 Original article
https://doi.org/10.21683/1729-2646-2020-20-1-47-56

Comprehensive analysis of the strength and safety of potentially hazardous facilities subject to uncertainties

Nikolay A. Makhutov[1], Dmitry O. Reznikov[1]*

[1] *Mechanical Engineering Research Institute of the Russian Academy of Sciences, Russian Federation, Moscow*
* *mibsts@mail.ru*

Nikolay A. Makhutov

Dmitry O. Reznikov

Abstract. *Aim. This paper aims to compare the two primary approaches to ensuring the structural strength and safety of potentially hazardous facilities, i.e. the deterministic approach that is based on ensuring standard values of a strength margin per primary limit state mechanisms, and the probabilistic approach, under which the strength condition criterion is the non-exceedance by the target values of probability of damage per various damage modes of the standard maximum allowable values.* **Methods.** *The key problem of ensuring the structural strength is the high level of uncertainties that are conventionally subdivided into two types: (1) the uncertainties due to the natural variation of the parameters that define the load-carrying ability of a system and the load it is exposed to, and (2) the uncertainties due to the human factor (the limited nature of human knowledge of a system and possibility of human error at various stages of system operation). The methods of uncertainty mitigation depend on the approach applied to strength assurance: under the deterministic approach the random variables "load" and "carrying capacity" are replaced with deterministic values, i.e. their mathematical expectations, while the fulfillment of the strength conditions subject to uncertainties is ensured by introducing the condition that the relation of the mathematical expectation of the load-carrying capacity and strength must exceed the standard value of strength margin that, in turn, must be greater than unity. As part of the probabilistic approach, the structural strength is assumed to be ensured if the estimated probability of damage per the given mechanism of limit state attainment does not exceed the standard value of the probability of damage.* **Conclusions.** *The two approaches (deterministic and probabilistic) can be deemed equivalent only in particular cases. The disadvantage of both is the limited capability to mitigate the uncertainties of the second type defined by the effects of the human factor, as well as the absence of a correct procedure of accounting for the severity of consequences caused by the attainment of the limit state. The above disadvantages can be overcome if risk-based methods are used in ensuring structural strength and safety. Such methods allow considering uncertainties of the second type and explicitly taking into consideration the criticality of consequences of facility destruction.*

Keyword: *structural strength, safety, uncertainty, strength margin, probability of damage, risk.*

For citation: *Makhutov N.A., Reznikov D.O. Comprehensive analysis of the strength and safety of potentially hazardous facilities subject to uncertainties. Dependability. 2020;1: 47-56. https://doi.org/10.21683/1729-2646-2020-20-1-47-56*

Received on: *02.11.2019 /* ***Revised on:*** *12.02.2020 /* **For printing:** *20.03.2020*

1. Introduction

Structural strength represents the initial complex characteristic of a technical system, which is described as a combination of differentiated indicators of static, dynamic, cyclic strength and strength reliability, and determined by the ability of the system to withstand various limit states in real operating conditions. The fulfillment of the structural strength requirements of the potentially hazardous facilities (PHF) is the key element of ensuring technological safety [1, 2]. Structural strength is deemed to have been ensured when for all involved limit state mechanisms the following condition is satisfied:

$$Q_i^S / Q_i^O > 1 \ (\forall_i = 1,2,\ldots,m), \quad (1)$$

where Q_i^S and Q_i^O are the parameters of a load-carrying capacity with the *i*-th limit state mechanism associated with negative consequences in the form of economic losses and casualties; *m* is the number of limit state mechanisms. As the analysis of national and foreign information sources on the scenarios of technological accidents and disasters shows, this interpretation of the structural strength provides the basis for research, regulation and ensuring technological safety.

There are three main matters related to ensuring structural strength and safety of PHF for all life cycle stages:

- calculation and experimental analysis of the stress-strain states taking into account mechanical Q_m^O, thermal Q_t^O, aerohydrodynamic Q_{ah}^O, electromagnetic Q_{em}^O, radiation and chemical Q_r^O effects. In addition, local stress σ^O_{max} and strain e^O_{max} depend on operating number of load cycles N^O, time τ^O and temperature t^O:

$$\left\{\sigma^O_{max}, e^O_{max}\right\} = F_O\{P^O, Q_t^O, Q_{ah}^O, Q_{em}^O, Q_r^O, N^O, \tau^O, t^O\}; \quad (2)$$

- analysis of the laws of cyclic and elastic and elastic-plastic deformation within and outside the concentration zones for varying frequencies f_τ, stress amplitudes σ_a^O and deformations e_a^O, temperatures t^O and time τ^O:

$$\left\{\sigma^O_{max}, e^O_{max}\right\} = F_{1O}\{f_\tau, \left(\sigma_a^O, e_a^O\right), t^O, \tau^O\}; \quad (3)$$

- analysis of the criteria and conditions for the damage accumulation d^O, as well as the determination of the cyclic life N_C^O for the stages of the formation and development of cracks, and damages:

$$\left\{d^O, N_C^O\right\} = F_{2O}\{f_\tau, \left(\sigma_a^O, e_a^O\right), t^O, \tau^O\}. \quad (4)$$

The tasks of ensuring the structural strength of potentially hazardous facilities are solved under conditions of a high level of uncertainty regarding operation loading on the one hand, as well as load-carrying capacity of PHF elements at various stages of its operation cycle, on the other hand [3-5]. Uncertainty factors include: natural variety of object's parameters (geometrical dimension, mechanical characteristics of the material); stochastic nature of the degradation processes and loading modes; limited knowledge of the developments and processes in load-carrying elements; limited available statistic data; imperfection of the used mathematical model; inaccuracy of the available measurement equipment.

