Design Problems and Knowledge Management

Electronic Journal

Volume 2, Issue 5

September - October 2024

In this issue:

Editor and publisher: Dr. Yuri Spirochkin, Saint Petersburg, Russia
yu.spirochkin@gmail.com

Date of publication: October 30, 2024

Cite (Harvard style):
Spirochkin Y (2024) Towards minimizing uncertainty in the design of technical systems. Design Problems and Knowledge Management, 2(5). https://desproknom.wixsite.com/info/journal. Accessed *date*

Towards Minimizing Uncertainty in the Design of Technical Systems

Yuri Spirochkin[1]

International Consultancy and Analysis Agency "Aviation Safety"

Abstract

This article addresses the issue of uncertainty faced by designers of aircraft, spacecraft, aerospace vehicles, nuclear power plants or other complex technical systems at the design stage. Uncertainty covers the range from stochastic variation in the values of known variables – system properties, and factors acting under typical operating conditions – to the lack of knowledge about all possible adverse events during the service life and the behavior of the system in such situations. Errors in forecasting extreme impacts and the system's ability to withstand them pose a threat of an accident or disaster with the possibility of significant material losses, damage to the environment and fatal consequences for human life or health. Obviously, such a threat must be minimized using appropriate design methods.

Existing methods aimed at achieving this goal are based on the understanding of uncertainty as a combination of aleatory and epistemic components, on the quantitative estimate of the former, presented in the form of risk, and on the opportunities of its reduction. These ideas, supported by experience in the creation and operation of a number of similar systems, allow designers to reduce risk to levels that are acceptable given the predictability of future operating conditions. However, the methods used, despite the high level of their development, leave unresolved the problems of risk substantiation when statistical data is insufficient or when forecasting events that go beyond the scope of experience, i.e. when ensuring safety in conditions of unknown factors.

The object of the presented research is to find a way to solve such problems, and among them minimizing the epistemic component of uncertainty in design. As a first, necessary step on this way, a more detailed vision of the structure of uncertainty and the genesis of its various items is developed. From the designer's point of view, seven main sources of uncertainty are identified. A wide range of engineering approaches to reducing uncertainty at the design stage is analyzed – from existing and commonly used methods to promising concepts under development. Each of them makes it possible to refine to some extent the a priori, based on previous statistics, assumptions about the behavior of the designed system at the operation stage by obtaining current information and its comprehensive processing. When analyzing any approach, that provides quantification of the aleatory component of uncertainty, its limitations are revealed, which contribute to the epistemic component. They can be overcome by another, more advanced method or concept in the series considered. The most effective in this regard seems to be a SPARS design concept, which provides for the creation of a Smart, Pro-Active, Resilient System.

Keywords

Uncertainty, technical system, design, safety, risk, probability, philosophy of design

1 Introduction

The design of a complex technical system: an aircraft, a spacecraft, an aerospace vehicle, a nuclear power plant (NPP), an infrastructure facility, etc. is carried out using assumptions about

[1] E-mail: yu.spirochkin@gmail.com

the values of factors acting during operation[2] as well as assessments of the system's response to these factors. The assumptions about operational factors are based on relevant data obtained from operating experience of systems similar to the one being developed (serving as prototypes) and previously produced specimens, as well as from research experiments. These data are transformed into knowledge through theoretical analysis and generalization. The system's response is assessed through calculations with the use of mathematical models and (or) through testing of physical objects that reflect, to varying degrees, the properties of the system. But even with such substantiation, design decisions are made under conditions of uncertainty. Uncertainty occupies a range from stochastic variation of system properties and values of known factors to the lack of knowledge about all possible impacts during operation and the behavior of the system in unforeseen situations. The left boundary of this range includes repetitive, frequently occurring and predictable events that fit into the category of *aleatory uncertainty*. The right boundary corresponds to adverse factors that are unknown at the time of design and therefore unpredictable – they are covered by the category of *epistemic uncertainty*. Between these boundaries are events of a known nature with extreme but unknown intensity, extremely rare combinations of random events that can disrupt the operation of the system or make it unusable, errors in analyzing the behavior of the system in poorly defined conditions, and other factors that are difficult to estimate.

Underestimation of hazardous factors combined with an erroneous conclusion about the ability of an aircraft, NPP or other large and complex system to withstand them can lead to its destruction with the release of accumulated energy and the emission of hazardous technological substances, which threatens the life and health of people, as well as the environment. Also, as a result of an accident, and especially a catastrophe, the expensive technical system itself can be lost. It is obvious that the uncertainty that exists at the design stage and creates such a threat during the operation of the system must be minimized.

The necessary conditions for minimizing uncertainty are: understanding its nature, the possibility of quantitative assessment (quantification) and controllability – of course, in the direction of reduction. The goal of minimization is achieved, inter alia, by the division of uncertainty into two components, which differ in genesis and measurability (Willett 1901), (Knight 1921):

1) objective, or measurable uncertainty, corresponding to the concept of risk, and
2) subjective, or immeasurable component, associated with the lack of knowledge about all possible outcomes of an event or all possible events in a given context.

This division coincides with the above categorization of uncertainty as aleatory or epistemic.

The measure of aleatory uncertainty, or risk of any adverse event, is its probability, the severity of the harm caused by this event, or their combination. A common combined risk indicator, proposed in the early 18th century by de Moivre, is the product of the severity of harm, or the magnitude of loss, and the probability of loss (Bernstein 1996). Thus, to take into account aleatory uncertainty, an approach is used that includes an assessment of the probability of an event related to a series of repeating ones based on accumulated statistical data. But since the result of the design must be clearly defined geometric characteristics and physical and mechanical properties of all elements of the system, the probabilistic approach is usually implemented indirectly – through deterministic safety factors, safety margins or reliability

[2] And in some cases, during the manufacturing of system elements and its construction.

factors[3]. The values of these factors are specified depending on stochastic variation (stochastic scatter) of the loading parameters and the properties of the elements characterizing resistance to them, the corresponding probability distribution laws and the required safety or reliability indicators. – see e.g. (Taylor 1965), (Makarevskii et al. 1975), (Rzhanitsyn 1978), (Gladkii 1982), (Spirochkin 2019). Due to the control of stochastic scatter under conditions of standardized mass production and normal operation, the statistical validity of distribution laws, and the conservatism of the values of the above factors specified in regulatory documents, the target risk indicators in modern projects are very low: they correspond to the probability of an accident of 10^{-6} and a catastrophe of 10^{-7}. The question of how much these indicators correspond to reality remains open, as a consequence of – among other circumstances – the insufficient duration of operating experience of some systems, for example, NPPs (Spirochkin 2023).

However, predictions about the future based on past experience, even long-term one, may be wrong because the potential of induction by which they are made is limited (Russell 1912). The limitations are caused by the epistemic uncertainty inherent in our knowledge of the world. Beyond the boundaries of knowledge lie unpredictable adverse events not captured by existing experience and statistics. The metaphor of a "black swan" has become generally accepted to characterize such events (Taleb 2007). It is now applied to any unexpected and large-scale disaster, including the one that occurred at the *Fukushima Daiichi* NPP in 2011. The unexpectedness of such events, coupled with the extreme severity of their consequences, raises doubts about the applicability of the probabilistic approach, and proposals to change the design paradigm based on it appear (Dédale 2013). In this regard, it should still be noted that the real cause of the disaster at the *Fukushima Daiichi* NPP was the underestimation by the designers of the maximum tsunami wave height, based on the available statistical data. Since tsunami phenomena are known and recurring, the possibility of their probabilistic assessment is, in principle, beyond doubt. The problem that caused that disaster was the insufficient conservatism of the assessment made and the incomplete implementation of the *defense-in-depth* principle in the design (Spirochkin 2023).

The uncertainty associated with known natural events whose magnitude is difficult to predict is aleatory rather than epistemic. The creator of the "black swan" image himself, although he did not abandon the idea of the unpredictability of catastrophic events, later focused on the research of "fat-tailed" probability distributions that are able to approximate statistical series that include rare (or even single) extreme deviations (Taleb 2020). But in such circumstances the following questions arise:

1) if the magnitude of a sudden single deviation differs significantly from the scale of other events in the series, does this not indicate the entry into force of some new unknown factor?
2) can such a series be considered a statistical population (an immanent property of which is the qualitative homogeneity of events)?

It is the idea of a statistical population that allows us to obtain reasonable probabilistic estimates, not to mention the ideal image of the general population, against the background of which the entire probabilistic methodology develops. In these questions, which remain unanswered, the influence of epistemic uncertainty is undoubtedly evident.

The extension of probabilistic methods to rare adverse events, for which the volume of statistical data is small, is possible on the basis of the Bayesian approach (Ventsel 1969). It operates on subjective probability estimates that will be refined as new relevant data becomes

[3] Different branches of technology use different terms, the essence of which is the same.

available. An example is the analysis of the terrorist attack on the World Trade Center in New York in 2001 (Silver 2012). The prospects of such an approach to taking into account marginal manifestations of human factors in the design of technical systems (in the context of aleatory uncertainty) were considered by the author (Spirochkin 2023). When applying Bayesian methodology to the full spectrum of rare events that can affect the configuration and properties of the system being created, the above questions become even more important, since epistemic uncertainty only increases in the case of poor statistics and insufficient understanding of the nature of events.

Perhaps the best characterization of the two different categories of uncertainty is given by Donald Rumsfeld: "…There are known unknowns, that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know"[4]. In his book, he described epistemic uncertainty as follows: "There are many things of which we are completely unaware – in fact, there are things of which we are so unaware, we don't even know we are unaware of them" (Rumsfeld 2010).

In order to reduce subjective, or epistemic, uncertainty, attempts are made to structure it. One such attempt is to identify the component associated with known outcomes but unknown probabilities. The corresponding idea has its origins in socio-economic studies (Keynes 1937), (Stirling 2007), (Aven and Steen 2010)[5], (Saunders et al. 2015), and then has found its place in the engineering sciences (Beer et al. 2013), (Patelli et al. 2014), (Beer et al. 2016). This component can be classified as aleatory uncertainty if estimates of *subjective imprecise probabilities* are feasible. Having such probabilities compatible with the general probabilistic approach, one can further refine them according to the Bayesian methodology or process them based on random set theory using probability boxes (p-boxes), Dempster-Shafer structures (Dempster 1967), (Shafer 1976), etc. This approach narrows the area of epistemic uncertainty that cannot be managed.

