Original article
https://doi.org/10.21683/1729-2646-2019-19-4-53-64

On the nature of risk in the safety management of structurally complex systems

Alexander V. Bochkov, *Gazprom Gaznadzor Ltd, Russian Federation, Moscow*

Alexander V. Bochkov

Abstract. Aim. *In the general case, a risk-oriented approach encompasses probabilistic methods of emergency processes and events simulation as well as deterministic methods. The use of probabilistic and deterministic estimations has been the focus of research aiming to improve safety and operational procedures. However, the experience of using probabilistic analysis only (essentially, one-criterium tool) has shown that this approach does not encompass all the required aspects of safety. The aim of the paper is to introduce (update) the definitions of the very concepts of "analysis" and "synthesis" as regards the risks for the purpose of research of safety of structurally complex systems (SCS) and design of systems for monitoring hazards and threats to their stable development thereof.* **Method.** *The paper examines – from the point of view of systems science – the method of analysis and synthesis of risks as a development tool of advanced systems for monitoring SCS safety threats. The paper compares the primary current concepts of risk management in SCS and has shown that they should be developed and improved. A type of risk functionality is proposed that allows defining a safety solution by the value of mathematical expectation of losses, with appropriate corrections taken into account.* **Result.** *The concept of "risks synthesis" is introduced as a scientific tool integrated with analysis that takes into consideration the existing connections between the elements of considered SCS in terms of a whole system in its entirety. Principles are formulated for the collection of comprehensive sets of data required for decision-making.* **Conclusion.** *The proposed approach paves the way for the development of the method of risks synthesis and suggests the development of advanced expert systems to support decision-making regarding the safety of SCS as multifunctional and multilevel systems intended for both recording and analysis of each individual case (event), and prediction of trends and preparation of prevention measures as necessary.*

Keywords: *structurally complex system, critical infrastructure facilities, risk, synthesis, analysis, safety, management.*

For citation: *Bochkov AV. On the nature of risk in the safety management of structurally complex systems. Dependability 2019; 4: 53-64. https://doi.org/10.21683/1729-2646-2019-19-4-53-64*

Received on 26.08.2019 / Revised on 23.10.2019 / For printing 14.12.2019

…Most scientists strive to learn the structure, composition and content of their subject, decomposing it into parts. They try to understand how parts make up a whole. Sometimes it resembles the desire to take a watch apart to understand what the time is.

Aksyonov G.P. [1]

Introduction

Risk analysis and risk assessment are the focus of many researches, whose number has been growing rapidly lately. Figure 1 shows the increase in the frequency of the word "risk" occurrence (per million words per year) in English-language publications from the moment it was first mentioned in 1661 till present.

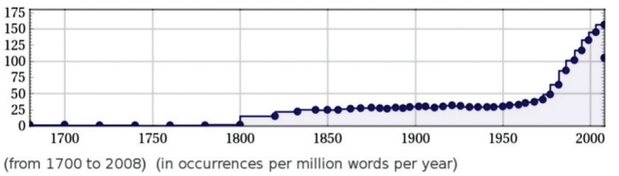

Figure 1. Frequency of occurrence of the word "risk" [2]

This is partly due to the general "trend" for research in this area, but partly it is a response to the challenges of the time when a large number of mutually overlapping and partially integrated systems of different purposes made by man significantly has shaken the general sustainability of social development and has given rise to dangers and threats that are hard to predict. A whole new direction in systems engineering has even appeared that deals with the engineering of systems, whose individual parts can exist independently, were developed independently, and thus are a complete target system. Risk is often a conscious threat, and therefore being the focus of researchers' increased interest. However, their efforts are often very clearly illustrated by the words of G.P. Aksyonov, biographer of V.I. Vernadsky, cited in the epigraph.

In this regard, it is especially relevant to introduce (update) the very concepts of "analysis" and "synthesis" as applied to risks. Analysis and synthesis are not two different ways of cognition, but are opposites of one cognizing consciousness, separable only in abstraction. For example, A. Kazennov [3] shows that the basis of this unity is their origin from practical analysis and from research in general. "... the generic word for analysis," he writes, "is not "decomposition" (including mental decomposition) of a subject, but "research". And a specific difference of a definition is "distinguishing parts of the whole and their relationship to each other through this whole." Not decomposition, but distinction... It is only necessary to find the point of identity of the "part" and the whole, one part and the other "parts".

At the same time, the identification of different parts with each other unites objects (in this case, parts) into a whole. And that is already synthesis. While analysis should be defined as follows: analysis is a study that distinguishes parts of an object and correlates them with the whole and with each other through this whole. The whole in the analysis is the initial thing, mediating the whole course of research. In general parts are already distinguished before this study by previous practical and theoretical studies: analytical and synthetic cognition... synthesis is a study that considers the ratio of different parts of an object and their whole through the essence (essential part) of the whole. Finding such an essence or an essential part is a fundamental scientific discovery that sheds new light on all previous concepts expressing the essence of an object. It reorganizes the whole system of concepts and, accordingly, the whole theory".

