Chapter 10

Approaches to Ensuring the Reliability and Safety

Jaroslav Menčík

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/62363

Abstract

This chapter presents various ways to reliability ensuring. The philosophies fail-safe, safe-life and damage-tolerant are explained briefly, as well as deterministic and probabilistic approach. Then, the important methods are explained, such as allowable stress, use of standards, load and resistance factor design, probabilistic approach and proof testing.

Keywords: Reliability, safety, design, fail-safe, safe-life, damage-tolerant design, allowable stress, codes, load and resistance factor design, proof testing, probability

From a reliability point of view, every technical object can be either in a serviceable state or in a failed state.The boundary between both is the **limit state**. Some objects fail suddenly. The condition of other objects changes gradually (e.g. due to wear or corrosion). They are able to fulfill their purpose for a long time, though in a limited extent (worse technical parameters or lower safety); the failure is partial. However, if certain parameter exceeds a specified **limit value**, the object either becomes destroyed or unfit for further use; the failure is complete.

In civil and mechanical engineering, two kinds of limit states are distinguished: limit state of load-carrying capacity and that of serviceability (usability). Exceeding the limit state of load-carrying capacity leads to the destruction of the object, often with fatal consequences. If the limit state of usability is exceeded (e.g. large deformations), the object cannot fulfill its function properly, but the consequences are not fatal. Correspondingly, the demanded degrees of safety of an object can differ depending on the kind of the limit state and consequences of its exceeding.

The boundary between serviceable and failed state can be described by one number (e.g. the stress value, whose exceeding means fracture of the component) or by some analytical expression (e.g. the relationship between the critical load for buckling of a compressed column and its slenderness). Also, the condition of the fracture of a shaft loaded simultaneously by twisting and bending depends on the ratio of both load components; see also Figure 1.

The **basic condition of reliability and safety** says: "The resistance to load effects must be higher than these effects".

1. Basic philosophies for ensuring safety in the design stage

The two most common approaches are (1) Fail-safe and (2) Safe-life. A special case of the safe-life approach is the (3) Damage-tolerant design.

The **Fail-safe approach** understands that the important parts of the object can fail and tries to do everything that such failure will not be fatal for the whole object. This is mostly achieved using redundant components or circuits. **Redundancy** can be **active**, with all parts loaded or working simultaneously, or **standby**, where the redundant component is switched-on only if the principal component has failed; see also Chapter 5.

The **Safe-life approach** tries to do everything to ensure that the component or object can sustain all expectable loads during the assumed life. Basically, it means sufficient dimensioning (the knowledge of all possible loads is important) and the use of materials that do not deteriorate or whose rate of degradation is acceptably low. The dimensioning for "infinite" life of the items exposed to fatigue or ample dimensioning of parts exposed to creep also belongs here.

In contrast to the previous case, which assumed a "perfect" object at the beginning of service, the **damage-tolerant approach** assumes that the component contains some defects (e.g. cracks), which will gradually grow during the operation. The components are dimensioned so that these defects cannot attain critical size during the expected lifetime. The knowledge of the defect growth velocity as a function of load is necessary. This approach uses fracture mechanics, but it is similar to the safe-life approach.

The determination of the time to failure, or dimensioning of a component for the demanded life was explained in Chapter 6.

2. Deterministic versus probabilistic approach

The procedures for the design and check of reliability depend on whether random influences are considered. Some quantities can be considered as deterministic (e.g. the number of teeth in gears or the distance of bearings in a gearbox). Other quantities, such as the strength of material, loads, or action of environment (e.g. wind velocity), have random character, with values varying in some intervals. There are also other sources of uncertainties (e.g. the

http://dx.doi.org/10.5772/62363

computational methods and models characterizing the limit state). Historically, various approaches for ensuring reliability have been developed. They can be divided into two groups: deterministic and probabilistic.

In the deterministic approach, every quantity (load, strength, etc.) is described by one number of constant value. The design in this case is simple, as well as the check of safety, as it will be shown in this section.

The probabilistic approach is based on the fact that some quantities (e.g. load or strength) vary due to random reasons and cannot be sufficiently described by one number only. This approach works with the probability distributions of the pertinent quantities and determines the probability of failure or probability of exceeding the allowable values. The component or structure is considered safe (or reliable) if the probability of failure is lower than certain allowable value.