Structural strength of PHF at different stages of its life cycle can be ensured through two radically different approaches [3, 4, 7, 8]:

1) Deterministic (normative) approach to ensuring structural strength that is based on ensuring standard values of the strength margin per primary limit state mechanisms.

2) Probabilistic approach to ensuring structural strength that is based on reducing the probability of reaching the limit state to the level that is acceptable at the defined level of technology development.

For many centuries, the first approach has been developing. It implies that uncertainties during design, development and operation of technical systems were taken into consideration through the use of a system of strength margins for various limit state mechanisms. The second approach became widespread in the middle of the 20th century with the development of such disciplines as probability and reliability theories for assessing uncertainties using the probability of system reaching the limit state. This approach has become an important element in the development of the theory of technical risks and safety. A comparative assessment of the deterministic and probabilistic approaches and conditions for equivalence will be discussed below.

2. Uncertainties of the problem

The uncertainties related to ensuring structural strength of technical systems of PHF can be divided into two fundamentally different types [9-14]:

1) Uncertainties of natural, material and technical behavior caused by non-determination of parameters, events and processes of the real world. This type includes the uncertainties related to the variability of the system parameters and effects on it with the stochastic nature of the degradation processes of its characteristics, as well as the uncertainties caused by possible deviations from nominal values of impact intensity of external and internal force factors, operating modes, geometric dimensions of the system's elements, mechanical and physical properties of materials, environmental conditions, etc.

2) Uncertainties related to the human factor (in a broad sense) are divided into: (a) uncertainties related to the limited knowledge of the designer, manufacturer and operator regarding complex technical systems of PHF and operating conditions (in particular, the nature of the complex processes of reaching limit states of the system); (b) uncertainties caused by the possibility of personnel's actions leading to a violation of the existing standards for design, construction and operation of PHF, as a result of which system properties (behavior, characteristics) will be different from the design and planned (i.e. failures at the design, development and operation stages of the system); and (c) uncertainties caused

by the possibility of unauthorized action (sabotage/terrorism) against PHF under consideration.

As the limited knowledge of technical systems of PHF and neglect of important factors caused by it, as well as the violation of the established standards can be regarded as a kind of failures, then the group of uncertainties caused by the human factor can be called, for short, the uncertainties related to the failures made by designers, developers and operators of PHF, where the term *failure* is used in a broad sense.

The particularity of PHF protection against accidents and disasters is that their description requires the consideration of a vast number of factors. At the same time, a number of PHF operating modes become underdetermined [15]. This is due to the complex nonlinear interactions of the PHF components, the strong connection between the various subsystems, as well as the fact that PHF and environment change faster than they can be described and studied. Therefore, there is a situation of lack of information about the development of hazardous processes in PHF, and thereby, limitations for predicting their behavior and managing them. At the same time, it is impossible to describe in detail the principles of PHF operating and develop management rules in certain modes. A distinctive feature of the underdetermined systems is the inability of the full description of their behavior and prediction of their state under various conditions and in different operating modes. The distinction between fully determined and underdetermined systems becomes extremely important when developing a set of security measures.

Uncertainties of the first type are considered within the framework of the strength reliability theory. However, the experience in operating technical systems shows that the estimates of the system breakdown probabilities obtained via methods of reliability theory are significantly underestimated and differ from the values observed in practice by at least an order of magnitude. The main reason for this discrepancy is that the theory of the strength reliability does not take into account the uncertainties of the human factor, which are dominant in many cases. The second type of uncertainty is assessed within the framework of new approaches focusing on the study of the human factor.

3. Deterministic approach to ensuring structural strength

As part of the deterministic approach, the random parameters of load Q_i^S and carrying capacity Q_i^O are replaced with their mathematical expectations $E\{Q_i^S\}$ и $E\{Q_i^O\}$, and the fulfillment of the strength condition taking into account the uncertainties is ensured by adding into the right member of the inequality (1) of the standard allowable margin $[n_i]$, which must be greater than one:

$$n_i = \frac{E\{Q_i^S\}}{E\{Q_i^O\}} > [n_i] \; i = 1,2,\ldots,m. \qquad (5)$$

The matter of strength margin $[n_i]$ selection is very complex. The standard strength margin for the considered limit state is assigned based on: the experience of operating such systems; uncertainty level; socio-economic conditions in the country; the accuracy of the computational models and the level of damage expected in case the limit states are reached. Thus, the values of the strength margin are determined by both objective factors (the uncertainty level in relation to the loads and carrying capacity of the structure; the criticality of consequences associated with limit state achievement) and subjective circumstances (safety culture in particular sectors and in the country as a whole, threats perception by society). Current values of standard margins for structural elements of technical systems for various purposes vary within the ranges below (Table 1).