This approach seems to be the most constructive for risk assessment. This is especially important when studying a system of systems and the so-called critical infrastructure problem related to that and often discussed in recent years [4-9]. The problem is that almost in all of the most important economy's sectors there are systems with such spatially distributed elements (sometimes these systems are also classified as geographically distributed) that it is practically impossible in practical terms to fully protect all objects of one particular sector, not to mention all the sectors of a system. The main issues and problems of a decision maker (DM) in the field of ensuring the safe functioning of such systems are the issues related to assessing threats and risks that are significant for the system as a whole and for its elements and prioritizing the protection of critical infrastructure elements and objects, taking into account usually limited resources at his disposal.

Besides large sizes, many sectors are so complex that it is technologically and economically impossible to predict and calculate all the consequences of any incident, regardless of whether the incident is caused by the malicious actions of people or is the result of natural disasters. Generally, it is extremely difficult to predict the consequences of small disturbances in one part of the critical infrastructure for its other sections. For example, all Internet communications in South Africa were completely terminated due to the fall of the twin towers as a result of the terrorist attack on the United States on September 11, 2001. And the relatively minor malfunctions in First Energy's electric payload in Ohio (USA) accelerated blackout in August 2003, affecting 50 million people thousands of kilometers away from the source of the problem [10-12].

In fact, the existing infrastructure is vulnerable simply because it contains so many very closely interconnected components that for most technical consultants, analysts and decision makers who determine its safety policy, this becomes an impossible task.

The notion of structural complexity, as well as the notion of a system in general, has not yet been unambiguously defined. At the same time, modern requirements for the construction of safety systems and the effectiveness of their

functioning have been and still are quite high. As a result, there are tasks of choosing priority equipment facilities from their total population and the optimal distribution of financial and material resources available to the system owner (proprietor, state) for their protection. The notion of optimality regarding risk synthesis will be discussed later. First, it is necessary to deal with the notion of risk, its ontology. You can only measure what is clearly defined, although A. Einstein argued that "the world is not a quantitative concept, but a qualitative one".

People would get rid of half of their problems if they could agree on the meaning of words…

René Descartes

1. On the nature of risk and safety approaches

Risk is a notion arising at the boundary of dependability and safety. The technology itself and the production systems do not take risk. It is a man who always takes risk. Dependability is the ability of a technical object to function continuously and fail-safely with 100% level of efficiency. When analyzing dependability, the main criterion is the failure criterion, which divides everything into "yes" (operational state) and "no" (non-operational state). Dependability depends, so to speak, on the internal properties and characteristics of an object (quality, time to failure, technological features, operation requirements, etc.). Safety is the ability of the same object to perform its functions without causing damage to maintenance personnel, the environment, etc. Safety depends on the external properties (environment, threats, personnel qualification). Moreover, safety is both a sense and a state. The safety status is determined by the development of appropriate technologies and is evaluated using mathematical modeling methods; it is based on the analysis and assessment of risks and the effectiveness of various measures, means and mechanisms of protection. A sense of safety is a person's psychological reaction to threats and risks, and the psychological perception of the adequacy of protective measures; what is known as the level of acceptable risk (i.e. from what threats a person is ready not to defend themselves, what damages are acceptable to them). In the meaning that the sense of security can subjectively change, one can agree with the statement of Bruce Schneider, an American cryptographer, writer and computer security specialist: "Security is a process, not a product". But this does not mean that the safety process has no purpose. The purpose of safety is to achieve a state of safety of man and environment that corresponds to their subjective sense of danger (i.e. an acceptable level of risk). To achieve this goal, the so-called "risk-oriented approach" is used.

Risk occurs as a hazard assessment for a person performing work using technical devices. Since there are latent defects and uncertainties in the place and time of failure and hazard occurrence both in dependability and safety assessment, risk is often interpreted as the effect of uncertainties on the achievement of the goals set by a human operator. Specifics occur when a specific mechanism (an object, an industrial enterprise, a corporation, etc.) used by man person uses to realize the goals of an activity in a certain environment (which, in turn, is characterized by the presence of threats, environmental features, and the presence of competitors with their own goals, etc.) is considered.

In living systems, for example, instability is used practically: it is one of the most important driving forces of evolution. One can say that the high adaptability of living organisms is a consequence of their instability. A well-known advocate of "controlled instability" Nassim Taleb also repeatedly emphasized that multilevel redundancy is the main property of natural (living) systems that controls risk [13]. Just like in living systems, unstable processes in safety systems are key to their adaptability to changing threats and dangers.

With some reserve, risk can be considered as the best measure to quantify a hazard. This concept is widely used in modern literature and often implies completely different meanings. In the most general case, risk is characterized by the probability of a negative effect, the probability that a negative effect of a particular type occurs, and the probability that this type of effect causes a certain amount of deviation of the state of an effected subject from its dynamic balance. In other words, risk is a vector variable that can describe different types of hazards with all its values given above being its constituent parts. Since the main issues discussed below are one way or another related to ensuring the safety of industrial facilities, the term "risk" shall mean the risk of anthropogenic or, more specifically, industrial origin, unless otherwise specified.