The probabilistic approach can give more accurate answers but is more demanding than the deterministic approach. It needs a basic knowledge of the probability theory, some computer tools for the work with random quantities (even Excel is sufficient in simple cases), and, of course, the knowledge of probability distributions of the pertinent random variables. If their types and parameters or histograms are not known, this kind of analysis cannot be made. One must also be sure that the statistical characteristics (of the materials or parts) used in the design will correspond to reality. The probabilistic methods for reliability assessment are described in Part 2 of this book.

3. Design using allowable stress

This is a traditional approach in mechanical engineering. The safety condition is

"The maximum operating stress must not exceed the allowable stress".

The allowable stress is obtained by dividing the nominal strength of the material $\sigma_{n,s}$ (ultimate strength or yield stress; do not confuse it with standard deviation) by the so-called **factor of safety** k_S:

$$\sigma_{allow} = \sigma_{n,s} / k_S. \quad (1)$$

The meaning of this factor could be interpreted roughly as "failure would occur at k_S–times higher stress". However, the situation is more complex. The value of safety factor is chosen to "cover" all uncertainties related to the material, the component, and the conditions of operation. Therefore, this approach is also somehow related to probability, but only very loosely. For example, the allowable stress is such value that practically all pieces of this material will be stronger. For metallic parts, σ_{allow} is calculated so that the "minimum" strength, given in material data sheets as 5% quantile (i.e. corresponding to 5% probability that weaker pieces can appear), is divided by a factor of safety, which is chosen, in accordance with the years of

experience, so that the probability that σ_{allow} will be lower than the maximum acting stress is negligibly low.

The factor of safety k_S is a number usually between 1 and 3 and, in some cases even more. Generally, the higher the uncertainties, the higher the k_S. Its values are based on experience; they can be found in the literature; manufacturers use their own well-proven values. The safety factor is often given as a single number (e.g. 2.5), but sometimes it is calculated as the product of several partial coefficients; for example,

$$K_S = s_1 \times s_2 \times s_3 \times s_4 \times s_5 \times s_6, \tag{2}$$

where s_1 characterizes the importance of the component (low or high), s_2 – the technology of manufacturing, s_3 – the material testing, s_4 – the way of strength calculations, s_5 – the quality of manufacturing (e.g. casting or machining by turning or grinding), and s_6 characterizes the possible overloading; s_j is closer to 1 for smaller uncertainty in the j-th factor. This approach enables the consideration of the variability and level of knowledge about the individual factors.

Two values of safety factor should be distinguished. The first is the demanded or target value, which is used in the design stage. The other is the value corresponding to the actual situation. Sometimes, the dimensions of the cross-section (e.g. the wall thickness) should satisfy various criteria, and another criterion than strength can be decisive (e.g. thermal resistance). In such case, the wall will be thicker, so that the actual safety against overloading will also be higher than that originally demanded in design.

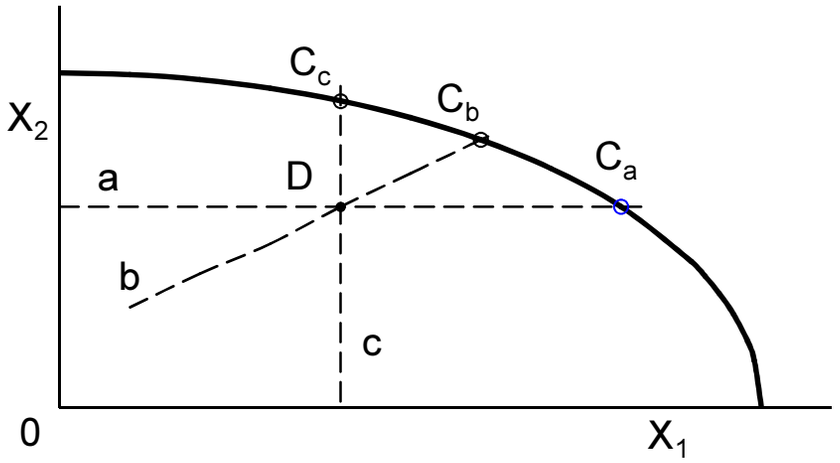

Figure 1. Limit curve, separating safe and failure regions. The failure depends on two quantities: X_1 and X_2. Curves a,b,c show the various paths of overloading.