When it is possible to make assumptions about some outcomes of an event, but their entire set is unknown (as are the probabilities), and there are only notions about the boundaries within which the outcomes lie, then researchers try to identify other components in subjective uncertainty. Among these components the following are considered: *ambiguity* (Lempert et al. 2003), (Stirling 2007), (Saunders et al. 2015), *fragmentary or dubious information*, *imprecise variables* (Beer et al. 2016). Each of these, although falling primarily into the category of epistemic uncertainty, differs from complete ignorance by the presence of certain logical constructions – limited and controversial, opinions – including alternative ones, and assessments of varying degrees of validity. Several approaches are used to handle such incomplete, vague and unreliable information. Thus, in relation to ambiguity, a common psychologically based practice is ambiguity aversion (also known as uncertainty aversion) – this is reflected in the fact that people prefer known risks to unknown ones (Ellsberg 1961) and reject decisions associated with the latter. The use of the precautionary principle is also widespread (Stirling 2007). It encourages caution and detailed research before embarking on innovations that could have disastrous results. In safety-critical areas, the worst-case scenario postulation method is used, which is an extension of this principle (Schneier 2010), (Capitanescu and Wehenkel 2013). A similar method is extreme case analysis, which involves identifying events that lead to the worst-case behavior of a system (Patelli et al. 2014).

---

[4] Donald Rumsfeld said this in 2002, when he was US Secretary of Defense, at a press briefing at the Pentagon; quote from (Rumsfeld 2010).

[5] With reference to the article by Klauer and Brown (2003).

Among the analytical tools that can handle ill-defined information for which probability estimates are not possible or practical the following should be mentioned: fuzzy logic (Zadeh 1965), (Yen 1999), (Singh et al. 2013), (Gupta 2021), interval analysis (Moore 1966), (Rao and Berke 1997), (Moore et al. 2009), (Modares and Mullen 2014), (Sotiropoulos and Tserpes 2022), (Gong et al. 2023), sensitivity analysis (Haug et al. 1986), (Patelli et al. 2014), (Blumsack 2023), and heuristic strategies (Nielsen and Molich 1990), (Nielsen 1994), (Yilmaz et al. 2011), (Pierre 2015). In the conditions of conflicting alternative opinions, controversial and contradictory assessments (sometimes reflecting only peculiar aspects of human factors), a reduction in the corresponding component of uncertainty can be achieved through appropriate methods of managing design activities.

In each of the above mentioned attempts to structure uncertainty, as in its basic dichotomy, there is an epistemic component in the form of ignorance that cannot be managed in the given circumstances. It is closely intertwined with the controllable aleatory component, and this relationship complicates the task of minimizing the overall uncertainty in a certain project.

The presented overview of existing approaches to uncertainty shows that they are based on its understanding as a combination of two main components: aleatory and epistemic, a quantitative estimate of the first, which can be presented as risk, and the opportunities of its reduction. Methods of risk reduction in the design of technical systems, based on experience, ensure the reliability and safety of technologies to the extent that society considers acceptable. The constant accumulation of experience, its theoretical generalization and transformation into knowledge contribute to the reduction of epistemic uncertainty as well. However, the area of technologies is constantly expanding, uncontrolled changes are taking place in the world, and the volume of epistemic uncertainty does not seem to decrease. When the operating conditions of the created system change significantly relative to those specified for design (and changes are very likely over a long life cycle), such properties as resistance to unexpected adverse effects and the ability to recover from them acquire particular importance. It is clear that these properties can be realized only within certain limits: no system can be resistant to any impact or have unlimited recoverability. Increasing the reliability and safety of technical systems taking into account difficult-to-predict events, especially in the long term, is possible by expanding the limits of resistance and recoverability. To do this, it is necessary to improve approaches to uncertainty, including methods of handling its epistemic component.

The aim of this article is:

- to improve the understanding of uncertainty in the design of technical systems: its structure and sources of various components, suggesting that in this way the possibilities of quantifying, managing and minimizing uncertainty can be expanded;
- to analyze, based on this understanding, existing approaches to reducing uncertainty and identify their limitations that that make minimization difficult;
- to explore the possibilities of overcoming the identified limitations using new design approaches that promise to reduce epistemic uncertainty.

We try to achieve this goal at the level of the philosophy of design, in the context of safety-critical industries. It is worth noting the difference in the meaning of the two notions that we operate with: *minimizing uncertainty* is the goal, and *reducing uncertainty* expresses the capability of each approach under consideration to facilitate the movement towards this goal. At present, we cannot quantify the goal, but we can quantify the movement towards it.

2 Improving the understanding of uncertainty in design

2.1 Sources of uncertainty in design

As shown in the Section 1, existing approaches to uncertainty in the design of technical systems leave unresolved the problems of risk management with insufficient statistical data or safety substantiation, when events beyond the existing experience are possible. To ensure safety, given the scarcity of statistics and the possibility of unknown factors, a deeper understanding of uncertainty is needed that would help designers manage it, reducing it to the minimum achievable level in each specific situation.

Uncertainty in design is caused by the following reasons (they can also be called sources of uncertainty):

1) stochastic scatter, inherent in any population in the real physical world, due to which there is a lack of precise data on the properties of a certain element of the created system and the loads applied to it – as a result a priori assessments of the condition and behavior of the element during operation are inevitably accompanied by errors;
2) hidden imperfections in the system, including its structure, subsystems, control loop, etc. (poor design solutions, anomalies or defects[6]), and undetected discrepancies in the operating documentation (gaps or inadequate provisions) – they can manifest themselves unexpectedly and lead to violation of normal operation;
3) a fundamental feature of any system: the emergence of new properties after connecting its elements – some of the emerging properties may be undesirable and non-obvious until certain, previously unknown conditions occur;
4) possible uncontrolled impacts and abrupt changes in the operating conditions of the system with an exit beyond the limits provided for by the design, up to the occurrence of an emergency situation, when the further state of the system and its behavior become difficult to predict;
5) insufficient understanding of human factors embodied in operating personnel and other people involved in the life cycle of the system or located in the area of its operation;
6) errors in the experimental and computational substantiation of the system's operability and safety due to incomplete similarity of prototypes, research make-ups and small-scale physical models to the properties of the created system, shortcomings and inaccuracies of mathematical models, defects in software and inaccuracies of simulation results;
7) the possibility of the impact of unknown factors on the system, which entails the unpredictability of its state and reaction.

The first of these causes covers many difficult-to-control deviations in the processes of manufacturing system elements, its construction and normal operation. It is almost entirely consistent with aleatory uncertainty. Accounting for such uncertainty in the design is based on the approximation of relevant statistical data and is carried out both directly by probabilistic methods (in some cases) and using deterministic safety factors (mainly). The risk associated with stochastic scatter of the properties of system elements and loading parameters is reduced mostly through high quality of design and production work, compliance with prescribed operating rules, performance of operational control, maintenance and repair, and timely decommissioning.

---

[6] A *defect* differs from an *anomaly* only by its regularized characteristics: it must belong to a known, specific type of imperfection (for example, a macrocrack in a structural element), and its quantitative parameters must not be lower than the established limits.

Practical specialists are trying to apply probabilistic methods also to other sources of uncertainty. Thus, they use probabilities to assess the presence of hidden imperfections in the system (the second position in our list), which remain undetected during technological control, acceptance and certification tests (Sukhoruchenkov and Okorokov 2014). The possibility that not all poor design and construction solutions, anomalies and defects will be detected before commissioning is due to the limited scope of control or testing, insufficient technical characteristics of the tools used and the negative influence of human factors embodied in the personnel performing the relevant work. This influence covers the range from the inability of designers to foresee the full variety of potential imperfections and prevent their appearance in the system to the omissions of inspectors and testers when detecting imperfections. Similarly, human factors are “responsible” for gaps and inadequate provisions in the system operating manuals. As some researchers have argued, “there is no means for quantifying the probability of … inconsistencies in written materials” (Swain and Guttmann 1983). Thus, the epistemic component manifests itself in the second source of uncertainty.

This component fully characterizes the third cause of uncertainty – the emergence of new properties in the system. Along with the planned useful qualities, after connecting elements into a system (by assembly or other technological operations), a side effect may be obtained in the form of emerging undesirable properties. These properties are sometimes hidden and unexpected, becoming apparent only under special operating conditions, and for a fundamentally new development they are difficult to predict. An example of emerging undesirable property is the so-called *elastic follow-up* in mechanical joints operating at high temperatures, causing creep. This effect occurs when the stiffness of one of the connected components differs significantly from that of another. It means the forced following of the more flexible component after the elastic unloading of the more rigid one, which results in increased deformations in the former. The effect of such following on the cyclic strength of the connection is a reduction in the predicted service life compared to the value obtained by elastic analysis that does not take this effect into account (RCC-MR 2007), (Jawad and Jetter 2009), (ASME 2010). After its discovery and explanation of its nature, a significant difference in the stiffness of the connected components began to be considered as a marker of the possibility of an undesirable property emerging in the structure being created. It is obvious that probabilistic methods are not applicable for the analysis of such properties. These properties are determined by experimental and theoretical studies conducted at the design stage. It can be assumed that for any of the emerging properties a specific marker can be found.

The possibility of uncontrolled natural and man-made impacts on the system and abrupt changes in operating conditions (outliers) that threaten to exceed design limits (item 4 in the list above) are sometimes considered within the framework of statistics of extremes (Gumbel 1962). The problem is that when impacts are characterized by power-law distributions, and outliers are reflected only in the fat tails, the length of statistical series which are required to ensure the robustness of probability estimates may exceed the available experience. On the other hand, a variable distributed according to a power law with exponent α has a definite mean only if $\alpha > 2$, and a finite dispersion if $\alpha > 3$ (Newman 2005). The distributions of earthquake magnitudes, as well as the intensity of a number of other natural and social phenomena that obey a power law, are characterized by exponent values $2 < \alpha < 3$. Therefore, among such phenomena, “black swan” events (see Section 1) can occur, characterized by an unpredictable scale (and uncertainty of the moment of implementation). Consequently, the fourth source generates uncertainty with a significant and difficult to eliminate epistemic component.