The first approximation in issues related to ensuring safety is very often the requirement to achieve a negligibly small or "zero" risk associated with some (generally) production activities. Therefore, the safety systems that were created and used in industries were often engineering solutions aimed at fulfilling the requirements of absolute safety. The basic principle in creating these systems is the so-called ALAPA principle (As Low As Practicably Achievable). According to this principle, the industrial safety should be increased by any means and regardless of the level achieved, if it is technically feasible. In other words, according to ALAPA, one should construct technical safety measures that would prevent emergency situations, i.e. eliminate the very possibility of the occurrence and development of an accident. The complication of technologies has led to the fact that it is often simply impossible to predict all scenarios of an accident development and, therefore, to provide engineering and organizational solutions to prevent them, that being once again shown by the accidents in Chernobyl and Fukushima. All that required a fundamentally new approach to solving safety problems.

Over the past three decades, a significant number of works have been devoted to these issues, which convincingly confirmed the already axiomatic notion that achieving absolute safety is impossible.

The risk philosophy based on the concept of absolute safety inevitably came to the concept of acceptable risk. The concept of acceptable risk required the abandonment of the ALAPA principle and the adoption of a new ALARA principle (As Low As Reasonably Achievable). According to ALARA, the required level of safety is determined based on the social and economic conditions of the society development. For accidents with a risk higher than acceptable, it is necessary to use engineering solutions to prevent and mitigate the consequences, and for accidents with a risk less than acceptable, only mitigating measures are needed. In the nuclear energy sector, for example, this principle is reflected in the relevant safety provisions. For SCS, the concept of acceptable (maximum allowable) risk is introduced meaning the level of risk which is acceptable and justified on the basis of economic and social considerations. To this date there are still no full-fledged methods for determining the acceptable risk for hazardous industrial facilities of the SCS. It can be said that at present, the safety problems are resolved by deciding by what means and to what level the risk should be reduced to reach the optimal safety level of both humans and the environment, based on certain criteria.

Risk analysis is the only way to investigate those safety issues that cannot be answered by statistics, such as low probability accidents with severe potential consequences. Naturally, risk analysis is not a solution to all safety tasks, but it is the only way to compare risks from various sources of danger, identify the most significant of them, choose the most effective and cost-effective systems to increase safety, develop measures to mitigate consequences, etc.

In foreign literature, along with the concept of "risk analysis" (Risk Analysis), they use the PRA method (Probabilistic Risk Analysis) established by the NRC (Nuclear Regulatory Commission). There is no fundamental difference between them, although PRA is believed to be mainly aimed at analyzing low probability accidents. However, PRA is frequently used to analyze the events with a wide range of probability of occurrence. There is no such distinction in Russian literature.

Currently, the risk analysis procedure can be divided into two main components and several intermediate parts, each with its own problems and inherent methods and models: assessment and management. It is important to bear in mind that risk analysis issues cannot be considered separately from the game setting. Risk as a dynamic characteristic dependent on time, means and information is reduced to "two-dimensional estimates" of probability and damage.

It is forgotten that, first of all, there is a fundamental difference between stochastic factors leading to decision making under conditions of risk, and uncertain factors leading to decision making under conditions of uncertainty. Both lead to a scatter of possible outcomes of management results.

But stochastic factors are completely described by known stochastic information, which allows for deciding on the optimal solution. Nonetheless, basic formulas in risk analysis (RA) are distorted and simplified, their association with game theory is forgotten. There are several reasons for this. The word risk has become "trendy", as a result, specialists "seized on the term" without understanding where it comes from, what axioms are "behind" this term. As a result, for many years economists, insurers, ecologists, and others have been producing false scientific results based on false definitions they invented. Sometimes ("false" multiplied by "false" results in "true") acceptable results are obtained. But this usually only applies to static and stationary cases (where the "reliability" theory applies), but not to dynamic cases. For a number of applications, it was required that a formula was "simpler", so that it could be understood by developing countries that joined the IAEA, for example. As a result, the risk as a dynamic characteristic, depending on time, means and information, was reduced to two-dimensional snapshots in which only probabilities and damage are present. The case was given to the "civil defense forces" (now the Ministry of Emergency Situations), which did not have the corresponding scientific "potential" at the time and was acting as the "customer" of research work. The most influential Ministries (Ministry of Medium Machine-Building Industry, Ministry of General Machine-Building Industry) had their own general ideas of risk, which normally differed significantly from each other. The establishment of the opinion that risk analysis can be conducted through "statistics" of the observed phenomena was overwhelmingly influenced by Western scientists (Netherlands Organisation for Applied Scientific Research and others). The influence was so strong that the "strength theory" and "reliability theory" were left in the modern risk analysis. But research on the "survivability theory", "homeostasis theory", adaptive theories, including "decision making theory", "perspective activity theory", "reflections theory", and "the theory of self-organizing systems" were nipped in the bud.

For uncertain factors, such information is not available. In the general case, the uncertainty can be caused either by the counteractions of an intelligent opponent (a more complicated case is related to the opponent's reflections (terrorist threat)), or lack of knowledge of the conditions under which the decision is made.

