognized, uniform sampling plans (according to DIN ISO 2859-1 "Sampling procedures for inspection by attributes").

In the case of production of single items (one-offs), the suitability of the material must be indicated on the basis of an analogous procedure with a specific method of verification.

3.4.3.5.3 Verifiability of Requirements

It must be ensured that only suitable products and services are procured which can also comply with requirements. In this case, a check must be made of all

subcontractors and suppliers to ascertain whether they have the necessary quality capability, and the procurement documents must contain all relevant data and be verifiable. Traceability should make it possible to track the creation process, utilization or location of a structural unit on the basis of its identification, which has also been recorded. Traceability relates in particular to

- the origin of materials and structural units,
- the processing history of the product and
- the distribution and whereabouts of the product after delivery.

3.4.3.5.4 Consideration of the Potential Conflict Between Cost-Effectiveness and Technical Safety

The profit-oriented market principle is not a sufficiently suitable safety instrument for the field of public-technical safety and can, for a number of reasons, only be applied to a limited extent here. In this case, the main factors of interest should be individually examined and taken into consideration:

- The product "safety"
  In addition to other factors affecting technical safety—such as training or expertise, the general safety culture and the degree to which regulations are observed—safety is here classified under goods and services.
- The user
  In evaluating the products and services on offer, the user makes decisions primarily for himself/herself and normally does not taken into consideration the interests of the common good. Therefore, this case cannot be included as a robust variable in safety-related analyses. Taking into consideration, the interests of third parties or the general public must therefore be enforced or achieved through positive incentives.
- The public interest
  The state intervenes in the market in order to protect the general public and the environment. It thus implements precautions for the common good and public safety and order. In order to enforce this, requirements are made regarding quality and operation and a graduated control system is also provided with instruments for independent proof of conformity.
- Governmental supervision (market surveillance)
  In the liberalized testing and certification market in Europe—possibly the intended future of the majority of the countries participating in the EU—it cannot in some cases be assumed that goods and services with a safety function are provided for the public benefit. In such cases, the instrument of market surveillance is an indispensable element in safeguarding the public safety interest. Setting up a market surveillance body is a necessary though not sufficient instrument for the field of technical safety. Safety is both an individual and a collective need which cannot be consistently satisfied by market forces.

This is especially true of forward-looking collective needs. Therefore, Germany as a state must **regulatively** intervene in the market—in other words, be in disagreement with a change in the possibly intended future of the majority of European countries.

3.4.3.5.5 Responsibilities

The responsibilities for all verification or inspection measures, especially as regards the implementation of measures when verification or inspection results are inadequate, must be clearly and unambiguously regulated. All verification or inspection results must be recorded. If several contractors and subcontractors are involved in the manufacturing or production process and wrong decisions or gaps in verification can cause significant consequences, a verification or inspection plan will be necessary.

3.4.3.6 Implementation Process

The implementation process consists of the development and engineering phase and the production phase. The basic objective of the implementation process essentially coincides with that of the planning process (see Sect. 3.3.5.4). In the production phase, however, it is only possible to work with the instrument of agreement on objectives under very specific constraints, and the instrument of definition of objectives will have to be applied more often.

3.4.3.6.1 Objective and Purpose

The main points of emphasis in the development and engineering phase (see Sect. 3.3.5.4) as regards safety are the following activities:

- checking the organization of safety-relevant work and, if necessary, its adjustment to any possible changes during the development and engineering phase,
- setting up quality and safety management with a redefinition of responsibilities and competences in the safety field if changes in responsibilities and competences have arisen for the development and engineering phase,
- continuation in the collection of all technical requirements relevant to safety from, for example, technical standards, relevant legislation and other rules and regulations,
- determination of probabilities of occurrence and the extent of damage for each type of failure,
- continuation of "lessons learned" and evaluation for each technical component to be developed or engineered,

- involvement of relevant institutions (authorities, public-interest bodies, notified bodies, experts, etc.) in the generation and verification of safety insofar as this is legally and factually necessary for effective supervision,
- application of safety requirements and their implementation for every structural unit to be developed or engineered here by the safety methodically concept, which is applied precisely for this purpose,
- verification that the safety requirements applied and implemented here
  - are effective for subordinate structural units,
  - are not in conflict with the higher-level safety requirements catalogue,
  - comply with the relevant regulations and
  - comply with the safety requirements as defined in detail:
- optimization of specified safety precautions (e.g. inhibition of the utility function, fail-safe, fail-operational),
- Checking and verification of the specified safety requirements for the individual concepts concerned here and doing so during the course of qualification (type test, etc.) and
- submission of a safety report (as the formal conclusion of safety verification)—if necessary, as a component of the safety case (see Sect. 3.2.2.8).

As regards the main focus of the production phase (see Sect. 3.3.5.4), there are the following activities in the field of safety which, in part, represent a further detailing of activities from the development and engineering phase but are, for the most part, specific to the production process:

- review of the organization of safety-relevant work and its adaptation to possible changes in the production phase where necessary,
- within the framework of quality management, redefinition of responsibilities and competences for the field of safety should changes have arisen in responsibilities and competences for the production phase,
- involvement of the appropriate quality assurance organization (either in-house or external) in the production process with emphasis laid on safety requirements and attributes,
- ensuring that the manufacturing processes used are not only cost-effective but also always reproducible—and that with the emphasis on safety,
- involvement of relevant institutions (authorities, public-interest bodies, notified bodies, experts, etc.) in the generation and verification of safety insofar as this is legally and factually necessary for effective supervision,
- implementation in production of the relevant state of the art or application in production of generally accepted sound engineering practice and, in all cases, paying due regard to technical requirements relevant to safety: for example, in technical standards, production and quality regulations,
- verification that the safety requirements applied and implemented here
  - are effective for subordinate structural units,
  - are not in conflict with the higher-level safety requirements catalogue,

- comply with the relevant regulations,
- meet the detailed safety requirements and
- are checked, verified and traceably documented during the course of technical acceptance (acceptance testing or similar).

During acceptance testing, verification is required of the conformity of the manufactured products (or system or technical facility) with the safety requirements worked out and laid down in the preceding phases.

3.4.3.6.2 Hazard Analysis

Hazards and their causes must be analysed using a tried and tested method of investigation. In this way, sufficient thoroughness and depth of testing can be assured. The structural unit to be investigated may need to be divided into manageable sections.

A comprehensive hazard analysis should be carried out for the entire structural unit. This should take into account facility-specific and environmental hazard sources, including natural conditions and events and interference by unauthorized persons.

The documents and data which have been collected together with information from facility and, where applicable, site inspections will serve as a basis for the work.

If hazard analysis covers one or more hazard sources, it should be determined which measures should be taken according to the state of the art. Independently of this, the possible consequences of nonetheless conceivable disturbances should be determined and evaluated with regard to the risk of damage occurring and its effects. Safety measures should be taken while paying due regard to the normative requirements applicable to the limiting risk.

3.4.3.6.3 Verifiability of Requirements

The requirements emerging from the preceding phases are verified as follows:

- As regards the type and importance of tests and inspections, a distinction should be drawn between serial production with the objective of consistent quality and single-item production with the objective of complying with planning specifications.
- Deviations detected can be managed by corrective measures. With regard to control of the manufacturing process, attention should be paid to the reproducibility of the production process (non-conformities) in the case of series production while priority is given to preventive measures in single-item production.

3.4.3.6.4 Inspection and Approval of the Planning Documents

- Examination of draft design, dimensioning and structural design
  It is important to check that all relevant hazards have been identified and appropriate measures provided for their prevention. This particularly concerns the appropriate choice of the system, materials and designs, processes and auxiliary resources for both the execution and the layout (accessibility). Among other things, a check should also be made whether
  - all essential organizational requirements, such as specific trade and operational qualifications, can be met,
  - all tests or inspections required for the execution are provided, and
  - all terms of use and, where applicable, necessary conservation measures are specified before commissioning.
- Planning documents can be inspected in different ways with different amounts of effort. Among other things, a check will be made to see whether
  - the calculation includes the relevant requirements and actual influences, boundary conditions and conditions of use,
  - verifications are maintained for all major components,
  - suitable computational models are used,
  - there are no contradictions in the calculation,
  - all design assumptions are correctly tracked through the system, and
  - no damage is caused by modifications of either components or the system.

As regards the type of inspection, a distinction may be drawn between:

- a full comparative calculation carried out independently of the present calculation and in which important dimensioning results are compared,
- a partial checking calculation in which only crucial parts of the calculation are checked in detail by recalculation or comparative calculation and
- inspection of manufacturing/construction documentation.

- The manufacturing/production documentation must contain all information necessary for the execution, such as tolerance limits or changes as well as instructions relating to the course of production. In addition, it is important here that dimensioning results were correctly transferred, the drawings meet given requirements, additional necessary constraints must be observed, and the plans are clear and unambiguous.

3.4.3.6.5 Traceability of Documentation

The manufacturer must have a quality management system which typically includes the following items:

- documentation and traceable archiving of design documents,
- provisions to ensure an appropriate selection (e.g. sample matrix, particle size, concentration range) of possible reference materials,
- preparation methods,
- assessment and quantification of the required degree of homogeneity of the material,
- evaluation of the stability of the material, even continuously if necessary,
- procedure for characterization of the required properties,
- practical implementation of the traceability of legal units of measurement to national or international standards,
- assignment of attribute values, including preparation of certificates or statements in accordance with ISO Guide 31 "Reference materials" if appropriate,
- provision of suitable production facilities and
- regulations regarding suitable possibilities for identification, labelling and packaging, packing and shipping procedures, as well as after-sales service.

The documentation and archiving system must clearly indicate which activities are to be carried out by the manufacturer and which by collaboration partners. It must also contain the regulations and procedures being used by the manufacturer.

3.4.3.6.6 Approval Procedure

The manufacture of certain important safety-related products may already be subject to mandatory official approval or authorization. These obligations (approval process) must be included in the quality management system and complied with.

The safety management system should, in all cases, be considered a constituent part of the quality management system. Approvals also often stipulate that consideration must be given to protection against unauthorized access ("security").

The quality management system itself is subject to a periodic certification process by third parties, the so-called accredited certifiers.

3.4.3.6.7 Utilization of Materials

- Quality assurance system (in-house and external monitoring with documentation for traceability):
  - Several factors can cause the actual performance to deviate unacceptably from nominal specifications. These factors include, for example, changes in material and component properties, uncertainties in installation or construction or faults and errors in the different manufacturing steps. To combat this, control measures should be included in all major phases of execution (precautionary monitoring of the execution of work).

  - If there is a risk of attributes changing impermissibly or contrary to expectations during the utilization phase, special conservation measures may be necessary (accompanying monitoring before commissioning).

- Compatibility of the components
  The manufacturer must conduct internal audits of his/her activities at regular intervals and in accordance with a previously defined plan and procedure. By doing so, he/she demonstrates that the activities still comply with the requirements of the quality management system.
  The internal auditing programme of must address all elements of the quality management system described in the quality management manual. This also includes the technical and production activities which result in attribute values being assigned to a reference material (material compatibility, "fit, form, function"). It is the responsibility of the quality assurance representative to schedule and organize audits in accordance with the established programme and at the request of management. Such audits must be performed by trained and qualified personnel. Where resources permit, the personnel must be independent of the activity being audited.
  Personnel may not audit their own activities unless this is necessary and its effective performance can be demonstrated.

3.4.3.6.8 Market Surveillance/State Supervision

The instrument of market supervision is an indispensable element of the state's regulatory action for enforcement of public safety concerns in legal aspects. Availing itself of its legal options, the state can intervene in the market and eliminate undesirable developments. The state does this in a variety of ways, either by retaining suitable supervisory officials or by using "appointed contractors".

The manufacturer must create transparency (traceability) for the action of (state) market surveillance.

3.4.3.7 Operation Process

The operation process includes the operation and utilization phases into which, at the completion of utilization, the dismantling, disposal and recycling phases can also normally be integrated (see Sect. 3.3.5.4).

3.4.3.7.1 Objective and Purpose

As an instrument for achieving objectives, the objective definition by which cost-effective, reliable and safe operation is to be achieved stands to the fore.

In the operation and utilization phase (see Sect. 3.3.5.4), a distinction should be drawn between products (technical facilities, goods and services) not requiring and those requiring an approval before going into operation. In either case, the following aspects must be taken into consideration:

- safety management,
- safety monitoring and
- safety during the course of retrofitting work.

The same procedures apply, in principle, to the dismantling, disposal and recycling phases (see Sect. 3.3.5.4) as described in the preceding phases but, due to a frequent lack of relevant sound engineering practice, with a greater testing or surveillance effort. Making matters more difficult is the fact that the processes involved in the dismantling, disposal and recycling phases are not standard processes and, therefore, the personnel concerned must perform their duties with special attention and responsibility. Above all, managerial staff must set up an appropriate and suitable quality management system oriented to the special process steps in the dismantling, disposal and recycling phases.

As regards safety, the focus in the dismantling, disposal and recycling phases is on the following activities:

- organization of work relevant to safety,
- definition of responsibilities and competences in the field of safety,
- evaluation of the "lessons learned" from previous events in order to determine preventive measures,
- grandfathering from earlier limiting values,
- definition of the higher-level safety requirements catalogue for the entire dismantling, disposal and recycling phases and
- verification that this higher-level safety requirements catalogue is coherent in itself and satisfies the relevant regulations and that the safety requirements stipulated in this catalogue can also always be tested and verified.

3.4.3.7.2 Approval

Industrial plants and business enterprises which are sources of environmental pollution or important as regards safety require an approval in accordance with the relevant legislation. The approval procedure should ensure that

- employees and, where applicable, the neighbourhood and even general public are protected against injurious environmental influences and other hazards,
- necessary precautions are taken against injurious environmental influences and other hazards as well as against significant disadvantages or annoyances,
- waste is avoided, recycled or, if not avoidable or recyclable, properly disposed of, and
- energy is used thriftily and efficiently.

A check is also made during the approval procedure to see whether other regulations under public law (such as nature conservation legislation, legislation relating to water and building code legislation) have been observed and measures for occupational health and safety implemented.

An approval can include numerous other official decisions (concentration effect).

The official procedures are bundled by, for example, building permits, permits for installations requiring monitoring as required in the Equipment and Product Safety Act and declarations of suitability for facilities used for storing, filling, trans-shipping, manufacturing, treating or using substances hazardous to water.

3.4.3.7.3 Status Checks

All operational procedures need to be systematically checked at regular intervals. In this way, it is possible to identify not only potential sources of non-conformities but also all possibilities for improvement, either of a technical nature or within the quality management system. Flow charts must be developed, implemented and monitored so as to reduce the probability of the occurrence of non-conformities and to observe the benefits arising from the improvements. The results of the preventive measures must be submitted for purposes of management review.

3.4.3.7.4 Instructions for Use

Instructions for use help in maintaining quality during operation and must be prepared in writing and in detail in the quality agreements and handed over to the user by the manufacturer. Instructions for use are a constituent part of quality planning on the basis of the quality management system. Due observance should be given here to the Equipment and Product Safety Act and relevant legal regulations.

3.4.3.7.5 Maintenance

In order to meet the requirements applicable to technical facilities, products only need to contribute to the extent that these facilities are also properly maintained.

According to standard DIN 31051:2012-09 (see Chap. 2), maintenance is understood as all the measures taken to maintain or restore the nominal condition of technical systems and facilities in as far as they are not modified. This includes terms such as routine maintenance, inspection and repair.

3.4.3.7.6 Retrofitting

For complex systems and industrial goods with a long service life (such as commercial aircraft, rail track networks, large-scale chemical plants and power stations),

efforts are often made to secure an extension of their service life. Depending on the extent of the necessary retrofitting, subordinate measures undertaken during the various phases of the life cycle may need to be repeated so that the same operational and service condition is secured with a return to service as was present before retrofitting.

In certain areas, the law requires retrofitting in accordance with the state of the art or the state of scientific and technical knowledge.

3.4.3.8 Quality Management in Safety Engineering

3.4.3.8.1 Role and Benefits of Quality Management Systems

The systematic evaluation and realization of technical requirements is the basis of every quality management system such as, for example, according to DIN EN ISO 9000 "Quality management systems". These requirements apply to all phases. Since they are already included in the planning process, this situation represents a decisive step for quality management as the costs arising from mistakes increase with every subsequent step.

A quality requirement which can be fulfilled involves well thought-out quality planning consisting of the following main elements:

- planning for the identification, classification and prioritizing of the quality characteristics of the product, specification of objectives and quality requirements,
- planning management and implementation activities, such as preparing the application of the quality management system with flow charts and time schedules,
- preparation of quality management plans with utilization of the non-conformities management system and
- establishment of a process for continuous quality improvement (e.g. "lessons learned").

Provided the quality management system is applied consistently, achievement of the required product quality may be expected. This expectation must be able to assume a high degree of reliability in the system used. The successful conformity of the product with the requirements and the relevant documents is an outward indication of this expectation.

For laboratories, for example, which determine the characteristic data of materials, there is an auditable management system in the form of the Good Laboratory Practice (GLP) standards of the Organization for Economic Cooperation and Development (OECD). A directive has made this mandatory for the members of the EU.

3.4.3.8.2 Quality Management System and Qualified Personnel

At predefined intervals, the product supplier must audit the quality management system. These intervals should be chosen in such a way that suitability and effectiveness can be ensured in complying with both requirements and the established quality policy and its objectives. For the purpose of traceability, the corresponding records must be kept and archived to a sufficient extent.

The manufacturer must set up, implement and maintain a quality management system—usually according to DIN EN ISO 9000 "Quality management systems"—appropriate to his field of activity and including the type, scope and scale of production. The manufacturer must define and document his/her quality management policy, objectives and commitments.

The quality management must further engage in producing reference materials. These must comply with the definitions given in ISO Guide 30 "Reference materials—selected terms and definitions" and the characteristic values evaluated by using approved statistical methods. The quality management system must also commit itself to complying with the provisions of ISO Guide 31 "Reference materials" with regard to material certificates and the provision of the corresponding information to users. Furthermore, quality management must also specify the intended use of the supplied material and commit the manufacturer's organization to ensuring that customers are fully informed.

The obligations of the manufacturer in detail:

- The manufacturer must have at his/her disposal managerial staff supported by technical staff who, in turn, must have the powers and resources to perform their duties. The technical staff must also identify deviations from either the quality management system or the procedures for preparing the reference material and be able to initiate processes to prevent or minimize such deviations.
- The manufacturer must have arrangements in place which ensure that his/her management and personnel are free from any commercial, financial or other internal or external pressures which could adversely affect the quality of their work.
- The manufacturer must have regulations and procedures in place to ensure that confidential information and the ownership rights of customers are protected.
- The manufacturer must have regulations and procedures in place which prevent any involvement in activities that lower confidence in his/her competence, impartiality, judgment or operational integrity.
- With the aid of organizational charts, the manufacturer must define his/her organization and management structure, his/her position within a supporting organization and the relationships between management, technical processes, support services, collaborative partners and the quality management system.
- The manufacturer must describe the responsibilities, powers and mutual relationships of all of the personnel who manage, carry out or check the work which influences the quality of the production of the reference materials.

- The manufacturer must have a technical management team which has overall responsibility for technical operations and providing the necessary resources to ensure the required quality of production processes.
- The manufacturer must have an archiving system for traceable documentation
  - for control of documents (specified requirements, release and change management),
  - for control of records (verification Nachweisführung, inspection reports),
  - for internal audits (scheduled, ad hoc),
  - for control of non-conforming products (non-conformities management system),
  - concerning corrective measures and
  - concerning preventive measures.

The competences and responsibilities for all verifications, especially for the enforcement of measures in the event of unsatisfactory inspection results, should be regulated clearly and unambiguously. If a large number of contractors and subcontractors are involved in a construction project and incorrect decisions could have serious consequences, it makes sense to prepare an inspection plan for integrated verification. All of these individual measures must also pursue the common goal of an integrated safety management system.

The operator must, as a minimum, comply with the manufacturer's conditions of use with safety requirements having absolute priority here. To this end, he/she must set up, implement and maintain a suitable quality management system appropriate to his/her field of activity and including the type, scope and scale of the business. Manufacturer and operator must define objectives and obligations and, where appropriate, document them. Quality can thus ensure and maintain

- all aspects of production,
- material properties (e.g. strength, homogeneity and other characteristics),
- characterization (e.g. equipment calibration and the validation of measurement methods),
- assignment of attribute values (e.g. the use of suitable statistical methods) and
- procedures for material handling, storage and transportation.

The operator must have sufficient personnel who have both the necessary education and training and the technical knowledge and experience for their assigned tasks. The operator must ensure that operating personnel are, in cases of doubt, given additional training to ensure competent performance of measurements, operation of equipment and other activities affecting quality. If possible, the achievement of competence should be assessed by training courses on the basis of objective standards.

If management systems are required, they must comply with the requirements. The quality management system may integrate other systems such as safety or safety management systems.

3.5 Social Considerations

3.5.1 Prevention of Safety-Critical Failures

3.5.1.1 National and International Developments

On the national level, target values for public technical safety are laid down in regulations ranging from the Basic (Constitutional) Law, laws and ordinances to standards and codes of conduct. Its society-dependent form on the international level implies differences in its structures in the various states and regions. Increasing interaction in economic areas crossing state and regional boundaries makes it necessary to adjust and open up regulations which previously have been predominantly national. The scale of the measures to be taken extends from the mutual recognition of structures which have further differences regionally to globally uniform, harmonized structures and regulations for hazard control in specific sectors. In both form and content, verifications in inspection and safety engineering are undergoing a radical change whose implications need to be assessed.

The transfer of national powers to supranational institutions is bound up with a change in national practices in matured and often well-proven traditions, even in technology and business. These changes should be reviewed with regard to negative effects on safety and countermeasures to be taken if necessary.

The conclusion to be drawn from this is that not only the established German system but also other systems should be comparatively analysed and evaluated in the European and, ultimately, global requirements for a further development of public-technical safety. The legal background, state of the art and needs of the economy must be taken into account when determining a suitable system for ensuring public-technical safety. This future-looking problem analysis must also include the activities of independent third parties against a background of the full span ranging from organizations authorized to conduct testing on behalf of the state to service providers acting in the market (problem area: the state's guarantee and implementation responsibilities).

The technical risk should first be examined and analysed to develop approaches for solutions which can be agreed on for systems that are incontestably safe. Whatever the case, engineering must take the forefront in any discussion about consensual solutions and the forms taken by organizations in the safety landscape.

3.5.1.2 Safety and Legislature

Ensuring technical safety should not be regarded in its importance as anything other than the responsibility for internal and external safety. One of the core tasks of the state is to establish a suitable general framework for this. The state and the public are called on to answer the question as to which risk is acceptable and which not

(where risk means opportunity). The state does this through the appropriate legislation, such as the Atomic Energy Act, Chemicals Act, Carriage of Dangerous Goods Act and Explosives Act. Ordinances express the necessary precautions in a concrete form, and this regulatory system is completed by the standards and rules to which reference is made.

Direct governmental activities within the regulatory system are being supplanted by market surveillance procedures which are being increasingly applied. In this case, a risk-dependent balance of role apportionment between the state and the private sector must be found in the future.

3.5.1.3 Safety and Deregulation

In fields of relevance to safety, the state should not limit itself to issuing regulations and punitive sanctions. It should, rather, concern itself with actively specifying standards and structures to the extent required and simultaneously ensuring they are implemented and complied with. The political will is for tasks previously performed by the state to be increasingly passed over into the hands of private bodies or the business sector. Maintaining the required balance calls for an appropriate orientation of state tasks within the changing testing and approval systems.

Structures in the field of safety engineering must be balanced between the state and business just as the balance is to be maintained between precautions, prevention (hazard prevention) and repression (punishment for damaging events). This grading of the necessary requirements profile by the potential for endangerment or damage does not relate solely to technical requirements but also to measures in the fields of approval and surveillance. The inclusion of all interested groups (manufacturers and operators as well as the state and independent third parties) and their active participation must be organized systematically. This means that the state must play its part in a level-headed manner in the duties of approval and supervision. It must also act within the overall context of the mechanisms which ensure that the maximum still acceptable risks is not exceeded.

3.5.1.4 Safety and the Economy

The establishment of standards and rules which are as uniform as possible and assigned to major economic fields is of great importance to the economy. In efforts to find a balanced compromise for the different aims of the groups involved, adjustments may need to be made which no longer adequately reflect the original national implementation of standards and regulations. The regulations must be formulated all the more carefully if public-technical safety within the overall system is not to suffer any impairments.

Organizational aspects (behavioural requirements in operation and detailed activity-related rules) are more strongly emphasized in the Anglo-American economic sector than in Germany, where more stress is laid on product-related safety

(quality requirements concerning construction and fittings). A weighted balancing of these aspects in comprehensive systems could bring benefits, and simply adopting more organization and fewer constructional requirements would be disadvantageous. Whatever the case, in the future the desired level of public-technical safety will need to be verified by looking at the interfaces of quality and behaviour requirements. This is all the more so since, as part of the Europeanization of safety legislation, the requirements applicable to technical products are increasingly being laid down on the European level, this being done with the aim of ensuring the free movement of goods.

3.5.1.5 Safety and Assignment of Competences

Not only is a well-balanced inclusion of manufacturer and operator interests necessary but also the participation of specialized agencies and independent experts. Attention must be paid to the risks of damage occurring and its effects and also to differences in the structures for products on the one hand and technical facilities on the other. Codes of conduct are thus very visibly gaining great importance in the European area and in the American interpretation. This is happening against a background in which standards relating to components and products can represent compromises within which existing German objectives cannot be entirely accommodated.

Since the stringent enforcement of the Basic Law's precautionary imperative is no longer implemented by state institutions or institutions acting directly on behalf of the state, another necessity arises: for the sake of neutrality and objectivity as well as continuity and its consequences (legal uniformity, legal certainty), the state must entrust independent bodies with the tasks of coordinating and ensuring the sharing of experiences among private bodies.

3.5.1.6 Safety as a Paramount Quality Characteristic

The quality management measures practised today in some areas of application are not sufficient by themselves to enable timely discovery and correction of safety-critical quality defects and potential causes of failure. Notwithstanding this, many people do not seem sufficiently aware of the fact that a system cannot be classed as safe unless there is certainty that the safety-related quality characteristics actually correspond to their required form. In this case, the necessary awareness must be created among engineers and scientists: quality management is the approach which adequately describes technical safety attributes and, thus, first provides those responsible with the possibility of making the necessary interventions, corrections and improvements.

3.5.1.7 Quality Management as a Concept for Safety Management

As with any other quality characteristic, safety must be planned, monitored and verified. In this regard, however, it is possible to fall back on the tried and tested—that is, the DIN EN ISO 9000 standard "Quality management systems". In the demands this standard makes regarding quality management, a description is given of the requirements for a reliable safety system on which a potentially successful quality management system depends or, in connection with technical safety, a reliable safety management system. A corporate management system certified in accordance with the requirements of this standard is deemed to have quality capability, and a safety management system geared to the requirements of this standard may thus be regarded as having safety capability. DIN EN ISO 9000 was introduced in the European airlines sector. The question is to what extent this standard has also been introduced and practised in other fields of application with a connection to public safety.

In the field of civil engineering, this system has been anchored in a similar way in the building codes of the German federal states and must be applied to all building products with a major safety aspect (see Model Building Codes, Articles 20 ff. and the inspection, surveillance and certification regulations of the German federal states). Safety or quality management systems are mandatory in other fields of engineering for technical facilities coming under the Hazardous Incident Ordinance, production of hazardous goods packaging. In this case, however, the choice of a quality management system is left to the individual in charge, provided the system is effective.

Safety methodology and engineering are implemented for complex systems with safety management. It must be possible within this context to direct to a central contact point not only unanswered questions regarding all organizational, methodological and safety-related problems but also suggestions for improvements to specified stipulations.

3.5.1.8 Configuration Control and Change Procedures

A general specification for "safety" must, like any other specification, be subject to a formal approval and change procedure. This must be on the basis of a proper configuration control system, whose principles and processes can be specified in a guideline on configuration control.

3.5.1.9 The Individual as a Criterion for Safety Management

Technically complex systems are usually included among human–machine systems in which the personnel employed are entrusted with crucial operational functions. These functions also include safety-related ones. In human–machine systems of this

kind, particular attention should be paid to the involvement of the personnel in operations.

In this matter too, the requisite awareness must be created among engineers and scientists. Personnel who

- know about the practical side of safety,
- have unlimited access to the necessary safety-related facilities,
- are kept constantly and comprehensively informed about the current operating status and safety environment and
- are always being re-evaluated with regard to their "operational function"

should not become weak links in the chain of operational and safety functions.

With his/her natural abilities and shortcomings, the individual is an essential factor in safety management in the context of human–machine systems.

3.5.2 Communication with the Public About Technical Safety

The scientific world strives to provide enlightenment about difficult topics, especially those which could even produce fear in the general public. This is true of medicine, the environment, urban planning, the labour market, tax policy, energy supply and the safety of technical facilities. The representatives of science tackling these issues often slip unintendedly into a role in which they are supposed to legitimize various vested interests and lobbies. The ideal of scientific consistency, the consensus of science, is lost as a result of the conflict among scientists thus created, and this comes to be seen by the public as scientific helplessness. This conflict arises in most cases from the complexity of many current unresolved problems. "Proof" is then necessarily hypothetical in nature. Different conclusions can be drawn depending on the selected hypotheses and the boundary conditions in place.

The ambiguity and opaqueness of the terminology used means that the public becomes more unsettled than enlightened. Let us take the term "safety" as an example here. The competent scientist would have to correctly point out that there has never been 100% safety anywhere. Figures cited for the probability of occurrence of 10^{-7} (1 in 10 million) evoke only a blank response in the layperson. The term "frequency", by which of course "rarity" is meant here, has a different meaning for the specialist engineer than it does for the general public. For the public, there is a qualitatively quite different content of associations: danger, the catastrophic potential of the damaging event, the presumed horrific nature of the damage, personal impacts, effects on one's own children, being helplessly exposed and lack of controllability. In this respect, the two levels of discourse remain dissociated. Since science has the obligation of risk communication in an

understandable way, it must recognize and take into account at least five important psychological factors of risk perception:

(a) Voluntariness
Hazards to which one exposes oneself voluntarily tend to be underestimated. This applies to smoking as well as driving a car.
(b) Controllability
Hazards which seem to be controllable by one's own skills tend to be underestimated. One example is the work of the roofer.
(c) Disaster potential
Hazards with a high potential for disaster tend to be overestimated, such as the possibility of many fatalities in a plane crash.
(d) Concern
Hazards which affect oneself tend to be overestimated, such as the possible side effects of taking medicaments.
(e) Awareness and familiarity
Hazards of which one is aware tend to be underestimated. Smoking may serve as an example here.