Table 1. Values of the standard strength margin

	Sector, type of technical system	Range of values [n]
1	Space technology	1.00…1.25
2	Aviation technology (airframe)	1.25…2.0
3	Equipment and pipelines of nuclear power plants	1.07…3.0
4	Vessels and machines operating under pressure	1.5…4.0
5	Metallurgical equipment	2.07…8.0
6	Railway transport	3.33…5.56
7	Handling machinery	1.3…1.6

The data presented in Table 1 shows that the values of the standard margins significantly vary (both within particular sectors and between sectors). This demonstrates not only the lack of a single methodological framework for their substantiation, but also the difference in the sector-specific PHF risk levels. The application of this approach when designing new (unique) objects is fraught with great difficulties and high uncertainty level, associated with the lack of experience in assigning allowable margins for limit states that can be implemented in the system.

It should be noted that PHF consisting of complex systems is characterized by the various limit states corresponding to different damage mechanisms (single overload, cumulative mechanism of fatigue, long-term, corrosion, thermal cyclic damage, etc.). In this case, the system of margins n_1, n_2, …, n_q for the basic limit state mechanism is used. The margins for various limit states also normally prove to be unconnected. Additionally, the system may have excess strength per some limit states and insufficient per others.

The results of experimental and calculation studies using samples, models and full-scale structures allow determining margins for stress n_σ, strain n_e, number of cycles n_N, time n_τ and defect (crack) size n_l:

$$\left\{n_\sigma, n_e, n_N, n_\tau, n_l\right\} = \left\{\frac{\sigma_S}{\sigma_{max}^O}, \frac{e_S}{e_{max}^O}, \frac{N_S}{N^O}, \frac{\tau_S}{\tau^O}, \frac{l_S}{l^O}\right\}, \qquad (6)$$

where "*S*" refers to the critical (limit) value of the corresponding characteristic of strength, durability and crack resistance, and "*O*" refers to the corresponding values in operation.

The generalized surfaces of the limit (hazardous) states of V^S are constructed based on expressions (2) – (4) (Fig. 1). The surface of the allowed states [*V*] is determined upon the construction of the limit state surface by adding the margin coefficients $[n_i]$ for each of the specified limit parameters in accordance with the corresponding coordinate of the state space:

$$[V_i] = V_i^S / [n_i].$$

The condition for ensuring structural strength and safety is that the time varying vector of operational states V^O throughout all life cycle stages remains within the area of permissible states that is below the surface of the permissible states [*V*].

Deterministic approaches are usually used at the initial stage of the design to determine the size of the most loaded sections of the designed structural elements, when there is no sufficient statistical material for the analysis with significant changes in the construction and their operating conditions. The task of ensuring the strength of the structural elements of technical systems has traditionally been solved through the application of deterministic approaches which allow compensating for the uncertainties by adding differentiated margins for the basic limit state mechanisms based on the experience of PHF design and operation. However, with the rapid development of technologies and implementation of new structural material, the possibilities of the normative deterministic approach are close to exhaustion.

4. Probabilistic approaches to ensuring structural strength

Probabilistic approaches to ensuring structural strength are based on reducing the probability of reaching limit states to a specified level. Within the framework of the probabilistic approach, structural strength is ensured if the calculated probability of damage by the *i*-th mechanism of reaching limit state $P_{Fi} = P\{Q_i^S/Q_i^O < 1\}$ does not exceed the standard value of damage probability $[P_F]$:

$$P\{Q_i^S / Q_i^O < 1\} \le [P_F], \quad \forall i = 1,2,\ldots,m. \qquad (7)$$

Probabilistic approaches are effective when significant amounts of initial statistical information on levels of operating loads and variability of the basic mechanical properties of carrying structural elements of PHF have been accumulated (or can be obtained). The above approaches, with their numerical implementation, allow determining the probabilistic initial characteristics of strength, service life and survivability and enable the quantification the most important damage parameters *U*, identification of the risk *R*, safety *S* and protection *Z*.

For high-risk PHF, the variations of τ^O, N^O reach 5-8 orders of magnitude, t^O reaches 4 orders of magnitude, l^O reaches 3 orders of magnitude, *P* reaches 10 orders of magnitude, *U* reaches 6 orders of magnitude, *R* reaches 3-4 orders of magnitudes [1, 2]. The value of margins $[n_i]$ vary within the same order ($1 \le [n_i] \le 10$).

Probabilistic approaches to ensuring structural strength have been in development since the middle of the 20-th century, first within the framework of the classical strength theory, and later as part of the strength reliability theory. The limit permissible value of the damage probability $[P_F]$ is set depending on the value of damage that may occur in case of failure, taking into account the social significance of the object and its useful life. In particular, the Construction Industry Research and Information Association (CIRIA) proposed the following interpolation formula for estimating the maximum permissible calculated probability of damage [3] of complex engineering structures (dams, bridges, offshore platforms):

$$[P_F] = \frac{10^{-4}\xi_S \cdot \tau}{L \cdot k_{HF}}, \qquad (8)$$

where τ is the estimated useful life of the system; *L* is the average number of people who may die in case of a system failure; k_{HF} is the coefficient that takes into account damage associated with the human factor (usually, k_{HF} = 10); ξ_S is the coefficient of the system's social significance (see Table 2). Thus, the value $[P_F]$ is usually in the range of $1 \cdot 10^{-5} \ldots 1 \cdot 10^{-7}$.