Decision making with the insufficient knowledge of the conditions in which the choice is made is called "games with nature". In terms of "games with nature," the decision-making problem can be formulated as follows. Let the decision maker choose one of the M possible options: $X_1, X_2, \ldots, X_M$ and let N assumptions be made regarding the conditions under which the possible options will be implemented: $Y_1, Y_2, \ldots, Y_N$ The estimates of each solution in each condition (X_m, Y_n), where $m = 1 \ldots M$, $n = 1 \ldots N$, are known and given in the form of a gains matrix for the decision maker: $A=A(X_m, Y_n)=|A_{mn}|$.

Assume that a priori information about the probabilities of a particular situation Y_n is absent. The theory of statistical decisions offers several criteria for optimizing the choice. The choice of the criterion cannot be formalized, it is carried out by the decision maker subjectively, based on their experience, intuition, etc. Let us consider these criteria.

Laplace criterion. Since the probabilities of occurrence of some situation Y_n are unknown, all situations will be considered equally probable. Then, for each row of the gains matrix, the arithmetic mean value of the estimates is calculated. The optimal solution is the solution with the maximum value of this arithmetic mean, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\frac{1}{N}\sum_{n=1}^{N} A_{mn}\right).$$

Wald criterion. In each row of the matrix, the minimum estimate is selected. The optimal solution is the solution with the maximum of this minimum, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

This criterion is very cautious. It focuses on the worst conditions, among which the best and now guaranteed result is only found.

Savage criterion. In each column of the matrix the maximum estimate $\overline{A}_n = \max_{1 \le m \le M}\left(A_m\right)$ is found, and a new matrix is compiled, the elements of which are determined by the relation $R_{mn} = \overline{A}_n - A_{mn}$. This is the amount of regret that the optimal choice X_m was not made in the strategy Y_n.

The value R_{mn} is called the risk, meaning the difference between the maximum gain, that would take place if it were reliably known that the most favorable for the decision-maker situation $\overline{Y}_n$ would occur, and the real gain when choosing X_m under condition Y_n.

This new matrix is called the risk matrix. Then a solution with the risk that has the lowest value in the most unfavorable situation, i.e. $\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\max_{1 \le n \le N}\left(R_{mn}\right)\right)$, is chosen from the risk matrix.

The point of this criterion is to minimize risk. Like the Wald criterion, the Savage criterion is very cautious. They differ in their understanding of the worst situation: in the first case, it is the minimum gain, in the second, the maximum loss of the gain compared to what could have been achieved under the given conditions.

Hurwitz criterion. A certain coefficient α is introduced, named the "optimism coefficient",. In each row of the gains matrix the largest estimate $\max_{1 \le n \le N}\left(A_{mn}\right)$ and the smallest estimate $\min_{1 \le n \le N}\left(A_{mn}\right)$ are found.

They are multiplied by α and $(1-\alpha)$, respectively, and then their sum is calculated. The optimal solution is the solution with the maximum of this amount, i.e.

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M}\left(\alpha \times \max_{1 \le n \le N}\left(A_{mn}\right) + (1-\alpha) \times \min_{1 \le n \le N}\left(A_{mn}\right)\right).$$

For (α=0) the Hurwitz criterion is transformed into the Wald criterion. This is a case of extreme "pessimism". For (α=1) (a case of extreme "optimism"), the decision maker expects the most favorable situation. The "optimism coefficient" α is assigned subjectively based on experience, intuition, etc. The more dangerous the situation, the more cautious the approach to choosing a solution should be and the lesser value is assigned to the coefficient α.

It is important to note that this criterion is not relevant to risk analysis, only to the subjective perception of "random" and "voluntary" risks.

Then how is the risk calculated?

It follows from the above that risk assessment is only possible if there are alternatives to choose. If there is only one single option, then the risk is automatically equal to zero and the spread of gains is just a characteristic of an uncontrolled natural environment. However, it should be noted that the alternative is always present in the form of a refusal to make a decision.

In some cases, with the refusal to make a decision an optimum for the columns may appear, then there will be non-zero risks in the options due to the choice of a wrong decision. For example, it is more profitable not to play in a casino than to play, aligning to some strategy. On the contrary, in chess it makes sense to play even in the case of a single (forced) move. For example, when the opponent declares a "check", there is no way to interpose, and retreat is only possible on a single square, then the risk is also equal to zero, since refusing to play means automatic defeat.

Probability estimates $\sum_{n=1} p_n = 1$ describing the state of the environment $p_1 = p\left(Y_1\right)$, $p_2 = p\left(Y_2\right)$, …, $p_N = p(Y_N)$ allow preventing choosing the most unfavorable case when using the Savage criterion, and the desired solution takes the form:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{N} p_n \times \left(\max_{1 \le n \le N}\left(A_{mn}\right) - A_{mn}\right)\right),$$

which is a more correct formula.

For the case when the gain is determined only by the loss amount A_{mn}=B–C_{mn} for any pair (X_m, Y_n):

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

For the case when the loss level at the optimal option for the conditions Y_1, Y_2, …, Y_N does not depend on n and is equal to $\overline{C}$:

$$\overline{F} = F\left(\overline{X}, Y\right) = \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times \left(B - C_{mn}\right)\right) =$$

$$= B - \overline{C} + \min_{1 \le m \le M}\left(\sum_{n=1}^{M} p_n \times C_{mn}\right).$$

Only in this case the solution will really be determined by the value of the mathematical expectation of losses. But adjusted for B and $\overline{C}$. In many works these corrections are not taken into account. Usually B and $\overline{C}$ are considered equal to zero. For example, in ecology, improving the "air" costs nothing (does not bring profit), and if no one is sick, then the optimal damage is taken as 0.