Risk communication requires constructive handling as well as factually based argumentation in the assessment of risks. Playing down risks, glossing over susceptible disturbances, covering up accidents or acting contrary to one's own statements are examples of risk communication which destroys the confidence of its audience. Similarly negative in effect is a delayed response to public allegations instead of proactive information or the publication of misleading information.

Risk communication must therefore seek new paths. Appropriate strategies of risk communication include:

- Certain forms of representing **low probabilities**: the significance and realization of probabilities in the form of numbers, including boundary conditions, must be explained in each case.
- **Risk comparisons** such as, for example, comparing the risks inherent in a waste incineration plant and the risk of a railway accident: only when dimensions such as controllability, voluntariness or disaster potential can actually be compared can risk comparisons have a chance of being understood.
- **Risk compensation**: in this case, expected risks and expected benefits are compared with each other (construction of a chemical plant and its impact on the local labour market).
- **Confidence and credibility** only develop when there is an intelligible and consistent preparation of information, a respectful treatment of those whom risk communication addresses and an information policy in which nothing is withheld.

Since risk communication is becoming increasingly important in our society, risk concepts as a whole must be presented which are not entirely oriented towards limiting the probabilities of accidents and incidents occurring. Expressed in

conventional engineering terminology, they are basically very hard for the layperson to understand. It is much more a matter of emphasizing the **reduction in the extent of damage** and taking into account both the psychological insights into risk perception and the conditions of successful communication.

Communication between interest groups with opposing objectives is futile without an arbitrating body when openness to compromise within these groups is interpreted as weakness in asserting one´s own interests. It is therefore no longer a balancing process between risks and opportunities for the community—however that is defined—when the welfare of the individual is "the measure of all things". Representatives of interest groups have, nevertheless, a clear mandate. When they appear under the banner of their group, their role in public discourse will generally be recognized.

The position of the administration is more difficult to define. According to the general understanding, the administration is assigned the role of mediator between the accepted state of scientific and technical knowledge and the need of the public for safety. In practice, however, policy institutes are sometimes in a relationship of dependency on a higher-level political entity (which may be only a "perceived" one). In such a case, it is not necessarily their task to pledge themselves to scientific objectivity alone. They are in some measure biased, and their task is the almost unswerving pursuit of specific objectives (public safety, health and environmental protection). The drive to success to which they are or believe they are committed results, in the most unfavourable case, in a clash of opposing maximum requirements which will be decided on the expediency principle in a detached political arena. The essentially desirable balance of interests, which, on an interdisciplinary expert level, should result in a fact-based report for political options, will be missing in such a case.

We should therefore welcome the trend towards solving this problem of representative democracy wherever it is possible. The first thing to do is to inform the public in advance of a safety-related decision by giving it the facts about opportunities and risks. The public must be put into a position where it recognizes the consequences of the options in all their aspects so that any interested party can make a decision in the light of his/her personal background. In this matter, the idea should be discarded that a collectable debt of the individual is concerned and that there is always the possibility of involvement. The "silent majority" is to be animated by an offer which cannot be overlooked of taking an active part in the consensus of the informed.

This option does, in principle, exist. The public media could take on the role of an educational institution and be the forum for risk communication if they were not already also generally following the trend in journalism that only "bad" news is "good" news. Today's partly trivialized talk shows could be replaced by a readily graspable transfer of knowledge within a discourse whose participants were committed to the culture of dialogue (if necessary, using generally accessible techniques

of information and communication). If there were success in establishing as a routine this form of debate about the consequences of scientific and technological innovation, there would be increased pressure on the experts to make their specialist knowledge available to the public and be measured by the response of the audience.

Risk communication within a discourse regarded as democratic in nature is an arduous undertaking and, in addition, one with an uncertain outcome. Nevertheless, this is the only serious way of problem-solving.

3.6 Recommendations

Although a different impression may currently prevail among the general public, we engineers notice again and again that the development of technical safety has always kept in step with the overall development of engineering. It should, however, also be noted that interdisciplinary cooperation, with which increasing specialization in engineering is countered, is found in safety engineering only in a rudimentary form. In general engineering, generalistic approaches and systems engineering management procedures have long proven themselves and, with their help, specializations based on the division of labour can be brought together again in an interdisciplinary approach. On the other hand, safety engineering, safety legislation and the relevant standards seem to have remained unaffected by this today. There is an urgent need for action in bringing generalistic approaches and systems engineering management procedures into safety engineering in the same way as has been common practice in general engineering for decades. The safety methodically concept **mentioned in this publication may serve as a generalistic concept for safety engineering** and DIN EN ISO 9000 “Quality management systems” might be used as a suitable systems management procedure. The VDI can offer the interdisciplinary working platform for both elaborating the outlines presented here to the extent necessary and keeping them up to date.

The preceding sections have shown how technical safety is planned, generated and permanently maintained. Descriptions were also given of how different influences, be they of technical or human origin, affect a production process. The persons responsible for the product must be aware of the level of safety achieved in every planning and production step since each successively builds on the previous step (and therefore progresses). Undetected errors would otherwise be carried forward. However, it is evident in this matter too that one only sees and attends to what one knows.

The society which pays for teaching and research and promotes technology has a right to information. There is, therefore, an obligation on the part of engineers and scientists to supply information about interrelationships in technical safety. The relevant areas are addressed below.

3.6.1 The Research Landscape

The research landscape can be divided into four fields:

- tertiary education institutions (universities, colleges and music and art schools, predominantly under the legal and financial responsibility of the federal states),
- research (and research funding) organizations (the German Research Foundation, the Helmholtz Association, the Max Planck Society, the Fraunhofer Society and the Gottfried Wilhelm Leibnitz Scientific Association),
- research centres in industry, including small- and medium-sized enterprises (SMEs), and
- research centres and institutes of the federal and state governments.

Research in Germany thus has a high potential, which is evidenced by the share of gross domestic product taken by research and development. In a press release of December 2013, the Federal Ministry for Education and Research wrote: "In 2012 expenditure on research and development (R&D) in Germany rose to a record level of more than 79.5 thousand million euros. The R&D share of the gross domestic product (GDP) thus reached its highest value of 2.98% for the first time in Germany. […] Germany is investing in the future to a degree higher than ever before. Together with business and science we are reaching the 3% target for the first time. It is now a matter of securing this positive development in the long term. This cannot succeed unless business and the state together continue to invest strongly in research and development—in other words, in the future of our country". The press release continues: "Germany has significantly strengthened overall its position as one of the world's leading innovation hubs, also via the successful high-tech strategy. Its strong position in international competition is reflected in, for example, global trading in R&D-intensive goods, scientific publications and transnational patents".

While taking account of both the isolated areas of focus in economic research on products and the small quotas devoted to safety research, it is still, however, necessary to point out the present deficit in research as regards the solution to obvious problems in the field of safety engineering. The VDI offers with this publication on technical safety an approach soundly based in professional knowledge and expertise by which these obvious problems can be properly solved.

If we assume that not only quality but also safety are expected of products from Germany—almost like a trademark—and that a market expectation is expressed thereby, research must again devote itself more strongly to questions of safety.

- First of all, an evaluation of safety research can help to clarify whether quality is at the required level.
- In response to this, a reorientation must begin. The Dechema/GVC research committee "Safety technology in chemical plants" accordingly complained, for example, about

- the lack of public-sector sponsorship for issues in safety engineering,
- the trend which has seen university departments and institutes that used to have primarily a safety orientation now increasingly turning to other research fields,
- the restrictions in course content and possibilities linked with the decline in university research capacity in the field of safety technology,
- the lack of an adequate fund of basic knowledge in the field of safety engineering on the part of graduates, who then have to acquire this from in-house or external technical seminars,
- a marked drop in students studying process engineering and technical chemistry, which in turn also limits the propagation of safety-related knowledge, and
- the increasingly more limited freedom of action of German industry in research and development, even in safety engineering, among other things as a result of global competition which is, in part, becoming more fierce due to a lack of uniformity in general conditions at the international level.

This is also the case in general and reinforces our recommendation for a reorientation of safety research.

Complexity, economic integration, the necessary depth of detail and the new fields in the dynamic progress of innovation call for research in Germany to be integrated into international networks, in particular those of the EU. New organizations are constantly coming into existence here, such as the European Technology Platforms (ETPs). The "Safety for Sustainable European Industry Growth" platform alone has several focus groups dealing with topics relating to risk and human factors engineering.

The international integration of German safety research must be defined and managed, and the appropriate structures must be designated and set up.

The subject of internationalization is dealt with in more detail in Sect. 3.6.5.

3.6.2 Education and Training Options of the Universities

Courses can be maintained at the required high level only in conjunction with sound research if industry is to be provided with sufficiently qualified engineers. Safety technology must therefore equally form an integral part of the curriculum at all polytechnics, technical colleges and universities and be a subject of training and further training courses at private institutes.

The training measures necessary for offering a basic course in safety engineering must be the responsibility of technical colleges and universities within the framework of the engineering curriculum. The content of courses which must be offered by tertiary education will, above all, include:

- technological impact assessment and risk analysis,
- risk communication,
- influences of human behaviour on safety (human factors),
- interdisciplinary cooperation competence,
- emergency planning,
- the role of national and international regulatory efforts and
- vocational ethics in engineering activities.

In view of the range and social significance of the courses required here, the currently observable cutback in qualified teaching capacities and the rededication of safety-oriented departments to other fields in technical colleges and universities are not satisfactory. In the interests of ensuring technical safety in the future, the cultural administrations responsible for the universities are urged to stop rapidly this decline and reverse it. Private business would have to consider setting up endowment chairs in safety engineering as an **immediate measure** to counteract the associated shortage of competent teaching staff.

It is, in particular, up to the private educational institutions in the industrial sector to make long-term provisions for securing competence in safety engineering and adapting this competence to new technical and social challenges. It is a welcome fact that setting up academies and other training institutions (such as simulator centres for the periodic review and further development of the necessary competences) has already been promoted for a long time now in some branches of industry. However, questions relating to safety only play a subordinate role in the curricula, and this needs to be corrected urgently. Private business is therefore called on to train and employ personnel with safety-engineering qualifications and do so on a long-term basis in order to ensure that no shortages in safety competence arise due to the natural retirement of experienced personnel coupled with a possible lack of growth in the numbers of younger technical staff. This presupposes that a future-looking management of knowledge and information is effected via a thorough documentation of technical decisions and the corresponding measures for the further dissemination of accumulated knowledge (in this connection, see Sect. 0).

3.6.3 Thematic Focuses

3.6.3.1 The Public

Acceptance of technology by the general public depends largely on how the benefits for the individual and society are made clear and a preferably comprehensive understanding of the conditions and limits of safe technological development is achieved for the people affected by technical factors. In the sense of a debt to be discharged, all experts and institutions (scientists, research institutions, engineers, the courts, industry and the public sphere) are under an obligation to implement

comprehensible information and communication strategies in order to inform the public of the demands and possibilities of safe technology.

Multipliers and opinion leaders have a special value in conveying factual information to the public: media representatives, senior members of political parties, teaching staff in schools, universities and other private and public-sector educational institutions and representatives of engineering and industrial associations.

To make it possible to transfer appropriate information from the "producers" of technology to the "end users", consideration should be given to setting up networks for technical safety with topic-specific contact desks ("nodes"). These nodes should be staffed by not only media professionals but also qualified experts in their particular fields in order to meet the needs of an interested general public for information or handle referrals to the appropriate technically competent bodies.

3.6.3.2 Technology Council

Safety technology must be treated holistically and considerably more systematically. The boundaries of technical fields must be overcome, just as the fields of responsibility of organizational units must be open in the event of questions of safety. Today, the structure of safety engineering historically developed on the basis of application-oriented specialist and technical areas is leading to the emergence of countless committees. In the case of interdisciplinary technology projects, their field-specific regulations are bringing about a multitude of interfacing problems.

As a vision, a "safety engineering" code would be an ideal solution for increasing the efficiency of activities in engineering and, in this case, for all of the business sector, including the "safety" evaluation of the corresponding elements of engineering activities. The target—the long-term creation of a "safety engineering" code—could be a primary task of a Technology Council, which would be created analogously to the Science Council.

This Technology Council would advise the federal government and federal state governments. One main focus would be the development of universities, science and research. It would make recommendations and statements in two core areas: scientific institutions and questions spanning the scientific system. A Technology Council should, of course, inform and advise not only the federal government and, where applicable, the federal state governments but also trade, industry and social groups about questions relating to dealing with engineering and technology.

As one of its fields of operation, the Technology Council could take over responsibility for the "safety engineering" code mentioned above and, with the appropriate structures, guide and support it. Another field of operation could then be safety engineering, which would have an optimal overall view of all elements of technology and engineering with this section of the Technology Council. Other fields, such as ethics and science, are conceivable and should be defined and set up in consultation with private business. Both the potential for innovation in engineering and the transformation of research findings into marketable products in the

technical area certainly belong to this area of additional fields of operation ((Lenhart: Aussage muss noch geprüft werden.)).

The entities responsible for the Technology Council would be both the state, represented by the federal and federal state governments, which would look after the interests of their citizens, and private business and other non-governmental bodies such as trade unions and environmental organizations.

Since it is not a simple matter with more complex systems to describe and easily control technical safety concepts and human–machine interfaces, the documentation and communication of technical and organizational sub-concepts have become an important component of the holistic safety concept. The field of information or knowledge management provides useful tools for documentation and communication. The term "information management" was introduced in the mid-1980s in the USA in connection with the idea of the paperless office. Nowadays, "knowledge management" is a synonym although, strictly speaking, the knowledge which is in the minds of people cannot be managed. What is referred to as "knowledge management" is, in the final analysis, information management and is used for creating the general conditions for knowledge work. For historical reasons, the term "knowledge management" has, however, prevailed. The discipline of information or knowledge management has its roots in information technology with a focus on documentation and the electronic exchange of information. Information management instruments have been heavily supplemented by contributions from not only economics and the social sciences but also cybernetics, behavioural and communication psychology. It is probably not coincidental that safety and hazard prevention management have been introduced parallel to information and knowledge management in the last 30 years. This means that information management tools can gradually be used for safety management too. Highly sensitive safety systems, such as in commercial aviation or nuclear and chemical plants, could not be kept at the high level of safety required in an industrial society without perfect management. In the field of technical safety, information management instruments must be used more intensively in those technical and economic sectors in which, due to their structure (e.g. small and medium-sized enterprises), variety and individuality in safety issues (e.g. in process plants), modern information management tools are only being partially used. A new special focus must be placed on "technical safety" for the future-oriented project in the Industry 4.0 high-tech strategy of the German federal government.

The objective of information management is sometimes strikingly expressed by the slogan "the right information at the right time in the right place". Ultimately, only the aspect of efficiency is missing here since the outlay on information management must be commensurate with the security-related question. This is so on account of not only the risks and their various facets but also the economic constraints within which a company, testing organization or public authority must operate.

Various questions can be derived from this slogan relating to the specific challenges to information management:

- For the task in question, have all safety-relevant aspects been taken into account? Nowadays, it is not difficult to gather all of the necessary information from libraries or the Internet.

Nevertheless, more questions arise:

- How can information relevant to the specific task be filtered out and condensed task-specifically?
- Have all data, even those relating to peripheral fields, been collected?

In the search for safety solutions, increasing specialization of technical disciplines makes it necessary to look more and more frequently at neighbouring disciplines—ultimately, the age-old question remains:

- Are the data and information collected correctly?

Technical experts have always been, and will remain in the future, the key to success in solving questions of this kind. Although there is broad consensus that suitable IT platforms, such as the intranet and Internet or databases and research systems, are necessary requirements here—as pen and paper and printed matter once were—the success of information management does, nevertheless, depends on whether and how the individual is placed at the centre. If this realization is pursued, current work in the field of information and knowledge management can be focussed so that there is support for interactions between the individuals involved. It no longer matters in this regards to what extent the people who belong to open expert networks or closed "communities" are experts or stakeholder groups, or whether they are communicating within a company or public authority or between different institutions or stakeholder groups. In this matter, there are both national networks and European and international networks. For example, the EU encourages the creation of European networks especially with the aim of not only strengthening the economy but also securing the level of safety which is expected by society. However, networks focussed predominantly on safety-related aspects are struggling since the funds for supporting networks mainly flow into projects which promise immediate economic success. Therefore, we appeal to the competent bodies, companies, politics and administrations to take into account the special importance of technical safety in an increasingly complex society and provide the necessary funds to enable the right safety-related information to be in the right place at the right time.

3.6.4 Emergency Planning

Emergency planning for large-scale damaging events must also be organized on a more international basis. In the case of only Germany, numerous products and systems, despite their inherent safety having been adequately demonstrated and documented, do nevertheless reveal additional risks during their utilization phase.

Hazard sources of this kind can significantly overstep the product's or system's own boundaries and endanger a broader area of the environment which is not causally linked to the product or its operation. In such cases, the safety philosophy behind product management must also include emergency planning for the potentially affected environment. In addition to bodies within companies and associations, this usually involves not only bodies in the government executive (such as district authorities, county council chairpersons and mayors) but also agencies directly responsible for disaster protection (such as the fire brigade and the technical relief agency). The entire network needs to be defined more clearly in its structure and responsibilities, and the interface with the planners and operators of products, systems and technical facilities needs to be more institutionalized.

Not only are cross-border effects possible—they are increasingly to be expected. The clearer structuring of the network recommended for Germany must analogously be transferred into a recommendation for the international structuring of relief organizations. Some good approaches to this are already in place in Germany, Poland and the Czech Republic and need to be strengthened from the institutional point of view and expanded.

3.6.5 Internationalization

Globalization of the markets also calls for the internationalization of safety engineering among product and system manufacturers. Goods and their production must increasingly conform to safety principles which ensure their free circulation and safe utilization in all recipient countries. Market forces are not strong enough on their own to adequately secure the necessary safety attributes of products and systems as they are often opposed by economic aspects. Therefore, a safety structure is required which will establish the minimum standard of technical safety in the market and also avail itself of state supervision and effective sanctions.

Cross-border agreements at governmental level are indispensable for this.

Chapter 4
Interdisciplinary Safety Guideline

4.1 Understanding of the Term Safety

4.1.1 Safety as a Legal Term

After incidents and accidents, the call is heard over and over again for "more safety". In the wake of such events, politics and the media often point out that people were endangered, injured or even killed and objects of legal protection threatened or otherwise affected. The call for better rules often gets loud but without an analysis being done first to see whether existing rules have been inadequately implemented. Aside from the general mood of alarm, the next step is generally a scheduled review of the rules and enforcement provisions with the corresponding options for action, including optimization of legal orders. In the German-speaking world, the legal term "Sicherheit" covers the two terms of "safety" and "security" as used and differentiated in the English-speaking world. The English term "security" principally stands for **protection against** (unauthorized) **access** (or entry), while the term "safety" is, on the other hand, understood as "technical safety" in the sense of "**freedom from unacceptable risks**" (as an example, see DIN EN 61508-4:2010 "Functional safety of safety-related electrical/electronic/programmable electronic systems"—Part 4: Terms and abbreviations, Sect. 3.1.8). The German term "Sicherheit" covers diverse issues, such as "internal and external security", "social security", "collateral", "public security" or even "law and order". This VDI publication dealing with technical safety does not include the idea of security which is inherent in the German term but, as far as technical products are concerned, refers only to "safety". It should, however, be noted that security problems—the security of information—do lead to safety problems, and this, therefore, has to be taken into account as well.

As already mentioned, the German legal system provides "indeterminate legal concepts", so-called general clauses, for legal norms (laws and statutory orders) and the drafting of contractual documents. In many fields of technology, it is sufficient

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_4

to refer to the relevant applicable design product development, design and production in order to be sure that no unacceptable risks will arise during utilization and operation of the product in question.

However, not all fields of technology are covered by normative codes of practice with whose aid the safety of technical products can be comprehensively determined. Each field today has its own code of practice for technical safety. Irrespective of whether civil engineering, transportation, chemical engineering, power engineering, aeronautical engineering, plant engineering, mechanical engineering, electrical engineering and so on, application-specific safety concepts determine the conceptual design, definition, development and engineering, production and integration of the technical equipment in question. Detailed constructional regulations, operating instructions and regulations and maintenance instructions are drawn up for its operation and conditions formulated for retrofitting. Even the monitoring of operations by the owner and supervisory bodies is regulated in an application-specific field. However, this is far from being the case everywhere: there are also analytical methods relating to failure such as, for example, in the field of aerospace engineering. As yet, there is no safety concept which covers all areas of application, in other words, with interdisciplinary validity.

This has a particularly obstructive effect for innovative technologies since the state of the art and state of scientific and technical knowledge in this case are supposedly to be extended beyond their current boundaries. The guideline presented here lays the foundation for an orderly approach by means of its cross-application validity and the particular attention paid to innovative projects. In this matter, it is necessary to regard safety as no longer being solely a legal term. "Technical safety" is one of the outstanding features of a technical product. The generation of technical safety is a particularly demanding task for primarily engineers and often scientists too. More than any other technical discipline, the generation and verification of technical safety also call for the special care and attention of industrial management and the administration in general.

4.1.2 The Term "Technical Safety"

Technical products are characterized by properties which manifest themselves as quality and functional attributes that are individually manageable from the engineering point of view (such as dimensions, colour, performance parameters, switching times and displays). Attributes of special importance on account of ethical, legal or contractual requirements are referred to as "quality characteristics". Every quality characteristic relevant to technical safety needs not only the special care and attention of technical management throughout the entire design and manufacturing process but also to a greater degree, verification from state supervisory institutions (as a "competent lawyer" in the generally uninformed public) so that the product in question is free of unacceptable risks and will remain so.

4.1.3 Technical Safety as a Requirement for Product Design and Implementation

At the suggestion of its Scientific Advisory Council, the VDI set up the VDI "Technical Safety" Committee with an interdisciplinary membership. The VDI entrusted the committee with the task of identifying the **hidden commonalities** of the safety concepts in individual fields of application—such as civil engineering, transportation systems, chemical engineering, energy technology, aviation, plant construction, mechanical engineering or electrical engineering—and putting together a safety concept valid across all applications which can be used on an interdisciplinary basis. This task was first presented to the public in the VDI memorandum "*Technical Safety*", *an Attribute of Quality* (Düsseldorf, June 2010, ISBN 987-3-931384-68-5). The safety concept is now presented in its entirety (with the present VDI publication *Technical Safety*). A product is deemed to be "technically safe" when the safety-relevant measures mentioned below are verifiably implemented during the design and realization of a product or any other technical facility.

The requirement for a product to have "freedom from unacceptable risks" is fulfilled when the safety-relevant quality characteristics of the product comply with this requirement. The design and implementation of the product are thus to be oriented specifically to these quality characteristics—as also to every other quality characteristic. The safety-relevant quality characteristics of a product include its **emission behaviour**, **passive quality characteristics** and **active functional characteristics**. The procedures necessary in each case do, however, differ and should be methodologically aligned to the function structure (function tree) with main functions, subordinate sub-functions and the corresponding function elements. In this matter, the following aspects must be taken into consideration.

4.1.3.1 Emission Behaviour

The material, chemical and physical emissions for a technical product must be demonstrably kept within the limits specified by law or in the individual contract by means of a technical design appropriate to the operating state in question. A clear distinction should be drawn here between "unwanted side effects" and "necessary utility functions":

- "Unwanted side effects" include, for example, leaks (such as gas and nanoparticles), losses in efficiency in energy conversion, function-related noise emissions and residual radiation. They can be limited by means of seals, energy-related or acoustic insulation measures, radiation protection or similar protective measures. The nature and scope of the protection measures which may be necessary can basically be determined on the basis of "generally accepted sound engineering practice". In certain special fields, such as

immission control and radiation protection, specification of what protection is necessary may, where applicable, be made by direct reference to the "state of safety technology" and "state of scientific and technical knowledge".

- "Necessary utility functions" include, for example, "transmission radiation"—in other words, electromagnetic data transmission waves for terrestrial or satellite-based radio and television technology, telephony, ground-based or airborne radar technology, satellite communications and navigation (GPS, Galileo). There are not only low-risk and risk-free but also risky or hazardous propagation areas for these utility functions. This distinction between risk-free and risky or hazardous propagation areas is drawn in the relevant legal regulations on the basis of "generally accepted sound engineering practice", the "state of the art" or "state of scientific and technical knowledge". Clear safety provisions are defined here for risky or hazardous propagation areas which must be strictly observed in practical operational application. These provisions may be supplemented by a general minimization requirement for utilisation as e.g. applied in the Radiation Protection Ordinance.

4.1.3.2 Passive Quality Characteristics

Passive quality characteristics are characterized by the fact that they do not change over time and neither "deplete" nor are subject to any physically or chemically verifiable "ageing". With a proper constructive design, they can be relied on permanently. Passive quality characteristics are deemed to be "**captive**".

- If these characteristics are captive on account of their **natural** origin—for example, as a result of the effects of gravity, decay of radioactive substances, magnetic field of the earth or speed of light—the corresponding characteristics of a product are deemed to be **naturally** captive. On the basis of the principle of operation, this natural captivity is present **permanently**. It should nevertheless be noted that the product (technical product) with which natural influences interact is still subject to a process of degradation or ageing. Regular compliance checks are therefore indispensable.
- If these characteristics are captive on account of the **technical** design, the corresponding characteristics of a product are deemed to be **technically** captive. Examples include holding and support functions, standardized shrink fittings, secure fasteners, forced guides, permanent magnets and guided, unbreakable compression springs as well as adequate creep and flashover distances from high-voltage equipment. On the basis of the principle of operation, this captivity can be **permanent** (taking a **process of degradation or ageing** into consideration) or even **temporary** (taking a **process of functional depletion** into consideration). Regular compliance checks and maintenance inspections are therefore essential.

- Permanently or temporarily, captive quality characteristics of a product or technical product which are relevant to safety can be grouped under the term "**inherent safety**". Regular compliance checks and maintenance inspections are relevant to safety, normally require state supervision (state supervisory agencies such as the Rail Ministry or Air Ministry) and, for this reason alone, require traceable documentation and archiving.
  Products or technical facilities to which safety-related design regulations must apply are not deemed to be "inherently safe" unless their "inherent safety" has also been demonstrated and approved.

4.1.3.3 Active Functional Characteristics

Any "active functional characteristic" can fail. They are deemed to be losable since it should be assumed that their function or function elements can, in principle, fail at any time. This is stochastic failure, which can in turn be handled with methodologically appropriate procedures.

4.1.3.3.1 Safety Precautions Against Function Failure

The quasi-classic precautionary measures taken against stochastic failure are the use of safety devices (redundant elements or even diversitarily redundant elements), operational safety measures (load-dependent precautionary replacement of elements) or utilization restrictions laid down in operating regulations. Two safety concepts are applicable in this context:

- **Fail-safe**:
  When an active functional characteristic fails, the technical product must be put immediately into a "safe state" (fail-safe) as defined during the course of the planning process (e.g., an automatic train stop). The result of such a safety measure is termination of the current operating function (possibly temporarily).
- **Fail-operational**:
  In the event of an active functional characteristic failing, the technical product is put into a state of "safe functional behaviour" (fail-operational) as defined during the course of the planning process. With this type of safety measure, the current operating function continues but normally only in a limited form (e.g., an emergency landing at the nearest airport).

4.1.3.3.2 Controllability of the Probability of Failure

For the purpose of safety precautions, it is vital in subsequent operation (in utilization) to make not only the probability of failure controllable but also the extent of potential damage—in other words, to keep it within acceptable limits.

This safety-related approach of **reliability engineering** has proven itself over six decades or so in both aviation and space travel and has made a major contribution to the outstandingly high level of safety in civil aviation throughout the world. It is now being applied increasingly in other fields of engineering, too.

4.2 Introduction to Interdisciplinary Safety Engineering

4.2.1 Organization and Management

Technical safety not only is one of the properties of a technical facility but, alongside the actual functional purpose, also represents the outstanding quality characteristic. Trust in the functioning of a technical facility is the essential basis of modern technology. During conceptual design, definition, development and engineering, manufacture, trials, utilization, maintenance, retrofitting, decommissioning and subsequent disposal, special care and attention must always be devoted to this quality characteristic. Not only the individual's interest in his/her personal integrity but also the state's interest in safety and public order demands this safety, which must be present throughout the entire life cycle of a technical facility, technical product or even technical system.

It is notable that, with regard to the quality characteristic of "technical safety", it is largely the purchaser alone who decides what specific level of safety should be implemented. This affects not only relationships in civil law but also public safety/security. Both of these are based on the corresponding legal foundations, compliance with which is mandatory and non-compliance generally punishable. The demand for technical safety in legislation largely takes the form of so-called indeterminate legal concepts such as "generally accepted sound engineering practice", the "state of the art" and the "state of scientific and technical knowledge".

The following basic principles form part of the general state of knowledge in the field of safety engineering:

- Absolute (100%) safety does not exist in engineering.
- A legal demand for technical safety is not capable by itself of creating safety or guaranteeing it—irrespective of how harsh the penalties are for non-compliance with this requirement.
- The quality characteristic of "technical safety" must be both generated and demonstrated for every technical facility and preserved during the course of maintenance work. "Technical safety" is one of those quality characteristics generated as the result of an engineering process of analysis and design. Safety requirements and safety inspections alone do not suffice here.

What is needed in this matter is a methodologically appropriate approach in defining a suitable safety concept and thereby preventing weaknesses or defects.