When the safety against overload is to be determined, one should consider the actual "path" of overloading leading to the collapse (Fig. 1). Sometimes, several loads act simultaneously, but some of them are constant, such as the dead weight of a bridge, and only some can increase,

http://dx.doi.org/10.5772/62363

for example the traffic load. The actual safety against overloading by traffic is here obtained as the ratio of the actual traffic load at the instant of collapse to the nominal traffic load. These issues are important in dimensioning. A misunderstanding of the term "safety" can lead to unnecessarily high costs.

4. Design according to standards

Standards are often used for the design and dimensioning of bridges, cranes, pressure vessels, and many metal or other important constructions. Also, vehicles, aircrafts, and electric appliances are often designed using various standards, such as ISO, ASME, or Euro-codes; see Appendix 2. In some cases, their use is compulsory, but sometimes it is only a matter of agreement between the manufacturer and the customer. The advantage of standards is that they are usually created as a result of cooperation of many specialists, often from various countries, and are based on a thorough analysis and experimental verification. They are updated from time to time to reflect the progress in the state of knowledge. Generally, standards represent an efficient way for obtaining safe items and constructions. The advantage for the design engineer, manufacturer or builder is that the design and calculations according to proven formulas and procedures in standards are straightforward and simple. Moreover, if the structure fails and the designer or builder can prove that he has done everything according to the standards, he cannot be prosecuted. On the contrary, the design according to codes is somewhat conservative, and the standards do not solve all eventualities (e.g. certain combinations of loads). In such cases, other approaches can be more appropriate.

5. Load and Resistance Factor Design (LRFD)

This approach is common in the design of civil engineering structures, where it is used in some standards, e.g. for steel constructions [1]. The safety condition, in general, is

"The design value of load effect must not exceed the design value of the resistance."

The term "design value" means the value assumed in design (e.g. recommended or prescribed in a standard), because the actual values are not known exactly yet.

For a component or structure, this condition can be written as

$$\gamma_n S_d \leq R_d; \tag{3}$$

S_d is the effect of maximum load, R_d is the resistance (e.g. the load-carrying capacity or the allowable deformation), and γ_n is the factor characterizing the purpose of the object. The subscript **d** means "design" and denotes the value considered in design; the pertinent standards usually show how the design value is related to the mean or nominal value.

In this approach, the uncertainties are divided into two groups: those related to the load and those related to the material or components. The design value of the load effect F_d is obtained as the product of characteristic load F_k and partial safety factor γ_F for the load,

$$F_d = \gamma_F F_k. \tag{4}$$

The design value of the resistance (or strength) f_d is obtained as the characteristic value of strength f_k divided by the partial factor of reliability of the material γ_m; for example

$$f_d = f_k / \gamma_m; \tag{5}$$

f_k can be either the characteristic value of the yield strength or the ultimate strength (e.g. 5% quantile). The characteristic values and the partial safety factors are given in pertinent standards (e.g. [1]).

As we can see, the actual values of loads and properties were replaced in the LRFD approach by the design values given in codes. This approach is reasonably conservative and the procedures are arranged so that they enable fast control in standard cases.

Note: Load and resistance are also used in the determination of failure probability in the so-called load-resistance interference method, as described in Chapter 14.

6. Probabilistic approach

If probabilistic approach to reliability assessment is used, only general recommendations for allowable probabilities can usually be found instead of definite obligatory values. Generally, the allowable probability of a failure should be related closely to its consequences. Some idea about these probabilities can be obtained from two examples. The first one is from aviation technology. Usually, 1:10,000 is the acceptable probability of critical failure for an aircraft at the end of its service life, just before decommissioning. The acceptable probability of failure at the time of its putting into service must be several orders lower.

The second example is the Eurocode for metal constructions [1], which gives the following design probabilities of failure for the limit states of load-carrying capacity and usability. They are differentiated according to the assumed level of reliability or safety, as given in Table 1.