Bayes criterion leads to the same estimates:

$$\overline{F} = F\left(\overline{X}, Y\right) = \max_{1 \le m \le M} \left(\sum_{n=1}^{M} p_n \times A_{mn} \right) =$$

$$= \left(B = 0; \overline{C} = 0\right) = \min_{1 \le m \le M} \left(\sum_{n=1}^{M} p_n \times C_{mn} \right).$$

In general, the problem of safety insurance and risk analysis of SCS facilities in the face of changes in the composition and intensity of threats to the sustainable development of the industry remains relevant. Safety requirements established for objects of high and medium hazard categories are sometimes rather high and significantly surpass the capabilities of property owners. As a result, the question of ranking the objects within the given categories to determine the sequence of equipping them with the required protective means arises. In order to do that, it is necessary to set a criterion to determine the importance (and the serial number accordingly) of an object in the ranked list against it.

The methods used to rank objects are based on mathematical modeling, expert assessment, decision making theory, and interval estimation. To some degree, they take into account the interests of organizations operating these facilities, state supervisory authorities, and insurance companies. At the same time, the ranking methods available today (for example, ranking objects by protection against emergencies in railway transport, ranking objects of hazardous gas distribution production systems, etc.) do not take into account the structural connectivity of the ranked objects and the importance of a particular object operation for related systems and subsystems .

Ranking SCS objects is a typical task for the theory of measurement of some complex synthetic properties of objects. Technically, the solution of the problem is reduced to the construction of a value (utility) function linking the measured property with simpler resource indicators (factors) measured in physical quantities. The value function is used both to solve the problems of choosing some best option from a variety of alternatives, and to solve more composite problems, such as the task of forming a portfolio of orders for work with limited resources (funding for creating or modifying objects). The factors through which the ranks are built are often measured not in quantitative but in qualitative scales, therefore, the use of expert assessment methods and expert technologies is required to build dependencies between utility and primary resource factors. Due to the development of computer technology, it is now possible to evaluate objects whose description factors are specified with an error, which requires the development of a specific apparatus for the statistical processing of primary data and the use of fuzzy logic tools. An essential feature of ranking problems is the adaptive nature of decision-making procedures for selecting optimal options, in which several cycles of experimental data and expert preferences coordination are required to construct the final formula for the ranking function.

In this context, risk assessment is the stage at which the negative effects associated with a particular production activity are determined. And first the dander sources should be identified. In order to do that, the boundaries of the investigated system should be determined. In other words, when assessing risk in a region or of a particular system, one should choose which sources to be considered. There are no strict rules here, and there cannot be. However, today there are a number of developed provisions that should be taken into account when studying safety issues. The most comprehensive provisions for determining the boundaries of the studied regional or large industrial systems can be found in various sources. International organizations note that there are normally different values of risk assessments in different countries even when assessing one particular technology. Therefore, to facilitate data collection and processing, a single set of terms and provisions should be adopted to describe energy and industrial systems and their main components [14].

2. Comments on risk categories

The basic moments in risk assessment are the detailed description of a hazard and the definition of harm related to it. There are various models of hazard sources that allow identifying a probability of this or that scenario of an accident's development and defining the amount of dangerous emissions into the environment. Depending on the type of a source, three types of risk are identified.

Usual risk is related to normal operations of an enterprise. The conditions of normal operations include accidents with low harm that occur rather often. This category of risk is characterized by an occurrence probability equal or close to entity. In most cases usual risk is integral part of production process itself or easily controlled. The sources of such a risk are described by the amount of emissions or dissipations into the environment caused by normal operations or some accident. Assessment of emission or dissipation level for functioning enterprises can be made on the basis of measurements or the results of operational experience of analogous enterprises.

The other two risk categories are related to industrial accidents during transportation or storage of hazardous substances. An accident is understood as an event with a low probability of occurrence (for example, less than one for the entire life of an enterprise), but with significant or even catastrophic consequences. When analyzing emergencies, possible scenarios for the development of an accident are usually considered. Then factors such as

the type of an initiating event, the amount of hazardous substance, the effectiveness of emergency safety systems and many others should be taken into account. Usually there are a large number of possible scenarios for the development of an accident. Therefore, the entire spectrum of possible scenarios and their probabilities should be determined when assessing the risk. The probability values can vary from 10^{-6} to 10^{-8} events per year. Rarer events are so difficult to evaluate that they are considered almost incredible.

Periodic risk is associated with those accidents, which are often repeated, but cause limited damage that may include human casualties. This does not mean that such accidents are planned. They are, of course, undesirable, and safety systems are created and used to prevent them. However, despite these measures, such accidents can occur, and the risk associated with them has a fairly wide range of values depending on the type of production activity. The cause of such accidents is usually a violation of the procedure, improper use of equipment and human error. To assess the risk of this category, accident frequency and other necessary parameters are estimated using standard statistical methods based on available data.