This means that the well-proven technical organization structures and management procedures are also applied in the context of safety engineering:

- uniform project and system structure with assignment of responsibilities and the corresponding powers,
- establishment of central departments for cross-system topics, such as product planning, human factors engineering, technical safety, environment engineering (original and object-influenced environment, electromagnetic compatibility, lightning protection), reliability/dependability, operation and maintenance regulations, personnel qualification and certification, environmental compatibility and immission control, official and other approvals and permits, manufacturing/assembly/integration, supervision on site, commissioning and trials/test operation/demonstration,
- project planning and tracking through all project phases of the entire product life cycle,
- centralized configuration and interface management with uniformly structured verification,[1]
- centralized quality management system based on generally accepted technical rules (such as DIN EN ISO 9001), which is usefully supplemented by a suitable product and quality assurance system
  [Note: The quality of corporate and project processes is regulated with a quality management system as per DIN EN ISO 9001. In addition, both the product quality and technical safety can be made controllable by means of a product and/or quality assurance system] and
- centralized phase- and milestone-oriented release and reporting system (where applicable, with progress payments based on payment milestones).

Practices of this kind have been in general use for decades in the various fields of engineering and technology, although they take different forms. However, it must be noted that, when setting up a management organization of this kind, the overall system is more than the sum of its constituent parts.

In the case of complex products, such as technical facilities or systems, a suitable set of management instruments is essential. In this matter, it has proved useful for decades to combine

[1]Configuration and interface management assures that:

- the technical specifications of the subordinate structural units meet the contractuable specifications of the higher-level system (project) specification,
- all persons involved and all responsible persons are notified of changes to these specifications,
- interfaces between structural units are defined systematically between those responsible and laid down contractuably and
- safety attributes are fully captured, adapted to the extent necessary and verified.

- the “conceptual design phase” and the “definition phase” (grouped here under the term “planning process”),
- the “development and engineering phase” and the “production phase” (grouped here under the term “implementation process”),
- the “operation and utilization phase” and
- the “dismantling, disposal and recycling phases” (grouped here under the term “operation process”)

into a single centrally directed configuration management system. The quality characteristic “technical safety” is to be included within configuration management in the sense of a safety management system. In this case, the quality characteristic “technical safety” or the safety management system must be placed in an area of responsibility of its own which centrally covers all levels of the project or system structure. The phases of the product life cycle are illustrated in Sect. 3.2.1.2 in Fig. 3.1.

To ensure that sufficient transparency of technical and organizational issues is maintained in these complexly structured, technologically innovative and (from the safety point of view) exacting products, technical facilities or systems and their entire life cycles are divided into time periods (phases). A subdivision of this kind into content- and time-based segments means that it is possible, at the beginning of each of these transparently presented phases, to define clear objectives, the constraints to be observed and other requirements and procedural instructions. At the end of each phase, the results obtained can be checked with regard to how the objectives and requirements have been met. Should objectives not have been reached, the phase in question must be repeated. This recursive process is indicated in Fig. 3.2 by blue arrows. On the basis of the results achieved, the objectives, constraints to be observed and other requirements and procedural instructions can be specified for the next phase. A phase approach of this kind not only facilitates technical management but also secures to a special extent even the organizational management measures required and ultimately results in it being possible for the first time to properly track and monitor the specified objectives.

To this end, this guideline illustrates the basic principles behind the procedure for generating safety in the form of safety flow charts during

- the planning process with conceptual design and definition phases,
- the development and engineering phase.

The safety requirements generated in these first phases of the product life cycle must be observed and applied during the production and operation phase. Since the dismantling, disposal and recycling phases call for an autonomous treatment of safety, the generation of technical safety must be adjusted here to specific requirements and delivered but designed analogously in a methodological way to the preceding phases.

The product life cycle covers both the planning and implementation processes and the operation process, for which the procedure required for securing technical safety is described in each case. It is the intention here to cover the needs of all

technical disciplines and formulate common features relevant to safety—in other words, hidden commonalities—as regards both technology and language. In this regard, reference is made to the principles of a systems engineering phase approach (see Fig. 3.1) as presented in this memorandum (see Sect. 3.2.1.2).

In the example of the phase concept, the requirements are emphasized of safety controlling, safety-related documentation (the "safety case"), the state of the art, the state of scientific and technical knowledge and the assignment of responsibilities and powers in the respective phases. In addition to the necessary documentation of the individual steps and decisions, the loading assumptions[2] together with the intended and possible operating conditions and scenarios, the service life of the products and the safety level are shown as a function of the consequences arising. Finally, the path to the risk assessment is defined and the necessity for public involvement is described on the basis of the risk level determined and the necessary involvement of the individual in the development and manufacturing process.

In the event of changes in the technical requirements (as already laid down in specifications), a check should be made within the change management procedure as to the extent to which the quality characteristic of "technical safety" is affected. It may be necessary to repeat the decision and action steps taken in all previous phases.

Top priority should be given to ensuring that, from the systems engineering point of view, the structure and shape of the safety documentation (the "safety case", also termed the "safety assessment" according to IEC 1508 or "technical documents" according to DIN EN ISO 12100) satisfy the following eight requirements:

- The technical requirements in all phases must be unambiguous, clear and comprehensible.
- The conditions under which the answers for putting together the safety case are given must be clearly described with the reasons provided by the competent and responsible individuals for each phase.
- The evaluation criteria used must be clearly presented, and the underlying set of rules, consisting of legal provisions and technical regulations, must be specifically named. Any reference which may be necessary to the state of the art or state of scientific and technical knowledge should be integrated.
- Answers to phase-specific questions must clearly distinguish between facts, information from the people involved, calculations, assumptions, test results and conclusions. Furthermore, the evaluation must be carried out separately.
- Differences in the evaluations in the phases must be clearly emphasized by the responsible individuals and reasons given.
- Conclusions must be transparent, fully verifiable and consistent.
- The safety case arises from the individual phases of the product life cycle and must be understandable and verifiable in itself.

[2]All loads acting from both the outside and inside come under the term "loading assumptions". All other effects which do not come under the loading assumptions are accordingly referred to as effects coming from the **original** or the **object-influenced** environment.

- The documentation must be complete and, in particular, include all recursive iteration steps. Transparency must be continuously guaranteed over all three processes (see Fig. 3.1). Protection of interests can make special organizational measures necessary while not unacceptably impairing the interests of public-technical safety.

The importance to be attached to technical safety makes it essential to secure in the documentation not only the requirements but also verification with regard to effective traceability. Agreement with approval or licensing authorities or supervisory bodies must be secured with respect to both requirements and verification and this traceably documented. With a view to removing trade barriers, the EU is pursuing a strategy of deregulation and liberalization following which responsibilities previously exercised by the state will, as far as possible and permissible, be transferred to the market. The extent to which the standard of technical safety will be affected by this calls for vigilant and thorough tracking so that timely countermeasures can be initiated if necessary.

The following may be cited as components of a target-oriented configuration management system:

- model specification (formal template for project definition),
- general specifications (definition for central departments such as project management, systems engineering, human factors engineering, technical safety, environment engineering/EMC,[3] environmental protection and immission control),
- project and process guidelines (project structure and organization, tasks and responsibilities of project management on all levels of the system structure, position and responsibilities of central project management and central departments),
- system, subsystem and component specifications (uniformly structured according to the model specification),
- commissioning instructions (local site management, procedure strategy),
- manufacturing, assembly, integration and testing specifications,
- general and individual instructions for trials, test operation and system demonstration,
- operation and maintenance instructions,
- rules relating to personnel qualification and certification and
- central documentation of official and other approvals and licences.

"Technical safety" is a cross-system quality attribute which even cuts across interfaces in the system between parts which are otherwise kept clearly separated. If competences and responsibilities for technical safety are to remain clearly discernible even in the case of complex systems, special care will be required with regard to interface management within the context of configuration management. In this regard, it is particularly important to ensure that the interaction of different legal

[3]EMC—electromagnetic compatibility.

persons is regulated clearly and unambiguously. Individual components may, however, be dispensed within the case of simpler technical facilities or systems, or the form taken by interactions may be given in less detail. However, in all cases it must be ensured that the competences and responsibilities for technical safety are clearly described and assigned and the technical safety aimed at is not limited by simplifications or omissions.

Every field of technology still has its own code of practice, and this results in a large number of different "safeties" in, for example, civil engineering, transportation, chemical engineering, power engineering, aeronautical engineering, plant engineering, mechanical engineering and electrical engineering. All six phases of the product life cycle (conception, definition, development and engineering, manufacture, operation and utilization, as well as dismantling, disposal and recycling) are determined by specific security concepts. Detailed constructional regulations, operating instructions, operating regulations and maintenance instructions are drawn up and conditions formulated for retrofitting for each of these fields of technology. Even the monitoring of operations by the owner (self-monitoring) and supervisory bodies (external monitoring) is regulated in an application-specific set of rules. However, this is by no means everywhere: there are also analytical methods relating to failure such as, for example, in the field of aerospace engineering, where developers, manufacturers and operators work closely with the supervisory authorities. At the moment, there is no single safety concept which has cross-application validity.

What is required is a "uniform safety"—in other words, a uniform concept and evaluation of safety and a uniform definition of safety.

The following analysis will show how the "hidden commonalities" in the individual safety philosophy can be worked out from the engineers' wealth of experience with safety issues. On the basis of this preparatory work, a uniform and interdisciplinarily applicable framework for a safety concept is feasible in which all fields of technology can find room. Interaction between these extremely diverse fields is facilitated in the same way as communication is with non-technical disciplines and the general public interested in technology.

4.2.2 Systematics

4.2.2.1 Insights into Safety Engineering

4.2.2.1.1 "Technical Safety" as a Quality Characteristic

"Technical safety" is a quality characteristic which, within the context of product design engineering activities, must be specifically generated, justified and verified (see Sect. 4.2). Technical safety can be neither "**decreed into**" (e.g., by laws or other legal regulations) nor "**tested into**" (a technical product). Technical safety can only be generated by being "**conceptualized into**", "**developed into**", "**engineered**

into" or "**built into**" the technical product in question (e.g., into a technical facility, system or component) during the course of product design and retained over the entire product life cycle. The same applies to the case of retrofitting or modernizing measures applied to technical products. Technical safety requires a functionally structured organization which has a centrally located system architect who controls a management hierarchy with clear assignment of authority and responsibility. Unlike other quality characteristics whose verification may be at the discretion of contractual parties, "technical safety" is the quality characteristic which always requires verification.

4.2.2.1.2 The Term "Risk" in Safety Engineering

Since the initial publication of the DIN 31004-1 safety standard (see Sect. 4.2), the term "safety" has been defined in a technical code of practice on the basis of the concept of "risk"—that is, of a probabilistic parameter. In this way, risk assessment as a probabilistic analysis of the stochastic failure modes of technical products is now regarded as generally accepted sound engineering practice.

In defining a safety concept, we should remind ourselves once again of the following basic ideas:

- Absolute safety in the sense of a zero risk cannot be demanded by legislation or regulations (risk prohibition) because it is not possible in principle.
- However, all possibilities should be explored with this point of view so that there is a well-balanced relationship between conceivable damage and the benefits created for the objects of legal protection (risk equivalence) with different technical products, processes, facilities and systems.
- The yardstick for the greatest still acceptable damage is determined by not only the scope of protection of the relevant objects of legal protection but also the intention to satisfy social needs (benefits), whereby this generally requires a trade-off within the social consensus (risk management).

4.2.2.1.3 Inherency and Losability of Attributes

The quality characteristic "technical safety" is achieved on the basis of very specific attributes of the product in question or generated in its design as a quality characteristic. The way in which a property is anchored in a product basically determines the captivity, presence under certain conditions or losability of this property.

"Inherent safety" is such a fundamental property of a product that it is founded in the internal design of the product and is thereby a captive property and, thus, inevitably present. The product in question is therefore, in principle, safe at all times since it necessarily falls back into a safe state as long as it is not actively brought out of this state into another. Without an explicit external supply of energy, the unsafe functions running in a system of this kind come to a standstill.

A system which was originally not inherently safe can be brought into a state of inherent safety by the addition of certain components or properties. For example, an exothermic process can be terminated and thus put into a safe state by the addition of a forced cooling feature. A distinction is to be drawn here between a passive operating component (forced cooling without active coolant feeding) and an actively operating component (the component does not operate unless energy is supplied).

It follows from this that the "losability" determines how the quality characteristic "technical safety" is to be designed. In this regard, the following aspects should be taken into consideration:

- Inherently captive natural attributes (or constitutional characteristics):
  - On the one hand, these are the passive functional and state-related properties of an assembly which are by their nature captive if they can—assuming utilization as intended—be traced back to characteristics which not only correspond to known laws of nature but are also constantly and uninterruptedly effective. They can be affected by neither other natural influences nor influences originating in the overall system in which this assembly is a part of. Proper operation must be designed from the outset so that possible deviations through negligent handling (such as failure to comply with obligations or omissions) do not lead to a safety-critical failure in the system. This situation is referred to as "natural integrity". These constitutional characteristics include, for example, the effect of gravity, radioactive decay, the earth's magnetic field and the speed of light.
  - On the other hand, these are also the passive functional and state-related properties of an assembly that are, due to their technical nature, captive when they can be traced back to characteristics which were verifiably taken as a basis for the technical design and which cannot change over the course of the intended service life. However, ageing processes, wear or other influences on the basic nature of the assembly must be taken into account in this matter. This situation is referred to as "technical integrity". The constitutional characteristics have, for example, holding and support functions, secure fasteners, forced guides, permanent magnets and guided, unbreakable compression springs as well as adequate creep and flashover distances from high-voltage equipment.
    The captive constitutional characteristics of an assembly can be retained without limitation of time provided regular compliance checks are carried out to ascertain how long this can be depended on or alternatively, maintenance is carried out to ensure that this condition continues without interruption.
- Inherently losable technical attributes:
  - These inherently losable attributes (or constitutional characteristics) can only be relied on for a limited time. Since properties are linked here to the corresponding object or facility, they are only dependable to a limited extent due to their inherent capacity, which can be made usable from the safety

point of view. In this case, we are concerned with expansion with passively operating components.
This situation is referred to as "technical inherency". These constitutional characteristics are, for example, typical of the following: storage capacity for cooling water, charging cycles of operationally reserved backup batteries, the kinetic energy (momentum) in vehicles which can be used for arrival braking (at a route stop or held in readiness in evacuation and rescue facilities), lubricant dispensers for central lubrication and grit containers for wheel-to-rail braking devices (to improve the braking effect).

- Although the inherent constitutional characteristics of a structural unit are in themselves subject to time limitation, they can still be retained as "inherent safety" without a time limitation provided that regular compliance checks are carried out to ascertain how long this can be depended on.

- Losable constitutional or functional characteristics:

  - These are the active functional properties of a structural unit and their losability—in other words, their functional failure. The function elements in question can be lost and, therefore, require safety precautions in order to secure technical safety. In this matter, actively operating components are used to deliver technical safety.
    This situation is due to:

    temporally random failure,
    environment-related failure or
    utilization-related failure possibly caused by unintentional operator error with the respective function elements.

  - In the case of failure, safety precautions (technical safety devices) can be applied to put the no longer safe function element into a different function which is safe and which, in turn, leads to a restriction or loss of the actual operational function (fail-safe). As examples of this prevention of the consequences of failure, we might mention here the initiating of an automatic train stop or disconnection of the electrical power supply (electric fuse).
  - Failures are deliberately reduced in incidence by limiting the probability of safety-critical failures or faults with application of reliability engineering. With the reliability engineering toolbox—for example, redundantly designed function elements or highly reliable components ("hi-rel" parts)—it is possible to maintain the utility function for longer than the corresponding operational utilization range. The utility function can even be limited to a period from the time a failure occurred to the, perhaps premature, conclusion of the current utilization period (fail-operational) with prolonged utilization ranges as application examples of this reliability-related limitation of failure probability. Manned and unmanned spaceflight technology or the twin-engine long-haul airliners can be referred to here.

4.2.2.1.4 Relationship Between Deterministic and Probabilistic

"Deterministic" and "probabilistic" are terms of Western epistemology and the philosophy of science. The basic assumption is that there is no absolute certainty in human knowledge, and the human is, rather, only capable of gaining knowledge with a greater or lesser degree of probability (with causally secured underlying reasoning when there is statistical significance in its occurrence). Empirical findings are therefore considered probabilistic when gained on a probabilistic or statistical basis. A difference must be drawn here between purely syntactic (flat) and semantic (deep) empirical knowledge.

The term "deterministic" means that if the current state and the effect which then follows are known, the subsequent state and what the system does in this subsequent state are unambiguous, predictable and repeatable. Monocausality means that only one effect underlies the moment initiating the change of state. Multi-causality means that state transitions are triggered by multiple equivalent effects.

The deterministic approach is based on the axiom that all events—including human actions—are caused by one or more initiating events, and in this context, the behaviour of a system is completely determined. The possibility has also been discussed that there is actually no such thing as free will in biological systems. Cognitive psychologists, however, see the result as arising from different mutually interacting processes on different levels of abstraction. The result in question can be predicted since the initiating cause either is known or has the character of a previous event. The more complex a system is (this concerns its internal network), the more massively interaction processes step into the foreground in comparison with the functions of the individual components. The more strongly the deterministic approach is closed off, the more dominant will be the stochastic (randomly determined) failure behaviour. Even in this case, however, the failure of technical facilities is still always conceivable, but the time and circumstances of the occurrence of failure can no longer be predicted—they are no longer deterministically determinable. Stochastic failure behaviour is no longer adequately manageable using the classic methods of deterministic precautions against failure (material selection, manufacturing tolerances, quality assurance).

Methods based on probability theory are collected under the term "probabilistic". In this respect, we have come a full circle: scientific knowledge is only to be gained with greater or lesser degrees of probability. The term "reliability engineering" refers to the application in engineering of the findings of probability theory in order to master the failure behaviour of technical equipment. Today, the full range of probabilistic applications in technology is very extensive. It ranges from loading assumptions to damage mechanisms, environmental influences, the response behaviour of structures and wear behaviour. Probabilistic approaches are always to be recommended when the details of the physical and technical situation can no longer be determined with the required accuracy and the uncertainty (scatter) of the parameter under consideration falls within the order of magnitude of precisely this parameter. In such cases, reasonable distributions of the scattering

variables are introduced in order to present the parameters in question in a usable form.

What "usable" means in connection with safety engineering is that, while possible failure modes are on the one hand imaginable, their parameter values cannot be unambiguously determined. On the other hand, a failure mode can itself be so complex that it is no longer possible to determine and understand its causes clearly. In this regard, reference can be made to the Monte Carlo simulation, a stochastic method whose basis is formed by the performance of a large number of random experiments. Using the results so obtained, an attempt is made with the aid of probability theory (in accordance with the "law of large numbers") to solve problems numerically which appear to be insoluble by analysis. These random experiments can be performed either for real or by generating random numbers, possibly with the aid of a computer. Innumerable computer programs for generating random numbers are available on the market nowadays, although of varying quality.

On the one hand, in the field of software (source code), for example, possible errors are all predetermined since they are present in the program. However, since the errors are not known, it is also not possible to predict failure behaviour. Utilization profiles are therefore used and a failure probability statement prepared on the basis of knowledge of previously detected faults. On the other hand, when creating execution plans for parallel or concurrent processes in real-time programming, deterministically guaranteeing the feasibility of execution is explicitly demonstrated by means of worst-case assumptions. The corresponding mathematical procedures are available for this and also applied.

The deterministic analysis of safety is based on a maximum effect in the case of a damaging event or a maximum influence in the case of a loading case (worst-case analysis). For this worst-case scenario, either the dimensioning of the structure is assessed (technical design) or the necessary safety measures determined.

Example 1: Gas tank and gas pipe—safety clearance larger than or equal to the effective range of the worst case.

Example 2: High-rise building—design covers not only static loads but also the dynamic effects of wind load.

Load application and resistance are stochastically distributed and taken into account with their upper and lower quantiles.

Example 3: Materials in which inter-crystalline dislocations shift in response to dynamic loading change in their extent and whose frequency distribution can vary discontinuously (e.g., gear shafts).

This can, where applicable, be countered by recrystallization processes deployed preventively (e.g., by heat treatment of steel components).

The deterministic analysis of structural processes is based on a macroscopic consideration of a variety of microscopic elementary processes within the material and the statistically significant and homogeneously occurring properties assumed as basic.

In the probabilistic analysis of safety, the focus is on the frequency with which a damaging event occurs (probability assumption) linked with the possible extent of damage. In this case, it is not the worst case which is considered, but rather

reference is made to the "maximum still acceptable risk" (consideration of the limiting risk). However, the greatest still acceptable risk cannot be defined absolutely here. It is rather a product of cultural, social, technical, economic and possibly insurance-related considerations. Appropriate measures are taken to reduce the risk actually determined to the point where it is deemed acceptable. In this case, those individuals involved must always be aware that measures taken to reduce a risk can generally induce other different kinds of risks which, for their part, lead to an increase in risk. When manipulating risks, it is, therefore, always important to assess the resultant risks as well in order to ascertain to what extent the sum of all original and resultant risks can be assessed as acceptable. Depending on the individual viewpoint, this assessment can, however, vary considerably.

Both the deterministic and the probabilistic approaches are recognized fundamentals of the engineering sciences, and each in part contains elements of the other's approach. As regards safety-engineering application, the approach taken will follow the previously expressed preference for "worst case" or "limiting risk". Once this preference has been selected, it must be rigorously adhered to—with mutual exclusion on the macroscopic level.

4.2.2.1.5 Monitoring as a Link Between Safety Technology and Technology Law

The state fulfils its citizens need for protection against technical risks by being responsible for public-technical safety. In meeting this regulatory obligation, the state makes use of the technical monitoring of particularly risky equipment or facilities. It is characteristic of current technology law that, although the state's regulatory law remains intact, a controlled unburdening of technical monitoring tasks has, however, taken place which the state itself would otherwise have to look after. These supervisory tasks have been transferred to independent auxiliary bodies for technical safety which are entrusted with the task of carrying out state-backed safety inspections (compliance checks). In the meantime, it has become common legal practice in many industrialized countries for the state to look after public-technical safety even in the field of technology. In this matter, the state always arrogates regulatory legislation to itself yet, at the same time, unburdens itself in a controlled manner of even technical monitoring duties.

The approval or licensing of technical facilities whose operation is in the public interest does, however, continue to be predominantly exercised by public authorities. In addition to the upper-most federal and state agencies, subsidiary authorities are also active in this regard, such as, for example, the Federal Railway Authority (EBA), the German Aviation Authority (LBA), the Federal Office for Radiation Protection (BfS), the Federal Physical Technical Institute (PTB, the German national testing authority) and the Federal Institute for Materials Research and Testing (BAM), when so provided by legal regulations.

4.2.2.1.6. Directives of the European Commission

With its New Approach and Global Approach guidelines, the European Commission has now in the meantime taken into consideration the needs of the public for safety in products. However, over and above the purely product-related directives in this catalogue of measures, the "Directive on General Product Safety" 2001/95/EG dated 03.12.2001 also applies. This requires all products being put on the market in the European Economic Area to be safe. Violations are also punishable. However, this directive leaves open the question as to how this "product safety" is to be generated and secured and is thus in conflict with the basic idea of organized safety engineering (see Sect. 4.2.2.1.1). Rather, this is left to the creators of the corresponding European standards which, as harmonized documents designated by the Commission, give rise to a presumption of conformity with the directive's basic requirements identified in the standards.

These EU directives also provide for safety verifications to be increasingly left to the free market and only monitored by the state. The expertise this requires in the field of technical safety, which has so far been attached to state-backed bodies, must now be made available to the free market. Up until now, Germany has actively and comprehensively participated in risk minimization by governmental agencies or bodies authorized by the state to carry out in their sovereign function safety verifications or participate in them (**implementation responsibility of the state**). The relevant EU directives increasingly provide for even these verifications—previously a responsibility of the state—to be left to the free market. In other words, they are now only monitored by the state: **pure guarantee responsibility of the state** (subsidiarity).

In this matter, a control function must be deployed which, on the basis of the total risk for which there is responsibility, finds a balance between the implementation responsibility and the guarantee responsibility of the state.

4.2.2.1.7 Importance to Safety Engineering of the Interdisciplinarily Consensual Procedure

Since every field of application today still has its own code of practice for technical safety, application-related constructional regulations, operating instructions, operating regulations, maintenance instructions and conditions for retrofitting are being developed which include operation. Even state monitoring by state supervisory agencies or bodies authorized by the state (such as federal institutes or the TÜV) is regulated in application-specific regulations, although by no means universally. Methods based on failure analysis are mostly in the fields of aerospace engineering or nuclear engineering. As already stated, there is not yet one safety concept which has cross-application validity—that is, with interdisciplinary validity.

It would already facilitate safety monitoring today for planners, developers, manufacturers, operators, regulatory bodies and other supervisory institutions and their experts if similar and identically worded contents in safety regulations were

standardized. Furthermore, the public—not only in the event of accidents or incidents—would show more understanding for a uniform safety philosophy than the current variety of standards. People would react more insightfully to an incident.

This challenge, for which there is no equivalent in the history of technology, presupposes that the fragmented concept of safety requirements specific to particular areas of application is being superseded. To this end, empirical practical knowledge in the field of technical safety must be methodically assembled and the existing body of regulations systematically codified.

For this purpose, the VDI "Technical Safety" Committee has developed this working platform for safety methodology and now offers it for interdisciplinary application.

4.2.2.1.8. Importance of Safety Verification

The manufacturers of technical equipment must pay special care to planning a well-organized, appropriate and systematic procedure in the generation of technical safety within the context of the state's predominant guarantee responsibility. This is so because conventional structures must be dispensed with in some cases and replaced by equivalents appropriate for the intended purpose. The approach presented with this guide to both technical safety and the body of suitable instruments for generating, preserving and assessing technical safety makes it possible as an interdisciplinary foundation not only to produce verifiably safe technical equipment but also to make a judgement of accidents and incidents with regard to both civil and criminal law. This applies in particular to technologically innovative equipment for which neither sufficient experience nor technical regulations (state of the art, standards, building codes, etc.) can exist.

4.2.2.2 Objective of Safety Engineering

Safety engineering must ensure a sufficient degree of safety. In the conceptual design of object-related safety engineering, care should be taken that safety-related design criteria do not end up in avoidable opposition to reliability-related design criteria which are essential in achieving the other objectives in relation to economic reliability.

In this context, the term "technical safety" is understood as meaning that a technical system, technical facility or product fulfils its intended functions over a planned period of time (as the case may be, its planned lifetime) and, provided it is operated or used as intended, does not injure or damage any objects of legal protection. This means that neither persons nor property is injured or damaged in as far as the system, technical facility or product can be responsible for this. Reliability of function over the envisaged lifetime is thus not a necessary component of safety if loss of function does not lead to an unsafe state.

Technical systems must be considered and analysed in their totality to design them appropriately for safety requirements. A methodical approach therefore requires total system analyses to be carried out first of all. The tools suitable for this are—depending on the problem and the formulated objective—so-called behavioural analyses (e.g., in the first instance FMECA, FMEA or HAZOP analyses[4]). A targeted approach to the generation of technical safety in a system calls for the identification and evaluation of the functional dependencies and interactions of its units, components and assemblies. This applies to not only its intended use but also the safety required during operation and in commissioning and decommissioning. Corresponding to the system structure (system breakdown structure), all structural units are then systematically selected for consideration and the safety-oriented interaction of the individual structural units[5] should also be covered in this process.

4.2.2.3 Purpose of a General Safety Specification

Uniform conditions can be created for all safety measures in development projects for complex systems with a general safety specification in order to be able to define the requirements necessary for a safety-compliant technical design.

This results in the necessity of organizing such general specifications on the basis of the following aspects:

- The **safety methodology** represents a systematic approach to and a suitable body of instruments for generating, preserving and assessing technical safety and includes a procedure by which the possibilities of faults, failures and disturbances are systematically analysed and recorded, assessed with respect to their impact on the safety of the system and made the basis for safety precautions.
  Safety methodology is a methodological framework for processing and solving all problems and requirements relating to safe technical systems. This also includes the procedure, question of recording requirements, documentation.

---

[4]Behavioural analyses form part of the set of instruments for safety engineering/reliability **engineering** with which innovative technologies have been helped in readiness for application for economic breakthrough for many decades now. Apart from their technological innovation, they have found less acceptance in Germany than in countries with a comparably high level of industrial development. Therefore, a reference is provided here regarding its international origins:

FMECA: American standard MIL-STD-1629A "Procedures for performing a failure mode, effect and criticality analysis", 24.11.1980

FMEA: technical standard—DGQ vol. 13-11:2012 "FMEA—failure mode and effects analysis"

HAZOP: British standard BS IEC 61882:2001-08-28 "Hazard and operability studies (HAZOP studies)—Application guide".

[5]In the present publication, the term "structural unit" is used as a generic term for all elements of a project structure plan (work breakdown structure). The topmost hierarchical level of the work breakdown structure is the "system" or the "product", and the "sub-systems" and the subordinate "structural units" then come under either of these.

- With the **safety concept**
  - Cross-system relationships are represented.
  - Assignment of the causes and effects of safety-critical failure possibilities is clarified (e.g., on the basis of a function tree).
  - The corresponding safety criteria are defined as requirements for the safety-related design of the system in question and include the corresponding interfaces.
- Assignment and definition of the corresponding safety requirements for the structural units of the system,
- Requirements applicable to verification relating to fulfilment of the safety requirements in regard to the approvability and operability of this system as a necessary condition of any construction or operating licence which may be required.

4.2.2.4 Area of Application of a General Safety Specification

The general "safety engineering" specification is used for a fundamental establishment of safety requirements and as a technical platform for preparing specifications for all structural units top-down—from the system down to the smallest function unit. A model specification is used in this work which lays down the editorial structure of the system and subordinate specifications[6] for development and construction.

At the same time, it serves as an action and decision-making framework for the execution of all safety-related work and the cooperation of all participating companies (in the sense of "juristic persons") with supervisory and licensing institutions. Furthermore, this general specification can be used as a work-related basis for the issuance, where applicable, of construction and operating approvals on the part of the competent supervisory and licensing institutions.[7]

The requirements laid down in the general "safety engineering" specification are to be incorporated without omissions into the specifications of the structural units concerned (or, if applicable, pure functional units). All safety requirements here—as determined in the model specification—must be recorded in the corresponding same section of the specification which is to be prepared. It is quite acceptable to include such requirements also in a different location in the specification if a higher-level connection needs to be made visible there. In such cases, however, the corresponding cross-references should be provided.

---

[6] "Subordinate specifications" are the specifications of the structural units coming under the (overall) system according to the predefined system structure (system breakdown structure).

[7] This could be a guideline for interaction between the system manager (general contractor) and supervisory institution for the purpose of obtaining a building permit or operating licence for the system concerned.