Probabilistic methods are used to describe the variability of the actions of personnel operating a technical system, which is related to the fifth source of uncertainty (Swain and Guttmann 1983). However, they are poorly suited to assessing the impact on safety of other roles of human factors associated with the life cycle of the designed system: the public, vehicle occupants in crashes, or people under conditions of malicious actions (Spirochkin 2023). The epistemic uncertainty present in such the impact can be interpreted as ambiguity (see Section 1). Its analysis is feasible using mathematical agent-based modeling and simulation, but the current level of development of this methodology does not allow solving all safety problems, especially when considering mass human behavior.

The nature of the incomplete similarity of the means of experimental substantiation (prototypes, research make-ups and small-scale physical models) to the properties of the system being created, as well as the nature of errors in simulations using mathematical models and software (the sixth cause of uncertainty), is generally not stochastic. However, sources of errors in calculations may be software defects caused by human factors embodied in the personnel of the code developers. The limited variability inherent in professional activity makes it possible to use probabilistic-statistical approach to assess the quantitative indicators of such defects. In particular, the capture-recapture method is applicable, which helps to estimate the number of defects remaining in the code and the level of their detection by a row of independent random checks (Schofield 2007). As a result, the uncertainty corresponding to the sixth item of the list of sources can be considered as a combination of a small aleatory part with a predominant epistemic component.

The seventh cause in the list we are considering – the possibility of unknown factors – fits entirely into the category of epistemic uncertainty. This possibility should be expected primarily in research and innovation projects involving new or under-developed fields of science and technology. The presence of unknown factors is evidenced by phenomena unexplained by any theory, and facts that contradict each other or do not fit into the modern scientific paradigm. An example of unexplained phenomena is quantum entanglement; among the contradictory facts, it is worth mentioning the observed (judging by the values of redshift and brightness of extremely distant supernovae) accelerated expansion of the Universe[7].

Unknown factors may be generated by the complexity of the system being created, including the complexity of its life cycle processes. Complexity is understood as a specific property of systems in which “large number of components or subsystems, at times of a different nature, combine to produce surprising emergent phenomena apparent at multiple scales” (Hébert-Dufresne et al. 2024). In this context, not only the technical object under development should be considered as a system, but also a set of participants, tools and processes of its creation (production system), as well as a complex covering, along with the object, the environment and the processes of interaction with it during operation (operation system). Complexity of a system is often associated with the nonlinearity of its properties and interaction with the environment. Nonlinearity is expressed in the fact that the parameters of the system elements and the connections between them, established for any observed interval of interaction in the time or space domain, change when transferred to any other interval, and the previous values become incorrect. As a result, insufficient traceability and controllability of the entire system arises.

[7] The hypothesis of an expanding Universe is not accepted by all cosmologists and is currently being criticized.

Uncertainty caused by the possibility of unknown factors cannot be eliminated completely, but it can be reduced for a certain project using experimental and theoretical methods to obtain new or improved knowledge. Unexplained phenomena and contradictory facts, complexity and nonlinearity should be considered as markers of the action of unknown factors or the possibility of their manifestation in the life cycle of the system.

2.2 An improved framework for uncertainty in design

The above provisions allow us to build an improved framework for uncertainty in design. Its main items – sources and relative shares of the components they generate (aleatory and epistemic) – are presented in Table 1.

Table 1 Improved framework for uncertainty in design

Source of uncertainty	Relative shares of generated uncertainty components	
	Aleatory	Epistemic
1. Stochastic scatter of the properties of system elements and loading parameters	Present in full	
2. Hidden imperfections in the system and in the operating documentation	Present as part	Present as part
3. The emergence of new properties		Present in full
4. Uncontrolled impacts and abrupt changes in the operating condition	Present as part	Present as part
5. Insufficient understanding of human factors	Present as part	Present as part
6. Errors in the experimental and computational substantiation	Present as small part	Predominant
7. The possibility of unknown factors		Present in full

As can be seen from this table, only one of the seven sources of uncertainty in design fully correlates with aleatory uncertainty – the first one. All the others generate epistemic uncertainty to one degree or another, and such sources as the emergence of new properties and the possibility of unknown factors are characterized by it to the fullest extent. These features limit the range of approaches to uncertainty reduction based on probabilistic methods. Although the level of their development is quite high, the area of applicability can hardly be expanded beyond the boundaries established by the stochastic nature of known properties and phenomena. Within this "stochastic area", the potential for further reduction of aleatory uncertainty exists, and it should not be neglected. The implementation of such potential is discussed below, in Subsections 3.1 and 3.2. It should be noted that the boundaries of the "stochastic area" are not clearly defined and can themselves be the subject of research. However, the main focus of our attention and efforts to improve the safety of the designed systems will be epistemic uncertainty. Existing engineering methods for handling uncertainty, which allow designers to reduce the degree of ignorance about the system being created and its behavior at the operation stage, are analyzed in Subsections 3.3 and 3.4. Further opportunities provided by new design approaches are disclosed in Section 4.

3 Analysis of existing approaches to reducing uncertainty

3.1 Refinement of probabilistic characteristics

Reducing uncertainty in design is facilitated by refinement of probabilistic characteristics of factors that influence the parameters of the system being created and that have a stochastic nature. Such refinement is especially in demand when the system differs significantly from prototypes in terms of operating conditions (environmental factors, operating modes, designated service life), design and construction solutions (configuration, dimensions of the main elements and their connections), materials used and manufacturing technologies. In this case, it should be expected that the variation of geometric characteristics of elements, properties of materials and connections, as well as parameters of external loadings may go beyond the statistics collected for prototypes.

The refinement is achieved by obtaining new experimental data in the form of statistical series, specific for the system being created, and processing these data in order to find reasonable distributions and other probabilistic characteristics. They should ensure less error in estimating the parameters of the state and behavior of the designed system in predicted operating modes. Thus, the corresponding procedures are aimed at reducing the aleatory uncertainty generated by the first source (see Table 1).

New experimental data can be obtained during tests related to the category of *phenomena-exploration experiments* (Oberkampf 2003). These include, in particular, tests to determine the properties of basic materials and joints (mechanical, welded and others), which are carried out in a laboratory on samples and structural elements. The manufacture of experimental objects, the tests themselves and the processing of their results can be one of the intermediate stages of design, which must precede the adoption of final technical solutions. Methods for planning mechanical tests and statistical processing procedures can be found in the reference book Stepnov (1985). A methodology for handling aleatory uncertainty in a broader range of tests is presented in ASME PTC 19.1-2005 (2006). If such tests reveal increased scatter of properties compared to prototypes, then it may be necessary to improve technological processes, strengthen structural elements, or increase safety factors.

Similar experiments can provide data on the stochastic variations in the geometry of elements and joints. The main share in such variations is made up of initial technological imperfections: wall thinning, deflection, eccentricities and other deviations from the design forms and sizes, which are often combined with residual stresses after various processing operations.

Statistical data on the loading of a new system during operation can be obtained in research facilities using small-scale physical models or full-size mock-ups, on prototypes of the system manufactured before the start of its serial production, as well as on systems already put into operation, equipped with appropriate recording devices. The degree of reproduction of real processes using experimental objects of the first two types in research facilities is determined by compliance with the similarity criteria. Full-scale experiments on prototypes have no limitations in terms of similarity, but they are usually expensive and can only be carried out when the system design has been completed and the manufacturing stage has begun. If the results of these experiments require any changes to the system, this can become a problem due to additional costs and time constraints. The data recorded during the operation of a serial specimen of the system over a long period of time is the most valuable information resource. This resource may contain records of relatively rare natural impacts, but its technical support is associated with costs, and its use relates mainly to future projects. However, since the parameters characterizing natural impacts usually depend weakly on the properties of the system (primarily due to the large scale of natural phenomena), they can be obtained using similar objects that have been in operation for a long time (and, therefore, can act as prototypes). An example is atmospheric turbulence data collected using aircraft of various types (Taylor 1965).

Control of the error of probability estimates obtained by the methods described above is ensured by analyzing their sensitivity to the variability of the volume of the statistical base and the type of distribution law (if it is possible to use distributions of different types).

Along with its undoubted advantages, the considered approach has a significant shortcoming: within its framework, not the actual state of each element of a certain system or the actual values of loads are determined, but the parameters of probabilistic approximations of the corresponding statistical populations. In this case, it is possible to reduce the uncertainty for the entire fleet of similar systems and the range of typical conditions of their operation, the variation of which occurs within predictable limits corresponding to reasonable values of probability. However, it is impossible to guarantee that a certain system has precisely known properties or that it will not be subject to loads exceeding probabilistic estimates during its service life.

3.2 Experimental determination of the actual system properties and loads

The actual properties of a certain specimen of the system can be determined in the performance check experiments, where performance characteristics include strength, resistance to vibration and impact, etc. Such experiments fall under the category of *system and certification tests* (Oberkampf 2003). To determine the actual properties, experiments are also used to identify and refine mathematical models (in the referred publication they are called *mathematical-model-development experiments* and *calibration* (*model-updating*) *experiments*). The data obtained in this way are often applicable to assessing the properties of a real system that go beyond the immediate objectives of the experiment. For example, the results of horizontal frequency tests[8] of the Soviet space shuttle *Buran* (eigen frequencies and vibration modes of the structure, necessary primarily for substantiating safety taking into account aeroelasticity and other types of dynamic effects, as well as for vibration diagnostics) were used to validate the mathematical (finite element) model with the help of which its possible emergency landing was analyzed (Spirochkin 1987, 1993).

The actual maximum values of loads and their time profiles can be determined in phenomena-exploration experiments mentioned in Subsection 3.1. When simulating the emergency landing of *Buran*, one of the problems was determining the loads acting on the fuselage from the landing surface. For the case of emergency landing on the ground, these loads were calculated using experimental data accumulated during the landing tests of Soviet reentry ballistic-type vehicles (of *Soyuz* type). To determine the interaction of the bottom of the *Buran* fuselage with the landing surface under conditions of a glancing impact at a velocity characteristic of the landing of an aircraft-type vehicle, a special experimental facility was proposed (Spirochkin 1988), and subsequently patented (Patrushev et al. 1989).