Hypothetical risk is associated with accidents, which are believed to occur with a very low probability but have very severe consequences. This class of accidents is characterized by the absence or insufficient amount of statistical data. But because of the enormous potential damage, it is impossible to just wait until enough practical experience is gained. Therefore, an analysis of hypothetical accidents is carried out in order to determine the probability of this accident and assess its possible consequences. Typically, a lack of statistics refers to the behavior of a large industrial or energy system as a whole. Therefore, such an analysis is carried out either by means of an expert assessment, or by the "event tree" method, where the probability of a hypothetical accident can be predicted based on possible malfunctions or failures in the operation of individual nodes or mechanisms, for which relevant statistics are available.

It should be remembered that there is no need to use overly complicated models for risk assessment due to many uncertainties and averagings that arise in the calculation. By the way, finding the degree of uncertainty and the range of possible risk values is another composite characteristic of risk in general. Thus, according to various experts, the uncertainty in assessing the risk of accidents at industrial enterprises can be one or even reach two orders of magnitude. This is due to the lack of knowledge on a wide range of technical, environmental and social factors that must be considered in risk analysis. There are even opinions, which are based on the analysis of accuracy and uncertainty in risk assessment, that translation models that allow for obtaining the concentration of a hazardous substance in the study area with an accuracy of 10% (maximum 20%) are quite acceptable.

3. Comments on a monitoring system

Thereby, the stable functioning and development of any SCS are subject to the influence of many external and internal factors including negative impact factors. To monitor and assess these factors and make a decision aimed at reducing negative effects of their manifestations, the so-called systems of balanced scorecard and key performance indicators (KPI) (quantitatively characterizing the risk factors to which the system is exposed) are widely implemented. From these indicators one chooses strategic targeted indicators (STI) that quantitatively reflect strategic goals of the system's functioning and represent basic economic and production indicators, which characterize the effectiveness of its development (if they are not achieved, it indirectly characterizes the level of existing threats and degree of their implementation in the considered period of time).

Based on these indicators, one constructs threats and risks monitoring systems that allow collecting data on changes as well as analyze the effectiveness of the system for several hundred indicators in organizational, product, geographical and other sections on daily, quarterly and annual planning horizons. It is believed that the results of the analysis allow for "deviation control", focusing on the problem areas of each control object through a "traffic light" indication. However, as collected data is growing bigger, there arises a problem related to interpretation of signals of these hundreds of "traffic light indicators". It is not obvious what signal should be considered as "good" or "bad" for the system in general if, for example, half of the indicators are "green", and half are "red". The question is how to qualify the situation if there are a little more of "green" indicators than of "red" etc. One cannot also say that there is an obvious connection of the analyzed indicators with the high-level indicators (STI) and the degree of their influence on the achievement of STI target values approved by the company management. There arises the so-called "Big Data" effect, when analysts cannot manage to process the collected information, and standard statistical methods are just not coping.

Besides, based on the analysis of trend in indicators changes, a system of threats and risk monitoring is not capable to predict crises and situations with negative dynamics. Such events are rare and as a rule take place at various forecast backgrounds, and in case of the analysis of historical datasets of rare events there are discrete dynamic probabilistic processes in place.

The purpose of analysis of SCS as an object for forecasting in the field of operation safety and development sustainability is the creation of such a predictive model of situations dynamics arising out of its functioning that will allow reducing the degree of uncertainty of events dates and their scale by means of computing experiments and selection of acceptable parameters, i.e. obtaining predictive information on the forecast object owing to

detection of hidden regularities, which indicate changes of an object's state or the regularities of changes in the parameters of the external environment significantly influencing its functioning (the so-called laws of variability of "forecast background").

Due to the discrete nature of crisis situations, the application of data analysis apparatus based on classical laws of large numbers, is incorrect. Probability convergence is practically not observed in reality, except for the statistics accumulated in systems of mass service. The indicators panel realized in the form of "traffic light" constructed with the help of application of dispersion as the main indicator can indicate the normal state during the whole year when in fact the system passes in the area of pre-crisis values.

Besides, there is, as a rule, no univocal functional connection and mutual influence of indicators of lower and upper levels for an officially declared hierarchical system of indicators.

As a consequence, it is necessary to have a correct primary analysis of a long-term statistics, and only based on this analysis it can be concluded whether it is possible to develop a predicting instrument corresponding to a research problem and what share of randomness of dates in occurrence of unfavorable situations and their scale can be eliminated with its help. It is also obvious that as true laws of distribution of analyzed random processes and their determinants will be continuously corrected (any hi-tech system changes faster than adequate statistics are collected), it is necessary to use criteria "free from distributions". In particular, for example, as criteria of achievement of predictive purpose we should take not deviation values of model and real data, but the criteria used in classification and pattern recognition methods. For example, as measurement of prediction precision we can use the prediction error values of the first and second types for different classes and types of situations, depending on classes of a physical object and parameter values of the forecast background, if possible. The second circumstance is very important as, for example, it is incorrect to sum up accident statistics of different seasons, since during different seasons technological processes function differently.