Application of this general specification is restricted to the working field, which includes not only the registration of failure possibilities, the determination of the corresponding impacts on the overall system, the safety-related design of this system and its structural units but also the corresponding verification. Within this context, the following types of causes of failure are to be taken into account:

- temporally random failures,
- environment-related failures within the boundary conditions to be expected under which structural units must function as specified[8] and
- utilization-related failures caused by unintentional operator errors (usability).[9] In this context, use for the purpose intended must be assumed. Improper use of technical equipment cannot be covered as far as technical safety is concerned (misuse and sabotage).

The correctly engineered design of all structural units (e.g., regarding natural and technical integrity) forms a part of the corresponding engineering work and is an indispensable condition of a safety-compliant design. The corresponding rules of good engineering practice are to be given in the specification applicable to each structural unit. A general reference to the state of the art or generally accepted sound engineering practice—as is justifiably customary in legal regulations—is not, however, sufficient on its own for a safety-compliant design of systems in general, particularly complex systems or innovative technologies.

The user of a general specification is requested to make proposals for amendments if a better solution is possible for a safety-compliant design and the economic reliability of the system in question.

Safety is to be incorporated as a subject in:

- basic and/or specific stipulations and requirements,
- procedural steps in phases for the entire life cycle (product life cycle),
- responsibilities and roles and
- documentation.

Note: A general specification is provided as an aid for the preparation of specifications for structural units or as an action and decision-making framework. It will not, however, be possible to achieve the objective of an appropriate safety-related design if a general specification of this kind is simply handed directly to subcontractors or suppliers. This is because they normally have neither the system knowledge required for a correct interpretation nor responsibility for the entire design and implementation process.

[8]This would be, for example, a general specification regarding environmental influences and test methods.

[9]Deliberate abuse is not covered by the defined safety-methodological procedure and would, where applicable, be subject to special agreements with regard to protective equipment.

4.3 Generating Safety

4.3.1 Safety Methodology

4.3.1.1 Overview of the Procedure

The procedure for generating safety includes the following points of emphasis:

- work breakdown structure with definition of responsibilities and accountabilities,
- preparation, release and implementation of a configuration management system which, in particular, covers the quality characteristic "technical safety",
- definition of the quality characteristic "technical safety" for each element of the work breakdown structure,
- inclusion of supervisory institutions (e.g., the competent supervisory authorities),
- preparation, reviewing and release of the general "technical safety" specification and
- inclusion of all entities involved (e.g., contractors and consultants).

A general "safety" specification must lay down uniform procedures by which all possibilities of failure are systematically registered and their impacts on the safety of the system evaluated in order to make them accessible for safety precautions. This means, in particular, that all loads acting from the outside and inside are evaluated with regard to advisable measures in order to be able to decide about passive and active precautions. Effects coming from the **original** and **object-influenced** environment are to be evaluated accordingly.

The schematic diagram (see Fig. 4.1) gives a general overview of the basic procedure for the necessary system work in safety engineering—especially with regard to public safety.

It should be noted at this point that safety verifications do not have unlimited time validity but rather require a periodic review (e.g., in the form of compliance checks). Wear, fatigue, ageing and maintenance measures affect the validity of the initial safety assessment, as shown above. Conversion or retrofitting measures (e.g., in the form of similar but not identical replacement parts) in all cases require the control loop for creating technical safety to be repeated. As with any other quality characteristic, technical safety is also subject to a process of decreasing reliability (dependability).

4.3.1.2 Requirements for Safety-Methodological Procedures

In what follows, the requirements are specified for a systematic procedure with which a safety-compliant technical design can be achieved for all technologies. These uniform provisions are to be applied to all safety-related activities. In the case

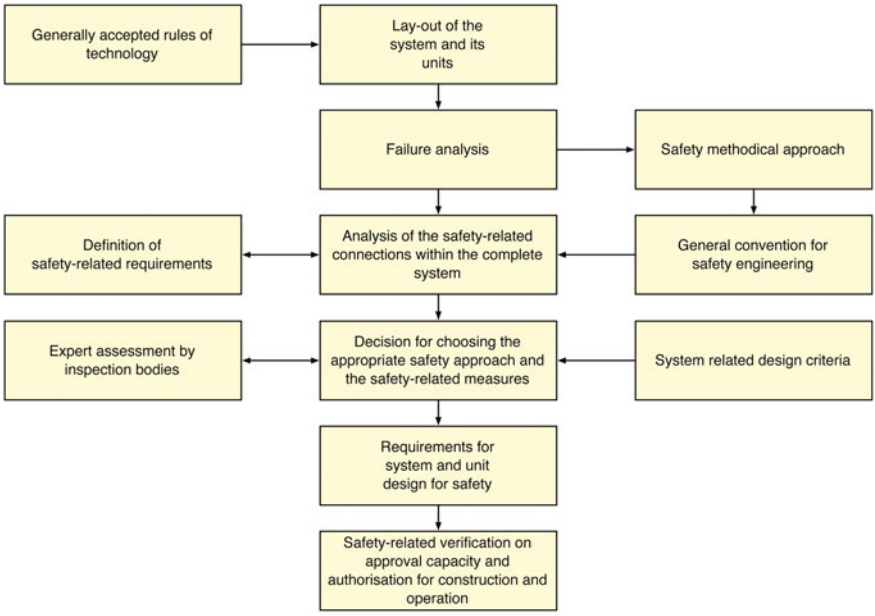

Fig. 4.1 Basic procedure for safety engineering

of new technologies, these provisions require a high level of detail, while for conventional technologies recourse can often be had to proven forms of structuring. However, should there be changes in conventional technologies, care should be taken that there is an adequate depth of detailing.

Note must always be taken of the fact that the quality characteristic of "technical safety" must be generated for every structural and function element (safety methodology). This also applies to the next higher system levels in every case.

- Safety definition:
  Requirements are to be gathered in a general "safety" specification which forms the basis for every single technical specification (product specifications, etc.).
- Safety engineering:
  The following applies to safety engineering:
  - Safety must be created for a product within the context of product design engineering.
  - Requirements relating to technical safety must be implemented in the manufacture of the product.
  - Safety requires the verification that safety has actually been established in the design and manufacture of the product.
  - The supplies and services of third parties must be included here.

- Safety management:
  Tried and tested management tools are available for this:
  - safety organization guided by "system architects",
  - critical items list (safety hazard list),
  - risk management (with the aid of a risk management list),
  - reporting (public safety) and
  - regularly scheduled safety reviews regarding conception, definition, development, construction and verification (technical qualification and technical acceptance).

4.3.1.2.1 General Agreements on Safety Engineering

Products (including technical systems) must be designed safety-compliantly such that they meet the current standard of public safety. In order to produce the corresponding current standard, conversion and retrofitting obligations must be incorporated in the legal framework, and this must include a risk-based balancing of protection of the status quo (grandfather rights). There is, however, no contradiction of this basic requirement when during testing of a system and/or its structural units—in accordance with the requirements of trial operation—safety is temporarily ensured by measures which do not apply to normal operation. In designing a technical system which complies with safety requirements, the following safety-related basic requirements must be satisfied and, thereby, their safety-related necessity demonstrated:

- A single failure of a function element must not cause or make possible a safety-critical failure in the overall system.
  In this connection, we may recall the constructive precautions in the sense of "fail-safe" and "fail-operational" (see Sect. 4.1.3.3.1).
  Redundant functions or function elements may be provided as a safety precaution thereby allowing the lost function to be taken over in the event of a failure. However, care should be taken that multiple failures of the same type (common mode failure) cannot occur as, in this case, even redundant function elements can fail spontaneously. To give an example: the shared supply of energy to redundant structural units (for example, when redundant cooling water pumps depend on one and the same electrical power supply).

Should a technical design meeting these criteria not be possible:

- concatenations of failures of the function elements of the various structural units—failure mechanisms such as spontaneous and/or multiple failures of the same type (common mode failure), causal chains and cascade effects—which could lead to a safety-critical failure within the overall system must be rendered discernible by active or passive operator checks.
  [Note: Consequences resulting in a failure which is of itself non-critical but which becomes a safety-critical failure event due to interaction with these consequences

must be investigated. Safety-engineering methodology thus requires every one of these individual failure modes to make itself visible or be made visible, although the individual failure mode is not, of itself, safety-critical.]

If a technical design which satisfies this requirement is not possible because, for example, this would impair dependability, the following will also apply:

- The probability of a multiple failure event (in other words, a simultaneous functional failure of different structural units) which could lead to a safety-critical failure within the overall system must not exceed a specific limiting value which is in each case related to the particular type of service.[10]
  The definition of such limiting values depends on the stochastic characteristics of the failure behaviour of the structural units concerned and the—specified—limiting value considered appropriate for the overall system.
  The limiting values defined in each case relate to the proper functioning of the function or structural unit concerned. Reducing the time base (e.g., due to early mission completion) or limiting the function results in the originally stipulated limiting value (of the probability of failure) retained does not contradict this fundamental safety requirement.
  In multi-processing or multitasking operation in real-time systems, overload effects sometimes occur to which the system does not react in good time. The cause is to be found in incorrect design or lack of proof of meeting worst-case requirements. This situation occurs randomly but can be deterministically detected and eliminated by using special methods.
  The definition of limiting values for the maximum permissible probability of failure must take into account the negative consequences to be expected in the case of failure (extent of damage). Since this parameter can depend very markedly on the spectrum of utilization (field of application of the system, such as, for example, the chemical industry, road transport, transportation of hazardous goods, shipping, energy conversion, structural steelwork), requirements valid for the particular service field must be applied. To this end, proper operation must be designed from the outset so that possible deviations due to negligent handling (such as failure to comply with obligations or omissions) do not lead to a safety-critical failure in the system.
  In this context, the term “fault tolerance” is readily used. This means “feed-forward” and “feedback” checks on safety and reliability. Since there is a lack of the requisite databases with sufficient statistical soundness, these methods work largely on the basis of expert opinions, so-called informed guesses. Thought should be given here to how such reporting systems are to be designed and implemented above and beyond the reporting obligation so as to obtain the maximum yield of the knowledge deemed to be necessary. This also calls for a reorientation of the error culture in Germany which culminates

[10]By “service” is here meant a utilization profile (function, course of time) which is to be defined in the system specification.

ultimately in communicating the first occurrence of an error and only taking action against its recurrence (legally). Only in this way is it to a certain extent possible to define "proper operation" so that it includes negligent and erroneous action taking place in the belief of it being action as intended.

A systematic and appropriate procedure for safety-compliant design assumes in addition that the following agreements are also taken into account in all safety-related activities:

- For the system and every structural unit, the "safe state" (fail-safe) or "safe functional behaviour" (fail-operational) must be clearly defined and recorded in the corresponding specifications.
- The transfer of the affected system into either an operating state defined as safe (e.g., an automatic train stop) or a function deemed safe (e.g., the emergency landing of an aircraft at a nearby airfield) is an example of this.
- The technical design should be such that, in the event of multiple failure, interactions in the failure mechanism which could lead to loss of function of a sub-system or the overall system are excluded.
- Limiting values for failure probabilities which are required for the respective structural units must be set such that fulfilling the safety requirements applicable to the overall system is not put into question.

As regards the time response of the failure rates concerning safety-critical failures, the requirements relating to service life ("useful life") as laid down in the specifications of the structural unit in question will apply.

4.3.1.2.2 Sequence in the Procedure for Safety-Compliant Design

For all safety-engineering activities—including the corresponding verification—the following sequence of methodologically appropriate measures applies with respect to conceivable hazards:

- Exclusion of safety-critical failure events (failure exclusion due to natural or technical integrity):
  These are deterministic actions against a single failure. The basis of the procedure here is the preparation of "safety-compliant design of technical facilities in the example of buildings and apparatus engineering installations" (see Sect. 4.4).
- Exclusion of the consequences of safety-critical failure events (exclusion of failure implications):
  The procedure to be applied here is classic safety engineering (as is known, e.g., from railway engineering).
- Limitation of the probability of safety-critical failure events and/or defects by application of reliability engineering:
  The procedural basis for this is the VDI manual on reliability [2] (see also VDI 4001 Part 1).

This sequence relates to the safety engineering work sequence and does not represent a ranking of these measures for a safety rating. Passive or system-inherent safety functions, which can be grouped under the term "inherent safety" (see Sect. 4.2.2.1.3), are always to be preferred before active safety functions. Safety-compliant design requires the exclusion from the outset of processes and actions which result in effects that are unmanageable and thus cannot be adequately limited. This is followed by the requirement of choosing from two alternative possible solutions the one which would produce a lower impact. In the same way, of two possible solutions the one should be chosen whose effects are better containable. Finally, the approach to a solution should be selected which comes closest to making reversibility (in the sense of controllability) of the effects possible. This procedure, which is defined through the sequence given above, assumes that the function elements of all structural units in the system are in a demonstrably fault-free and trouble-free state at the beginning of each utilization segment. Faults which can arise during not only the production process but also maintenance work must also be avoided or corrected by means of suitable precautionary measures.

4.3.1.2.3 Agreements About Demarcating Safety Engineering with Respect to Reliability Engineering

The qualification for licensing of a safety-compliantly designed overall system is based not only on its application maturity, which is characterized by an appropriate level of safety, but also on economic efficiency during practical application, which requires an adequate level of technical dependability and thus, possibly, of reliability as well. Since precautionary safety measures closely correlate with dependability, a meaningful mutual demarcation of their respective activities is required.

If it is assumed in this context that a technical facility should be designed to be only safety-compliant, the economic efficiency of its operation will remain questionable. In other words, if the objective of not only a safe but also a reliable or available overall system is not to be questioned, proposed precautionary safety measures should not be implemented until corresponding account has been taken of their effects on dependability. In this context, we might mention "commanded failure". One example of this is the automatic train stop initiated by the system following a safety-critical failure. Although this stop is defined as a "safe mode", it does, nevertheless, reduce the dependability of the system, which in turn restricts its economic usefulness. In this context, we are concerned with those cases in which there is not even any safety-critical failure but a monitoring device reports a safety-critical failure even though one as such has not occurred.

The deterministic analysis of safety is based on a maximum effect in the case of a damaging event or a maximum influence in the case of a loading case (worst-case analysis). In the probabilistic analysis of safety, the focus is on the frequency with which a damaging event occurs (probability assumption) linked with the possible extent of damage. In this matter, it is not the worst case which is considered but, while taking probabilities of failure into consideration, reference is rather made to the "maximum still acceptable risk" (consideration of the limiting risk).

A “pessimistic” analysis is one in which an attempt is made by costly efforts to exclude even the smallest risks. In an “optimistic” analysis, the emphasis is on excluding the really unacceptable risks.

In this context, “precautionary safety measures” are to be understood as all measures for controlling the development result which are to be applied to counter special cases of functional failure in structural units: these are failures which cannot themselves be excluded but which give rise to behaviour in the overall system that, under the given functional, environmental and utilization conditions can lead to injury to individuals and/or damage to property. A distinction should be drawn here between technical and operational precautionary measures on the one hand and preventive and corrective precautionary measures on the other. Priority should always be given to measures which can be taken preventively. With the aid of systems analysis methods (e.g., by means of timely failure analyses), corrective measures can be reduced to the unavoidable minimum. To reduce the possibility of human failure, which can never be entirely ruled out during the utilization phase, technical precautionary measures should be given priority in the safety-compliant design of systems and their structural units. The personnel operating the system should be instructed and trained to have cross-system understanding and thus be able to act as a possible “reserve” in the matter of system safety.

In a systematic approach, precautionary safety measures must, as regards the particular structural unit and its interplay with other structural units in the overall system, be selected and adjusted to each other so that the necessary safety verification is coherent. Furthermore, these measures should be so selected that they do not clash with the further goal of development—demonstrating with this technical facility the economically efficient utilization possible with the new technology implemented in it.

Observation of “good engineering practice” and legal regulations is a necessary but not sufficient condition for coherent proof of safety and dependability. Suitable conditions are rather to be created by which the overall context of possible failure causes and effects can be perceived and represented in a manageable form so as to allow them to be taken into account in the technical design. These conditions are created by the failure analyses[11] which are to be conducted as part of a project.

4.3.1.3 Practical Application

By using the global safety-methodological approach, we have presented that it is possible, in the interest of an increase in efficiency, to make it easier for the various technical disciplines not only to communicate among themselves but also interact on an interdisciplinary basis. The same applies to the collaboration of engineers, economists, legal experts and other technical laypersons, such as people working in the media. This has a beneficial effect in the case of technical innovation projects

[11]What is referred to here are the corresponding project arrangements, for example, in the form of a guideline about the performance of failure analyses.

and is conducive to an understanding of procedural concepts relating to safety. In this way, it is possible to prevent safety concerns from being thrust out of the engineer's field of awareness as soon as improvements or other changes are made to technical equipment, facilities or systems. In summary, it may be observed that application of the global safety-methodological approach as presented here means that all safety activities can be designed considerably more efficiently. Rescue routes, rescue facilities, shutdown devices, automatic train stop systems and the stability of structural units can all be designed more efficiently as regards safety compliance. The suitability of procedural concepts for fire and avalanche protection and occupational accident prevention can also be checked more efficiently.

The global safety-methodological approach presented here also takes into account the realization, first presented in DIN 31004-1:1982-11 (see Sect. 4.2), that absolute safety cannot exist, not even in technology. The Global Approach forms the "envelope", so to speak, which derives from the wealth of experience gathered over the history of technology. It covers a range extending from the failure-analysis approach of modern aerospace technology, methodologically appropriate solution principles and the application of design catalogues in modern construction methodology to the internationally established quality management system according to DIN EN ISO 9001 "Quality management systems" (2009). This methodological global safety approach exposes the hidden commonalities of classic safety procedural concepts (which are still entirely application-specific) that, when examined more closely, are only apparently different. On the basis of this understanding, both safety engineering and safety legislation must undergo a constantly advancing process of integration.

If the present-day quality of life when technical risks have been mastered and thus the personal safety of citizens is to be preserved in Germany and the EU, it must be ensured that sufficient creativity is available in industry. The economies of the EU cannot rely solely on the reduction of raw material reserves or trading in goods and money. Therefore, quality of life and personal safety can only be maintained in the long term if technologically creative forces remain effective in creating innovative systems, products and technical facilities whose usefulness must be guaranteed. In the creation of innovative technical products, this economic constraint makes it necessary to an ever greater extent to take objectives such as "safety" and "economic utility" also into account.

The approach described here also pursues the goal of how interdisciplinary interaction can be promoted in the field of safety engineering on the basis of an efficient global approach. It is also important to ascertain how the seemingly contradictory objectives of "safety" and economically reasonable "dependability" can be tackled as a holistic system concept. Only by means of an appropriate quality management[12] system, the creation of technical safety can be verified and traced.

[12]The term "quality management" used in this publication covers primarily the secondary field of "technical controlling", and this is the sense in which it has most recently been promulgated by politicians and journalists.

4.3.2 Implementation of the Safety Concept

The quality characteristic of "technical safety" usually includes—depending on the extent and complexity of the technical equipment in question—several relevant individual characteristics. Each of these individual characteristics must be generated during the design and manufacturing process of the technical equipment in question (product, technical facility, system). Technical safety must be demonstrated during the course of quality assurance measures and preserved by means of maintenance work. The safety concept thus created must be put into practice for the project design in this way:

- transfer of the systematically developed safety concept into project and system specifications,[13]
- safety requirements relating to the design of the system and its structural units or function elements,
- determination of the safety requirements which are subject to verification (public-technical safety),
- determination of the safety requirements on which obtaining operational approval depends and
- collection and evaluation throughout the entire product life cycle of all safety-critical failure modes occurring as "lessons learned" for "experience feedback".

4.3.2.1 Safety-Engineering Flow Chart

The conditions listed above have been coordinated systematically with each other in such a way that a procedure is established. This is uniformly applicable to not only the project, new technology thereby created and conventional technology employed but also the assessment by the competent supervisory body. A further general possibility of application would be for damage investigations of technical equipment.

A valid work and evaluation methodology is thus set up for the entire scope of a project, and it brings the indispensable safety-compliant design criteria for achieving approval into a quantitatively assessable relationship with those design

[13]The safety concept worked out within the context of the conceptual design and definition of a technical project corresponds to this early state of knowledge which is constantly expanded during the course of the project. The set of systemic instruments of configuration management ensures and will keep ensuring that all further findings emerging from the course of the project are systematically added to the rolling project definition and brought to the notice of those involved. This concerns, in particular, the quality attribute of "technical safety".

criteria that are important for the intended utilization and, thus, technical dependability.[14]

The procedural and decision-making methodology shown in Fig. 4.2 (flow chart) forms the appropriate working basis for developing and judging decisions regarding the adequacy of safety design features.

The procedural and decision-making methodology for creating safety in technical equipment is included in a legible resolution in this publication.

4.3.2.2 Explanatory Notes to the Flow Chart

4.3.2.2.1 General Structure

The individual elements of the flow chart are given a number as a cross-reference to the explanatory material. Due to this numbering, the various steps in taking action and making decisions can be demarcated from each other accordingly in both safety- and reliability-related works. For reasons of clarity, the elements of the flow chart are numbered in the form of a grid. The first numeral here indicates the nature of the step in question as follows:

1.*n*	Action and decision steps in which the causes and effects of failures are systematically determined in order that the necessary conditions are created for an effective execution of all safety activities
2.*n*	Safety-related action and decision steps in which, in the probabilistic approach, stochastic failure behaviour is dealt with
3.*n*	Safety-related decision steps in which, in the deterministic approach, failure behaviour that can be grasped in this form is dealt with
4.*n*	Action and decision steps which are necessary to be able to deal with the stochastically determinable effects on dependability of the safety-oriented technical precautionary measures provided
5.*n*	Safety-related action and decision steps which are necessary to be able to establish the deterministically ascertainable effects on dependability of the safety-oriented technical or operational precautionary measures provided
6.*n*… 11.*n*	Assessment of the chosen technical design with respect to its safety-compliant design and its impact on dependability

[14]It has become established in some fields of technology that technical safety is only obtained when, in the event of a safety-critical disturbance, the system concerned is put into a, by definition, "safe state". This "safe state" is often equated with a switching-off (to be commanded) of the actual utility function. Switching off the intended utility function does, however, impair the **dependability** which is essential for the practical application.

Dependability is also the measure of the ratio of the actual usability and the technically possible (intended) usability.

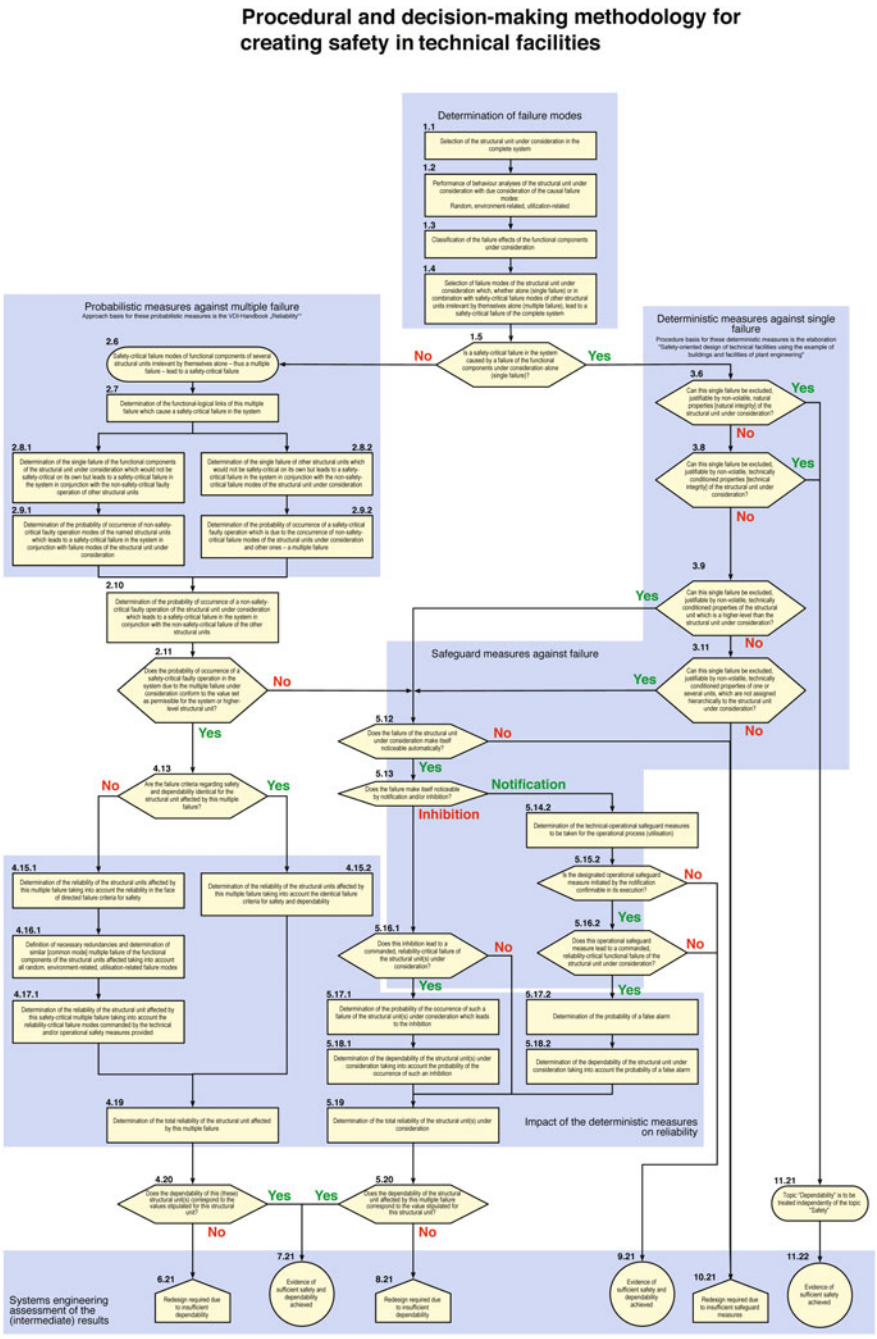

Fig. 4.2 Procedural and decision-making methodology (flow chart)

4.3.2.2.2 Using the Flow Chart for the Technical Design of Products

Firstly, a procedure should always be preferred which is oriented towards deterministically ascertainable relationships in order to achieve a safety-compliant technical design (keyword: "fail-safe"):

- A safety-compliant design and its assessment can be carried out without the additional effort required to capture and deal with stochastic failure behaviour.
- The advantage of the deterministic approach comes into play in particular when changes in the technical design become necessary.
- It is usually assumed that deterministic approaches tend to make it possible to keep costs within a manageable framework in safety-compliant design. This advantage—in many cases only a supposed one—is opposed by the fact that consequential costs will arise which could otherwise have been avoided with such short-sighted considerations of safety.

Note: The deterministic approach is based on the influence of stochastic phenomena being practically negligible (continuity view).

Application of probabilistic approaches for safety-compliant technical design (keyword: "fail-operational") does, however, expand the possibilities for providing proof of safety. Nevertheless, this approach should only be provided for cases where a deterministically justifiable safety-compliant design is not possible, whereby the following should be noted:

- Proof that the selected technical design ensures adequate safety is usually combined with greater effort.
- Reliability engineering, which is to be applied for probabilistic approaches, recognizes the following distinctions with regard to quantitative information:
  - the true behavioural parameters,
  - the forecast estimated parameter value and
  - the observed parameter.

The "**true behaviour parameter**" is not known until utilization is completed at final decommissioning and is, therefore, not suitable as a criterion for decisions about the technical design or its assessment.

The "**forecast estimated parameter value**", on the other hand, is an entirely usable criterion by which a decision can be made about the technical design. It is only suitable as an assessment criterion when—as is the case in space travel in particular—here is agreement between the system director and supervisory institution regarding the informativeness of the failure rates of structural units and elements used for reliability analyses.

Therefore, the adequacy of a safety design may be judged solely on the basis of the actual "**observed parameters**". The effort required for demonstrating an appropriate level of safety (mentioned at the beginning) results from the fact that the low failure probability permissible in this context can only be confirmed by statistical and, therefore, relatively lengthy, extensive and often quite costly qualification testing.

The parameters referred to in this context are stochastic in nature and therefore can only be quantitatively determined by using statistical methods. Thus, parameters derived from actually observed parameters by applying generally accepted statistical calculation methods are just as suitable for proof of safety as the actually observed parameters themselves. This does, however, depend on there being a sufficient level of statistical confidence.

What this means for the practical implementation of proofs of safety is that "observed parameters", statistically sound "forecast estimated parameter values" and, on this basis, "extrapolated estimated parameter values" are to be regarded as of equal importance.

Independently of the safety analyses explained here, which should be used for the technical design, even reliability analyses are of course based on the stochastic failure behaviour of these technical devices.

4.3.2.2.3 Explanations of the Technical Steps in Creating Technical Safety

Before the flow chart can also be used for assessing the individual technical design steps, detailed explanations of the individual activity and decision steps are necessary. They are listed below in numerical order.

Action Step 1.1

Preconditions for all safety-related activities are that the failure behaviour of all function elements of the structural unit under consideration is fully and correctly captured and presented in a clear and unequivocal form.

For this to be possible, both the function elements of this structural unit and its functional behaviour (according to the function tree) must be deterministically captured. The following VDI standards may be referred to here:

- VDI 2221 "Systematic approach to the development and design of technical systems and products",
- VDI 2222 Part 1 "Design methodology—methodical development of solution principles" and
- VDI 2223 "Systematic embodiment design of technical products"

in order to determine the function structure (function tree) with main functions, subordinate sub-functions and the corresponding function elements.

In order to cover stochastic failure behaviour as well, interactions with the structural units involved in the function (failure mechanisms) must be captured in the same way and presented in an unambiguous form.

Action Step 1.2

Performance of failure analyses[15] is the decisive action step in systematically capturing both failure possibilities and their causes and effects. The effectiveness of each subsequent action step crucially depends on the care with which these analyses are carried out, especially with regard to the elimination of possible causes of failure and the selection of suitable precautionary measures. In view of the importance attached to carrying out failure analyses for safety-related activities, such work should be performed according to a standard model and uniform criteria. This, in turn, is a precondition for the results of the individual analyses being directly comparable without further ado and—if necessary—always transparent. In this way, the situation is finally created in which even cross-system aspects can be fully captured and made accessible to all safety-related activities.