The described approach eliminates the shortcoming of probabilistic assessment noted in Subsection 3.1 – averaging of data over a statistical population – and can provide a reduction in aleatory uncertainty as applied to a certain specimen of the system (within the limits related mainly to the first source of uncertainty presented in Table 1). However, it is associated with

[8] Vibration tests with the test object in a horizontal position.

significant costs for conducting experiments for each specimen, and the obtained data determine only its initial properties, without taking into account their degradation during the operation of the system.

3.3 Pilot projects

Innovative activities aimed at implementing scientific and technical ideas in fundamentally new systems and promoting them to the market may have a high level of epistemic uncertainty. To reduce it, the concept of a *pilot project* is used. In the framework of this concept, neither the probabilities of various outcomes of the activity nor any other measurable indicators are assessed, but uncertainty as such is empirically investigated. A pilot project may be a stage of a large long-term project or a large-scale program. During such piloting, data is collected on unknown factors accompanying the innovation, and its technical feasibility and (or) commercial effectiveness are substantiated.

There are a number of strategies for implementing pilot projects. These include:

1) exploration of the space of possible outcomes through parallel promotion of several innovation options (by separate project teams) and identification of the most successful of them;
2) modeling key actions typical for the implementation of developed ideas or the release of new products, using a small representative example to identify existing problems and find ways to solve them;
3) limiting the scope of innovation to an area corresponding to low (acceptable) risk, interpreted as the amount of potential losses, learning lessons and identifying corrective measures.

The first strategy was used by NASA in the 1960s when developing the lunar module. It was used in the first half of the 1990s by Japanese consumer electronics firms. Similarly, many automobile companies develop several concepts for a new car model, taking them to prototyping to fully understand the complex design space before selecting the best prototype for production (Pich et al. 2002).

The second strategy is familiar to the author from his participation in 2006-2008 in a research program aimed at introducing *information support of the life cycle* in the design of transport-type nuclear reactors. The complexity, novelty, and degree of responsibility of this program necessitated a pilot project in the form of design and engineering work on a certain pipeline system as part of a specific reactor installation, with data exchange between the stages of work and the design organization's departments performing them.

The third strategy is largely inherent to innovations in defense and deterrence (Cocron and Aronhime 2022). It is also applicable to other pressing problems with high potential for uncertain dangers, such as the integration of artificial intelligence (AI) in aviation systems (Spirochkin 2024).

The direct "encounter with uncertainty" during the implementation of a pilot project determines the universality of this concept. Thanks to universality, such sources of uncertainty as the emergence of new properties (the third source in Table 1), errors in the experimental and computational substantiation (the sixth source) or the possibility of unknown factors (the seventh source) can be investigated.

In addition to solving research problems, pilot projects can also contribute to organizational learning (Turner 2005). They can also play a role in identifying hidden imperfections in the systems being created and in the operating documentation (the second source of uncertainty), as well as in minimizing other negative manifestations of human factors (the fifth source). In this way, gaps and inadequacies in the procedures for using the system can be found and corrected, at least in part, i.e. the problem pointed out by some researchers is solved: "There are no means to quantify the probabilities of … inadequacies in written materials" (Swain and Guttmann 1983).

3.4 In-service monitoring and diagnostics

Let us return to the idea of experimentally determining the actual properties of each specimen of a serially produced system and the loading parameters, which is presented in Subsection 3.2. As its shortcoming, it was pointed out that the data obtained once by system and certification tests before commissioning do not provide the necessary information about the degradation of system properties during the service life. This problem can be solved by in-service monitoring and diagnostics.

In-service monitoring includes observing, recording and collecting data that determinate the current health (state in terms of serviceability) of individual elements or the system as a whole, as well as their working conditions. The primary data are harvested using sensors located in certain places of the system, with a specified periodicity in time. Diagnostics involves the analysis of collected data and assessment of the health of elements (system) according to the integrity and performance criteria, taking into account possible malfunctions. The data providing such an assessment are the parameters of the reaction of elements (system) to the loads that act during normal operation or are applied in special tests. Degradation of the system properties during the service life can also lead to a change in the working conditions of elements and, accordingly, to a change in the loads applied to them. Therefore, diagnostics also includes the analysis and assessment of such conditions and loads. Diagnostics is carried out both periodically, together with monitoring procedures, and after extreme events that can cause adverse changes in the health (integrity and performance) of the system. The assessment of health is based on the direct detection of defects (visible breakdowns, traces of wear or corrosion, macro cracks, etc.), as well as on the identification of characteristic signs in the behavior of the system indicating hidden malfunctions. As a result of the assessment, recommendations can be developed to fix defects and correct malfunctions or to implement other measures to manage the life cycle of the system.

Data collection and analysis operations are currently performed by automated monitoring and diagnostic systems (AMDSs), which are a necessary part of each important, safety-related technical object (each specimen of a serially produced technical system). For example, all nuclear reactors being built now are equipped with such systems. The vibration and noise diagnostics tools included in them distinguish significant features from the broadband mechanical oscillations accompanying the reactor operation and identify these features as signs of deviations from the normal state. Thus, changes in the frequencies and amplitudes of vibrations of reactor vessel internals of WWER-type facilities make it possible to draw the conclusions (Arkadov et al. 2004):

- on reducing the stiffness of the elements pressing the reactor shaft to the vessel;
- on similar degrading the spring blocks and spacer grids of fuel assemblies;
- on wearing the fasteners (keys) through which the reactor shaft comes into contact with the reactor vessel in the lower unit of their mechanical connection.

Other capabilities of AMDSs intended for monitoring and diagnostics of the health of nuclear reactor elements can be found in the book Spirochkin (2019).

The development of AMDSs is also an important direction in the design of other complex technical systems with a long life cycle. The corresponding R&D currently forms a separate scientific and technical discipline: structural health monitoring (SHM). Its applications to aerospace structures are regulated, for example, by the guide SAE ARP6461A (2021). However, it would be premature to declare the widespread practical application of the relevant technologies in this area (Sause and Jasiūnienė 2021).

In-service monitoring and diagnostics can reduce the aleatory uncertainty for each specimen of a serially produced system and increase the level of safety due to knowledge of its current state and the possibility of more accurately predicting its future - in the form of an assessment of the remaining service life (under expected operating conditions). At the same time, the potential is created for improving economic indicators through *actual-state-based life cycle management* as opposed to a priori established and, as a rule, overly conservative regular plans for relevant activities.

In addition, in-service monitoring and diagnostics help to reduce epistemic uncertainty, which corresponds to the second source (hidden imperfections in the system and in the operating documentation). An important role in this is played by increasing the volume of recorded and analyzed data, as well as increasing the accuracy (resolution) of the devices used.

Also noteworthy is the effect of in-service monitoring and diagnostics on reducing the uncertainty associated with emerging properties (source #3), uncontrolled impacts and abrupt changes in operating conditions (source #4), based on experience gained from events that occurred during the past period of operation, and to some extent – with unknown factors (source #7).

The described approach has some inherent problems. They are caused, first of all, by the fact that the scope of monitoring and diagnostics is limited to the observing a relatively small number of safety-critical elements and recording a narrow set of key parameters. Otherwise, the complexity and energy consumption of the distributed structure of AMDS increase significantly, and its operation in real time becomes difficult. Another problem is the resistance of the AMDS components (sensors, communications and data processing units) to adverse operational factors, which must be maintained throughout the entire service life. The latter problem is especially relevant for nuclear power plants and spacecraft that operate for a long time without the possibility of repair or replacement of elements. In any case, the registration of physical processes is inevitably accompanied by errors, for the assessment and reduction of which the signals coming from the sensors must be periodically calibrated. In addition, a future forecast based on data collected during the past interval of the service life may prove invalid in the face of sudden, uncontrolled impacts and changes in operating conditions in the subsequent period. Finally, any decisions based on monitoring and diagnostics data are made by the operator, which means that human factors with its possible negative manifestations are not excluded from the system control loop.

4 Promising approaches to reducing uncertainty

4.1 Detecting and analyzing markers of potential sources of epistemic uncertainty

As shown in Section 2, the system under design and the conditions of its future operation may contain features that can serve as markers of potential sources of epistemic uncertainty. The approach presented below is aimed at detecting such markers and analyzing them in order to identify these sources and find opportunities to reduce uncertainty. The rationale for the approach is based on a retrospective examination of some situations in the past, when "unknown unknowns" hidden at the design stage unexpectedly emerged during operation. As a result of experimental and theoretical research, they were explained, thus moving into the category of "known unknowns". The essence of the proposed approach is as follows: despite the fact that the existing knowledge does not allow us to assume which unknown factors (existing beyond our knowledge) may emerge in a new design, some features of this design can indicate the potential for something unknown to appear, and these features are subject to preventive adjustment.

Markers of potential sources of epistemic uncertainty can be detected using special checks of the array of information representing the design. The first of them is the *check for emerging undesirable properties* of the system. The elastic follow-up discussed in Section 2 is one of these properties – a manifestation of metal creep at high temperatures in areas of discontinuity of geometric, and (or) mechanical characteristics of the structure and, accordingly, its stiffness. The criterion for the significance of this effect, when it should be paid attention to, can be considered an abrupt increase in the stiffness (or thickness) of one of the connected components relative to the other by at least two times. The fulfillment of such a criterion in a joint indicates adverse rheological behavior of this joint under cyclic loading. Before explaining the cause of this behavior, this structural feature served as a marker of the source of uncertainty in the cyclic strength of the joint. Currently, the quantitative assessment of the elastic follow-up is mandatory according to regulatory documents – see, for example (RCC-MR 2007) or (ASME 2010).

It cannot be excluded that an abrupt change in the characteristics of the system in the connections of its components (elements) may also be a marker of the source some other emerging undesirable properties (the third source in Table 1). To detect and analyze such markers, appropriate research is needed. It can form part of experimental and theoretical work to substantiate design solutions. Note that the specific properties of systems and their emergence are the subject of a special scientific and technical discipline – systems engineering, which has a developed methodological apparatus.