Table 2. Coefficient of social significance for various types of technical systems

Type of system	ξ_S
Places of mass gathering (sport centers, shopping centers)	0.005
Dams	0.005
Residential buildings, office centers, industrial plants	0.05
Bridges	0.5
Drilling rigs, offshore installations	5

It should be noted that formula (8) takes into account the uncertainties associated not only with the random nature of the loads and carrying capacity of structures, but also with the uncertainties caused by the human factor. This is achieved by adding coefficient k_{HF}, which, as a rule, equals 10. The so-called theoretical maximum permissible probability of damage $[P_{F,T}]$ is often mentioned in regulatory documents; this probability is estimated without taking into account possible failures or unauthorized human actions and is significantly lower than $[P_F]$. It is generally accepted that these values differ by one order of magnitude.

Today, the probabilistic approach to ensuring structural strength is increasingly implemented into the practice of a

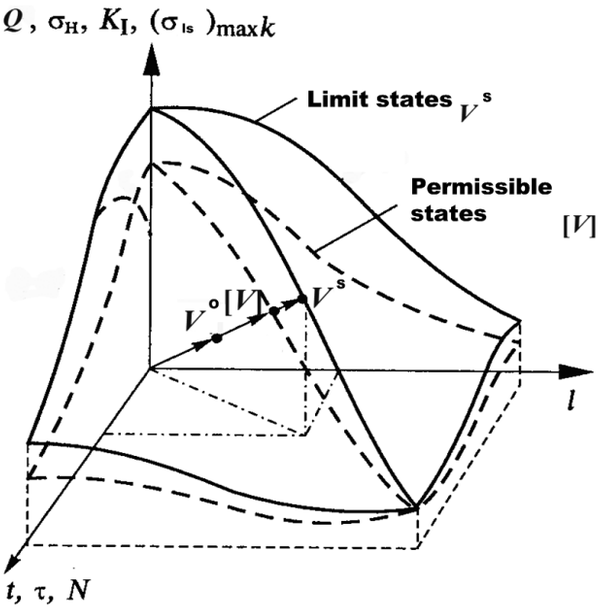

Figure 1 – Surface construction for limit and permissible states as part of assessing the strength, lifetime and survivability in a three-dimensional space of object states

number of industries, in particular, in the design of nuclear power facilities, hydraulic structures, offshore oil and gas platforms, shipbuilding, etc.

It should be noted that the social significance coefficient ξ_S of the system in formula (8) allows implicitly and highly approximately taking into account the scale of possible destruction consequences when deciding whether the considered system is protected. More comprehensive and mathematically correct way for considering destruction consequences is implemented as part of an integrated approach to ensuring strength and safety, which is based on the risk theory.

5. Comparison of deterministic and probabilistic approaches

It should be noted that designing and assuring the strength, life and safety of the PHF structural elements as part of the deterministic approach, which is based on margins, is less labour-consuming. Subject to this approach, in order to make sure that expression (5) is true, the relation $E\{Q_i^S\}/E\{Q_i^O\}$ should only be evaluated once, while the calculation by the probabilistic criterion (7) requires a multiple evaluation of Q_i^S/Q_i^O. Unfortunately, the deterministic approach, despite its simplicity, lacks analytical rigor and accuracy as well as uncertainty management. The human factor and experience in operating same-class systems in similar environmental conditions play a significant role in assessing the strength and life. The applicability of the deterministic approach when designing unique objects, for which there is no relevant statistical information, is very limited. Furthermore, the deterministic approach does not enable the optimization of the designed system, since it does not allow comparing the costs of its creation with a given margin and the positive

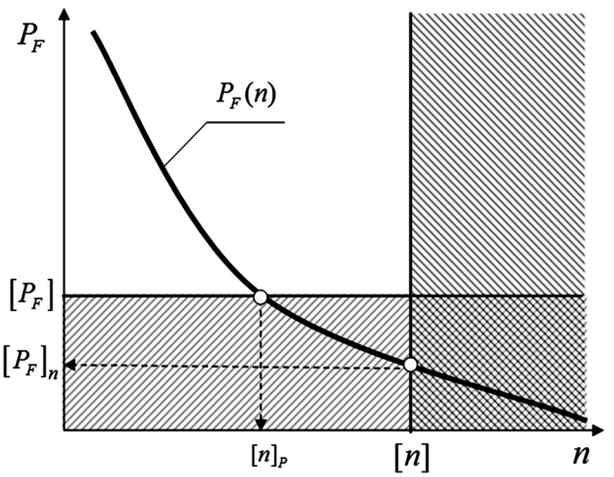

Figure 2 – Relationship between strength margin and damage probability

effect associated with an increase in strength that cannot be calculated without answering the question: *To what level can the probability of damage be reduced, if the fulfillment of the designated margin is ensured?* Thus, the deterministic approach does not allow selecting the optimal variant from a number of possible systems.

On the contrary, designing and ensuring structural strength by the criterion of dependability is a fairly rigorous mathematical procedure in terms of managing the load and carrying capacity-related uncertainties. This criterion allows making informed decisions when designing a system under uncertainty, making comparative assessments of strength and life for various parameters of the designed element and performing optimization. However, the probabilistic approach is labour-consuming and requires a highly qualified designer.