The above numbers correspond to the reliability of the whole object. If it consists of many components, the failure probabilities of single elements must be appropriately lower (see Chapter 6), of the order 10^{-5} to 10^{-10}. Similarly, if reliability is assessed via failure rate, the allowable failure rates of elements must be very low. In such cases, specific problems arise in design. First, it can be difficult to prove very high reliability of the pertinent item, because the number of tested samples must be high and the duration of tests are very long. For example, the failure rate of 10^{-6} h^{-1} could be (roughly) verified in a test with one component tested for 10^6 h or with 1,000,000 components tested for 1 h. None of these cases is practicable and a

Reliability level	Limit states of:	
	Load-carrying capacity	Usability
Reduced	5×10^{-4}	16×10^{-2}
Usual	7×10^{-5}	7×10^{-2}
Increased	8×10^{-6}	23×10^{-3}

Note: The unrounded numbers in Table 1 look rather strange. The reason is that reliability index β (see Chapter 14) was used originally instead of probabilities, and the relationship between β and P_f is nonlinear (e.g. $P_f = 23 \times 10^{-3}$ corresponds to reliability index $\beta = 2.00$; see the distribution function of standard normal distribution).

Table 1. Recommended design probabilities of failure P_f [1]

compromise must be found. Another example is related to the guaranteed strength. The value of 0.001% quantile of strength, determined from three tests only, does not make great confidence. Many more tests would be better. However, this would also cost much more money. The big manufacturers of standard electric and electronic components can make extensive tests and use sophisticated techniques for testing and processing the results, as it will be mentioned in Chapter 20, so that their data are trustworthy. Often, however, the means for testing are much more limited, and the predictions are less safe. Usually, the allowable reliability is a compromise between the demands for high reliability and the money available for reliability ensuring. In some cases, the optimum reliability can be found from the condition of minimum total costs consisting of the purchase costs and the costs caused by failure. This topic is treated in Chapter 17. However, this approach cannot be used if very high reliability or safety is demanded. In some cases, the so-called **ALARP** philosophy is used, demanding that the risk should be "as low as reasonably practicable".

Generally, the demands for increasing reliability should not be unrealistically high. Useful information on the actual situation can be obtained from the statistics of failures. If the current probability of failure of a certain item is $1{:}10^2$, it will be easier to reduce it to $1{:}10^4$ than $1{:}10^8$.

In some cases, quite different approaches are used for guaranteeing very high reliability. Sometimes, certain technologies or activities are prescribed or, vice versa, forbidden by law (e.g. building family houses in the areas endangered by flooding or avalanches). Another means is proof testing, as explained in the following paragraph.

7. Proof testing

In these tests, all components are exposed to certain overload, so high that the "weak" parts are destroyed during the test. Destruction is complete with components of brittle materials, whereas the ductile parts are often only permanently deformed. (For example, overpressure tests common for pressure vessels belong also to proof tests.) Basically, it is sufficient if the proof-test stress or load is equal to a certain value higher than the maximum load expectable in service. In some cases, proof tests are also used for ensuring a sufficient life of components from brittle materials exposed to static fatigue due to the corrosive action of environment. This

fatigue causes very slow growth of preexisting minute cracks until the critical size. The methods of fracture mechanics together with the knowledge of the velocity of subcritical crack growth under stress enable the calculation of the necessary proof-test stress guaranteeing a sufficient life of the parts that have passed the test. Such approach was used, for example, in the design of glass windows in the American orbital laboratory Skylab [2, 3]. Theoretical foundations of proof testing are explained in detail in [2, 3] and [4].

Author details

Jaroslav Menčík

Address all correspondence to: jaroslav.mencik@upce.cz

Department of Mechanics, Materials and Machine Parts, Jan Perner Transport Faculty, University of Pardubice, Czech Republic

References

[1] ENV 1993-1-1 Eurocode 3. Design of steel structures. (also Czech standard ČSN 731401, 1998.)

[2] Jacobs D F, Ritter J E jr. Uncertainty in minimum lifetime predictions. J. Am. Ceram. Soc. 1976; 59: No. 11/12, 481 – 487

[3] Wiederhorn S M, Fuller E R jr, Mandel J, Evans A G. An error analysis of failure prediction techniques derived from fracture mechanics. J. Am. Ceram. Soc. 1976; 59: No. 9/10, 403 – 411

[4] Menčík J. Strength and fracture of glass and ceramics. Amsterdam: Elsevier; 1992. 357 p.