Apparently, the most dangerous emerging property is the *cliff-edge effect*. This is the name given to an abrupt change in the properties of a system or in the process profile that occurs when the influencing parameter slightly deviates from some characteristic value. The result is a significant change in the current operating situation. Cliff-edge effects can lead to irreversible consequences and interfere with system control. In nuclear power engineering, any cliff-edge effect must be excluded at the NPP design stage as a potential cause of deterioration in safety during operation (NP-001-15 2016).

Cliff-edge effects may be inherent not only to systems formed by a number of structural components (elements). Sometimes they appear in simpler cases, when the system can be considered a combination of a structural element, its environment (boundary conditions) and applied loads. Let us demonstrate cliff-edge effects using two such examples.

As a first example, we consider the loss of stability of an element – a thin-walled cylindrical shell – under a compressive load. The diagram on Fig. 1 shows the relationship between the compressive force P applied to the end of the shell and the displacement δ of this end.

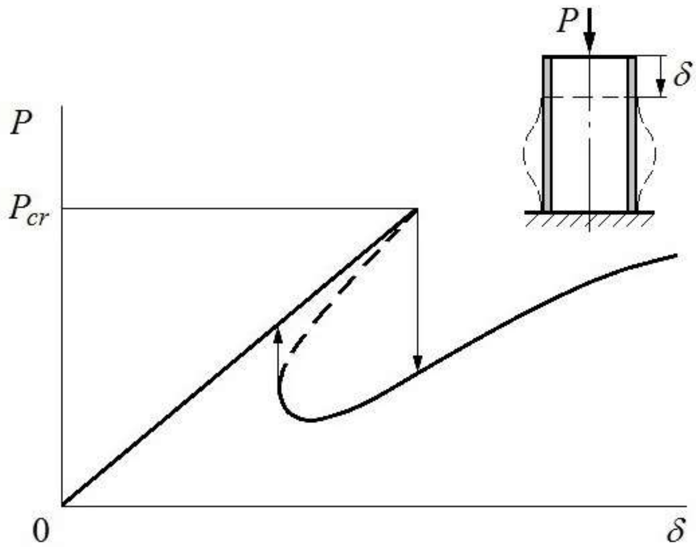

Fig. 1 First example of the cliff-edge effect: loss of stability of a cylindrical shell

Initially, the increase in P is accompanied by a proportional increase in δ, and the shell is being deformed in a stable manner. Upon reaching a critical value P_{cr}, which characterizes the loss of stability, the proportionality between the applied force and the displacement is violated, the shell collapses with the formation of buckling waves, and the deformation process jumps to the underlying branch of the $P(\delta)$ curve. This jump is shown by the downward arrow. Within the framework of the mathematical theory describing such phenomena, the loss of stability in the form of bifurcation (and, accordingly, the abrupt loss of the load-bearing capacity of a structural element) is considered a catastrophe (Arnold 1992). If there were no plastic strains during the deformation process and loss of stability, then the subsequent decrease in the compressive force P and accordingly displacement δ first corresponds to the lower branch of the curve, and then is accompanied by a reverse jump to the overlying branch (upward arrow), at which the buckling waves disappear. The occurrence of plastic strains makes the loss of the bearing capacity of the structural element irreversible.

Instability with catastrophic jumps from one state to another is also characteristic of oscillations in nonlinear systems. They are demonstrated by the second example: resonance in a nonlinear elementary oscillator – the simplest mechanical oscillatory system with one degree of freedom x. Its parameters are as follows: m (mass), $k(x)$ (nonlinear stiffness), and c (damping coefficient). The oscillations are excited by a force P that changes over time (t) according to a sinusoidal law with a frequency f and amplitude equal to 1, as shown in Fig. 2a. With a slow increase in the excitation frequency, starting from very small values, forced oscillations with amplitude $A = x_{max}$ arise in the oscillator. Fig. 2b shows the corresponding amplitude-frequency response curve $A(f)$, constructed under the assumption of small damping, which does not have a significant effect on the value of the resonant frequency.

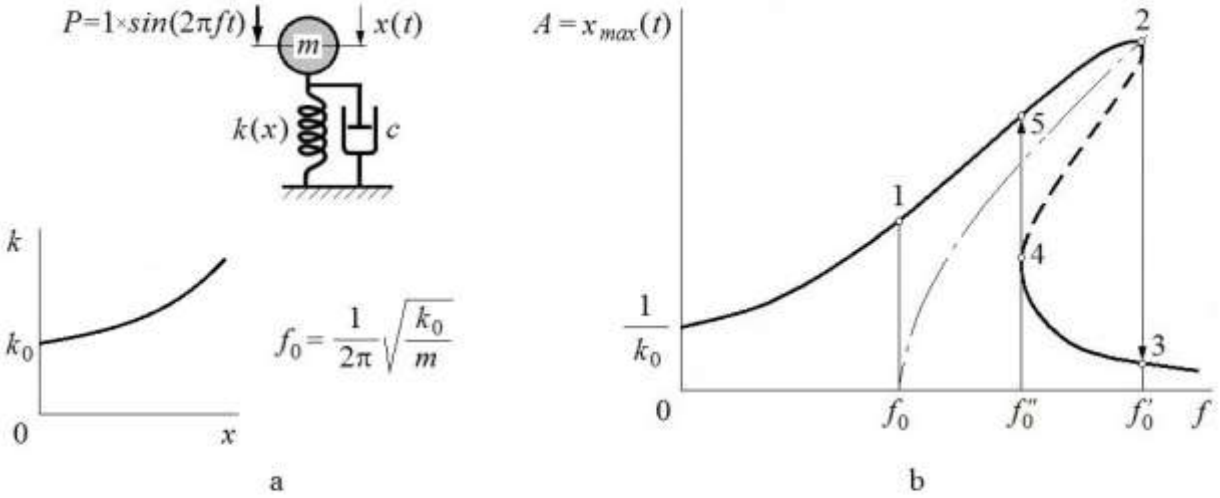

Fig. 2 Second example of the cliff-edge effect: resonance in a nonlinear oscillatory system: **a** nonlinear elementary oscillator, **b**: the amplitude-frequency response curve

If the system were linear, then as f approached the eigenfrequency (or natural frequency) of the system f_0, resonance would occur, i.e. a sharp increase in A. However, the nonlinear system passes the corresponding point 1 without resonance. It occurs when $f = f_0'$ $(f_0' > f_0)$, at point 2, and then the system jumps into the oscillation mode with a much smaller amplitude, corresponding to the lower, more stable branch of the amplitude-frequency response curve – to point 3. When moving in the opposite direction, i.e. slowly decreasing the frequency f and reaching the value $f_0^{"}(f_0 < f_0^{"} < f_0')$ at point 4, a jump into the oscillation mode with a larger amplitude occurs – to point 5.

When the exact properties of structural elements, including their critical loads P_{cr}, eigenfrequencies f_0, amplitude-frequency curves $A(f)$, jump frequencies f_0' and $f_0^{"}$ are not known (and this situation is typical for the design stage), the conditions of loss of stability, resonances and displacement values are difficult to predict. And these data can be crucial for ensuring strength, determining the parameters of control or diagnostic systems. This is why designers try to identify cliff-edge effects of a known nature in advance and prevent them using all available methods.

A marker of a potential cliff-edge effect – as one of the dangerous emerging properties or a source of possible unknown factors (the seventh source of uncertainty in Table 1) – can be considered a combination of the following aspects:

1) nonlinearity of the equations describing the behavior of the system (or its element) in a certain operating mode;
2) supplying the system (element) with energy due to working processes or interaction with the environment;
3) the existence in the state space of a system (element) of several possible states with close values of the main influencing parameter, but different levels of internal energy (this space is characterized either by an additional dimension free from applied loads, or by additional branches of state evolution; both options play the role of a channel through which excess internal energy can be released).

To the last aspect it remains to add that the release of the internal energy of the system through the above channel occurs very quickly; this process is practically uncontrollable and can have destructive consequences.

The next check of the design information may be the *detection and analysis of unexplained phenomena and contradictory facts* present in the data on prototypes or expected operating conditions of the system being created, as well as in the results of research substantiating the design. In this case, such phenomena and facts themselves serve as uncertainty markers – they indicate the presence of a source of uncertainty in the form of one or more unknown factors (the seventh source in Table 1). The detection of such markers necessitates their analysis within the framework of ongoing experimental and theoretical work or the conduct of new research with the corresponding goals and methodology.

Another procedure that helps to detect potential sources of epistemic uncertainty is the *check for complexity*. It should be carried out not only with respect to the technical system being created, but also to two other systems associated with it: the production system and the operation one (see Subsection 2.1). Complexity of any of them may cause unknown adverse factors to appear in life cycle processes. However, to act as a marker, complexity must be a measurable indicator, i.e. expressed quantitatively. The measure of the complexity of a system can be considered the amount of resources required for its monitoring, assessment of its state (health) and control. The resources can be considered the intensity of the corresponding work operations, the resolution of sensors and processor devices, time intervals of control actions and their intensity, etc. If sufficient resources are available, the system does not create any particular difficulties for its support even in the case of a large number of elements included in it. If the amount of resources is inadequate for the tasks of monitoring, assessment and control, the system is not fully traceable or controllable and should be considered complex. Thus, complexity depends on the scientific and technical level, material and organizational support for the design and post-design stages of the life cycle.

Nonlinearity has already been considered above as one of the factors that contribute to the emergence of cliff-edge effects that worsen the controllability of the system. Among the most adverse types of nonlinearity in this regard are the following:

1) nonlinearity with positive curvature in the control loop, when the gradient of the system response R to the control action X increases with increasing argument, as shown in Fig. 3a;
2) relay-type nonlinearity present in the dependence of some important property of the system C on the spatial coordinate or time θ – see Fig. 3b.

It is the detection of these types of nonlinearity that is the main goal of the *check for nonlinearity* due to their potential contribution to epistemic uncertainty. The corresponding markers are positive curvature and the above-mentioned peculiarities of functions describing the properties of the system that are important for performance, economy, or safety.

It should be noted that the second type of nonlinearity can not only generate a cliff-edge effect, but is also akin in form to it. The impact of nonlinearity as a source of uncertainty on the controllability of the system is similar to that of complexity. Thus, there is apparently a deep relationship between the three adverse features of the system: the potential for cliff-edge effects, complexity, and nonlinearity. The presence of such features in the system under design, if they are properly quantified, i.e. the presence of the markers described above, indicates possible sources of uncertainty pointed in Table 1 as #3 and #7.