Therefore, it would be useful to combine the advantages of both approaches to obtain, when possible, the relationship between the strength margin and the probability of damage. For example, this would allow evaluating the safety of a structural element designed with a given strength margin according to reliability criteria. Another important task consists in comparing the areas of protected states Ω_n and Ω_P, obtained by the safety criterion and the reliability criterion, respectively.

Based on the general principles of the reliability and strength theory, it can be assumed that, at least in some cases, there is a monotonously decreasing function between the strength margin n and the probability of damage P_F (Fig. 2). When this assumption is true, deterministic and probabilistic approaches can be considered equivalent. Then, if the deterministic approach is used, the limit probability of damage $[P_F]_n$, corresponding to the normative margin $[n]$, can be determined. Similarly, if the probabilistic approach is used, the limit value of margin $[n]_P$, corresponding to the maximum allowable probability of damage $[P_F]$, can be determined.

Unfortunately, in the general case there is no one-to-one correspondence between the values of $[n]$ and $[P_F]$,

and, therefore, these two approaches cannot be considered equivalent. However, such functions can be obtained for a number of special cases.

Let us consider the equivalence of the deterministic and probabilistic approaches for cases of single static loading. Per the deterministic approach, the condition for ensuring strength (1) and (5) can be rewritten as:

$$n \geq [n], \tag{9}$$

where Q_S and Q_O are parameters characterizing static strength and load; $n=E\{Q_S\}/E\{Q_O\}$ is the actual margin, which should not be lower than the standard minimum allowable margin $[n]$. Thus, margin n is determined by the ratio between the mathematical expectations of the load and the carrying capacity values.

Obviously, the introduction of margins cannot completely eliminate the possibility of system damage. Therefore, when the deterministic approach is used, the question arises of what limit probability of damage $[P_F]$ corresponds to a given standard margin $[n]$.

In the deterministic approach, which is based on assigning margins, only the ratio between the characteristic values of the distributions is taken into account (in this example, between mathematical expectations of load and carrying capacity $E\{Q_C\}/E\{Q_Э\}$).

If the values of Q_S and Q_O are uncorrelated and normally distributed, probability of damage can be estimated using a well-known expression [3, 6]:

$$P_F = \mathrm{F}\left(-\frac{E\{Q_S\} - E\{Q_O\}}{\sqrt{\left(S\{Q_S\}\right)^2 + \left(S\{Q_O\}\right)^2}} \right), \tag{10}$$

$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} exp\left(-\frac{t^2}{2}\right) dt$ is normal distribution function.

If coefficients of variation $v_{Q_O} = \frac{S\{Q_O\}}{E\{Q_O\}}$ and $v_{Q_S} = \frac{S\{Q_S\}}{E\{Q_S\}}$ are introduced, the required function takes the form:

$$P = \mathrm{F}\left(-\frac{n-1}{\sqrt{v_{Q_O}^2 + v_{Q_S}^2 \cdot n^2}} \right), \tag{11}$$

Thus, assuming the load and carrying capacity are normally distributed, and specifying the fixed values of variation coefficients v_{Q_S} and v_{Q_O} (which shall be considered invariant), the relationship between the probability of reaching the limit state and the strength margin can be built. Which is to say, in the case of normally distributed, uncorrelated Q_S and Q_O, if the variation coefficients v_{Q_S} and v_{Q_O} stay constant when the system parameters vary, then the probability of damage depends only on strength margin n.

In other words, formula (11) suggests that approaches based on assigning margins and reliability theory are equivalent when the coefficients of variation v_{Q_S} and v_{Q_O} do not change when the design parameters vary.

Figure 3 shows dependencies between probability of reaching limit state $P_F\left(n \mid v_{Q_O *}, v_{Q_S *}\right)$ and margin n for different values of load and strength variation coefficients v_{Q_S} and v_{Q_O} plotted in linear coordinates.

In strength reliability theory the system is considered protected if the calculated probability of local damage of the critical element is less than the standard value of the maximum permissible probability of damage: $P_F < [P_F]$.

According to (11), probability of damage P_F is a function of tree variables: central margin n, load variation coefficient v_{Q_S} and carrying capacity variation coefficient v_{Q_S}. Hence, there can be three methods of ensuring structural strength: increasing the margin, reducing the variation in strength, reducing the variation in load. The protection method is selected taking into account the specifics of the industry and operating conditions of systems. In those industries where there are no strict restrictions on the weight of

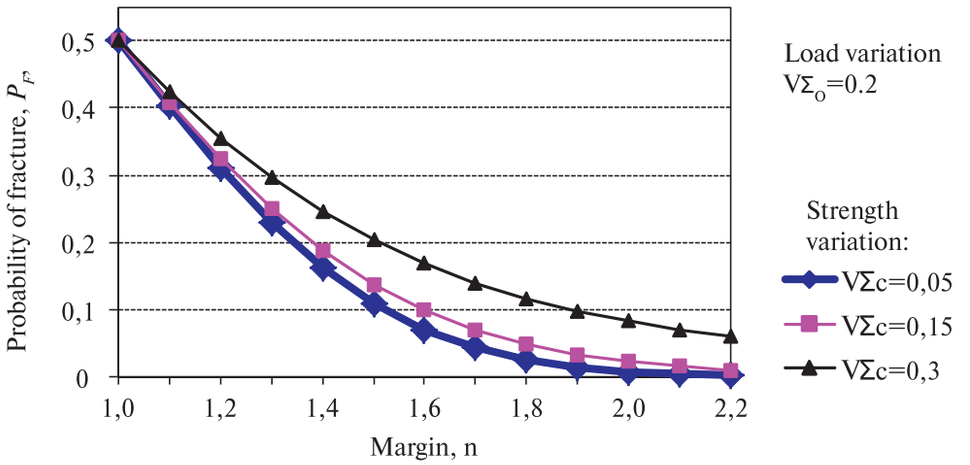

Figure 3 – Dependence of the probability of local damage on the margin for various combinations of load variation coefficients and strength at $v_{Q_O} = 0$