For the function elements determined with the aid of the previously mentioned function structure, their failure behaviour is analysed by assigning each of these function elements—where applicable—to one of the following possible failure modes:

- As regards the structure of the analysed function element:
  - untimely function structure,
  - unqualified function structure and
  - missing function structure.
- As regards maintaining the function element concerned:
  - degraded function and
  - lost function.
- As regards termination of this function element:
  - unqualified function termination.

The following categories of possible failure causes must be systematically taken into account here:

- temporally random failure of the structural unit concerned,
- environment-related failure of the particular function elements of the selected structural unit

[15]Failure analyses of this kind are also known under the terms

- "Failure and fault effect analyses" (FFEA),
- "Defect mode and effect analyses" (DMEA),
- "Failure mode, effect and criticality analyses" (FMECA),
- "Event tree analyses" DIN 25419) and
- "Fault tree analyses" (DIN 25424).

[It should be taken into account here that environmental influences can not only cause a failure in a deterministically transparent manner (e.g., failure occurring immediately after a lightning strike) but also lead to a higher probability of failure (failure rate) which can only be captured by a probabilistic approach (as would be the case, e.g., as a consequence of solar irradiation).] and

- utilization-related failure caused by unintentional operator error.

In order to make it possible to capture stochastic failure behaviour, the generalizing assumption is usually made that the causes of failure are independent of each other. Consequently, the safety-compliant design in particular must ensure that unwanted interactions or so-called cascade effects are prevented (see also Action Step 2.6). Notwithstanding this, it must be taken into account when capturing stochastic failure behaviour that even under this condition there can still be dependencies. This could be the case if the causes lay outside the technical equipment being designed—in other words, were due to jointly acting environmental conditions.

The independence of multiple failures is often assumed but it must be made (at least) plausible, for example, by reference to spatial or operational redundancy, diversity and similar factual contexts. If this is not possible, so-called common mode or "common-cause" failures should be considered.

Action Step 1.3

A whole series of proven analytical tools are available for carrying out this action step with which the following aspects can be systematically captured and assessed on a safety-methodological basis:

- complete definition of the failure mode,
- causing failures in higher-level functions,
- conceivable effect of failure chains (cascade effects),
- failures "delivered" to the function element under consideration,
- failures triggered by the function element under consideration,
- careful and clear distinction between failure mode, cause of failure and failure effect for each individual function element,
- the function tree represents the "scaffolding" for the derived fault tree
  [Note: The fault tree is independent and only to be drawn up on the basis of the function tree of the system and its components. In other words, project plans must already exist into which the results of the first FMECAs have been incorporated and which may have led to changes in the original system structure. The completed fault tree can then be compared with the original function tree for the purpose of locating any inconsistencies. The fault tree is a model of the logic structure of the relationships between possible faults. Furthermore, it is an interaction model of the possible faults and, ultimately, an algorithm for

determining the so-called minimal cut sets of events which can lead to various failure states of the system.
Not until the basic elements of the fault tree have been substantiated by probability values can a quantitative analysis be considered. Whether an event tree to which the corresponding fault trees are to be attached should be put first is a question to be clarified in the individual case.] and

- evaluation of the criticality of the effect for every individual failure mode of a function element:
  - safety-critical effect (basis for the conceptual design of safety functions and failure tolerance—keyword: "fail-safe") and
  - safety- and reliability-critical effects (keyword: "fail-operational").

The failure possibilities collected are to be classified as follows on the basis of their impact on the overall system:

Effect of the failure mode	Classification of the failure mode	Criteria for classification
Supercritical fault	Class A	Immediate danger since the behaviour unleashed by the failure cannot be controlled with the prescribed means
Critical fault	Class B	Hazard which may result in injury to persons or damage to property if the behaviour triggered by the failure is not made controllable by suitable precautionary measures
Major fault	Class C	Utilization is considerably restricted or entirely prevented
Minor fault	Class D	Utilization is impaired only slightly or not at all
Incidental fault	No failure	Negligible deviation without affecting functional behaviour

In this context, the following activity and decision principles apply:

- Class A failures are not permissible according to safety methodology. They must be prevented by a suitable structural design which complies with "generally accepted sound engineering practice" (keywords: natural and technical integrity).
- Class B failures must be combated by technical and/or operational precautionary methods in accordance with safety methodology. Class B failures are to be taken into consideration in safety engineering, may be identical to a Class C failures and usually make repair work necessary.
- A Class C failure is present when, due to this, the envisaged or specified utilization profile cannot be maintained. Class C failures are to be taken into consideration in reliability engineering, can contribute to a Class B safety-critical multiple failure and make repair work necessary.

- A Class D failure is present when, despite this failure, the utilization profile can still be maintained. Class D failures can contribute to a Class B safety-critical multiple failure and make repair work necessary.

Action Step 1.4

It is recommended for deterministic approaches that initially only the Class B single failure is to be taken into account within the context of safety activities.

As regards probabilistic approaches, the Class B single failure initially no longer needs to be taken into account in the context of the safety-methodological procedure. However, all those Class C and Class D failures must be taken into account which could result in a Class B safety-critical multiple failure. Even a Class B safety-critical single failure is to be taken into consideration only in cases where stochastic failure behaviour in interaction with facilities for precautionary safety measures, so-called safety-engineering or operational safety measures, is also to be captured.

Class C failures should be taken into consideration for reliability work. Where Class B safety-critical failures also impact reliability and thus dependability (keyword: "commanded failures"), they should also be regarded as Class C failures. This is then always the case when, upon a Class B safety-critical failure occurring, the safety-engineering equipment provided causes a Class C major fault (e.g., by shutting down or inhibiting operation).

Decision Step 1.5

In contrast to the single failure, multiple failure often involves more complex and not immediately comprehensible failure mechanisms. The failure mechanism in question must first be rendered transparent by capturing, without omissions, the interaction of all cases of single failure involved in the safety-critical multiple failure.

Note: For the sake of clarity, it is necessary to define reasonable boundaries as regards completeness by which the cases of single failure involved in the safety-critical multiple failure can be captured. It is essential to coordinate these demarcations with the competent supervisory institutions (public safety/legal approval).

Action Step 2.6

The following safety-methodological principles must be observed in connection with the treatment of a multiple failure:

- Every single failure is deterministically predictable, so its effect can also be determined deterministically in advance (determinable). Although the time when a failure occurs is always random, in other words stochastic, this has no relevance to the selection of suitable safety technology since this selection is also based on deterministic points of view.
- According to the general agreement on safety engineering, a single failure must not cause or make possible any safety-critical failure (Sect. 4.3.1.2.1). It follows

necessarily from this that a safety-critical multiple failure can result only from cases of single failure which are not of themselves safety-critical. It follows from this in turn that not only the time at which a multiple failure occurs is stochastic but also the occurrence of the multiple failure itself. This is why a multiple failure can be properly captured in its full extent in the final analysis only by a probabilistic approach.

- Although probabilistic approaches do require a certain mathematical systematics, for pragmatic reasons it may be necessary to make simplifying abstractions.
  Cases of single failure which are involved in the interaction with a multiple failure must, as regards their occurrence, be independent of each other. This independence is present when there are neither technical (function logic) nor operational (operationally necessary) links (logic operations). However, in this regard independence also means that no shared causes of failure are to be expected (see also Action Step 1.2). With the sequential occurrence of cases of a single failure which are mutually independent, even the (quasi-) "simultaneous" occurrence of multiple cases of single failure is covered as a borderline case.
  Consequential failure is to be treated in safety methodology in the same way as a single failure, namely in a holistic consideration with the initiating failure as cause.
- A multiple failure is to be expected when the technical design of the affected structural unit(s) has at least one of the following function-logic or operational link characteristics:[16]

  – Deterministically detectable links

    Conjunctive link
    A deterministically detectable link exists when technical functions and operational activities substitute for each other. This is usually achieved by function-logic and/or operational redundancy.
    Note: Redundancy is a measure in reliability engineering by which a reduction in failure probability is always achieved. However, a redundant arrangement will not ensure appropriate safety unless it can be demonstrated that the failure probability thereby achieved remains within permissible limits (see also Decision Step 2.11).
    Inclusive-disjunctive link
    A link of this kind, which is also deterministically detectable, is present when technical features and/or operational activities that are not provided as a redundancy are complementary to the envisaged overall function. In this case, it is to be assumed that failure of a sub-function will always entail a failure of the overall function. This type of link is present, for example, in devices whose function depends on energy supplies.

[16]The definitions given in DIN 25419-1 are used here. However, not every possible switching logic link is also usable for safety-related considerations, such as an "exclusive disjunctive link".

Negation link
This type of a deterministically detectable link exists when technical capabilities are mutually interlocked fully or partially. A failure of the overall function will only occur when the function of the mutual interlock fails. One example of this kind of link is the mutual interlocking of the electrical service brake and mechanical backup brake of a maglev train vehicle, which is provided to ensure that impermissible brake-related force effects on the vehicle are prevented. (Simultaneous operation of both braking systems would necessarily result in unacceptable overstressing of the track.)

– Stochastic manifestations

Complex meshing of functions
These are links which, due to their complexity, can no longer be properly and fully captured by a deterministic approach alone.
The modes of operation of integrated switching circuits come under this form of manifestation just as dynamic alternating functions do in automatically running open- and closed-loop control processes.
Note: Unlike deterministically detectable links, such complex functional meshings (Markov chains and Markov processes) are not suitable for the way in which a function tree is presented.
The failure behaviour of complex meshings of functions can only be fully captured by a probabilistic approach. The following abstraction is permissible within the context of this approach:
It must be ensured by a design of the structural unit in question which is suitable from the reliability engineering point of view that, with the functional and/or state features provided (which are taken as input parameters), the expected output parameter is present with sufficient probability at the predetermined time and specified location. It is not necessary here to consider the functional processes in the structural unit itself.
Within the context of safety engineering, an abstraction of this kind does, however, require additional function-logic plausibility analyses with regard to the interaction of mutually independent input parameters and the corresponding output parameters depending on them (e.g., non-equivalence, majority "decision").

Action Step 2.7

- Deterministically detectable links
  The form of representation showing a function tree with all relevant failure modes (following DIN 25424) is recommended as an aid in determining and presenting functional logic and operational links. In this matter, a sub-representation of the higher-level function tree must clearly show as a result of

which link the failure modes (not in themselves safety-critical) of function elements of the structural units concerned will lead to a safety-critical failure in the overall system.

- **Stochastic forms of manifestation**
  The type of representation suitable here is the state diagrams which have proved their usefulness in reliability engineering (see, e.g., VDI 4008 Part 5 "State flow graphs").

Action Steps 2.8.1 and 2.8.2

The interaction of the structural units involved in the safety-critical multiple failure is obtained from, on the one hand, the fault tree and, on the other, the state diagrams (see also Action Step 2.7). However, it must be ensured by a systematic (as a rule, formalized) flow of information that the failure mechanism in question is also fully and unequivocally captured when responsibility for the structural units concerned extends over different, legally mutually independent areas.

Note: The difficulties here are normally to be found not so much in the factual capture of the failure behaviour as in the willingness with which the necessary information is supplied in a comprehensive form that is comprehensible at all times. Both the capture and the evaluation of the required information about failure behaviour can be systematized with a **general specification for the performance of failure analyses**.

Action Steps 2.9.1 and 2.9.2

Before the probability of such a multiple failure occurring can be determined, the corresponding organizational conditions must be created for this action step as well. These are used for systematically determining failure probabilities for not only the structural unit under consideration (Action Step 2.9.1) but also the other structural units involved in the multiple failure (Action Step 2.9.2). The corresponding agreements on standardizing procedures while paying due regard to responsibilities can be regulated in a general specification: **general specification for the work fields "reliability" and "dependability"**.

Action Step 2.10

The probability values obtained in Action Steps 2.9.1 and 2.9.2 should first be made accessible to the field of responsibility for the structural unit in which the safety-critical effect of the multiple failure in question manifests itself.

This action step cannot on its own offer any guarantee that the failure mechanism concerned is fully captured or that any further possibilities of multiple failure are detected. Therefore, a central responsible body (contact point, and focal point) is essential where all relevant information converges.

Details of cooperation with a central contact point of this kind can be defined in a **general specification for the work areas "reliability" and "dependability"**.

Decision Step 2.11

In accordance with the measures for the standardization of project execution,[17] safety-engineering requirements must be stipulated in the specifications for each structural unit. Should the structural unit be expected to experience a safety-critical multiple failure, a limiting value for the failure probability should be indicated here and the corresponding failure modes listed.

This limiting value should be selected such that its fulfilment means a level of safety is guaranteed which is reasonable in an evaluative comparison with systems already generally accepted by the public. Provided compliance with a limiting value of this kind can be demonstrated for the technical design of the structural unit concerned, additional safety engineering can be dispensed with.

However, this will usually not be possible. If a case arises in which the probability of a safety-critical multiple failure exceeds the permissible limiting value of acceptability (risk assessment), it will be essential, even with regard to probabilistic procedures, to provide additional safety technology which is also appropriate from the cross-system point of view. At least, the consequences of a multiple failure of this kind are to be controlled by suitable precautionary measures (e.g., by shortening the duration of the specified utilization profile). The factual condition for this is that each case of single failure, although of itself not safety-critical, manifests itself early enough.

Note: If additional safety equipment is provided, more technical functional- or operational-action elements will necessarily be involved in a multiple failure of this kind than with the technical design originally envisaged. Consequently, it will be necessary to start again at Action Step 2.7 with the additional safety equipment included. This recursive process should be repeated until the transition from Decision Step 2.11 to Decision Step 4.13 is objectively justified.

original multiple failure
+
failure of the safety equipment
=
expanded multiple failure

Decision Step 3.6

The state-related and functional properties of a structural unit will, by their nature, be captive if they—provided they are used as intended—can be traced back to characteristics which not only correspond to known laws of nature but are also constantly and uninterruptedly effective. These properties cannot be affected by either other natural influences or influences originating in the overall system of which this structural unit is a part. This situation is referred to as **natural integrity**.

[17]In this context, please refer to the following management tool: the model specification.

Such characteristics include, for example, the effect of gravity, radioactive decay, the earth's magnetic field and the speed of light.

Decision Step 3.8

The state-related and functional properties of a structural unit will, by their nature, be captive if they can be traced back to characteristics which were verifiably taken as a basis for the technical design and which cannot change over the course of the intended service life.

A prerequisite for the admissibility of the corresponding verification is, however, that, on the one hand, the constructive design complies with generally accepted sound engineering practice. On the other hand, proof must be provided and documented that the execution of work actually corresponds to the intended constructive design (quality assurance and inspection). This situation is referred to as **technical integrity**.

Examples of these characteristics are found in holding and support functions, standardized shrink fittings, secure fasteners, forced guides, permanent magnets, guided, unbreakable compression springs and adequate creep and flashover distances from high-voltage equipment.

The special aspects of the "technical integrity" situation, which is to be considered deterministically, are presented in more depth in this guideline to "technical safety" (in this regard, see Sect. 4.4).

Decision Step 3.9

If the constructive design of the structural unit concerned does not permit the exclusion of a safety-critical failure, precautionary safety measures should be taken to tackle the hazardous consequences of this failure in an appropriate manner. In order to keep the effort involved within limits, it is advisable to investigate first the extent to which relevant safety equipment can be incorporated directly into the structural unit immediately superior in the hierarchy. A failure consequences exclusion will then be conclusively justified on grounds of natural and/or technical integrity when, despite a conceivable failure, a "safe state" is preserved as defined in the specification of the relevant higher-level structural unit (which is not the structural unit under consideration) or when "safe behaviour", also defined there, remains guaranteed.

However, a failure consequences exclusion which is justified by the function of a safety device will only be permissible when a failure exclusion or, if applicable, further failure consequences exclusion[18] is justified for the safety-engineering equipment itself.[19]

[18]Although entirely permissible from the methodological point of view, a further exclusion of the consequences of failure should, if at all possible, be avoided in order to maintain the clarity of the function elements of the structural unit in question.

[19]If this is not possible technically or objectively, the proof of safety may need to be provided with the aid of probabilistic approaches, such as, for example, the introduction of redundancies.

Decision Step 3.11

If the decision described under Decision Step 3.9 is not possible—that is, incorporating the safety-engineering equipment directly into the structural unit immediately superior in the hierarchy—the corresponding safety-engineering equipment can also be incorporated into a different and hierarchically non-assignable structural unit.

As a result of this measure, the corresponding interfaces must be defined as well.

A failure consequences exclusion will then be conclusively justified when, despite a conceivable failure, a "safe state" is preserved which arises as a result of reference to Action Step 2.6. This is to be defined in the specification of the structural unit concerned (which is not the structural unit under consideration). The aim here is for a defined "safe behaviour" to remain guaranteed in the system.

$$\begin{gathered}\text{original single failure}\\ +\\ \text{failure of the safety equipment}\\ =\\ \text{multiple failure (reference to Step 2.6)}\end{gathered}$$

Decision Step 4.13

The following failure modes are to be taken into account within the context of this decision:

- failure which, although of itself reliability-critical, is, however, involved in a safety-critical multiple failure,
- failure which, although of itself safety-critical, is, however, reliability-critical in effect as a result of the safety equipment provided and
- other reliability-critical failures of the structural units in question which need not be affected by the field of activity of safety engineering.

Safety-critical single failures which have no effect on reliability are not taken into consideration in this context.

Action Step 4.15.1

Where reliability-critical failures are commanded[20] for the structural unit concerned as a result of precautionary safety measures, the probability of their occurrence should be determined here (see Action Step 2.10).

However, the effort then involved in dealing with possible multiple failures should be taken into account (see Sect. 4.3.1.2.1).

[20]Definition based on DIN 25424-1.

Action Step 4.15.2

The value of the function-related failure probability of the structural units concerned as obtained in Action Step 2.10 should be accepted here.

Action Step 4.16.1

In this action step, any redundancies which may be required are specified. At the same time, the possible common mode multiple failure of the structural units concerned is determined while taking into account all random (spontaneously failing), environment-related and utilization-related failure modes.

Possible examples might be "overvoltage" as a cause of spontaneous (but otherwise random) failure, "lightning strike" as a cause of environment-related failure and "operator error" as a cause of utilization-related failure.

Action Step 4.17.1

In this action step, the degree of reliability is determined in which commanded reliability-critical failure is taken into account. All further reliability-critical failures of the structural unit affected by the multiple failure under consideration which do not have a direct relation to the safety-engineering equipment are also to be included here.

Action Step 4.18

The usual procedure in reliability engineering is applied as part of this action step to determine the overall reliability of that structural unit which, due to its hierarchical classification in the system structure, is affected by the multiple failure under consideration.[21]

Decision Step 4.20

In accordance with the measures for the standardization of project execution,[22] requirements relating to dependability and, where applicable, reliability are to be laid down in the specification for each structural unit on the basis of a centrally managed apportionment. The minimum limiting values for dependability and reliability should be given and the corresponding failure modes listed individually at this point.

The corresponding limiting value should be selected so that compliance with it means a degree of economic dependability is assured which is competitive in comparison with other proven systems.

Decision Step 5.12

Under certain circumstances, Decision Steps 2.11, 3.9 and 3.11 could lead to safety-engineering equipment having to be provided and used in order to obtain a

[21]As a working basis, see the VDI handbook on reliability VDI–Handbuch 'Zuverlässigkeit (VDI 4001 ff.) [2].

[22]In this context, please refer to the following management tool: the model specification..

safety-compliant technical design. Safety equipment of this kind cannot usually be a component part of the structural unit under consideration. In such cases, it will be necessary to apply the same safety-methodological procedure to this safety equipment as well. If a failure of this safety equipment cannot, for its part, be excluded (see Decision Steps 3.6 and 3.8), this failure, which in itself is already a safety-critical single failure of not only the structural unit under consideration but also the equipment provided by safety engineering, should be classified as a safety-critical multiple failure (see Action Steps 2.8.2 and 2.9.2). This applies even if other safety equipment is to be provided (see also the assessment according to Preliminary Result 8.21).

Decision Step 5.13

The general requirement for an appropriate level of safety assumes that there is a corresponding safety-compliant technical design in accordance with Action Steps 2.*n* and 3.*n*. This demand does, however, make it equally necessary for failures which lead to deviations from the safety-compliant target state to be made detectable in a timely fashion so that the technical and/or operational precautionary measures provided for this situation can become appropriately effective. This is crucial if deviations from the "safe state" or "safe behaviour" are to be countered at all times.

In this regard, there are deviations from the safety-compliant target state under the following conditions:

- With failure consequences exclusion (see Decision Steps 3.9 and 3.11):
  - Every function-related failure of the structural unit itself is always to be classified as safety-critical without taking into account any safety equipment which may be provided and
  - Every failure of the safety equipment provided which renders it ineffective is also to be classified as a safety-critical failure.
- With limitation of the probability of failure (see Decision Step 2.11):
  - Every function-related failure of the structural unit under consideration which is involved in a safety-critical multiple failure must automatically make itself visible. The presentation of the corresponding displays is to be assigned—appropriately and in compliance with human factors requirements—to not only the technical precautionary measures becoming effective in each case but also the operational precautionary measures to be taken.

To ensure that the consequences of a safety-critical failure really can be excluded, care should be taken in the technical design of the structural unit(s) concerned so that an adequate response time is left for the technical and/or operational safety measures provided. Only then can these precautionary measures take effect. For the treatment of safety-critical multiple failures by reliability engineering methods, account must also be taken of the response times which must be available to any safety measures provided depending on the failure mode.

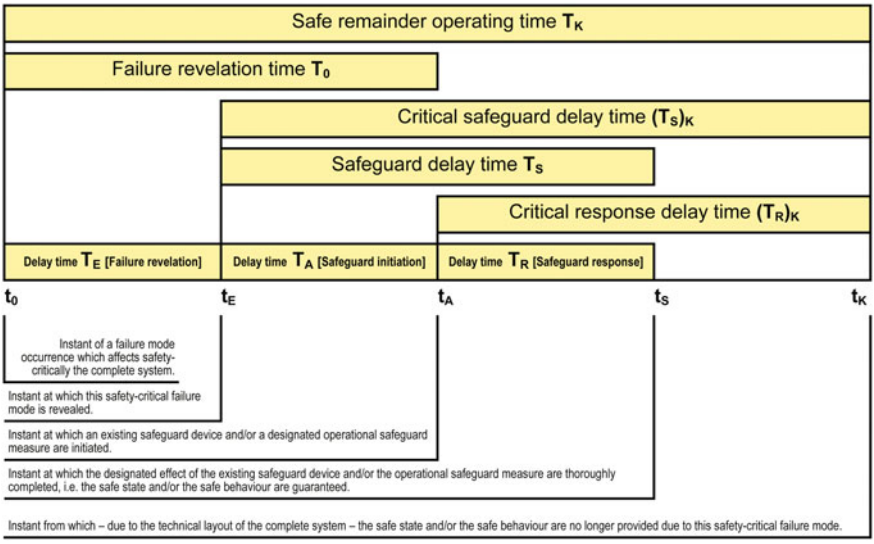

Fig. 4.3 Time context

The foregoing considerations indicate that even after the onset of a failure a period of time normally remains before the behaviour in the overall system becomes, with the means available, no longer controllable for countering injury to individuals and/or damage to property. The following decision depends on this "safe residual operating time" and the time-related possibilities for failure detection and (system) safety: whether inhibition of the (system) function is necessary or a failure (or fault) message (malfunction indication) will suffice for the appropriate operational safety measures to be initiated. Figure 4.3 shows the corresponding time relationships.

An envisaged safety measure is not suitable unless the total time span required for fault detection, tripping of a safety device and the safety response is shorter than or at least equal to the "safe residual operating time". This can also be taken to mean, for example, the amount of time which corresponds to the available braking distance in a braking operation.

The decision whether an immediate inhibition of function should be initiated or a message to initiate the appropriate operational measures suffices depends on the ratio between the safety delay time t_S and the critical safety delay time $(t_S)_K$. Should this ratio, taking into account the statistical confidence interval, take a value ≥ 1, the envisaged safety measure is regarded as unsuitable as such.

The following classification of safety measures applies in general to higher-level operations:

- Initiation of an immediate inhibition:
  - immediately initiated stopping of a function at a non-predetermined place making use of the normal operational equipment (e.g., electrical emergency brake in the case of a rail vehicle),
  - immediately initiated stopping of a function at a non-predetermined place making use of operational auxiliary equipment (e.g., mechanical emergency brakes in the case of a rail vehicle) and
  - continuation of the function with the earliest possible destination-related stopping of the function at a place provided for this purpose, irrespective of the permissible or possible operational state (e.g., driving speed in the case of a rail vehicle).
- Initiation of an operational stop or closing down the function:
  - Continuation of the function until the current operating cycle[23] has finished with a destination-related stop at the place provided for this purpose (e.g., a scheduled stop at a station in the case of a rail vehicle).
  - Continuation of the function until the current operating cycle has finished, with a destination-related stop at the place provided for this purpose and followed by the system being put into a maintenance cycle (e.g., a proper but unscheduled shutdown in the case of a rail vehicle).
  - Continuation of the function until conclusion of the envisaged mission cycle with a reduction of function to the necessary level followed by the system being put into a maintenance cycle (e.g., in the case of a rail vehicle, a proper but scheduled shutdown).

On the basis of this classification, suitable technical and/or operational safety measures are to be selected for the technical design of the structural unit concerned with a view to getting the ratio $t_S/(t_S)_K$ as close as possible to the limiting value of 1. This is a design criterion which not only ensures an adequate level of safety but also helps to prevent a disproportionate impairment of the reliability of the overall system.

Action Step 5.14.2

Unlike the immediate initiation of a function or operation inhibition, the influence of operational safety measures on reliability is often not readily apparent. Safety-critical fault messages (malfunction indications) are often routinely used as a way to take systems out of operation by means of operational safety measures. This creates a state corresponding to one with regard to reliability engineering which also arises following a technical failure (a technical disturbance).

[23]These cycles should be defined in the project or system specification.

In terms of effective reliability work, it is, however, essential to also take into consideration reliability-critical states commanded by operational safety measures. Nevertheless, a comprehensive knowledge of all operational safety measures is required in order to be able to determine those measures which have reliability-critical effects.

Signalling devices should be provided as technical safety equipment so that operational safety measures can be initiated.

Decision Step 5.15.2

Since operational safety measures are executed by individuals, the possibility of a safety-critical state arising due to erroneous execution cannot be excluded. Since human dependability or reliability still has its limits, even after comprehensive training, acknowledgement messages are essential to make even operational safety measures conclusive in themselves. The technical acknowledgement device required for this is a logical component of the signalling equipment provided.

Decision Step 5.16.1

This decision-making step should cover those technical safety features with which reliability-critical failure in the overall system is commanded. These failures should be attributed to the structural unit under consideration in every case.

It should be taken into account in this regard that the safety device provided to initiate inhibition can, as a self-contained structural unit, also fail. The safety-methodological flow chart should also be used for processing failures of this structural unit.

Decision Step 5.16.2

This decision-making step should cover those operational safety measures with which reliability-critical states in the overall system are commanded. These function-related failures should be attributed to the structural unit under consideration in every case.

It should be taken into account in this regard that the signalling and acknowledgement device provided for this as a technical safety device can, as a self-contained structural unit, also fail. In the same way, the operational safety measure provided in every case can be executed incorrectly. The safety-methodological flow chart should also be used for processing failures of the signalling and acknowledgement device.

Action Step 5.17.1

In this action step, the probability should be determined of the occurrence of a safety-critical failure of the structural unit under consideration which, due to the technical safety device provided, commands a reliability-critical failure in the overall system.

Action Step 5.17.2

In this action step, the probability should be determined of the occurrence of a safety-critical failure of the structural unit under consideration which, due to the

operational safety measure provided, commands a reliability-critical failure in the overall system.

Action Step 5.18.1

As part of this action step, the usual procedure in reliability engineering is applied to determine the dependability or reliability of the structural unit concerned. Those failures of the structural unit which, due to the operational safety device provided, command reliability-critical failures in the overall system are also to be included here.

Action Step 5.18.2

As part of this action step, the usual procedure in reliability engineering is applied to determine the dependability or reliability of the structural unit concerned. Those function-related failures of the structural unit under consideration which, due to the operational safety means provided, necessarily lead to a reliability-critical state in the overall system are also included here.

Action Step 5.19

In accordance with the measures for the standardization of project execution[24] requirements, requirements relating to dependability or reliability must be stipulated in the specifications for each structural unit. At this point, the minimum limiting values for dependability and reliability (apportionment) should be given and the corresponding failure modes listed individually.

Decision Step 5.20

This limiting value should be selected so that compliance with it means a degree of economic dependability is assured which is competitive in comparison with other, in some cases proven, traffic systems.

The inclusion of reliability-critical failures commanded by safety-critical failures of the structural unit in question supplies a comprehensive assessment standard for the reliability-compliant design of the structural unit under consideration. The advantage of this approach is that the causes of failures will always remain assigned to the structural unit in which these failures arise, no matter what impact they have on the overall system.

Preliminary Result 6.21

If the required dependability cannot be demonstrated for the structural unit concerned, it should be assumed that the result so far achieved is not suitable for the intended purpose. The technical design selected must be revised with regard to its reliability. It goes without saying that the failure behaviour of the resulting technical design of the structural unit concerned will need to be re-examined.

[24]In this context, please refer to the following management tool: the model specification..

Result 7.21

This result indicates that proof has been furnished that the requirements relating to technical safety and dependability which were specified for the structural unit concerned have been satisfied. To what extent this result is ultimately usable for the overall project depends on the following conditions:

- The experts of the supervisory authority (public safety) confirm from a holistic perspective the consistency of the safety verification for the entire system.
- The objective of usability of the overall system from the economic point of view is attained by the corresponding adequate dependability of the overall system being demonstrated.

The security-critical failure modes covered by this result are put together with the systematically developed safety precautions as "lessons learned" for experience feedback.