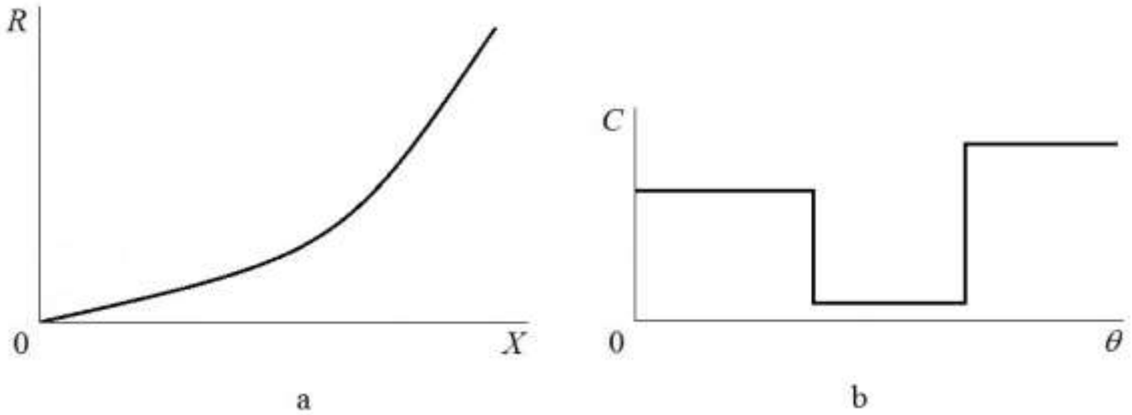

Fig. 3 Two adverse types of nonlinearity: **a** nonlinearity with positive curvature, **b** relay-type nonlinearity

4.2 Information support of the life cycle

When describing the concept of in-service monitoring and diagnostics in Subsection 3.4, the possibility of managing the life cycle of a technical system based on its actual state was mentioned. Creating such a possibility at the design stage is a significant shift in the existing design paradigm. It is obvious that a priori assumptions about the impacts on a system and the degradation of its properties during operation, specified in regulatory documents or taken from reference materials (all these are based on previous statistics), are justified for each specimen of a serially produced system only with some error. The presence of such an error generates uncertainty, which can lead either to insufficient economic efficiency (due to excessive conservatism of regulatory provisions or inevitable cautious when taking into account references), or to a safety deficit (in the case of rare extreme events not specified in regulatory documents and absent from reference materials). The approach outlined below is based on the principle that, in order to reduce uncertainty, each important, safety-related and long-operated technical object (or each specimen of a serially produced system of this kind) must be provided, along with in-service monitoring and diagnostics tools, combined in AMDS, with information support for the ongoing analysis of life cycle processes. This support must include:

– acquisition of data on all impacts on the system and changes in the state of its elements during the previous period of operation and construction on their basis of an *actual model of operation* (as an alternative to the a priori *design model of operation*);
– assessment of the actual damage (exhausted service life) of the structure and other subsystems of the system subject to degradation during this period;
– forecasting the further interval of safe operation (residual service life) provided that all operational factors are predictable and correspond to the actual model of operation.

Information support enables the operator to substantiate decisions on system life cycle management, including the following activities:

1) extension of operation when the forecasted residual service life of all elements is sufficient;
2) repair or replacement of elements that have exhausted their service life in order to maintain the operability of the system;
3) termination of operation of the system and its decommissioning when the service life of crucial elements that cannot be repaired or replaced is exhausted;
4) transition of the system with the service life of crucial elements exhausted to another, more gentle mode of use (as an object for training personnel, conducting research, etc.).

The idea of information support arose from the CALS (Continuous Acquisition and Lifecycle Support) concept, which emerged in the US military aviation in the 1970s, and its initial goal was to reduce logistical costs during aircraft maintenance and repair. Gradually, the CALS concept penetrated into other branches of technology, and its focus became reducing the overall costs of creating and maintaining a system by providing all participants in its life cycle with a single source of data in order to minimize errors in their transmission between different participants and stages of the life cycle. The carriers of data about a system are information and mathematical (including geometric) models. They are processed using application software of various types: CAE (Computer Aided Design), CAD (Computer Aided Engineering), CAM/CAPP (Computer Aided Manufacturing / Computer Aided Process Planning), etc.

The idea of information support led to the development of a corresponding scientific, technical and organizational concept, which was most developed, apparently, in the Russian nuclear power industry (Spirochkin and Evropin 2008), (SPiR-O-2008), (Evropin et al. 2009), (Spirochkin and Atroshchenkov 2009), (VERLIFE 2013), (OTT 1.5.2.01.999.0157-2013), (Spirochkin 2019). An important aspect of the research in which the author participated was the use of mathematical models of NPP elements taking into account the actual geometry and current properties, updated periodically in accordance with in-service monitoring and diagnostics data. The availability of such models makes it possible to go beyond the limited range of directly recorded parameters and conduct an analysis of the operating conditions and health of each element, as well as evaluate the main parameters of the NPP as a whole. This creates the potential to overcome at least those limitations of in-service monitoring and diagnostics that are associated with the complexity and energy consumption of a distributed network of sensors and communications. It is worth mentioning that complexity and energy consumption increase along with the growing requirements for data recording accuracy and processing speed.

Overcoming the above limitations contributes to a further reduction in aleatory uncertainty for each specimen of a serially produced system (the first source in Table 1) and, accordingly, to an increase in safety. In addition, information support of the life cycle can significantly reduce the epistemic uncertainty associated with the second source (hidden imperfections in the system and in the operating documentation). As with in-service monitoring and diagnostics, we note the influence of information support on reducing the uncertainty generated by the third, fourth and, in part, seventh sources (see Table 1).

At the same time, there remain problems associated with the participation of humans in information support (the fifth source of uncertainty) – as personnel maintaining the operation of the automated system, analytical engineers and chiefs making decisions on life cycle management. In addition, errors in analytical processing are not excluded, which are superimposed on errors in recording physical processes during in-service monitoring (the sixth source of uncertainty).

4.3 Designing a Smart, Pro-Active, Resilient System (SPARS Concept)

The concept of designing a smart, pro-active, resilient (including self-healing) technical system (SPARS) is based on the obvious position that when creating systems intended for long-term operation under conditions of insufficiently known factors, it is impossible to completely eliminate uncertainty. Therefore, solutions to the safety and efficiency problems associated with uncertainty, especially when systems are complex and important, should be sought by giving them properties similar to those of biological organisms – properties that increase their chances of survival in a dangerous, difficult-to-predict environment. These properties include: a sense of the internal state and the environment, understanding of emerging threats and readiness for them, situational response to any event, including unexpected one, and the ability to compensate for damage from adverse impacts (of course, in a certain range of their intensity).

The desired properties can be transformed into the following requirements: a system designed according to the SPARS concept must

1) "feel" its integrity, assess the performance of elements and draw a conclusion about the "safety of being in this state";
2) "observe" the environment, evaluate external factors in comparison with acceptable (specified for the design) conditions and conclude about the "safety of being here";
3) assess the possible danger of changes occurring inside and outside by comparing the changing impacts on the system with the potential for resistance to them based on actual (also subject to change) properties, and select a response mode that is acceptable from the prospect of "no loss of safety";
4) adequately respond to an adverse event (the possible culmination of the above changes), i.e. promptly perform actions aimed at minimizing the danger, for example, avoid extreme external impacts if the system is mobile and allows this to be done, or compensate for them by absorbing and dissipating energy;
5) assess in real time the development of adverse event (meaning the possibility of its transforming into an accident) and the current internal state according to safety criteria; in case of a safety deficit, perform special actions to protect people and maintain the operability of safety-critical elements, including localization and passivation of hazard factors, ensuring evacuation from the accident zone, as well as other actions that prevent an accident from developing into a catastrophe;
6) assess the state of the system and the environment according to safety criteria after the adverse event; draw a conclusion on life cycle management in relation to its subsequent interval, taking into account the efficiency criteria;
7) be able to recover, at least partially, if avoidance of extreme external impacts or their compensation were not fully successful and damage occurred in the system.

Design according to the SPARS concept is based on some ideas and technologies already used in practice and in turn develops them. Thus, the first two requirements correspond to the area of SHM presented in Subsection 3.4. Similar system properties, as well as partly items 4 – 6 of the above list, are close to the principles of Integrated System Health Management (ISHM) (Xu and Xu 2017) and Intelligent Health and Mission Management (IHMM) (Ranasinghe et al. 2022). Requirement 7 is in line with resilient engineering.

An important advance from the level of safety achieved by existing approaches (see Section 1) to the required higher indicators can be considered the property of proactivity (item 3), as well as the improvement of the active and reactive properties of the system (items 4 to 6). These properties should be implemented, given the high speed of physical processes characteristic of the development of accidents, obviously using AI tools, e.g. neural networks. A favorable outcome in each such case can become an additional practical example for training a neural network implementing the management of critical and emergency situations.

The described concept is a kind of refraction of the idea of bionic (biologically inspired) design. In this case, bionic principles apply primarily to the behavior of the system, and not to its structure, as is usually done. An important part of implementing the SPARS concept is the formation of multi-level protection that could ensure

- prevention of a critical situation that may arise as a result of one or more adverse events, with the threat of escalating into an accident;
- in case of ineffective prevention – management of the critical situation in order to prevent an accident;
- if it is impossible to prevent – accident management in order to minimize losses and prevent a possible catastrophe;
- the possibility of recovery after an accident, for example, using replaceable or repairable modules.

At present, such protection is provided, in particular, for nuclear facilities. The complex of protective measures against a possible radiation or nuclear accident is specified by regulatory documents being in use in various countries. In the Russian nuclear power industry, it includes five levels of protection (or defense) implemented both during design and operation of NPPs (NP-001-15 2016). The number of independent levels of defense-in-depth can be considered as one of the direct safety indicators (Spirochkin 2019). The same principle is also used in aerospace engineering, but a significant part of the control functions remains with human operator (pilot, air traffic controller or other members of the operating personnel), therefore negative manifestations of human factors in the control process are possible. Thus, air-, space-, and aerospace vehicles represent even broader area for implementing the SPARS concept than nuclear power industry. Research and development in this area is currently ongoing, and their results related to aerospace vehicles will be described in one of the author's next publications.