structures (nuclear energy, construction), protection can be mainly achieved by increasing the margins n = 2…5. In aerospace systems, where the requirements of weight limitation are dominant and, therefore, the margins cannot exceed 1.2 ... 1.6, ensuring protection should focus on reducing load variations and on the basic mechanical properties of materials.

6. Methods of compensating for uncertainties in structural strength and safety assurance

Damage of PHF due to technical factors is considered in the framework of the classical strength reliability theory. The traditional method of compensating for uncertainties associated with the variability of the load and the carrying capacity parameters is to introduce margins n.

The introduction of margins cannot completely eliminate the possibility of system damage. Therefore, when the normative deterministic approach is used, the question arises of what probability of damage $P(F)$ corresponds to the calculated margin n (Fig. 4). The relationship between the margin and the probability of damage (accidents and catastrophes) when there is an exact or approximate relationship between these quantities was addressed in detail in [3, 4, 7, 8].

The probability of damage due to human factor may also depend on the margin. However, it should be noted that operator errors can not only change the relative position of the load distribution and carrying capacity curves, but also lead to a change in the system probabilistic model itself, creating new functions of limit states or changing the dimension of the state space. Moreover, increasing margins for the initial limit state cannot compensate for the uncertainties introduced by errors [9].

In accordance with the types of uncertainties discussed in Section 2 above, two types of causes of PHF damage (accidents, catastrophes) can be distinguished:

- damage F_V caused by the variability of the state function. The probability of such event is estimated as $P(F_V)$;
- damage F_E caused by the human factor (or errors in the broad sense of the term), the probability of which is estimated as $P(F_E)$.

The simplest scenario model, which takes into account the uncertainties of these two types, can be represented by an event tree (Fig. 5) containing generalized scenarios of damage (accidents, catastrophes) due to technical reasons and the human factor [10]. For this model, let us assume that damage F to the system as a whole can occur when the system reaches the limit states due to (a) the damage of individual elements due to the variability of the limit state function, and (b) the errors of designers, builders or users made at different stages of the life cycle. Then, event F can be seen as a combination of two events: F_V, damage due to the variability of the technical parameters, and F_E, damage due to error (human factor): $F = F_V \cup F_E$. In this case, the probability of system damage can be expressed as:

$$P(F) = P(F_V \mid \bar{E}) \cdot P(\bar{E}) + \left[P(F_E \mid E) + P(F_V \mid E)\right] \cdot P(E), \quad (12)$$

where $P(E)$ is probability of error; $P(F|E)$ is conditional probability of damage due to error if an error is made; $P(F_V|E)$ is conditional probability of damage due to the variability of the technical parameters if an error is not made; $P(\bar{E}) = 1 - P(E)$ is probability of no error.

Traditional reliability theory focuses on estimating the value of $P(F_V|\bar{E})$, which describes the probability of PHF damage when no errors were made. However, the experience of PHF operation suggests that from 70 to

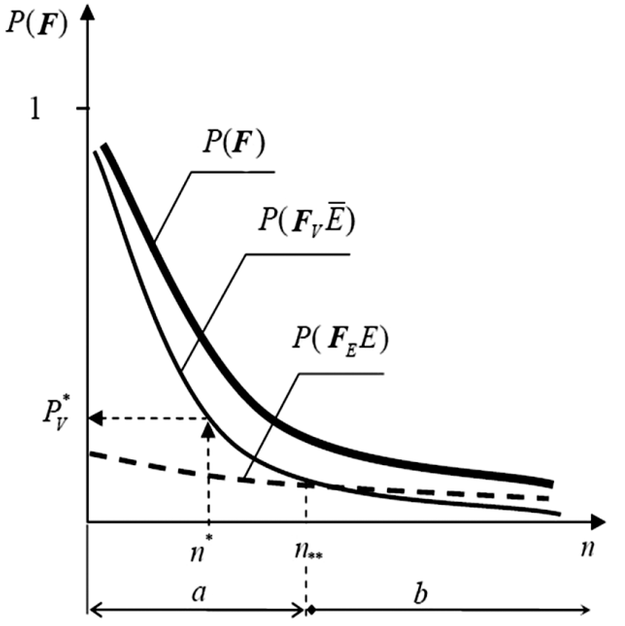

Figure 4 – The effect of the strength margin on the probability of damage of PHF [9].