Preliminary Result 8.21

This preliminary result shows:

- An adequate level of safety for the overall system cannot be achieved unless an additional structural unit is provided as a technical safety device. It goes without saying that the failure behaviour of even this part of the overall system will need to be investigated.
- Notwithstanding this, the design objective has been reached for the structural unit under consideration. A corresponding statement regarding the overall system is not, however, possible until not only the failure behaviour of the technical safety devices provided but also the effects on the overall system of the control operations intended have been investigated.
- If the required dependability cannot be demonstrated for the structural unit concerned, it should be assumed that the result so far achieved is not suitable for the intended purpose. The technical design selected must be revised with regard to its reliability. It goes without saying that the failure behaviour of the resulting technical design of the structural unit concerned will need to be re-examined.
- The structural unit under consideration does not have a safety-compliant design and requires revising from the safety point of view. It goes without saying that the failure behaviour of the resulting technical design of the structural unit concerned will need to be re-examined.

Result 9.21

This result indicates that proof has been furnished that the requirements relating to technical safety and dependability which were specified for the structural unit concerned have been satisfied. To what extent this result is ultimately usable for the overall project depends on the following conditions:

- The experts of the supervisory authority (public safety) confirm from a holistic perspective the consistency of the safety verification for the entire system.
- Reliability is not affected by this.

The security-critical failure modes covered by this result are put together with the systematically developed safety precautions as "lessons learned" for experience feedback.

Preliminary Result 10.21

The provisional result shows that an adequate level of safety for the overall system cannot be achieved unless an additional structural unit is provided as a technical signalling and acknowledgement device with which the corresponding control operations are initiated. It goes without saying that not only the failure behaviour of this signalling and acknowledgement device but also the effects of the control operations on the overall system must be investigated.

Note 11.21

Proof of an adequate level of safety has been provided but there is no impact on reliability work, which, when necessary, must be carried out independently of safety-engineering activities.

Result 11.22

This result indicates that proof has been provided that the requirements relating to technical safety which were specified for the structural unit concerned have been satisfied. This structural unit is, as regards its safety design, unreservedly suitable for the intended purpose (see also Note 11.21).

4.3.3 Software-Based Functionality and Human Factors

4.3.3.1 Software and Safety

Modern technology and systems have now come to have a significant proportion of software-based functions. Therefore, software is becoming more and more important in technical safety and must be treated like a product.

The safety of software can only be achieved by design and organizational measures. This means that the production of software must also be planned in a similar way as regards procedure, project management and the methods and processes used.

Reliability is the foundation of technical safety in software. Furthermore, technical safety requires that, in the event of a breakdown, a safe state can be achieved through a gradual reduction of function. Redundancy mechanisms, such as both diversitary redundant hardware and software, can be used for this. In addition, an integrative analysis of safety and security aspects is necessary. The latter concerns, in particular, open and networked systems such as, for example, critical infrastructures in the field of automation.

Security problems, such as tampering with data and programs, have a very basic impact on technical safety. Changes in programs or data due to data or memory

fields being overwritten can disable safety mechanisms and create danger to life and limb. The programming languages used must therefore have properties which support technical safety.

Implementation can be affected either by automatic code generation (model-driven architecture) or manually by an individual. Essential is a programming language which supports reliability and security, is fully defined semantically and syntactically, comprehensively supports implementation of the software model in all aspects and also avoids or detects errors. This calls for strict typification, checking for index areas or range infringements such as division by zero with exception triggering, syntactic bracketing for readable structures and an error distance (Hamming distance) in the grammar which detects typos and cannot classify as syntactically correct. Writing errors must not result in any syntactically correct code, and in this regard, at least two or more errors must occur. Programming languages must be designed not only to avoid errors but also prevent malfunctioning even at run-time (exception triggering). Ada is an example of a programming language which meets these requirements.

In this case, the program structure must remain algorithmically controllable and, accordingly, have a low level of complexity in its structure. Cyclomatic complexity is a measure of this. Values above ten indicate algorithmic structures which are no longer comprehensible or testable. Furthermore, operating systems or run-time systems must be designed such that errors can be detected and appropriately responded to in the program.

Fault tolerance mechanisms for increasing reliability, such as diversitary software, can for reasons of security be used simultaneously for both analysing the overall behaviour of a function and making comparisons at inspection points in order to detect data tampering.

Open systems should interact with external software without feedback at the interface so that external attempts at inward tampering are prevented. For example, dummy components which do not perform any specific action can be used here solely for checking inputs. In addition, both identities for the sources and destinations of information flows and encryption of transport routes should be provided.

A clear and mentally manageable function design should be implemented so that the complexity of software-based functions can be grasped mentally. Intelligent behaviour must be both predictable via interpretative algorithms and dependable (deterministically in the exact context). This applies, in particular, to the combination of complex functions, such as assistant systems in the modern car.

Examples of inadequate technical safety include a “certified” infusion pump implemented in C/C+ with 200,000 source lines of code (kLOC) and safety-critical requirements which, following several incidents, was taken off the market. A subsequent statistical analysis revealed an error rate of 127/200 kLOC, whereby in 29 cases a type conversion changed the value of variables and in 28 cases an empty pointer was dereferenced. In 36 cases, variables were used without prior initialization. This all occurred with a safety-critical medical device which had been successfully certified. Based on this, the demand necessarily follows for a programming language such as Ada, which through its syntactic structure and semantic

definition strongly supports the programming of highly reliable software systems. In the case of a certain automobile manufacturer´s vehicles, there were problems with the anti-lock braking system due to a faulty software update and also problems arising from an incorrect interpretation of steering signals and a subsequent blocking of steering. In cars of the model years 2008–2012 from another manufacturer, a software error could result in operation of the belt tensioners or the side airbags being delayed or not initiated at all. A defence system onboard an aircraft had a conversion error in time measurement which became larger the longer the system was working. The defence system thus missed an attacking rocket, and as a result, several people were killed. In an electric vehicle of the latest generation, a software error caused the headlights and tail lights not to switch on while the daytime running lights were not activated automatically when driving from dark into light conditions.

In software-based systems, safety as a two-sided property (operational reliability and information security) is vital. The opening of previously closed technical systems in the safety-critical field, combined with the problem of faulty and unreliable software, requires a stringent review of all safety aspects. SCADA systems (SCADA stands for supervisory control and data acquisition) for monitoring and controlling critical infrastructures above the regulatory level are increasingly becoming a target for IT attacks. A pumping system used as a lure provoked 39 attacks in 28 days, with 12 attacks targeted, 13 repeated on several days and the first attack occurring after just 18 h.

Automobiles can also be tampered with via vehicular communication systems. As experiments have shown, the engine controller for braking and acceleration can be controlled remotely by text messages with the driver being unable to intervene.

This shows that the technical safety of software-based functions requires an early integrative examination of software-based functions, and in the case of “open” systems, even IT security should be considered analogously with its significant implications for technical safety.

4.3.3.2 Human Factors

As was described in Sect. 3.2.2.3, analyses of serious events indicate that extreme importance is attached even to the control potential of human activity in reducing the adverse or even devastating consequences of accidents. The domain of “human factors” (HF) is becoming an ever more intrusive complex of problems which require specific answers. As such, the human contribution to the safety and reliability of socio-technical systems has a high relative importance.

Incidents and accidents in recent years have made one thing ever clearer in quite a few fields: the possible beneficial effect of additional improvements in technical system components in highly complex systems with a high hazard potential is constantly decreasing despite decades of improvements. Connected with this fact is how the relative importance of human actions in initiating accidents and incidents is on the increase. However, it would be an unacceptable simplification to focus every

time solely on the operator acting directly at the human–machine interface. It follows logically from the principle of deeply hierarchized system protection, which is indeed always implemented in technically complex systems, that an individual single failure must not lead to a serious incident or accident—various technical or organizational barriers should prevent this. Only where weaknesses are dormant and unrecognized in the system and an unfortunate constellation of "adverse" conditions occurs (often of a random nature) can an incident or accident path be opened up and be due to an individual single failure at the human–machine interface (HMI). This will, however, result in events rated as negative.

The so-called phase approach (see Sect. 2.1.2) makes it possible to take the entire product life cycle of technical equipment into consideration, even in detail. The product life cycle extends from conception, definition, development and engineering to manufacture, operation and utilization and, finally, to dismantling, including disposal and recycling. In all phases of this chain, human activity makes a significant contribution to the (lack of) reliability and (lack of) safety of technical systems. In other words, it is important to take the corresponding quality assurance into account in all phases of the life cycle of a product or service.

By "human factors", we therefore mean all those factors over the entire product life cycle which affect individuals in their interaction with a technical system or are affected by individuals. To that extent, the thoughtless and frequently encountered synonymous use of "human factors" and "human error" or even "human failure" is impermissible, as is the traditional restriction of the ergonomic aspect of the HMI. Organizational factors, division of labour, prior management decisions and even inter-organizational relations are relevant here in terms of a comprehensive, holistic understanding of "human factors".

The human contribution to the reliability and safety of socio-technical systems is made under general conditions which provide indispensable potential and unalterable limitations alike. Both must be taken into account in the design of the system since "man with his natural abilities and disabilities must take centre stage of all systems built up by men for men" (the Declaration of Saarbrücken on the occasion of the World Congress on the Safety of Modern Technical Systems, Saarbrücken, 2001). This ability basically makes the human superior to the machine—his/her ability to learn compensates for his/her susceptibility to error and is an important component in safety-oriented action.

Mistaken actions are defined as the failure to achieve the goal of an action. It would therefore be a contradiction in terms to assume that someone could deliberately make a mistake. Whether a mistake was made or not can therefore only be determined with hindsight and following clarification of the possibility of a "correct" purposeful action. Seen in this way, the very common kneejerk reaction of assigning blame ("human failure") for a mistake contradicts the "human right of error" which safety researchers call for. A reasonable error culture regards a mistake as a learning opportunity and does not ask "How could you have done such a thing?" but rather "How could this have come about?".

Mistaken actions arise for a variety of reasons, especially from an overtaxed mental capacity for processing information, unreasonable requirements for

attentiveness, monotonous work, inherent or learnt behaviour patterns (inappropriate for the tasks on hand) and limitations in knowledge. All of these are possibly stresses and strains which exceed the human capacity for action. In the interest of preventing injury to people and the environment, system design should take into account both natural human potential and human limitations. This can be achieved, for example, by fault-tolerant engineering and design.

The automation of socio-technical systems has particular significance here. From an engineering point of view, it often seeks a maximum level of automation in order to exclude as far as possible the "error-prone" human. In actual fact, the more complex systems become, the more necessary the human contribution is. Bainbridge speaks here of the "ironies of automation" (in [5]). In the first place, the developer of a system is, as a rule, an individual who is also susceptible to making mistakes and can thus have a negative effect on the engineered system since, by following a strategy of maximum automation, he/she leaves the operator only with tasks which cannot yet be automated. The result is something which psychologists have called "learned helplessness": the lack of use of motor or cognitive skills becomes a problem when an unforeseen event occurs and new behaviour is required of the inexperienced operator. In a similar way, the proven human weakness of an inability to remain attentive for long periods has a negative effect on the purely supervisory function remaining to the operator following comprehensive automation of a technical facility.

Furthermore, complex situations requiring a decision can become a problem. Provided all necessary elements of a decision in the production process can be specified, an automated, computer-aided decision can be taken faster and more multidimensionally than an operator decision. However, the operator may be left alone with judging the result of a decision on a meta-level whose algorithm he/she does not, or only insufficiently, understands. Automation may thus mask system failure and evade carrying out correct diagnosis and rectification. What is therefore required is not maximum but rather appropriate automation which grants the individual room to exercise his/her learning and functional abilities and thereby create optimally engineered safety functions.

All in all, three models can be distinguished of how HFE experts can be included in the process of designing and engineering complex socio-technical installations. These models are applied differently depending on the need in question:

(a) Integrated model
Here the HFE expert (work scientist, psychologist, medical scientist) is integrated from the outset in the design team so as to participate in the design of work places and the functions of personnel working there with regard to safety and reliability, occupational safety, health aspects and humane design.

(b) Intermittent participation model
Here the HFE expert is consulted in critical design phases such as, for example, to evaluate a prototype. In this way, experienced operators (pilots, control desk staff, etc.) can be brought in.

(c) Post hoc participation model
Only in rare cases are all design flaws detected before the system goes into operation. Technical or organizational barriers then have to be installed to prevent dysfunctional use of the system or hazardous system states. Under no circumstances, however, should post hoc involvement of HFE experts be misinterpreted as a standard form of participation in the sense of a repair workshop.

If an event cannot be controlled within the system and system limits are exceeded, steps must be implemented to deal with the interface. In this case too, the knowledge available in HFE must be deployed in order to incorporate unconditionally the HFE elements into emergency management planning too.

- Participatory integration of the future user:

The mental manageability of a system is a further basic necessity for safe use of the system. HFE must therefore include future users in conception and design work to point out weaknesses undetected early on and make the system behaviour accessible to the user. A deep understanding should be imparted by simulative operation. According to Dörner, years of dealing with complex systems are necessary before a mental model develops in the individual. Only this model allows also a targeted and correctly handled operation under critical situations. Conceptually speaking, three human–machine relationships can be distinguished:

– The machine dominates, and the competence of the individual is regarded pessimistically. Interlock systems prevent human intervention but all possible exceptional situations must be manageable in this case.
– The human dominates and can cancel any interlock and take over control. Such an approach demands a high level of mental competence of individuals—something which cannot always be assumed.
– The human and machine are cooperative partners. The possibility of intervention is granted depending on the need. This approach includes the two concepts above.

4.3.4 Supportive Management

4.3.4.1 General Outline

In regard to the quality characteristic “technical safety”, it is more important than with any other quality characteristic that planning, implementation and verification are fully and at all times traceably documented. Safety cannot be created and preserved unless all individual aspects of the quality characteristic “technical safety” are guaranteed at all times. Every individual aspect of the quality characteristic “technical safety”, which must be created and produced for a technical

object (product, technical facility, system), must therefore be both verified during the course of quality assurance measures and preserved during the course of maintenance work. This calls for special care and caution in the context of a proper management system. The procedures required are listed below:

- project management,
- configuration management and project definition (with project structuring and specification),
- reliability engineering,
- environmental engineering,
- manufacture and testing,
- quality management,
- verification,
- an appropriate complaints and non-conformities system,
- maintenance and
- safe operation.

In addition, it must remain assured during operation and utilization that no (operational) actions take place which run contrary to the technical safety achieved in the course of the creation process. This applies to not only the technical safety designed with inherent or passive measures but also to technical safety based on active measures. For this purpose, it is necessary to create safety rules:

- creation and pursuance of maintenance rules and
- operating rules.

These management measures are presented below as general requirements. Let it be emphasized that these management measures are necessary for controlling the quality characteristic "technical safety". The main criteria and principles are addressed in the present guideline. Reference should be made to the relevant specialist literature for a deeper treatment adequate for an appropriate application.

The demand for technical safety (just like safety in general) necessarily means the proper application of appropriate management practices and use of appropriate work resources, methods and procedures. These have long proven themselves in the various fields of technology but are still not used with blanket coverage. Their application and use are, however, essential when it is a question of safety being created, produced and verified methodically, correctly, systematically and without deviations during the design of a technical object. The following list should be regarded as a checklist that helps to determine which of the management procedures are necessary from the safety point of view. In each case, (not only are) the organizational responsibilities shown of the purchaser and contractor but also the corresponding appropriate work resources, methods and procedures.

As with every other characteristic, the quality characteristic "technical safety"—or simply "safety"—cannot be "tested into" a technical object. Characteristics are features of any technical object which, during the course of the entire design process (conception, development, execution of works), must be created systematically for this object. However, standardization bodies also offer so-called design

standards which include requirements relevant to safety among other design requirements. Examples of this are electrical products in compliance with Protection Class II (VDE 0100-410, -412.1). These have a reinforced or double insulation between the power supply circuit and the metal (and thus conductive) housing and do not then need to be connected to the PE conductor. In the case of products designed and built in accordance with such safety-relevant design standards, it will suffice for the proof of safety that their design complies with the standard in question. In this case too, it would be incorrect to assume that safety has been "tested into" the product. An inspection of this kind only ascertains that the actual design of the product complies with the applicable (design) standard. It is the applicable standard which prescribes how the product is to be designed so that it may be regarded as "safe". An inspection of this kind (compliance check) only affirms that the design rules in the standard and pertinent inspections have been satisfied.

In the sections which follow, the requirements, responsibilities and methods will be indicated in each case. The following rules and procedures must be complied with here:

- Safety-related stipulations for the individual management procedures must always be incorporated in good time in the product life cycle no later than the start of the phase in question and are applicable to a part or all of the product life cycle.
- Corrective work is essential in the event of checks finding gaps.
- All requirements must always be written down in a readily understandable form.
- The necessary proof that the design, constructive execution and operation, manufacture and testing of a technical object are safety-compliant can thus only be secured when the management conditions listed above have been met. The same applies to both safety-compliant reliability and dependability and environmental engineering and resistance to environmental influences. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.

4.3.4.2 Management Procedures in the Planning Process

4.3.4.2.1 Safety-Related Project Management

- With regard to the management of—and included in—technical safety, the following aspects must be put in place:
  - written definition of responsibilities, technical competences and powers for project management at the system level,
  - checking that the legal and contractual provisions are consistent in themselves and all technical and safety requirements are included in an

unequivocal form (including establishment of the natural or even juristic persons responsible for the project management with regard to technical, scheduling and cost-related responsibilities),
- organization of project planning and tracking with definition of project milestones and the nature and scope of the project-related verification—always including the proof of safety and
- obtaining confirmation that the purchaser and supervisory institutions can be included in project planning and tracking in the event of gaps, imperative requirement for rectification.

- Definition of organizational responsibilities:
  - written definition of responsibilities, technical competences and powers on the part of purchasers and contractors,
  - appointment of competent persons and binding assignment of the respective job descriptions,
  - creation of a single project structure for the technical object in question (product, technical facility, system) and definition of personnel responsibilities for each structural unit in the project structure,
  - explicit and legally binding definition of responsibility for "technical safety" in the relevant job descriptions and
  - contractually agreed or legal definition of the monitoring responsibility for technical safety (such as that of the competent supervisory institution).

- Work resources, methods and procedures to be used:
  - stipulation of the safety-methodological procedures in a "technical safety" general specification drawn up for this purpose,
  - creation of a **model specification** to serve as a template for every structural unit which contains the explicit requirements relating to the quality characteristic "technical safety",
  - contractualization of the **cooperation of purchaser and contractor** with possible supervisory institutions,
  - unequivocal definition of accountable responsibility for safety inspections on the part of purchaser, contractor and possible supervisory institutions,
  - checking that the specifications of structural units identified according to the project structure (the technical object under consideration) contain clearly understandable requirements which are in factual agreement with the general "technical safety" specification and
  - checking that the specifications of structural units identified according to the project structure (the technical object under consideration) contain clearly understandable requirements regarding safety verifiability which are in factual agreement with the general "technical safety" specification in the event of gaps, imperative requirement for rectification.

4.3.4.2.2 Safety-Related Configuration Management

- Creation of the necessary conditions for configuration management in general:
  - definition of responsibilities, technical competences and powers for configuration management at the system and structural unit level,
  - appointment of the competent natural or even juristic persons for configuration management,
  - checking that the system specification is coherent and all technical and safety requirements of the contract are included in an unequivocal form and
  - checking that the purchaser and supervisory institutions are included in the information flow of configuration management in the event of gaps, imperative requirement for rectification.

With regard to the configuration management of—and included in—technical safety, the following aspects must be put in place:

- Definition of the organizational responsibilities in the company:
  - definition of responsibilities, technical competences and powers for the document release procedure (such as specifications),
  - definition of responsibilities, technical competences and powers for change management (in connection with documents),
  - definition of timing and contents regarding regular notification or full interrogation of the configuration status (with the aid of a product-specific configuration status list) and
  - project-related definition of personnel responsibility for audits to verify the effectiveness and traceability of project-related configuration management.
- Work resources, methods and procedures to be used within the company:
  - definition of responsibilities, technical competences and powers relating to safety-compliant project definitions,
  - establishment of the auxiliary resources and procedures required for configuration management (such as IT programs),
  - central organization for full coverage of the configuration status (such as release and changes) of all documents coming under configuration management,
  - establishment of a standardized approval procedure in company regulations,
  - preparation, specification and release of the project definition taking safety requirements into consideration,
  - establishment of a standardized change management procedure in company regulations,
  - preparation of the regulations as to how and, if applicable, with what computer program the configuration status should be made known in the company and

- specification of the scheduling by which the effectiveness and traceability of project-related configuration management (such as, for example, the possibility of requesting the configuration status) can be regularly checked in the case of an audit.

4.3.4.2.3 Reliability Engineering

- Creation of the necessary conditions for reliability engineering in general:
  - for a more in-depth treatment, see the VDI handbook on reliability [2] and, in particular here, the standard VDI 4003 "Reliability management",
  - definition of responsibilities, technical competences and powers for reliability engineering at the system and subordinate structural unit levels,
  - compilation of all aspects, procedures and verifications for reliability engineering in a **general specification** "reliability and dependability" with which all relevant requirements can be both presented and qualitatively and quantitatively determined,
  - specification of the procedure in connection with the apportionment of the higher-level reliability requirement over the structural units of the subordinate project structure levels ("reliability apportionment" and "allocation")
    specification of which structural units in the project structure a deterministically based failure exclusion should apply to (the allocated reliability requirement is set to 1.00 = 100%) so that there is no need for a quantitative reliability verification,
    [This applies in the case of **technical integrity**, such as, for example, in holding and support functions, standardized shrink fittings, secure fasteners, forced guides, permanent magnets, guided, unbreakable compression springs and adequate creep and flashover distances from high-voltage equipment.]
  - specification of all inspection and testing procedures by which the reliability is to be verified of structural units whose function does not permit any failure exclusion,
  - checking that the **general specification** "reliability and dependability" is coherent and all technical and safety requirements of the system specification are included in an unequivocal form in the case of inadequacies, imperative requirement for rectification,
  - appointment of persons responsible for reliability engineering and
  - checking that the purchaser and supervisory institutions are included in the information flow of reliability engineering in the event of gaps, imperative requirement for rectification.

With regard to reliability engineering, the following aspects must be put in place:

- Definition of the organizational responsibilities in the company:
  - definition of responsibilities, technical competences and powers for the document release procedure (such as the general specification "reliability and dependability"),
  - definition of responsibilities, technical competences and powers for change management (in connection with documents),
  - definition of timing and contents regarding regular notification or full examination of the configuration status (with the aid of a product-specific configuration status list) and
  - project-related definition of personnel responsibility for audits to verify regularly the effectiveness and traceability of project-related reliability engineering.
- Work resources, methods and procedures to be used within the company:
  - establishment of the auxiliary resources and procedures required for reliability engineering (such as test equipment and IT programs),
  - list of the measuring sensors required stating purpose, accuracy, calibration cycles and presentation of the measurement result,
  - central organization for full coverage of the configuration status (such as release and changes) of all documents affected by reliability engineering and
  - specification of the scheduling by which the effectiveness and traceability of project-related reliability engineering can be regularly checked in the case of an audit.

4.3.4.2.4 Environmental Engineering

- Creation of the necessary conditions for environmental engineering in general (for a more in-depth treatment, see also standard VDI 4005 Parts 1–5):
  - definition of responsibilities, technical competences and powers for environment engineering at the system and structural unit level,
  - compilation of all aspects, procedures and verifications for environmental engineering in a general specification "environmental engineering" with which all requirements relating to the **original** and **object-influenced** environment, electromagnetic compatibility and lightning protection can be captured and both qualitatively and quantitatively specified,
  - definition of environmental limits for all anticipated storage, transport and operating influences during full and possibly restricted functioning,
  - specification of all simulation methods by which the resistance to environmental conditions of the technical objects in question is to be verified,

- checking that the general specification "environmental engineering" is consistent in itself and all technical and safety requirements of the system specification are included in an unequivocal form in the case of inadequacies, imperative requirement for rectification,
- appointment of persons responsible for the environmental engineering and
- checking that the purchaser and supervisory institutions are included in the information flow for environmental engineering in the event of gaps, imperative requirement for rectification.

With regard to the environmental engineering for technical safety, the following aspects must be put in place:

- Definition of the organizational responsibilities in the company:
  - definition of responsibilities, technical competences and powers for the document release procedure (such as the general specification "environmental engineering"),
  - definition of responsibilities, technical competences and powers for change management (in connection with documents),
  - definition of timing and contents regarding regular notification or full examination of the configuration status (with the aid of a product-specific configuration status list) and
  - project-related definition of personnel responsibility for audits to verify the effectiveness and traceability of project-related environmental engineering.
- Work resources, methods and procedures to be used within the company:
  - establishment of the auxiliary resources and procedures required for environmental engineering (such as test equipment for environmental simulation, IT programs, test reports),
  - list of the measuring sensors required stating purpose, accuracy and calibration cycles and presentation of the measurement result,
  - list of the structural units whose intended purpose requires proof of resistance to environmental influences,
  - central organization for full coverage of the configuration status (such as release and changes) of all documents affected by environmental engineering and
  - specification of the scheduling by which the effectiveness and traceability of project-related environmental engineering can be regularly checked in the case of an audit.

4.3.4.3 Management in the Implementation Process

4.3.4.3.1 Safety-Compliant Manufacture and Testing

The necessary proof that the manufacture and testing of a technical object are safety-compliant can only be secured when the management conditions listed above

regarding the safety-compliant planning, manufacture and testing of products have been met. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.

- Definition of the necessary conditions for safety-compliant manufacture and testing (quality inspection for verification) in general:
  - definition of responsibilities, technical competences and powers for safety-compliant and traceable manufacture and testing at the system and structural unit level,
  - checking that the construction file (manufacturing and testing documentation) is coherent and all technical and safety requirements of the specifications are included in an unequivocal form and
  - inclusion of the purchaser in planning the testing schedule (including mandatory inspection points).
- Definition (or confirmation) of organizational responsibilities at the system level for production, assembly, system integration and quality assurance as a certified part of quality management:
  - written definition of responsibilities, technical competences and powers for the release procedure for manufacturing, assembly and integration planning, and planning for quality assurance and testing,
  - project-related definition of responsibilities, technical competences and powers for maintenance of test records (with personnel certification and allocation of inspection stamps),
  - checking that the test sequence and test reports (with certified signature and inspection stamp) are recorded centrally and fully documented in the event of gaps, imperative requirement for rectification,
  - checking that "unintentional deviations" from the individual characteristics prescribed in the relevant specifications and construction file (**complaints**) and "envisaged one-off deviations" from the individual characteristics prescribed in the relevant specifications and construction file (**non-conformities**) are made known regularly by the testing department (notification of complaints or non-conformities within the context of the complaints system) in the event of gaps, imperative requirement for rectification,
  - project-related definition of personnel responsibility for audits to verify regularly both the effectiveness and traceability of project-related testing activities and the complaints or non-conformities system and
  - checking that test reporting (including logging of complaints or non-conformities) is always fully accessible (if necessary, using appropriate IT programs).
- Work resources, methods and procedures to be used on the project level:
  - establishment of the auxiliary resources and procedures required for project definition (such as IT programs),

- checking that the release process for manufacturing and testing planning (construction file) is defined either in central company rules or project rules in the event of gaps, imperative requirement for rectification,
- checking that both manufacturing and testing planning (construction file) and the relevant change management are defined in company regulations or project rules and applied in the event of gaps, imperative requirement for rectification and
- specification of the scheduling by which the effectiveness and traceability of project-related manufacturing and testing planning (such as, for example, the possibility of requesting test, complaint and nonconformity records) can be regularly checked in the case of an audit.

4.3.4.3.2 Safety-Related Verification (Quality Inspection for Product Acceptance)

The necessary proof for safety-compliant acceptance testing of a technical object can only be delivered when the conditions listed above regarding the safety-compliant planning and performance of product or technical object acceptance tests have been met. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.

- Definition of the necessary conditions for safety-compliant test planning (quality inspection for verification) in general:
  - ensuring that the contractors and company responsible for the project are certified by DIN EN ISO 9001 (for verification of the quality and safety capability of the contractor),
  - ensuring that master data records (material and functional data, acceptance conditions, etc.) are set up on the system and structural unit level and released,
  - written definition of responsibilities, technical competences and powers for safety-compliant and traceable acceptance tests on the system and structural unit level,
  - checking that the construction files in question (manufacturing and testing documentation) are coherent and all technical and safety requirements of the specifications are included in an unequivocal form and
  - inclusion of the purchaser in planning and carrying out the testing schedule (for product acceptance on the basis of the implemented mandatory inspection points).
- Definition (or confirmation) of organizational responsibilities on the system level for manufacturing, assembly, system integration and quality assurance:

  - definition of responsibilities, technical competences and powers for both the planning documents release procedure for product acceptance and the underlying plans for quality assurance and testing,
  - project-related definition of responsibilities, technical competences and powers for maintenance of test records (with personnel certification and allocation of inspection stamps),
  - checking that the test sequence and test reports for product acceptance (with certified signature and inspection stamp) are recorded centrally and fully documented in the event of gaps, imperative requirement for rectification,
  - checking that complaints and non-conformities (both being deviations from the individual characteristics required by the corresponding specifications and construction file) are made known regularly by the testing department (notification of complaints or non-conformities within the context of the complaints and non-conformities system) in the event of gaps, imperative requirement for rectification,
  - ensuring that the results of tests for product acceptance are recorded centrally within the context of "lessons learned", fully documented and used for process improvement,
  - ensuring that poor results during product acceptance will lead to preventive measures (product improvement),
  - project-related definition of personnel responsibility which regularly verifies the effectiveness of test procedures for product acceptance in the case of an audit and
  - checking that recording of acceptance testing (including the decisions of the complaints and non-conformities system) is always fully accessible (if necessary, using appropriate IT programs).

- Work resources, methods and procedures to be used on the project level:
  - establishment of the auxiliary resources and procedures required for acceptance tests (if applicable, using appropriate IT programs),
  - checking that the release process for the rules of acceptance testing is defined in company regulations or project rules in the event of gaps, imperative requirement for rectification,
  - checking that the testing rules for both acceptance testing and the relevant change management are defined in company regulations or project rules and applied in the event of gaps, imperative requirement for rectification,
  - checking that measuring and test equipment is suitable for the measurement and testing tasks required,
  - checking that measuring and test equipment undergoes regular calibration cycles if demonstrably necessary,
  - proof (logged verification) that measurement and test activities on the system and structural unit level are laid down in the relevant testing rules,
  - ensuring that it has been specified on the company or project level how the configuration status list (if applicable, using appropriate IT programs) is maintained for the inspection regulations for product acceptance and

- specification of the scheduling by which the effectiveness of project-related planning and the performance of acceptance tests (e.g., the possibility of accessing acceptance results and decisions relating to complaints and non-conformities) can be regularly checked in the case of an audit.