The reliable execution of its functions by a system is characterized by retaining some specified characteristics (reflected in the corresponding STI and KPI values) in set limits. In practice, it is not possible to completely avoid deviations, but it is necessary to aim at minimizing deviations of the current state from some specified ideal – the target set, for example, in the form of STI values of the first level.

The threat of non-achievement of STI set values of the first level (in fact, we again speak about the risk) is considered in this case as a variable value, which is a function to the current state of the system: it increases with the assessed situation approaching to some permissible limit after reaching which the system cannot fulfill its obligations and reach respective STI set values of the first level.

General mathematical statement of a task in question: let there be a set of signs of the current situation X (for example, current KPI values, risk factors etc.), the set of admissible realization of Y situations (for example, the current STI value of the first level is higher (or less) than the previous one etc.), and let there be the target function $y^*: X \to Y$, whose values $y_i = y^*(x_i)$ are known only on the finale subset of objects $\{x_1,\ldots,x_l\} \subset X$ (for example, the KPI values that correspond to the current STI state of the first level). Pairs "object-answer" x_i, y_i are precedents. A set of pairs $X_l = \sum_{i=1}^{l} x_i, y_i = 1$ will make a training sample. It is required based on the sample X_l to recover y^* dependence, i.e. to construct a function $A: X \to Y$, which would approach a target function $y^*(x)$, and not only on objects of a training sample, but also on the whole set X. As a decisive function A should allow for a effective computer realization, it is possible to call it an algorithm.

Conditionally, there are two object classes faced by experts in the field of management automation: "simple" and "complicated". "Simple" ones are objects, whose precise mathematic models, for example, in the form of algebraic equations or linear programming models with all necessary quantitative factors that influence the object's behavior considered, are suitable for implementation on computers of a specific class and are quite adequate to the object. "Complicated" objects have the following distinctive features: not all purposes of the choice of decisions and conditions influencing this choice can be expressed as quantitative ratios; formalized description of a control object is absent or is unacceptably difficult; a significant part of information necessary for the mathematical description of an object is in the form of the ideas and proposals of experts etc. The construction of the exact mathematic models of the "complicated" objects suitable for implementation on modern computers is either difficult or often completely impossible.

But it does not mean that the task has no decision. In general, there are two possible ways of search. The first one is to try to apply a nontraditional mathematical tool for the creation of the model considering all object's features and suitable for implementation. The second one is to construct not an object's model, but an object control model (i.e. not an object itself is simulated but a human operator in the process of controlling an object). In its essence, the algorithm in this case is associated with the construction of a data structure field and the analysis of its effects, including the improvement of the structure itself. All data are structured and unstructured at the same time. As excluding OR is difficult to "construct", it is possible to realize the idea of the construction of solving rules (hereinafter is a solver) on the monotone function defining network order [15, 16].

The geometric significance of a solver is rather simple: it is necessary to select attributes in such a way, while keeping the characteristics of a specific order, that objects

Table 1. Payoff matrix

	Success	Unsuccess
Profit (payment for action)	X_0	X_1
Feasibility measure	p_0	$p_1=1-p_0$

on a subset of attributes would be divided. This is a classical task of discrete mathematics on finding a logical function, and this task is solved in dozens of different ways, which are based on the method of decomposing any logical function into a superposition of simpler functions. With all successes of the heuristic mathematics, solution methods with optimization lead to a large enumeration of options, which does not guarantee the optimality of the solutions found. Methods of construction of optimum formulas (containing fewer variables, or with nonoverlapping multipliers in logical sums) for partially defined logical functions have combinatorial complexity algorithms with an exponential increase in the consumption of computing resources in line with the size of tables to be solved (both in the number of variables and in the number of training objects).

4. Principles for compiling a complete dataset

Based on the verbal definition of "risk action is an action for luck with the hope of success", the ideology of risk assessment, analysis and management follows. What does this definition include? The first is the presence of at least two outcomes: "successful", for which there is hope, and "unsuccessful", where the expected does not happen or happens on a smaller scale. In those rare cases, when there are only two outcomes, the risk situation is described as a payoff matrix (Table 1).

Lost profit (X_0–X_1) is usually called harm, and the mathematical expectation of lost profit is called risk R:

$$R = p_0 (X_0 - X_0) + p_1 (X_0 - X_1) = p_1 (X_0 - X_1). \quad (1)$$

In the case when there is a threat of implementation of unsuccessful outcomes with different harms (X_0–X_n), the risk is calculated in accordance with the following formula:

$$R = \sum_{n=1}^{N} p_n (X_0 - X_n). \quad (2)$$

Formula (2) can be correctly applied for the current assessment of the risk action in those cases when this action is "reversible", i.e. when there is a possibility to repeat this action several times in order to ensure convergence "in probability".

When analyzing poorly formalizable threats, this situation is not observed.

First, as a rule, researchers do not know anything about the possibility or impossibility of the appearance of "new" scenarios with unsuccessful outcomes, except for those that are included in the analyzed payoff matrix (Table 1). Therefore, although the standard condition $\left(p_0 + \sum_{n=1}^{N} p_n = 1 \right)$ should be fulfilled, the values p_n(n=0, …, N) are not probabilities (probability is posterior probabilities, calculated frequencies), but the possibilities (likelihood is priory probabilities, estimated proportions of outcomes).