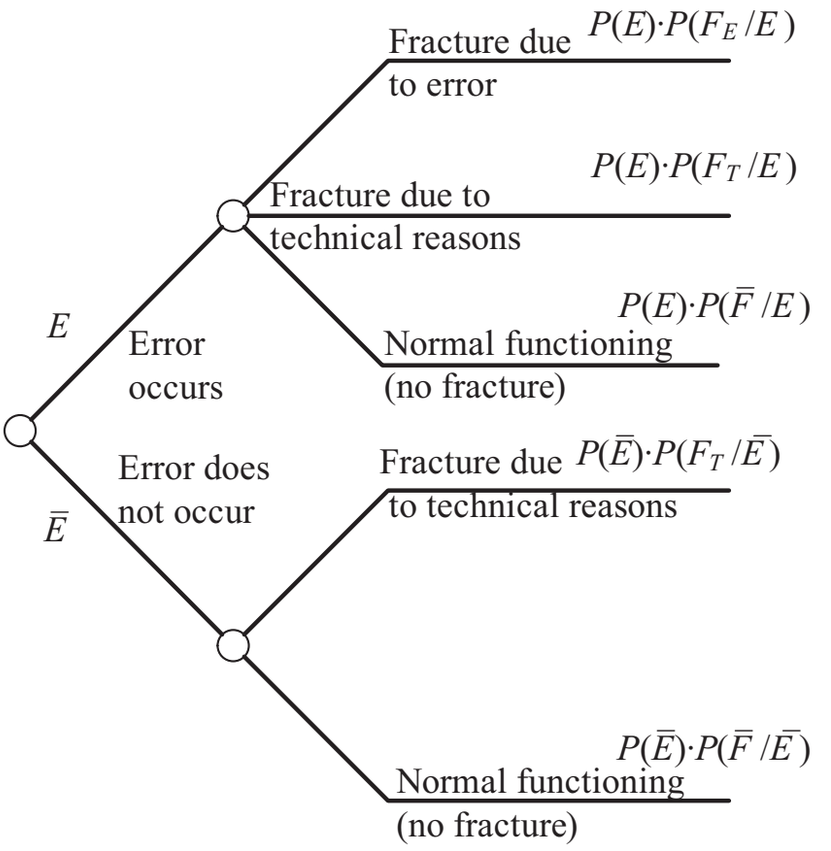

Figure 5 – Simple model for assessing the probability of damage of PHF, with account of the uncertainties caused by the variability of the state function and human errors [10].

90% of PHF damage is associated with the human factor [1]. The important thing is that both primary types of damage causes can be described by expression (12). It should be noted that the mechanisms of damage due to technical reasons can fundamentally differ from the mechanisms of damage due to human errors. Therefore, the structure of the scenario graph, which takes into account the human factor, should be substantially revised.

Let us suppose that after a serious error the probability of system damage due to error is significantly greater, than the probability of damage due to the variability of load and carrying capacity parameters: $P(F_E|E) >> P(F_V|E)$. This assumption is true for sufficiently large margins. In this case, the value of $P(F_V|E)$ in expression (12) can be neglected in comparison with the value of $P(F_E|E)$, in other words, let us assume $P(F_V|E) \approx 0$. Then expression (12) can be rewritten in the form:

$$P(F) = P(F_V \mid \bar{E})\cdot P(\bar{E}) + P(F_E \mid E)\cdot P(E) = \\ = P(F_V\bar{E}) + P(F_E E). \qquad (13)$$

The first summand in expression (13) determines the probability of damage due to technical factors, and the second summand determines the probability of damage due to errors made at different stages of the PHF life cycle.

The conclusions made are aligned with the available statistical data, which shows that the most effective way to increase reliability and safety of systems designed with a small margin and, therefore, operating in modes close to the exhaustion of their carrying capacity, is to increase the margin. At first, with an increase of margin n, the probability of damage decreases sharply (Fig. 4, section "a" of the $P(F_V)$ curve) [9]. However, as the margin grows, the rate of damage probability decrease begins to drop noticeably and, after the transition to the area of highly reliable systems (the conventional border of which is the margin of n_{**}), the probability of damage depends on a further increase in the margin very weakly (Fig. 4, section "b" of the $P(F_V)$ curve). This is due to the fact that at $n > n_{**}$ the main cause of damage is no longer the variability of the load parameters and carrying capacity, which can be compensated by introducing a larger margin, but errors during design, construction and operation, which cannot be effectively parried by increasing the margin (since these errors change the form of the limit states function or may even create new limit state mechanisms) (Fig. 4, $P(F_E)$ curve). Therefore, in this case reducing the probability of damage should be done by improving the operational strategy ξ, including technical monitoring measures, control procedures, routine maintenance and repair work, etc., allowing timely identification and elimination of errors, i.e. compensating for Type

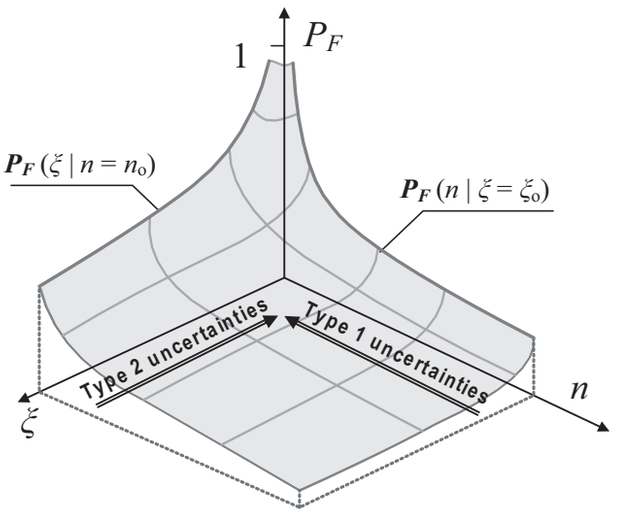

Figure 6 – Dependence of the probability of damage on the margin and the quality of the operation strategy

2 uncertainties[1]. Thus, the probability of PHF damage can be seen as a function of two generalized variables: margin n and quality of the operating strategy ξ (Fig. 6), which characterize two fundamentally different types of uncertainties associated with PHF operation [5].