Creating a technical system according to the SPARS concept allows designer to reduce uncertainty generated by almost all its sources listed in Table 1. In particular, it is possible to solve problems related to the impact of human factors (the fifth source of uncertainty), which limit the potential of information support (see Subsection 4.2). The development of analytical methods and AI tools used within the framework of this concept should also affect the reduction of uncertainty caused by errors in experimental and computational substantiation (the sixth source).

It can be expected that the innovative aspects of the SPARS concept will be difficult to implement and/or uneconomical for serially produced systems, such as airliners, which are characterized by a combination of high levels of performance, cost-effectiveness, and safety. As a rule, these three indicators contradict each other, and in reality only a certain compromise between them is achievable. Thus, modern civil aircraft have very limited capabilities for accident management, in particular, ensuring the survival of occupants in a crash landing. In this case, one has to rely only on the skill of the pilots, seat belts, and the correct "emergency" position (Spirochkin 2021). Regulatory documents in this area contain provisions that "should be considered minimal requirements and not representative of the current state-of-the-art in occupant protection" (Shanahan 2004).

It is likely that manufacturers of serially produced systems, pursuing primarily economic goals, are not sufficiently motivated to finance research and development aimed at increasing safety beyond the level currently accepted by society. It is certain that the costs of designing according to the SPARS concept will increase the cost of the system being created. However, they should be compared with the potential losses in an unpredictable adverse event. This is especially true for new types of systems, the full testing of which may take years, but does not guarantee that all dangerous situations have been investigated. Given the possibility of unspecified hazards, a reasonable strategy of design should be considered one that increases the chances of a safe outcome even in an unforeseen situation. It is this strategy that corresponds to the SPARS concept.

Conclusion

The main motive of this research is that in order to guarantee safety of a technical system under design, the existing uncertainty regarding the conditions of its future operation, response to operational impacts and changes in the internal state should be reduced to a minimum. The presented results of the research allows for concluding:

1. The currently widely used methods of accounting for uncertainty and reducing it at the design stage are based mainly on statistical data from previous experience and on the conservatism of probabilistic or other analytical estimates. Due to the limited experience and difficult-to-predict extreme events, the corresponding a priori assumptions about the operation stage of a new designed system may contain a significant amount of uncertainty, which is why safety is not fully ensured.
2. In industries important for safety and innovation-driven, in addition to traditional methods, approaches are used that allow designers to correct a priori assumptions and, accordingly, reduce uncertainty to a greater extent. They include: refining probabilistic estimates through experiments at the design stage, determining the actual properties of the system and the impacts on it through post-design tests, pilot projects, in-service monitoring and diagnostics.
3. Along with the above, promising approaches capable of ensuring a further reduction in uncertainty through a more in-depth analysis of design information, its updating during operation and the implementation of bionic principles in combination with the minimization of the negative impact of human factors are becoming increasingly important. These approaches cover detecting and analyzing markers of potential sources of epistemic uncertainty, information support of the life cycle, designing a smart, proactive, resilient system (the SPARS concept).
4. Each of the presented approaches has the potential to suppress one or more sources of uncertainty, and the combination of these approaches provides a significant reduction in overall uncertainty.
5. The implementation of these approaches undoubtedly leads to additional expenses that increase the cost of the system being created. However, such an increase should be considered an inevitable price for safer technologies in the world full of uncertainty and unpredictability.

References

Arnold VI (1992) Catastrophe theory. 3rd ed. Berlin, Springer

ASME (2010) 2010 ASME Boiler & Pressure Vessel Code. Section III. Rules for Construction of Nuclear Facility Components. Division 1, Subsection NH – Class 1 Components in Elevated Temperature Service. ASME, New York, NY

ASME PTC 19.1-2005 (2006) Test uncertainty. An American National Standard. ASME, New York, NY

Aven T and Steen R (2010) The concept of ignorance in a risk assessment and risk management context. Reliability Engineering & System Safety, 95(11):1117-1122

Beer M, Ferson S, Kreinovich V (2013) Imprecise probabilities in engineering analyses. Departmental Technical Reports (CS). 734. https://scholarworks.utep.edu/cs_techrep/734. Accessed 2024-10-17

Beer M, Ferson S and Kreinovich V (2016) Do we have compatible concepts of epistemic uncertainty? Departmental Technical Reports (CS). 1006. https://scholarworks.utep.edu/cs_techrep/1006. Accessed 2024-07-15

Bernstein PL (1996) Against the gods: the remarkable story of risk. Wiley, New York, NY

Blumsack S (2023) Decision analysis without probabilities. The Pennsylvania State University. EME 801: Energy Markets, Policy, and Regulation. Lessons. Lesson 6 – Cost-Benefit Analysis and Decision Making. https://www.e-education.psu.edu/eme801/node/577. Accessed 2024-10-24

Capitanescu F and Wehenkel L (2013) Computation of worst operation scenarios under uncertainty for static security management. IEEE Transactions on Power Systems, 28(2):1697-1705

Cocron A and Aronhime L (2022) Risk, uncertainty and innovation. NATO Review. Opinion, analysis and debate on security issues, 14 April 2022. https://www.nato.int/docu/review/articles/2022/04/14/risk-uncertainty-and-innovation/index.html. Accessed 2024-03-11

Dédale JP (2013) Why a paradigm shift is needed. IAEA International Experts' Meeting on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant. Vienna, Austria, May 21-24, 2013. Conference ID: 45441 (I2-CN-212). https://www-pub.iaea.org/iaeameetings/IEM5/IEM5_Jean%20Paries_Dedale_France.pdf. Accessed 2024-03-11

Dempster AP (1967) Upper and lower probabilities induced by a multivalued mapping. Annals of Mathematical Statistics, 38(2):325-339

Ellsberg D (1961) Risk, ambiguity, and the Savage axioms. Quarterly Journal of Economics, 75(4):643-669

Evropin SV, Obushev AE, Spirochkin YK, Petrenko AV (2009) Guidelines and dataware for life cycle management for NPP pipeline supports. Proceedings of the 20th International Conference on Structural Mechanics in Reactor Technology (SMiRT 20), Division 6. Design and Construction Issues, Paper 1774. http://www.lib.ncsu.edu/resolver/1840.20/23809. Accessed 2024-05-06

Gong J, Wang X, Lv T (2023) A credible interval analysis method for uncertain structures under nonprobabilistic framework. Computer Methods in Applied Mechanics and Engineering, Volume 404, Article 115833

Gumbel E (1962) Statistics of extremes. Columbia University Press, New York, NY

Gupta AK (2021) Fuzzy logic and their application in different areas of engineering science and research: a survey. International Journal of Scientific Research in Science and Technology, 8(2):71-75

Haug EJ, Choi KK, Komkov V (1986) Design sensitivity analysis of structural systems. Academic Press, Inc., Orlando, FL

Hébert-Dufresne L, Allard A, Garland J, Hobson EA and Zaman L (2024) npj Complexity 1(4). https://doi.org/10.1038/s44260-024-00004-0

Jawad MH, Jetter RI (2009) Design and analysis of ASME boiler and pressure vessels components in the creep range. ASME Press, New York, NY

Keynes JM (1937) The general theory of employment. The Quarterly Journal of Economics, 51(2):209–223

Klauer B, Brown JD (2004) Conceptualising imperfect knowledge in public decision-making: ignorance, uncertainty, error and risk situations. Environmental research, engineering and management, 1(27):124-128

Knight FH (1921) Risk, uncertainty and profit. Houghton Mifflin Company, The Riverside Press Cambridge; Boston and New York

Lempert RJ, Popper SW, Bankes SC (2003) Shaping the next one hundred years: New methods for quantitative long term strategy analysis, MR-1626-RPC. The RAND Pardee Centre, Santa Monica, California

Modares M, Mullen RL (2014) Dynamic analysis of structures with interval uncertainty. Journal of Engineering Mechanics, 140(4), https://doi:10.1061/(ASCE)EM.1943-7889.0000660

Moore RE (1966) Interval analysis. Prentice-Hall, Hoboken, NJ (Prentice-Hall series in automatic computation)

Moore RE, Kearfott RB, Cloud MJ (2009) Introduction to interval analysis. Society for Industrial and Applied Mathematics, Philadelphia, PA

Newman MEJ (2005). Power laws, Pareto distributions and Zipf's law. Contemporary Physics 46(5):323-351

Nielsen J (1994) Enhancing the explanatory power of usability heuristics. Proc. ACM CHI'94 Conference "Human Factors in Computing Systems", Boston, MA, April 24-28, 1994, pp. 152-158

Nielsen J and Molich R (1990) Heuristic evaluation of user interfaces. Proc. ACM CHI'90 Conference "Human Factors in Computing Systems", Seattle, WA, 1-5 April, 1990, pp. 249-256

Oberkampf WL, Trucano TG, and Hirsch C (2003) Verification, validation, and predictive capability in computational engineering and physics. Report SAND2003-3769. Sandia National Laboratories, Albuquerque, NM, and Livermore, CA

Patelli E, Alvarez DA, Broggi M, de Angelis M (2014) Uncertainty management in multidisciplinary design of critical safety systems. AIAA. https://core.ac.uk/download/pdf/80778445.pdf. Accessed 2024-10-22

Pich MT, Loch CH, De Meyer A (2002) On uncertainty, ambiguity, and complexity in project management. Management Science, 48(8):1008–1023

Pierre RSQ (2015) Heuristics in design: a literature review. Procedia Manufacturing, 3:6571-6578. https://doi.org/10.1016/j.promfg.2015.07.961

Rao SS and Berke L (1997) Analysis of uncertain structural systems using interval analysis. AIAA Journal, 35(4):727-735

Ranasinghe K, Sabatini R, Gardi A, Bijjahalli S, Kapoor R, Fahey T, Thangavel K (2022) Advances in Integrated System Health Management for mission-essential and safety-critical aerospace applications. Progress in Aerospace Sciences, Vol. 128, 100758

RCC-MR (2007) Design and Construction Rules for Mechanical Components of Nuclear Installations. Section 1 – Nuclear Installation Components. AFSEN, Paris

