

## 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

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”<sup>1</sup> 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.

---

<sup>1</sup>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”.

Technical Safety – An Attribute of Quality

An Interdisciplinary Approach and Guideline

Keller, H.; Pilz, W.-D.; Schulz-Forberg, B.; Langenbach, C.

2018, VIII, 190 p. 6 illus., Hardcover

ISBN: 978-3-319-68624-0