The quantitative estimation of integral risks indicators for damage, accidents and catastrophes is at the core of traditional and new approaches to assessing the structural strength and safety of potentially hazardous facilities. Parameters such as strength margins and the probability of transfer of the carrying elements to the limit state and the corresponding damage must be considered in these approaches. Uncertainties associated with the variability of the system and the environment parameters and with the manifestation of the human factor at all stages of the objects' life cycle play an important role in the quantitative estimation of these parameters. Modern strength and safety theories allow both evaluating the role of these factors and developing methods for compensating for uncertainties.

References

[1] [Safety of Russia. Legal, socioeconomic and technological aspects]. Moscow: Znanie; 1998-20019; Vol. 1 to 55. (in Russ.)

[2] Makhutov N.A. [Strength and safety: Fundamental and applied research]. Novosibirsk: Nauka; 2008. (in Russ.)

[3] Elishakoff I. Safety Factors and Reliability: Friends and Foes? Dordrecht: Kluwer Academic Publishers; 2004.

[4] Ching J. Equivalence between reliability and factor of safety. *Probabilistic Engineering Mechanics*. 2009;24(2):159-171.

[5] Reznikov D.O. [Methods of uncertainty mitigation as part of ensuring the protection of complex technical systems and optimization of life cycle costs]. *Engineering and automation problems*. 2013;3:57-64. (in Russ.)

[6] Makhutov N.A., Reznikov D.O., Zatsarinny V.V. [Two types of emergency scenarios in complex technical system]. *Safety and emergency problems*. 2014;2:28-41. (in Russ.)

[7] Makhutov N.A., Reznikov D.O. The comparison of deterministic and probabilistic estimates of strength of structural elements of technical systems under serial loading. *Machinery manufacture and reliability*. 2014;5:384-388.

[8] Makhutov N.A., Reznikov D.O., Petrov V.P. et al. [Normative and probabilistic approaches to the assurance of critical facility protection]. *Safety in technosphere*. 2011;4:5-12. (in Russ.)

[9] Beeby A.W. Safety of structures, and a new approach to robustness. *The Structural Engineer*. 1999;77:16-21.

[10] Ellirtgwood B. Design and Construction Error Effects on Structural Reliability. *Journal of Structural Engineering*. 1987;113(2):409-422.

[11] Dhillon B.S. Human Reliability and Error in Transportation Systems. London: Springer-Verlag; 2007.

[12] Makhutov N.A., Reznikov D.O. Consideration of threats associated with the human factor when assessing the security of hazardous production facilities. *Occupational safety in industry*. 2015;1:60-67.

[13] Makhutov N.A., Akmetkhanov R.S., Dubinin E.F. et al. [The effect of the human factor on the safety of technical systems]. *Safety and emergencies problems*. 2014;3:80-98. (in Russ.)

[14] Makhutov N.A., Abramova N.A., Akimov V.A. et al. [Safety of Russia. The human factor in safety problems]. Moscow: Znanie; 2008. (in Russ.)

[15] Makhutov N.A., Reznikov D.O., Petrov V.P. Specific features of critical infrastructures safety ensuring. *Safety in technosphere*. 2014;3;1(46):3-14. (in Russ.)

[1] Here ξ is a generalized parameter characterizing the quality of the chosen PHF operation strategy, with $\xi = 0$ corresponding to the strategy, when PHF operation does not involve any control, maintenance and repair procedures, and $\xi = 1$ corresponding to the strategy that involves the highest possible control and repair level.

About the authors

Nikolay A. Makhutov, Doctor of Engineering, Professor, Corresponding Member, Russian Academy of Sciences, Lead Researcher, Federal State Publicly Funded Scientific Establishment Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), address: 4, Malyy Kharitonyevskiy Per., 101990, Moscow, Russian Federation, phone: (495) 930 80 78, e-mail: kei51@mail.ru

Dmitry O. Reznikov, Candidate of Engineering, Lead Researcher, Federal State Publicly Funded Scientific Establishment Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), address: 4, Malyy Kharitonyevskiy Per., 101990, Moscow, Russian Federation, phone: (495) 930 80 78, e-mail: mibsts@mail.ru

The authors' contribution

Makhutov N.A. generalized the data on the assignment of strength margins subject to various mechanisms of limit state attainment, substantiated the strength criteria of structural components and parts of machines in deterministic terms and developed the probabilistic approaches to the strength assessment subject to the spread of the mechanical characteristics of structural materials.

Reznikov D.O. compared the deterministic and probabilistic approaches to ensuring the strength and safety of technical systems, examined the applications of graphological methods in the assessment of strength-related dependability of technical systems subject to various types of uncertainty.