Rumsfeld D (2010) Known and unknown: authors note. From pages XIII-XVI. The Rumsfeld Papers. December 2010. https://papers.rumsfeld.com/about/page/authors-note. Accessed 2024-03-11

Russell B (1912) The problems of philosophy. Home University Library, 1912; Oxford University Press paperback, Oxford (UK), 1959

SAE ARP6461A (2021) Guidelines for implementation of structural health monitoring on fixed wing aircraft. Rev. A. Aerospace Recommended Practice. SAE International

Saunders FC, Gale AW, Sherry AH (2015) Conceptualising uncertainty in safety-critical projects: a practitioner perspective. International Journal of Project Management, 33(2):467-478

Sause MGR, Jasiūnienė E (eds) (2021) Structural Health Monitoring damage detection systems for aerospace. Springer (Series: Springer Aerospace Technology)

Schneier B (2010) Worst-case thinking. Schneier on Security, May 13, 2010. https://www.schneier.com/blog/archives/2010/05/worst-case_thin.html. Accessed 2024-10-22

Schofield J (2007) Beyond defect removal: latent defect estimation with Capture-Recapture Method. CrossTalk, The Journal of Defense Software Engineering, 20(8):27-29

Shafer G (1976) A mathematical theory of evidence. Princeton University Press, Princeton and London

Shanahan DF (2004) Human tolerance and crash survivability. In: RTO Educational Notes. EN-HFM-113. The Research and Technology Organization of NATO, 2005, pp 6–1, 6–16. Paper presented at the RTO HFM Lecture Series on "Pathological Aspects and Associated Biodynamics in Accident Investigation", held in Madrid, Spain, 28–29 Oct 2004; Königsbrück, Germany, 2–3 Nov 2004

Silver N (2012) The signal and the noise. Why so many predictions fail – but some don't. Random House, New York, NY

Singh H, Gupta MM, Meitzler T, Hou Z-G, Garg KK, Solo AMG, and Zadeh LA (2013) Real-life applications of fuzzy logic. Advances in Fuzzy Systems. Volume 2013, Article ID 581879, http://dx.doi.org/10.1155/2013/581879

Sotiropoulos DG, Tserpes K (2022) Interval-based computation of the uncertainty in the mechanical properties and the failure analysis of unidirectional composite materials. Mathematical and Computational Applications, 27(3):38, https://doi.org/10.3390/mca27030038

Spirochkin Y (2023) Human factors and design. Springer, Singapore

Spirochkin Y (2024) What artificial intelligence brings to aviation: new opportunities or new risks? ResearchGate, 18.02.2024. http://dx.doi.org/10.13140/RG.2.2.19525.63203. Accessed 2024-03-11

Stirling A (2007) Risk, precaution and science: towards a more constructive policy debate. Talking point on the precautionary principle, EMBO Reports, 8(4):309–315

Swain AD, Guttmann HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. SAND80-0200. RX, AN. Final report. Sandia National Laboratories, Albuquerque, NM

Taleb NN (2007) The Black Swan. The impact of the highly improbable. Random House, New York, NY

Taleb NN (2020) Statistical consequences of fat tails: real world preasymptotics, epistemology, and applications (Technical Incerto Collection). STEM Academic Press

Taylor J (1965) Manual on aircraft loads. Pergamon Press, Oxford; London

Turner JR (2005) The role of pilot studies in reducing risk on projects and programmes. International Journal of Project Management, 23(1):1–6

VERLIFE (2013) Guidelines for integrity and lifetime assessment of components and piping in WWER nuclear power plants. IAEA, Vienna. Appendix F – Component and piping supports (Contributors: Obushev A, Spirochkin Y)

Willett AH (1901) The economic theory of risk and insurance. The Columbia University Press (Reprint for the S.S. Huebner Foundation for Insurance Education, University of Pennsylvania, by Richard D. Irwin, Inc., Homewood, Illinois, 1951)

Xu J, Xu L (eds) (2017) Integrated system health management. Academic Press

Yen J (1999) Fuzzy logic – a modern perspective. IEEE Transactions on Knowledge and Data Engineering, 11(1):153-165

Yilmaz S, Daly SR, Seifert CM, Gonzalez R (2011) A comparison of cognitive heuristics use between engineers and industrial designers. In: J.S. Gero (ed) Design Computing and Cognition '10, pp 3-22. Springer, Dordrecht, Netherlands. https://doi.org/10.1007/978-94-007-0510-4_1

Zadeh LA (1965) Fuzzy sets. Information and Control, 8:338-353

Sources in Russian:

Arkadov GV, Pavelko VI, Usanov AI (2004) Vibroshumovaya diagnostika WWER (Vibration and noise diagnostics of WWER). (Ed. by A.A. Abagyan). Energoatomizdat, Moscow

Gladkii VF (1982) Veroyatnostnye metody proektirovaniya konstruktsii letalelnogo apparata (Probabilistic methods for designing spacecraft structures). Nauka, Moscow

Makarevskii AI, Korchyomkin NN, Frantsuz TA, Chizhov VM (1975) Prochnost samolyota (metody normirovaniya raschyotnykh uslovii prochnosti samolyota) (Aircraft strength (methods for standardizing the design criteria of aircraft strength)). Ed. by academician A.I. Makarevskii. Mashinostroenie, Moscow

NP-001-15 (2016) Federalnye normy i pravila v oblasti ispolzovaniya atomnoi energii. Obshchie polozheniya obespecheniya bezopasnosti atomnykh stantsii (Federal regulations and rules in the field of atomic energy use. General provisions for ensuring safety of nuclear power plants). Federal Environmental, Technological and Nuclear Supervision Service of Russia, Moscow

OTT 1.5.2.01.999.0157-2013 (2013) Opornye konstruktsii elementov atomnykh stantsii s vodo-vodyanymi energeticheskini reaktorami. Obshchie tekhnicheskie trebovaniya (Support structures for elements of nuclear power plants with water-water power reactors. General technical requirements). JSC Concern Rosenergoatom, Moscow (Contributors: Spirochkin YK, Obushev AE, Filimonov SV, Sorokin AN, Tarakanov PV et al.). https://meganorm.ru/Index2/1/4293736/4293736524.htm. Accessed 2024-10-11

Patrushev VS, Pletnyov IV, Spirochkin YK (1989) Aviatsionno-kosmicheskii trenazhyor (Air-spacecraft simulator). Patent SU 1799479, 24 Nov 1989

Rzhanitsyn AR (1978) Teoriya rascheta stroitelnykh konstruktsii na nadezhnost (Theory of calculating building structures for reliability). Stroiizdat, Moscow

Spirochkin YK (1987) Metodika raschyota dinamicheskogo nagruzheniya gruzhov pri avariinoi posadke letatelnogo apparata (Method for analyzing dynamic loads on items of mass during an aircraft emergency landing). Dissertation. NPO *Energia*, Kaliningrad (now Korolyov), Moscow region

Spirochkin YK (1988) Iskhodnye dannye na provedenie eksperimentalnykh issledovanii parametrov reaktsii posadochnoi poverkhnosti s ispolzovaniem zhyostkikh maketov. Otchet P 26478-017 (Baseline data for experimental studies on the landing surface reaction parameters using rigid mockups. Report P 26478-017). NPO *Energia*, Kaliningrad (now Korolyov), Moscow region

Spirochkin YK (1993) Komp’yuternoe modelirovanie dinamiki konstruktsii pri avariyakh (Computer simulation of structural dynamics in accidents). Matematicheskoe modelirovanie (Mathematical Models and Computer Simulations), 5(6):85–103

SPiR-O-2008 (2009) Svod Pravil i Rukovodstv po Opornym konstruktsiyam elementov AES s WWER (Code of rules and guides on supports for elements of nuclear power plants with WWER). Standard of organization. ENES, Moscow (Contributors: Evropin SV, Filatov VM, Golovlyov YN, Obushev AE, Rodchenkov BS, Spirochkin YK et al.)

Spirochkin YK, Evropin SV (2008) Podkhody k informatsionnomu soprovozhdeniyu prochnosti YaU v techenie zhiznennogo tsikla (Approaches to information-driven support of the strength of nuclear facilities during the life cycle). Godovoi otchyot FGUP NIKIET - 2008: Sb. statei/ Pod red. E.O. Adamova (In E.O. Adamov (ed) Annual report of NIKIET - 2008: Collection of articles), pp 120-121. NIKIET, Moscow

Spirochkin YK, Atroshenkov RS (2009) Primenenie IPI (CALS-tekhnologii) v sovremennoi yadernoi energetike (Application of IPI (CALS technologies) in modern nuclear power industry). Komp'yuternye tekhnologii analiza inzhenernykh zadach mekhaniki: Lektsii I Mezhdunarodnoi nauchnoi shkoly dlya molodezhi (Computer technologies for analysis of engineering problems in mechanics: Ist International Scientific School for Youth), IMASh RAN, 9-13 November 2009. Sbornik lektsii (Collection of lectures), pp 36-42. A.A. Blagonravov Institute of Machine Science of the Russian Academy of Sciences (IMASh RAN), Moscow

Spirochkin YK (2019) Bezopasnost rossiiskikh AES s tochki zreniya inzhenera-mekhanika (Safety of Russian nuclear power plants from the viewpoint of mechanical engineer). SUPER Publishing House, Saint Petersburg

Spirochkin YK (2021) Bezopasnost i ekonomichnost – pravilno li vybran kompromiss? (Safety and economy – is the compromise chosen correctly?). AviaSafety.ru, December 22, 2021. https://aviasafety.ru/39382. Accessed 2024-10-11

Stepnov MN (1985) Statisticheskie metody obrabotki rezultatov mekhanicheskikh ispytanii: Spravochnik (Statistical methods for processing mechanical test results: Handbook. Mashinostroenie, Moscow

Sukhoruchenkov BI, Okorokov MV (2014) Otsenki pokazatelei vozmozhnykh defektov tekhnicheskikh system, ne vyiavlennykh posle otrabotochnykh ispytanii (Estimates of indicators of possible defects of technical systems not identified after development tests). Dvoinye tekhnologii (Dual technologies), No. 1(66), pp 12-18

Ventsel ES (1969) Teoriya veroyatnostei (The probability theory). 4th ed. Nauka, Moscow