4.3.4.3.3 Safety-Compliant Complaints and Non-conformities Management

The necessary proof that the manufacture and testing of a technical object are safety-compliant can only be secured when the management conditions listed above regarding the safety-compliant planning, manufacture and testing of products (technical objects) have been met. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.

- Definition of the necessary conditions for safety-compliant manufacture and testing (quality inspection for verification) in general:
  - ensuring that the contractors and company responsible for the project are certificated according to DIN EN ISO 9001 (for verification of the quality and safety capability of the contractor),
  - definition of responsibilities, technical competences and powers for safety-compliant and traceable complaints and non-conformities management on the system and structural unit level and
  - informal or active inclusion of the purchaser in complaints and non-conformities management.
- Definition (or confirmation) of organizational responsibilities on the system level for manufacturing, assembly, system integration and quality assurance:
  - definition of responsibilities, technical competences and powers for quality assurance within which complaints and non-conformities management are to be located,
  - project-related definition of responsibilities, technical competences and powers for decision-making regarding complaints and non-conformities (with personnel certification and allocation of inspection stamps),
  - checking that the decision-making sequence and logging (with certified signature and inspection stamp) are recorded centrally and fully documented in the event of gaps, imperative requirement for rectification,
  - checking that complaints and non-conformities (both being deviations from the individual characteristics required by the corresponding specifications and construction file) are made known regularly by the quality assurance department in the event of gaps, imperative requirement for rectification,
  - project-related definition of personnel responsibility for regular audits to verify the effectiveness and traceability of project-related complaints or non-conformities management and

  - checking that test reporting (including logging of complaints or non-conformities) is always fully accessible (if necessary, using appropriate IT programs).

- Work resources, methods and procedures to be used on the project level:
  - establishment of the auxiliary resources and procedures required centrally for complaints and non-conformities management (such as IT programs),
  - checking that the complaints and non-conformities system are laid down centrally in either company regulations or project rules in the event of gaps, imperative requirement for rectification,
  - checking that the complaints and non-conformities system are laid down in company or project regulations and applied in the event of gaps, imperative requirement for rectification and
  - specification of the scheduling by which the effectiveness and traceability of the complaints and non-conformities system (such as, for example, the possibility of accessing records relating to decisions) can be regularly checked in the case of an audit.

4.3.4.3.4 Safety-Compliant Maintenance

The necessary proof of the safety-compliant maintenance of a technical object can only be delivered when the conditions listed above regarding the safety-compliant planning of maintenance of products (technical objects) have been met. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.[25,26]

- Creation of the necessary conditions for planning safety-compliant maintenance in general:
  - definition of responsibilities, technical competences and powers for safety-compliant and traceable maintenance on the system and structural unit level,
  - checking that the construction file (manufacturing and testing documentation) is coherent and all technical and safety requirements of the specifications and the construction file are included in an unequivocal form and
  - inclusion of the purchaser, participating companies and supervisory institutions in planning the maintenance (including, where appropriate, general inspections).

[25]Hansen, Michael: The effects of monitoring measures on the reliability of concrete elements. Dissertation, Universität Hannover. IRB-Verlag, 2004.

[26]Hansen, Michael: Monitoring-based risk assessment of existing concrete structures. Postdoctoral thesis, Leibniz Universität Hannover. IRB-Verlag, 2014.

- Definition (or confirmation) of organizational responsibilities on the system level for preventive maintenance, corrective maintenance and general inspections:
  - definition of responsibilities, technical competences and powers for the release procedure for both maintenance regulations and planning quality assurance and testing (no maintenance without subsequent quality inspection),
  - project-related definition of responsibilities, technical competences and powers for carrying out maintenance (with personnel certification),
  - checking that **complaints** (**unintentional deviations** from the individual characteristics prescribed in the relevant maintenance regulations) and **non-conformities** (**envisaged one-off deviations** from the individual characteristics prescribed in the relevant maintenance regulations) are made known regularly by the testing department (notification of complaints or non-conformities within the context of the complaints system) in the event of gaps, imperative requirement for rectification,
  - central, real time/immediate, full capture and traceable documentation of the configuration status of maintenance regulations,
  - project-related definition of personnel responsibility for audits to verify regularly the effectiveness and traceability of project-related maintenance management and
  - checking that test reporting (including logging of complaints or non-conformities) is always fully accessible (if necessary, using appropriate IT programs).
- Work resources, methods and procedures to be used on the project level:
  - establishment of the auxiliary resources and procedures required for maintenance (such as IT programs),
  - checking that the release procedure for maintenance regulations is defined centrally in the company or project-specifically in the event of gaps, imperative requirement for rectification,
  - checking that not only maintenance planning including the relevant change management but also the application of maintenance regulations are defined company- or project-specifically and applied in the event of gaps, imperative requirement for rectification and
  - specification of the scheduling by which the effectiveness and traceability of the project-related maintenance system (such as, for example, the possibility of requesting test, complaint and nonconformity records) can be regularly checked in the case of an audit.

4.3.4.4 Organization of Safe Operation

The necessary proof of the safety-compliant operation of a technical object can only be delivered when the conditions listed above regarding the safety-compliant

planning of operating regulations for products (technical objects) have been met. In the event of gaps being discovered and the consequent safety-related inadequacy, replanning of the technical object in question is unavoidable.

To ensure a safe design also for operation and utilization of the product concerned, the appropriate safety-compliant operating regulations should be planned, observed and applied in operation.

- Creation of the necessary conditions for planning safe operation in general:
  - definition of responsibilities, technical competences and powers for planning a safety-compliant operation on the system and structural unit level,
  - checking that all operating regulations (control mode, backup mode) are consistent in themselves and all technical and safety requirements of the specifications and construction file are included in an unequivocal form and
  - inclusion of the purchaser, participating companies and supervisory institutions in the planning of operation (including, where appropriate, any "preoperational checks" to be provided, checking operational readiness—"preflight check").
- Definition (or confirmation) of organizational responsibilities on the system level for operation (appointment of operation managers):
  - definition of responsibilities, technical competences and powers relating to the release procedure for operating regulations,
  - project-related definition of responsibilities, technical competences and powers for the performance of operation (with personnel certification such as a driver's licence),
  - project-related written definition of responsibilities, technical competences and powers for keeping the operating log with full recording of all incidents and accidents,
  - checking that complaints (unintentional deviations from the individual characteristics prescribed in the relevant operating regulations) and non-conformities (envisaged one-off deviations from the individual characteristics prescribed in the relevant operating regulations) are made known regularly by the testing department (notification of incidents and accidents within the context of the complaints system) in the event of gaps, imperative requirement for rectification,
  - central, real time/immediate, full capture and traceable documentation of the configuration status of operating regulations,
  - project-related definition of personnel responsibility for audits to verify regularly the effectiveness and traceability of both the project-related control mode operation and the incidents and accidents reporting system and
  - checking that the operating log and logging of the incidents and accidents reporting system are always fully accessible (if necessary, using appropriate IT programs).
- Work resources, methods and procedures to be used on the project level:
  - establishment of the auxiliary resources and procedures (such as IT programs) required for operation (control mode, backup mode),

- checking that the release procedure for operating regulations is defined centrally in the company or project-specifically in the event of gaps, imperative requirement for rectification,
- checking that not only the planning of operating regulations including the relevant change management but also the application of operating regulations are defined company- or project-specifically and applied in the event of gaps, imperative requirement for rectification and
- specification of the scheduling by which the effectiveness and traceability of the project-related operation (such as, for example, both the possibility of accessing the operating log and a logging of incidents and accidents reporting system) can be regularly checked in the case of an audit.

4.3.4.5 Management of Safe Disposal

To ensure a safe design for dismantling, recycling and disposal as well (system, technical facility, product), the appropriate safety-compliant procedures must be planned and observed and applied in the course of dismantling, recycling and disposal.

- Creation of the necessary conditions for planning a safe procedure in general:
  - written definition of responsibilities, technical competences and powers for planning a safety-compliant procedure on the system and structural unit level,
  - checking that all procedure regulations are coherent and all technical and safety requirements of the specifications are included in an unequivocal form and
  - inclusion of the purchaser, participating companies and supervisory institutions in planning the procedure, including all necessary preconditions.
- Definition (or confirmation) of organizational responsibilities for the procedure (appointment of managers) on the system level:
  - written definition of responsibilities, technical competences and powers relating to the release procedure for procedure regulations,
  - project-related written definition of responsibilities, technical competences and powers for execution of the procedure (with personnel certification),
  - project-related written definition of responsibilities, technical competences and powers for keeping the process log with full recording of all incidents and accidents,
  - checking that complaints (unintentional deviations from the implementations prescribed in the relevant procedure regulations) and non-conformities (envisaged one-off deviations from the implementations prescribed in the relevant procedure regulations) are made known regularly by the testing department (notification of incidents and accidents within the context of the complaints system),
  - central, real time/immediate, full capture and traceable documentation of the configuration status of procedure regulations,

  - project-related definition of personnel responsibility for audits to verify regularly the effectiveness and traceability of both the dismantling project and the relevant incidents and accidents reporting system, and
  - checking that the procedures log and the logging of the incidents and accidents reporting system are always fully accessible (if necessary, using appropriate IT programs).

- Work resources, methods and procedures to be used on the project level:
  Since all methods have to be very specifically focused on task and objective, only general requirements will be made here which must also be made sufficiently specific for the application case in question. The following are necessary:
  - establishment of both the auxiliary resources (such as IT programs) required for the processes and procedures,
  - checking that the release procedure for procedure regulations is defined centrally in the company or project-specifically,
  - checking that the planning is defined company- or project-specifically and applied, and
  - specification of the scheduling by which the effectiveness and traceability of the project-related dismantling (such as, for example, the possibility of accessing the procedures log of the incidents and accidents reporting system) can be regularly checked in the case of an audit.

4.4 Safety-Compliant Design in Civil Engineering and Process Plant Engineering

Section 4.3 showed not only how technical safety can be systematically generated and applied interdisciplinarily but also everything which is to be observed in this connection. Attention is drawn here to the relevant safety procedures: deterministic (in the sense of "exclusion of failure"), probabilistic (in the sense of "reliability") and safety engineering (in the sense of "fail-safe" and "fail-operational"). The approach practised in civil engineering and process plant construction also requires a thorough examination of possible failure causes as it is necessary in safety engineering in other ways as well. The "exclusion of failure" represented via the deterministic path must be just as well substantiated as any other precautionary safety measure. The complexity of modern structures in civil engineering and process plant construction calls for a correspondingly adapted approach, as is presented compactly in this section.

As long as classically compensatory approaches in the safety architecture are conducive to reaching these goals, they will also be best practices. In the case of highly complex structures as, for example, in the fields of aeronautical and space technology, deterministic approaches are not always applicable and probabilistic approaches therefore more suitable. In many fields, the approach leading to the best result is a

combination of deterministic and probabilistic (semi-probabilistic) procedures. In this case, for example, the distributions of properties and loads are regarded as a convention and inserted into the schema of the classically compensatory approach.

This approach is increasingly pronounced in civil engineering and thus forms the basis for its safety architecture. In what follows, the procedure for civil engineering is described and discussed and applied analogously to process plant engineering and fields in which a safety-compliant design is a requirement and the distributions of properties and loads necessarily have to be observed.

The flow chart entitled "Safety-methodological flow chart" (see Sect. 4.3.2.1) shows how the principles of the safety-methodological approach are used in generating and securing technical safety. The principle is described in detail in Sect. 3.2.1.2 of this publication on "technical safety". The steps and decisions necessary for generating technical safety are described on the basis of the six phases of a product life cycle (see Fig. 1 in that section) in which the first three phases describe the planning and implementation and the following two describe utilization and recycling in real products. An attempt is made to cover all technical disciplines and formulate safety-specific commonalities both technically and terminologically.

Generally speaking, the "exclusion of failure" is used for structures in civil engineering in order to generate technical safety. This exclusion of failure is deterministically justifiable on the basis of technical integrity, and there is thus no need for a quantitative proof of reliability. In the case of supporting structures, the exclusion of failure is, however, guaranteed by a so-called semi-probabilistic safety concept according to DIN 1055-100 "Effects on supporting structures—Basis of structural design—Safety concept and design rules" (now DIN EN 1990).[27] The aim is to capture the uncertainties in the design at the place where they occur with their scattering properties. This is done with the aid of partial safety factors on the side of influences/loads (such as stress resultants, stresses) and component resistances.

The partial safety factors are directly dependent on the coefficients of variation on the influence and resistance sides. By calibration and validation of previous empirical safety requirements in civil engineering, reliabilities or failure probabilities are laid down as a function of the risk class aspired to (see also the hazard categories in Table 3.1 in Sect. 3.2.1.1) and a reference period, usually of 50 years for normal buildings and 100 years for civil engineering works. For risk class RC2

[27]Formulation and explanation of basic principles:

Construction Standardisation Committee (NaBau) within DIN, "Safety of buildings" working committee: Basic principles of determining safety requirements for buildings, Berlin, Vienna, Zurich: Beuth Verlag, 1981

Spaethe, Gerhard: Safety of load-bearing structures. Vienna, New York: Springer Verlag, 1992

Grünberg, Jürgen: Basic principles of structural design—safety concept and design rules for structural engineering—Explanations for DIN 1055-100 Civil engineering practice, published by DIN German Institute for Standardization, Berlin, Vienna, Zürich: Beuth Verlag, 2004

Hansen, Michael: On the impact of monitoring measures on the reliability of concrete components. Dissertation, Leibniz University of Hannover. IRB-Verlag, 2004

Hansen, Michael: Monitoring-assisted risk assessment of existing solid building structures. Postdoctoral thesis, Leibniz University of Hannover. IRB-Verlag, 2014.

according to DIN EN 1990:2010-12 "Eurocode: Basis of structural design", this corresponds to a probability of failure of 10^{-6} for a reference period of one year or 7×10^{-4} for a reference period of 50 years.

The safety justification for structural safety is presented in the flow chart "Procedural and decision-making methodology for safety-compliant design in civil engineering and process plant construction" (Fig. 4.4).

On the basis of the phase concept, the requirements are emphasized relating to controlling, safety case, state of the art, state of scientific and technical knowledge and assignment of responsibilities in the phases in question. In addition to the necessary documentation of the individual steps and decisions, this shows the load assumptions with the envisaged and possible operating states, scenarios and service life of the products and the classification of the failure modes as a function of the consequences arising. Finally, the path to the risk assessment is defined and the necessity for involvement of the public is described on the basis of the risk level determined and the necessary involvement of the individual in the development and manufacturing process (human factors).

4.4.1 Notes to the Flow Chart

1.	Locality, environment	The influence of the locality of the wider environment on the product can be important for its utilization and should, where appropriate, be taken into account
2.	Public (**P**)	The product can have an impact on the public, and consumer protection and, possibly, legal regulations must be observed
3.	Human factors engineering (**H**)	The effects of human–machine relationships should be examined
4.	Inspection classes	DIN EN 1990:2010-12 "Eurocode: Basis of structural design; German version EN1990:2002"
5.	Approval	Approval may come under contract law but consent/release be formally under public law
6.	Replanning	Replanning will be necessary when, according to the safety analysis, improvement is not possible with the current data
7.		The standard case in design is a semi-probabilistic analysis with partial safety factors (Level I). A probabilistic approximation is achieved, for example, by the reliability method of the first order (FORM) (Level II). A full probabilistic method (Level III) is, for example, the Monte Carlo analysis
8.		Safety analyses with current data recognized by inspection and not yet been taken into account
9.	Project controller	The project controller takes over only the functions of the purchaser during project control but not project management itself. He/she thus has primarily organizational duties and is not authorized to make decisions, for example, about changes to the construction plan

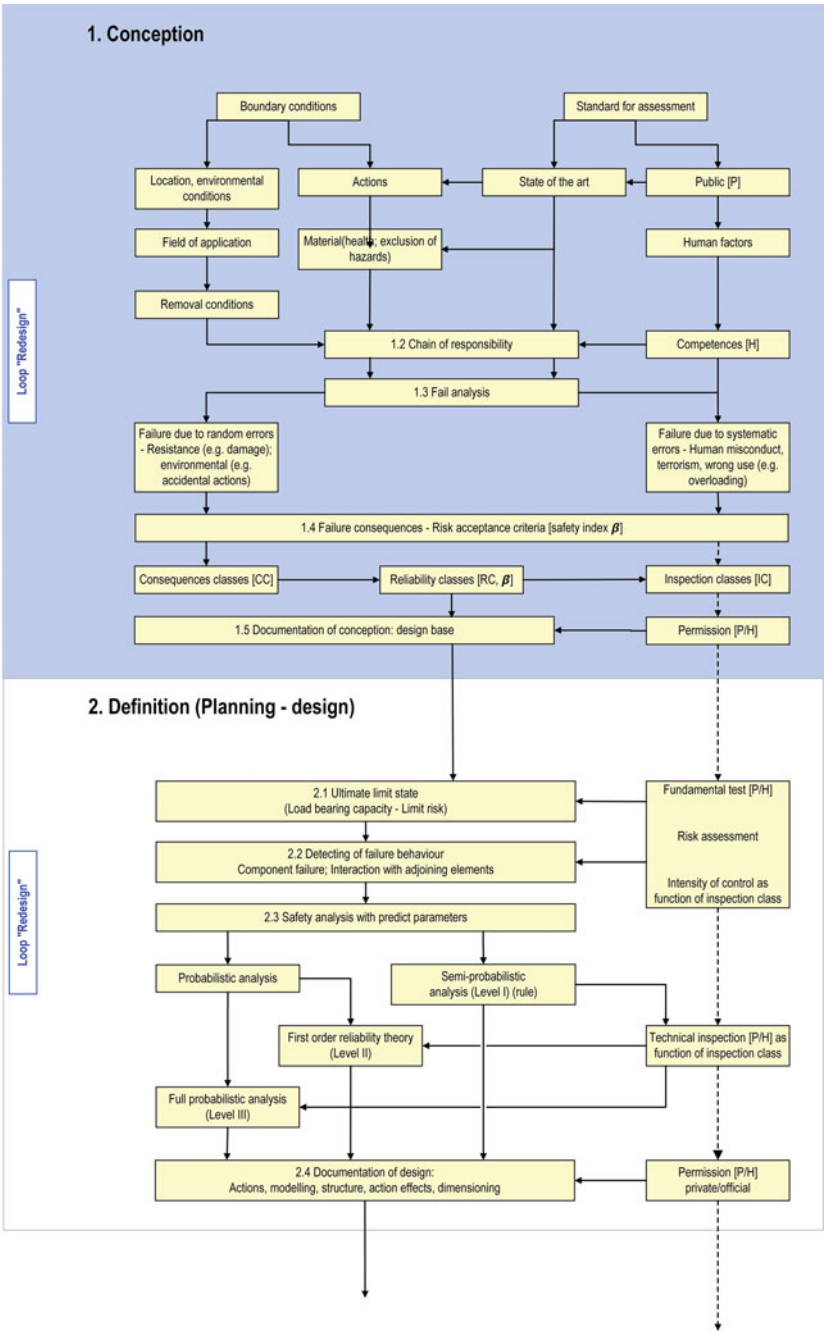

Fig. 4.4 Procedural and decision-making methodology for safety-compliant design in civil engineering and process plant construction

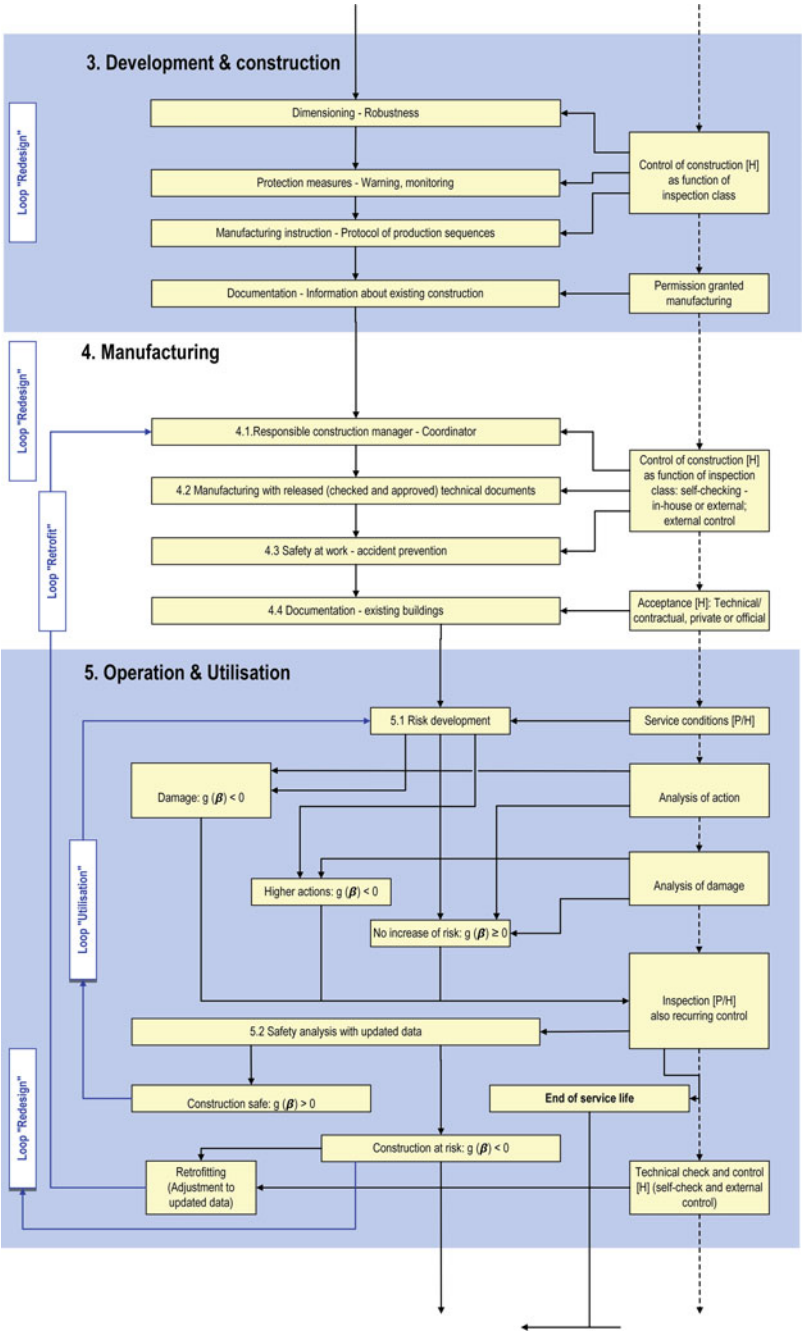

Fig. 4.4 (continued)

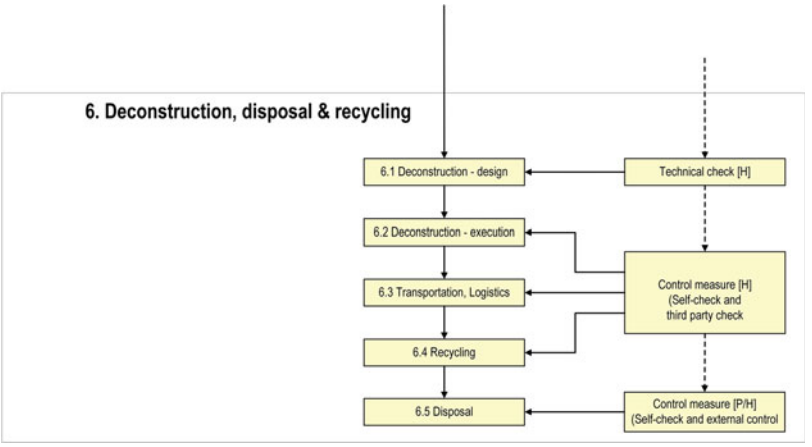

Fig. 4.4 (continued)

4.4.2 Definitions with Regard to the Flow Chart

Action Step 2.1: Ultimate limit states of structural safety—limiting risk
$g(\beta) = 0$
Danger: $g(\beta) < 0$
Safety: $g(\beta) > 0$

- Positional stability, static equilibrium, strength failure, stability failure, fatigue failure

Action Step 2.2: Determination of failure behaviour

- Component failure, linear elastic analysis,
- Interactions with adjacent components: failure mechanisms, such as kinematic chains, system redundancies, nonlinear analysis or theory of plasticity.

Action Step 2.3: Safety analysis

- Semi-probabilistic analysis—partial safety factors

  Suitable for linear, nonlinear and also plastic structural analysis:
  $E_d(G \cdot G_k; \gamma_Q \cdot Q_{rep}) \leq R_d\ (\eta_1 \cdot f_{1k}/\gamma_{M1}; \eta_2 \cdot f_{2k}/\gamma_{M2})$

- Probabilistic analysis:
  - Reliability theory of first order (FORM)
    Linearized limit state equation, normally distributed basic variables (basic variables without normal distribution are appropriately transformed by, for example, the Rackwitz-Fiessler algorithm), approximation
  - Complete probabilistic analysis, for example, with the Monte Carlo simulation.

Action Step 5.1: Damage—risk
$g(\beta) < 0$

- Fatigue (cyclic mechanical effects)
- Corrosion (chemical effects)
- Ageing (physical effects)

Action Step 5.2: Higher impacts—risk
$g(\beta) < 0$

– Increased imposed loads (change of use)
– Increased environmental impacts (climate change)
– Unforeseen unusual impacts.

Chapter 5
Proposal of the VDI "Technical Safety" Committee

The Scientific Advisory Council of the VDI felt called on by virtue of its interdisciplinary competence to launch and promote the process of safety awareness. In exercising this technical expertise the VDI "technical safety" Committee describes in the present publication the basic principles of a safety-methodological concept applicable across disciplines.

The presentation of this concept should demonstrate to a broader technical audience how technical safety is created, and what methodological approaches are required. The paths shown are realistic and, assuming consistent, ethically considered actions, feasible in practice for specialists working interdisciplinarily. A basis of trust between society and technology is important, and this can only be achieved in an open, honestly conducted dialogue between them. Observable technophobia on the part of a non-technical public must be reduced by explaining the risks involved in dealing with technical products and doing so in a manner understandable to the layperson. This, in turn, can only be successful when terminology and methods in the field of safety engineering are interdisciplinarily harmonized among the experts and can be presented on a sound basis. As with general engineering, safety engineering also needs both generalistic concepts for an interdisciplinary approach and systemic management procedures. Great efforts are still needed here in the fields of science and business.

The steps taken by the EU Council and EU Commission with the introduction of the New Approach and the Global Approach are certainly leading in the right direction. In industrial sectors in which EC verification of the products concerned is not followed by any system inspection conducted by a state agency; these steps do however have, as far as technical safety is concerned, clear weaknesses in certain sectors with their emphasis on the free movement of goods within the EU. The concepts in some cases thus remain a long way behind the effectiveness of the historical system which met demands and has now been relieved. These weaknesses, which at the time of introduction were already known to the experts dealing

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_5

with safety issues, are diverse, and improvements are currently being made by the European Commission. In addition to the product-related directives, the "Directive on General Product Safety" 2001/95/EG dated 03.12.2001 also applies, which requires all products being put on the market within the European Economic Area to be safe. How this is to be secured requires further regulation—however, not only in the field of safety legislation but also, above all, in the field of safety engineering.

Chapter 6
Summary—Lessons Learned

We who have the privilege of living in a civilized, democratic state governed by the rule of law are well aware that we can depend on the numerous technical facilities which we use in some form or other in our daily lives. This is ensured by not only the democratic legal system but also, above all, the centuries of experience of our engineers which have been systematically collected in technical standards and guidelines. Nevertheless, time and time again a disturbance or even accident occurs. An overhasty search for a "culprit" then takes place. Engineers do, however, know that absolute, 100% safety is impossible. The question still arises: can't the occurrence of these—apparently inevitable—incidents and accidents be even further restricted?

Almost thirty years ago the realization first arose that the subject of "technical safety" was being handled very differently depending on the field of application. Probabilistic approaches have thus proven themselves over many decades in the aerospace industry, while many other fields of application restrict themselves to the deterministic exclusion of failure, which all too often is still misunderstood as "absolute safety". The existing orientation of safety engineering towards the particular field of application constantly creates confusion as soon as interdisciplinary collaboration is required such as in innovative technology projects. The situation results here in an absence of a "state-of-the-art", and the corresponding codes of practice by which technical safety can be rendered transparent. Knowledge about what is required from the safety point of view is nevertheless available but until now has not been readily accessible.

Therefore, the VDI "technical safety" Committee has taken on the task of identifying the "hidden commonalities" of the various technical safety concepts and putting together the corresponding—interdisciplinarily usable—procedure in a single guideline. In order to gain support for the idea behind this "technical safety" guideline the committee brought to mind a number of examples which have probably become permanently engraved in the public consciousness. Although all

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7_6

of these cases of failure could have been avoided with a safety methodological approach, the causative deficiencies were only identified after the event.

The VDI "technical safety" Committee is of the opinion that even causes of this kind must be prevented. Undeveloped safety concepts offer no reason for their continued existence, even when they present what is still common practice and are tolerated by our legal system.

VDI "Technical Safety" Committee

The Scientific Advisory Council of the VDI has tasked the interdisciplinary "Technical Safety" committee with the objective of providing a transparent presentation of the situation regarding the various procedures and concepts for achieving technical safety in all industries and engineering disciplines and identifying possible needs for action. The committee presents its findings in the present publication.

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7

References

1. Marburger, P.: Die Regeln der Technik im Recht. Köln: Heymann, 1979
2. VDI-Handbuch Zuverlässigkeit. Berlin: Beuth Verlag
3. Report 31 "Ethische Ingenieurverantwortung – Handlungsspielräume und Perspektiven der Kodifizierung", VDI-Hauptgruppe Mensch und Technik, Düsseldorf, 2000
4. Ethik und Kernenergie – Expertise für den Fachausschuss Kerntechnik (FA-KT). VDI-Gesellschaft Energietechnik (VDI-GET), Düsseldorf, Mai 2006
5. Rasmussen, J.; K. Duncan, J. Leplat (eds): New technology and human error, Chichester: Wiley, pp. 281–283, 1987
6. Bons, W.: Zeitschrift "Kunst und Technik" des Deutschen Museums, München, Vol. 4, S. 18, 1999
7. Lenk, H.; M. Maring Technik zwischen Können und Sollen – Wer verantwortet die Technik? In: TÜV Saarland Foundation (Hrsg.): Congress Documentation Saarbrücken 2001: World Congress on Safety of Modern Technical Systems. Köln: TÜV-Verlag pp. 725–738
8. Ada 2005. Language Reference Manual. Heidelberg: Springer, 2005
9. Ada Reference Manual ISO/IEC 8652:2012(E), Language and Standard Libraries. International
10. Standard ISO/IEC 8652/2012 (E), Series: Lecture Notes in Computer Science, Vol. 8339, Subseries: Programming and Software Engineering Taft S.T., Duff R.A., Brukardt R.L., Ploedereder E., Leroy P., Schonberg E. (Eds.), 2013, XXVIII, p. 921
11. Adams, H. W.: Integriertes Managementsystem für Sicherheit und Umweltschutz. München, Wien: Carl Hanser Verlag, 1995
12. Alscher, H.; Nowack, S.; Pilz, W.-D.: Projektleitung des Konsortiums Magnetbahn Transrapid. Schlussbericht für die Vorhaben TV 78684 und TV 82088. Entwicklung, Bau, Integration und Inbetriebnahme der TRANSRAPID-Versuchsanlage Emsland, 29.03.1985
13. Aoki, S.: Transport of Radioactive Materials. Nuclear Power Engineering Corporation, 1990. ISBN 4902719-01-0
14. Apostolakis, G. E.; Farmer, F.; van Otterloo, R. W. (Hrsg.): Reliability Engineering & System Safety. Elsevier Applied Science Publishers Ltd., 1988
15. Audsley, N.; Burns, A.; Richardson, M.; Tindell, K.; Wellings, A.: Applying New Scheduling Theory to Static Priority Pre-emptive Scheduling. Report RTRG/92/120. Department of Computer Science. University of York, 1992
16. Audsley, N.; Burns, A.; Richardson, M.; Wellings, A.: Hard Real-Time Scheduling: The Deadline Monotonic Approach. In: Real-Time Programming (ed. W.A. Halang and K. Ramamritham). Pergamon Press, 1992, pp. 127–132
17. Banck, J.; Berg, K. H.; Dyck, H. P.; Gies, H.; Hübschmann, W. G.; Karlsson, F.; Messer, K. P.; Oeser, H.-R.; Patermann, C.; Roth, K.; Schmidt, M. W.; Viehl, E.: Entsorgung von Kernkraftwerken. Köln: Verlag TÜV Rheinland, 1981

H.B. Keller et al., *Technical Safety – An Attribute of Quality*,
https://doi.org/10.1007/978-3-319-68625-7

18. Baum, H.; Schnitzler, W.; Schulz, W. H.: Arbeits- und Verkehrssicherheit im Straßengüterverkehr insbesondere im Gefahrgutstransport auf einem deregulierten Verkehrsmarkt. Hrsg.: Bundesanstalt für Arbeitsschutz. Wirtschaftsverlag NW, Bremerhaven 1, 1989
19. Beck, K.: Extreme Programming Explained. Embrace Change. 1st Edition, Addison Wesley, 2000. ISBN 0-201-61641-6
20. Behrens, D.; Gundlach, V. G.: Praxis der Sicherheitsanalysen in der chemischen Verfahrenstechnik. DECHEMA Frankfurt am Main: Verlag Chemie, 1985
21. Benra, J.; Keller, H. B.; Schiedermeier, G.; Tempelmeier, T.: Synchronisation und Konsistenz in Echtzeitsystemen. In: Benra, J. T. (Hrsg.): Software-Entwicklung für Echtzeitsysteme. Berlin u. a.: Springer, 2009, S. 49–65
22. Boehm, B. W.: A Spiral Model of Software Development and Enhancement. In: IEEE Computer. Vol. 21, Ausg. 5, Mai 1988, S. 61–72
23. Booch Grady et al.: The Unified Modeling Language User Guide. Addison Wesley, 1999
24. Bressin, M.: Unfälle beim Transport gefährlicher Güter auf der Straße 1982 – 1984. Hrsg.: Bundesanstalt für Arbeitsschutz. Bericht der Bundesanstalt für Straßenwesen, Bereich Unfallforschung. Bergisch Gladbach, 1985. Bremerhaven: Wirtschaftsverlag NW, 1989
25. BSI-Grundschutzkataloge (siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/kataloge.html
26. Buttazo, G. C.: Hard Real-time Computing Systems, Kluwer Academic publishers, 1997
27. CMMI – Capability Maturity Model Integration CMU/SEI-2002-TR-029, ESC-TR-2002-029. August 2002
28. Congress of the United States, Office of Technology Assessment. Transportation of Hazardous Materials. Washington D. C., 1986
29. Daimler AG (Hrsg.): Der Ursprung der Sicherheit. Stuttgart: Daimler AG, 2008
30. DeMarco, T.: Warum ist Software so teuer? … und andere Rätsel des Informationszeitalters, München, Wien: Carl Hanser Verlag, 1997 (Titel der englischen Originalausgabe: “Why Does Software Cost So Much? And Other Puzzles of the Information Age”, 1995 by Tom DeMarco)
31. Der Bundesminister für Forschung und Technologie (Hrsg.): Deutsche Risikostudie Kernkraftwerke – eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko. Köln: Verlag TÜV Rheinland, 1979
32. Deutsche Risikostudie Kernkraftwerke. Köln: Verlag TÜV Rheinland, 1979
33. Deutscher Verband für Materialprüfung e. V.: Behälter aus Sphäroguss für radioaktive Stoffe, Seminar der Bundesanstalt für Materialforschung und -prüfung (BAM) in Zusammenarbeit mit dem Deutschen Verband für Materialprüfung e. V., 1987
34. Deutsches Atomforum e. V. (Hrsg.): Beförderung von Kernmaterial. Bonn: Wilhelm Tempelhoff, 1985
35. Deutsches IDNDR-Komitee für Katastrophenvorbeugung e. V. (Hrsg.): Journalisten-Handbuch zum Katastrophenmanagement. International Decade for Natural Disaster Reduction Komitee. Bonn, 1996
36. DIN 1055-100:2001-03, Einwirkungen auf Tragwerke – Teil 100: Grundlagen der Tragwerksplanung – Sicherheitskonzept und Bemessungsregeln. Zurückgezogen 2010-12, ersetzt durch DIN EN 1990
37. DIN 25419: 1985-11, Ereignisablaufanalyse; Verfahren, graphische Symbole und Auswertung
38. DIN 25419-1:1977-06, Störfallablaufanalyse; Störfallablaufdiagramm, Methode und Bildzeichen. Zurückgezogen, Nachfolgedokument DIN 25419
39. DIN 25424, Fehlerbaumanalyse; Methode und Bildzeichen
40. DIN 31004-1:1982-11, Begriffe der Sicherheitstechnik – Grundbegriffe. Zurückgezogen, jetzt
41. DIN 820-12
42. DIN 55350, Begriffe zu Qualitätsmanagement

43. DIN 57831:1980-02, Elektrische Bahn-Signalanlagen (VDE-Bestimmung). Zurückgezogen, Nachfolgedokument DIN EN 50129, VDE 0831-129
44. DIN 820-12:2014-06, Normungsarbeit; Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen
45. DIN EN 1990:2010-12, Eurocode: Grundlagen der Tragwerksplanung; Deutsche Fassung EN 1990:2002 + A1:2005 + A1:2005/AC:2010
46. DIN EN 61508-4:2012-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen
47. (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010
48. DIN EN 9100:2010-07, Qualitätsmanagementsysteme – Anforderungen an Organisationen der Luftfahrt, Raumfahrt und Verteidigung; Deutsche und Englische Fassung EN 9100:2009
49. DIN EN 50129 (VDE 0831-129:2003-12), Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung EN 50129:2003
50. DIN EN ISO 12100:2011-03, Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010
51. DIN EN ISO 9000:2015-11, Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015
52. DIN EN ISO 9001:2015-11, Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015
53. DIN ISO 2859-1:2014-08, Annahmestichprobenprüfung anhand der Anzahl fehlerhafter Einheiten oder Fehler (Attributprüfung) – Teil 1: Nach der annehmbaren Qualitätsgrenzlage (AQL) geordnete Stichprobenpläne für die Prüfung einer Serie von Losen (ISO 2859-1:1999 + Cor. 1:2001 + Amd.1:2011)
54. DIN VDE 0100-410 (VDE 0100-410:2007-06) Errichten von Niederspannungsanlagen – Teil 4-41: Schutzmaßnahmen – Schutz gegen elektrischen Schlag (IEC 60364-4-41:2005, modifiziert); Deutsche Übernahme HD 60364-4-41:2007
55. DIN VDE 0831 (VDE 0831:2006-04), Elektrische Bahn-Signalanlagen
56. DIN VDE 31000-2:1987-12, Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse; Begriffe der Sicherheitstechnik; Grundbegriffe. (zurückgezogen)
57. Dombrowsky, W. R.; Hornnczuk, J.; Streitz, W.: Erstellung eines Schutzdatenatlasses, Zivilschutzforschung. Neue Folge, Bd. 51. Bundesverwaltungsamt – Zentralstelle für Zivilschutz. Bonn, 2003
58. Droste, B.; Sorenson, K. (Hrsg.): Brittle Fracture Safety Assessment International Journal of Radioactive Materials Transport Vol. 6. Nuclear Technology Publishing, 1995
59. Eisenbahn-Bau- und Betriebsordnung (EBO)
60. Ensthaler, J.; Gesmann-Nuissel, D.; Strübbe, K.: Gestaltung von Aufsichtssystemen im Produkt-Sicherheitsrecht. Regensburg: Transfer-Verlag, 2005
61. Ericsson, A.-M.; Elert, M.; Intertran: A System for Assessing the Impact from Transporting Radioactive Material. Vienna: IAEA-Tecdoc-287, 1983
62. Farmer, F. R. (Hrsg.): Reliability Engineering. An International Journal, Vol. 2, No 1, 2 and 3. London: Applied Science Publishers Ltd., 1981
63. Freiling, F.; Grimm, R.; Großpietsch, K.-E.; Keller, H. B.; Mottok, J.; Münch, I.; Rannenberg, K.; Saglietti, F.: Technische Sicherheit und Informationssicherheit – Unterschiede und Gemeinsamkeiten. Accepted for: Informatik Spektrum, GI, Springer, Ausgabe Nr. 1 (37) 2014, S. 14–24
64. Gesamtverband der Deutschen Versicherungswirtschaft e. V., Berlin (Hrsg.): Risiko – Wie viel Risiko braucht die Gesellschaft? Karlsruhe: Verlag Versicherungswirtschaft e. V., 1998

65. Gesellschaft für Anlagen- und Reaktorsicherheit (Hrsg): Zur Sicherheit des Betriebs der Kernkraftwerke in Deutschland. Europäisches Zentrum für Wirtschaftsforschung und Strategieberatung. Die längerfristige Entwicklung der Energiemärkte im Zeichen von Wettbewerb und Umwelt. Prognos und EWI für das Bundesministerium für Wirtschaft und Technologie. Berlin, 1999
66. Gherbi A. et al.: Software Diversity for Future Systems Security. CrossTalk, September/October 2011, p. 10 ff.
67. Grimm, R.; Keller, H. B.; Rannenberg, K.: Informatik 2003 – Mit Sicherheit Informatik. Lecture Notes in Informatics (LNI). Bonn: Köllen Verlag, 2003
68. Großmann, G.; Leitung der VdS-Fachtagung Anlagensicherheit und betriebliche Störfallvorsorge: VdS Schadenverhütung im Gesamtverband der Deutschen Versicherungswirtschaft. Köln, 1997
69. Großmann, G.; Leitung der VdS-Fachtagung Anlagensicherheit und betriebliche Störfallvorsorge: VdS Schadenverhütung im Gesamtverband der Deutschen Versicherungswirtschaft. Köln, 2003
70. Grünberg, J.: Grundlagen der Tragwerksplanung – Sicherheitskonzept und Bemessungsregeln für den konstruktiven Ingenieurbau. Erläuterungen zu DIN 1055-100. Praxis Bauwesen, Hrsg.: DIN Deutsches Institut für Normung. Berlin, Wien, Zürich: Beuth Verlag, 2004
71. Gründer, T.; Schrey, J. (Hrsg.): Management Handbuch IT-Sicherheit. Risiken, Basel II, Recht. Berlin: Erich Schmidt Verlag, 2007
72. Guide for the use of the Ada Ravenscar Profile in high integrity systems ISO/IEC JTC 1/SC 22/ WG 9 N 435, Draft for PDTR Approval Ballot, ISO/IEC TR 24718, 14 Feb. 2004
73. Hansen, M.: Monitoringgestützte Risikobewertung bestehender Massivbauwerke. Habilitationsschrift Leibniz Universität Hannover. IRB-Verlag, 2014
74. Hansen, M.: Zur Auswirkung von Überwachungsmaßnahmen auf die Zuverlässigkeit von Betonbauteilen. Dissertation Leibniz Universität Hannover. IRB Verlag, 2004
75. Hansen, M.: Zur Auswirkung von Überwachungsmaßnahmen auf die Zuverlässigkeit von Betonbauteilen. Stuttgart: Fraunhofer IRB Verlag, 2004
76. Harding, A. B.: Tank Container Failures. AEA Technology, Health & Safety Executive. Warrington, Cheshire WA3 6AT, 1996
77. Hartwig, S. (Hrsg.): Große technische Gefahrenpotenziale. Risikoanalysen und Sicherheitsfragen. Berlin, Heidelberg, New York: Springer-Verlag, 1983
78. Hauptmanns, U.; Marx, M.: Kriterien für die Beurteilung von Gefährdungen durch technische Anlagen. Schriftenreihe Recht & Technik. Berlin: Verlag VdTÜV, 2010
79. Health & Safety Executive. Her Majesty's Stationary Office, Norwich NR3 1BQ, 1997
80. Heilmund, S. (Hrsg.): World Congress Safety of Modern Technical Systems – Congress-Documentation. Publisher: TUEV Saarland Foundation by TÜV GmbH. Köln, 2001
81. Hermann, A. G., Röthemeyer, H.: Langfristig sichere Deponien. Berlin Heidelberg: Springer Verlag, 1998
82. Humphrey, W. S.: The Software Quality Challenge. Crosstalk – The Journal of Defense Software Engineering, June 2008, p. 4 ff.
83. IAEA Safety Standards No. 6. Regulations for the Safe Transport of Radioactive Material.
84. Vienna: IAEA, 1985
85. Ibrahim, L. et al.: Safety and Security Extensions for Integrated Capability Maturity Models. Washington: Federal Aviation Administration, 2004 (www.faa.gov/ipg)
86. IEC 1508: Functional Safety – Safety-Related Systems
87. INES: The International Nuclear Event Scale User's Manual Jointly prepared by IAEA and NEA (OECD). IAEA, 1992
88. Information Technology – Programming Languages Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use. ISO/IEC TR 24772 Edition 2 (TR 24772 WG 23/N 0389), ISO/IEC JTC 1/SC 22/WG 23, 2012

89. Internationale Sektion der IVSS für die Verhütung von Arbeitsunfällen und Berufskrankheiten in der chemischen Industrie (Hrsg.): Gefahrenermittlung, Gefahrenbewertung – Praxisbewährte thematische Methoden. Heidelberg: Berufsgenossenschaft der chemischen Industrie, 1997
90. Isermann, H.; Huth, M.; Schröder, K.: Entwicklung eines risikoanalytischen Systemmodells der Gefahrgutsbeförderung. Forschungs- und Entwicklungsvorhaben 96517/97 des BM V, 2000. Persönliches Exemplar Dr. Hubert B. Keller
91. ISO Guide 30, Verwendete Begriffe und Bezeichnungen beim Nachweis mit Referenzwerkstoffen
92. ISO Guide 31, Referenzwerkstoffe
93. ISO/IEC 15939:2007, Systems and Software Engineering; Measurement Process
94. Jaeger, T. A.: Zur Sicherheitsproblematik technologischer Entwicklungen Qualität und Zuverlässigkeit, Heft 1 QZ 19 (1974)
95. Jäger, P.; Haferkamp, K. (Hrsg.): Die Auswirkung des Risikos von Lagerung und Transport gefährlicher Stoffe auf die Entwicklung verbesserter Transporttechnologien (Straßentransport). Phase I Grundlagenuntersuchung. Der Bundesminister für Forschung und Technologie, Bonn. Köln: Verlag TÜV Rheinland, 1983
96. Joint Aviation Requirements of the European Aviation Safety Agency (EASE) on Basic Regulations, Initial and Continuing Airworthiness (Maintenance), Air Operations, Aircrew Licensing
97. Jones, A. V.: The Regulation of Major Hazards in France, Germany, Finland and The Netherlands.
98. Keller, H.; Plöderer, E.; Dencker, P.; Klenk, H. (Hrsg.): Sicherheit und Zuverlässigkeit für automobile Informationstechnik. Aachen: Shaker Verlag, 2010
99. Keller, H. B. et al.: Programmiersprachen. In: Lang, M.; Scherber, S.: Perfekte Softwareentwicklung. Düsseldorf: symposion Verlag, 2013
100. Keller, H. B.: Ada. In: Henning, P.A. (Hrsg.) Taschenbuch Programmiersprachen. Leipzig: Fachbuchverlag Leipzig im Carl Hanser Verlag, 2004, S. 195–214
101. Keller, H. B.: Im Kampf gegen Cybercrime. Chemie&more, 6.12
102. Keller, H. B.; Müller R.; Schiedermeier, G.; Tempelmeier, T.: Programmierung. In: Benra, J. T. (Hrsg.): Software-Entwicklung für Echtzeitsysteme. Berlin u. a.: Springer, 2009, S. 129–170
103. Kolloquium des Technischen Überwachungs-Vereins Rheinland e. V.: Sicherheitstechnische Bauteilbegutachtung – Nutzung theoretischer und experimenteller Einzelverfahren. Köln: Verlag TÜV Rheinland, 1975
104. Konersmann, R.: Zur Festlegung von Ausschussflächen in Start- und Einflugschneise von Flughäfen und Landeplätzen gemäß Störfallverordnung. Dissertation im Fachbereich Sicherheitstechnik der Bergischen Universität – Gesamthochschule Wuppertal, 1997
105. Konsortium Magnetbahn Transrapid TVE/P/00000/0/RS/1/007 Rahmenspezifikation Sicherheit für das Vorhaben TVE 06.03.80
106. Krause, G.: Maßnahmen zur Verhinderung gefährlicher Vermischungen beim Umfüllen brennbarer Flüssigkeiten. Hrsg.: Bundesanstalt für Arbeitsschutz und Unfallforschung Wirtschaftsverlag NW, Bremerhaven 1, 1979
107. Kreysa, G.; Langer, O.-U.; Pfeil, N. (Hrsg.): Sicherheit bei Lagerung und Transport gefährlicher Stoffe. DECHEMA Frankfurt am Main, 2001
108. Kuhlmann, A. (Hrsg.): 1. Weltkongress für Sicherheitswissenschaft. Tagungsbericht Teil 1 und 2. Köln: Verlag TÜV Rheinland, 1990
109. Kuhlmann, A., Bresser, H.: Einführung in die Sicherheitswissenschaft. Friedr. Vieweg & Sohn, Verlag TÜV Rheinland, 1981
110. Kuhlmann, A.: Sicherheitskultur. Köln: TÜV-Verlag, 2001
111. Lautkaski, R.; Mankamo, T.: Chlorine Transportation Risk Assessment Technical Research Centre of Finland, Nuclear Engineering Laboratory, 1976

112. Leitfaden Informationssicherheit, IT-Grundschutz kompakt. Bundesamt für Sicherheit in der Informationstechnik – BSI53133 Bonn, 2012, BSI-Bro12/311
113. Ludwig, J.; Feutlinske, K.: THEBETA – thermische Belastbarkeit von Tanks. Forschungsvorhaben der Bundesanstalt für Materialforschung und -prüfung für das Bundesministerium für Verkehr, 1996
114. Mair, G. W.: Zuverlässigkeitsrestringierte Optimierung faserteilarmierter Hybridbehälter unter Betriebslast am Beispiel eines CrMo4-Stahlbehälters mit Carbonfaserarmierung als Erdgasspeicher im Nahverkehrsbus. Düsseldorf: VDI Verlag, 1996
115. Marburger, P.: Rechtsprobleme der technischen Sicherheit. Berufspolitische Jahrestagung des VDI "Sicherheit – Wohlstand – Umweltqualität: Zielkonflikte in der Ingenieurarbeit". Trier, 10.–11.09.1984
116. Matthees, W.; Brandes, K.; Liu, W. K.; Belytschko, T.; Droste, B. (Hrsg.): Impact – IV. Extended and Updated Selected Papers from the SMiRT-12 Post-Conference Seminar No. 12. Elsevier Science S.A., 1994
117. Messerschmitt-Bölkow-Blohm GmbH: Technische Zuverlässigkeit 2. Auflage. Berlin, Heidelberg, New York: Springer-Verlag, 1977
118. MIL-HDBK 217F, Notice 2, Reliability Prediction of Electronic Equipment und NPRD 95, Nonelectronic Parts Reliability Data
119. MIL-HDBK-217F, Notice 2 (217F-2) Reliability Prediction of Electronic Equipment Reliability Analysis Center & Rome Laboratory at Griffiss AFB, NY., U.S.A. 1995-02
120. Molnarne, M.; Schendler, T.; Schröder, V.: Sicherheitstechnische Kenngrößen. Band 2: Explosionsbereiche von Gasgemischen. Hrsg.: Bundesanstalt für Materialforschung und -prüfung. Bremerhaven: Wirtschaftsverlag NW, 2003
121. NASA Software Safety Guidebook NASA Technical Standard, NASA-GB-8719.13. Space Administration March 31, 2004
122. National Research Council of the National Academies (Editor): Going the Distance – The Safe Transport of Spent Fuel and High-Level Radioactive Waste in the United States. Washington: National Academic Press, 2006
123. Neddermann, W.; Heins, B.; Dally, A.: Der Human Factor in der Sicherheitspraxis der Prozessindustrie – Aktivierung der Sicherheitsressource Mensch durch Beteiligung. Reihe Loccumer Protokolle. Rehburg-Loccum: Evangelische Akademie Loccum, 2003
124. Nohl, J.; Thiemecke, H.: Systematik zur Durchführung von Gefährdungsanalysen. Teil 1: Theoretische Grundlagen. Hrsg.: Bundesanstalt für Arbeitsschutz. Bremerhaven: Wirtschaftsverlag NW, 1998
125. Nohl, J.; Thiemecke, H.: Systematik zur Durchführung von Gefährdungsanalysen. Teil 2: Praxisbezogene Anwendung. Hrsg.: Bundesanstalt für Arbeitsschutz. Bremerhaven: Wirtschaftsverlag NW, 1998
126. Normenausschuss Bauwesen (NABau) im DIN, Arbeitsausschuss "Sicherheit von Bauwerken": Grundlagen zur Festlegung der Sicherheitsanforderungen für bauliche Anlagen. Berlin, Wien, Zürich: Beuth Verlag, 1981
127. NPRD-95 Nonelectronic Parts Reliability Data IIT Research Institute & Reliability Analysis Center, Rome, NY., U.S.A. 1999-10
128. Paturi, F. R.: 125 Jahre Sicherheit in der Technik. TÜV Bayern Holding AG, 1995
129. Pilz, W.-D.: Sicherheitsmethodische Arbeitsweisen bei der Entwicklung neuartiger Verkehrssysteme. 11. Tagung "Technische Zuverlässigkeit", Nürnberg, 13.–15.05.1981
130. Pilz, W.D.: Technische Probleme des Sicherheitsrechts. Berufspolitische Jahrestagung des VDI "Sicherheit – Wohlstand – Umweltqualität: Zielkonflikte in der Ingenieurarbeit". Trier, 10. - 11.09.1984
131. Pilz, W-D.: Versagens- und Schadensvorsorge aus der Praxis technologischer Entwicklungen. Symposium "Arbeitsschutz im Ingenieurstudium". 20. Deutscher Kongress für Arbeitsschutz und Arbeitsmedizin. Düsseldorf, 03.–06.11.1987

132. Plödereder, E.; Dencker, P.; Klenk, H.; Keller, H. B.; Spitzer, S. (Hrsg.): Proceedings Band 210, Automotive – Safety & Security 2012: Sicherheit und Zuverlässigkeit für automobile Informationstechnik, Tagung 14.–15.11.2012 in Karlsruhe. Bonn: Gesellschaft für Informatik e. V.
133. Programming Languages Guide for the Use of the Ada Programming Language in High Integrity Systems, ISO/IEC JTC 1/SC 22/WG 9 N 359r, 99-07-01, ISO/IEC DTR 15942, ISO/IEC JTC 1/SC22/WG 9, Technical Report type, 1999
134. Proske, D.: Catalogue of Risks – Natural, Technical, Social and Health Risks. Berlin, Heidelberg: Springer-Verlag, 2008
135. Ramberger, S.; Gruber, T.: Error Distribution in Safety-Critical Software & Software Risk Analysis Based on Unit Tests. Experience Report, WSRS Ulm – 20 Sep. 2004. ARC Seibersdorf research GmbH
136. Reaktorsicherheitskommission: Sicherheitstechnische Leitlinien für die trockene Zwischenlagerung bestrahlter Brennelemente in Behältern. Bundesamt für Strahlenschutz, RSK-Geschäftsstelle, 2001
137. Richtlinie 2001/95/EG über die allgemeine Produktsicherheit vom 03.12.2001 (veröffentlicht im Amtsblatt Nr. L 011 vom 15.01.2002)
138. Richtlinie 2008/57/EG des Europäischen Parlaments und des Rates vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft (Neufassung)
139. Ritzau, H. J.: Kriterien der Schiene. Landsberg: Verlag Zeit und Eisenbahn, 1978
140. Ritzau, H. J.: Von Siegelsdorf nach Aitrang. In: Zeit und Bahn, Band 1. Landsberg: Ritzau KG, 1972
141. Sauter, E.: Grundlagen des Strahlenschutzes. Berlin, München: Hrsg. und Verlag: Siemens Aktiengesellschaft, 1971
142. Schäfer, H. K., Jochum, C.: Sicherheit in der Chemie. Hanser Verlag, 1997
143. Schieler, L.; Pauze, D.: Hazardous Materials. New York: van Nostrand Reinhold Company, 1978
144. Schneider, A.; Masé, A.: Katastrophen auf Schienen. Zürich: Orell Füssli Verlag, 1968
145. Schulz-Forberg, B.; Droste, B.; Zeisler, P. (Hrsg.): Erfahrungen und zukunftsträchtige Verfahren auf dem Gebiet der Lagerung und des Transportes von abgebrannten Kernbrennstoffen. 1. deutsch-sowjetisches Seminar in Leningrad, Sowjetunion und 2. deutsch-sowjetisches Seminar in Berlin, Gorleben und Essen, Bundesrepublik Deutschland, 1998
146. Schulz-Forberg, B.; Hübner, H.W.: Klassifizierung und Sicherheitsreserven von Transportbehältern für radioaktive Stoffe. Vom Bundesminister des Inneren gefördertes Forschungsvorhaben mit dem Kennzeichen SR 35, 1979
147. Schulz-Forberg, B.; Masslowski, J.-P.: Prüfablaufanalysen an Beispielen – Darstellung von Grundlagen, Verfahren und Aussagen der Prüfungen. Bundesanstalt für Arbeitsschutz und Unfallforschung, Sonderschrift Nr. 11. Dortmund, 1983
148. Schwaigerer, S.: Festigkeitsberechnung von Bauelementen des Dampfkessel-Behälter- und Rohrleitungsbaues. Berlin, Heidelberg, New York: Springer-Verlag, 1970
149. Sorbe, G.; Stephan, U.; Strobel, U.: Anlagensicherheit und Störfallmanagement – praktische Umsetzung der Störfallverordnung im Betriebsbereich und Arbeitshilfen für Störfall- und Sicherheitsbeauftragte. ecomed Sicherheit in der ecomed Verlagsgesellschaft AG, 2003
150. Spaethe, G.: Die Sicherheit tragender Baukonstruktionen. Wien, New York: Springer, 1992
151. Steinmetz, G.: Im Marionetten-Theater – Freie Fahrt … aber nicht für den Transrapid? Bad Wörishofen: Masona-Verlag, 2014
152. Thierfeldt, S.; Schartmann, F.: Stilllegung und Rückbau kerntechnischer Anlagen. Erstellt im Auftrag des Bundesministeriums für Bildung und Forschung durch die Brenk Systemplanung GmbH. Aachen, 2009
153. VDI 2221:1993-05, Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte

154. VDI 2222 Blatt 1:1997-06, Konstruktionsmethodik – Methodisches Entwickeln von Lösungsprinzipien
155. VDI 2222 Blatt 2:1982-02, Konstruktionsmethodik; Erstellung und Anwendung von Konstruktionskatalogen
156. VDI 2223:2004-01, Methodisches Entwerfen technischer Produkte
157. VDI 4001, Allgemeine Hinweise zum VDI-Handbuch Technische Zuverlässigkeit
158. VDI 4003:2007-03, Zuverlässigkeitsmanagement
159. VDI 4005, Einflüsse von Umweltbedingungen auf die Zuverlässigkeit technischer Erzeugnisse, zurückgezogen
160. VDI 4008 Blatt 5:2014-11, Methoden der Zuverlässigkeit – Zustandsflussgraphen
161. Völkle, H.; Prêtre, S. (Hrsg.): Environmental Impact of Nuclear Installations Proceedings of the Joint Seminary at the University of Fribourg, Switzerland. Les editions de physique, Les Ulis Cedex France, 1992
162. Völzke, H.: Tragverhalten und die Dimensionierung faserverstärkter Druckbehälter. Dissertation an der Technischen Universität, Berlin, 1991
163. Wagner, K.: Sicherheit und Vorschrift. Zu zivilen Lufttüchtigkeitsforderungen. Deutsche Forschungs- und Versuchsanstalt für Luft- und Raumfahrt e. V. Bericht 01972/13
164. ZVEI Automation 2006: Integrierte Technologie-Roadmap Automation 2015+