Second, one must assume that there are too many different scenarios, and each of them has a negligibly small probability of implementation. In fact, only one scenario is realized in a life process, the one that is realized in real life. Therefore, unsuccessful outcomes should be grouped in classes. The first procedure when dividing the outcomes into classes is carried out on the basis of harm equivalence, which is incorrect in the context of the classical theory of probability: the values of the probability estimates, where the index g indicates a group of outcomes, depend on the subjective perception of harm (significance of harm). As a result, the distribution of "pseudoprobabilities" is analyzed on the researcher scale, not on the scale of the nature of a phenomenon.

Third, the decision on risk action is often implemented only once, so it is disputable to use probabilistic simulation analysis tools such as the Monte Carlo method.

Fourth, one must often solve the problem of choosing a risk action from many alternative options in order to exclude risks of an unacceptable level. An evaluation function, corresponding to the case of avoiding harm below the theoretically possible, suggests that actions for which there is at least one scenario, in which the harm $(X_0 - X_{\tilde{n}})$ exceeds the specified level, must be abandoned. An evaluation function corresponding to the "extreme care" policy is formed on the basis of minimax criterion.

To assess threats, however, such a criterion is hard to consider suitable for application; rare scenarios with great harm would cancel any activity except "unpunished". Therefore, in practice the situation must be "smoothed", and there are several ways to do this.

The first one is to assess harms and risks while taking a "balanced" position. It is assumed that in practice variants between extreme optimism (only success, there is no other way) and extreme pessimism (maximum efforts to prevent and/or smooth the harm are made but anyway the worst possible scenario for the threat is realized) take place.

The second one is to guess and correct proportions, in which possible threat scenarios are expected; for this purpose, it is necessary to assess "periodically" the cur-

rent state, trends and predicted threats. This means the construction of an adaptive scheme for correction of payoff matrices.

This distinction is extremely important, since different sources of information have different specifics of impact on risk assessment.

For example, "sources of expertise" can update the current state up to introduction of new alternatives for implementing threats (columns of payoff matrices). However, control of dynamics in the state of threats is not their main activity. Science and technology sources can correctly produce limiting characteristics of predicted values (dates of industrial application of some technology).

On the contrary, estimations of trends, rate of increase or diminution of threats can be obtained by analyzing of indicators of emergency and crisis situations.

The basis for the creation of monitoring modules can be numerous facts indicating that before a large-scale threat (for example, a large earthquake) is formed, there are series of smaller-scale threats (increasing small tremors).

An expert analytical system should be a multifunctional and multilevel system intended for registration and analysis of each specific case (event) as well as for prediction of trends and generation of preventive activities if any. The expectation of those situations that require actions is typical for fire services, the Ministry of Emergency Situations, emergency medical services. In case of poorly formalizable threats of permanent character, there are no negative events "by definition"; therefore, the system gets information on these threats from competent sources who inform about these threats in addition to their main activities or from generally available media sources when everybody talks about a threat. There are a wide range of sources like exhibition and conference proceedings, scientific publication, local press (which is closer to the subjects and objects of threats) etc. between competent sources and generally available media sources.

Thereby, all information sources form some two-dimensional scale. The first dimension reflects complementarity of the information source: "reliable", "approximate", "neutral", affiliated with competitors, "unfriendly". The second dimension reflects the specialization (competence) level of information source. For example, it is natural to have a greater confidence for the opinion of a specialist (highly specialized magazine) and to have a less confidence for the opinion of specialists in a wide professional sphere because such a source will "obviously" overestimate facts and results in their sphere, and downplay the importance of facts and results obtained from neighboring spheres considering them as competitors. Evaluating different information obtained from a source in terms of its relation to reality (on the stream of retrospective data), we can form an attitude to the source as some tool for measuring, classifying, identifying a particular situation.

A great variety of alternative information sources requires a comparative analysis of them and, if possible, their selection and optimization long before taking a decision to use them in the practical work of a safety ensuring system.

This requires an answer to the following key question: what criteria should be applied to assess information sources in order to ensure comparability of the results of their application? The indicators of information completeness and accuracy can be applied as technical criteria of sources' quality [17, 18].

Completeness coefficient *ComplMcl* of the classification method *Mcl* is equal to the share of correctly classified objects of *C* class from a test sample $\{X\}^{\in C \Rightarrow \in C}$ to the full number of objects of *C* class with $\{X\}^{\in C}$:

$$ComplMcl = \frac{\{X\}^{\in C \Rightarrow \in C}}{\{X\}^{\in C}}. \quad (3)$$

Accuracy coefficient *ExactMcl* of the classification method *Mcl* is equal to the share of correctly classified objects of *C* class from a test sample $\{X\}^{\in C \Rightarrow \in C}$ to the full number of objects of this sample, which were classified as belonging to the *C* class:

$$ExactMcl = \frac{\left|\{X\}^{\in C \Rightarrow \in C}\right|}{\left(\left|\{X\}^{\in C \Rightarrow \in C}\right| + \left|\{X\}^{\in C}\right|\right)}. \quad (4)$$

Completeness coefficient is associated with the mistakes of the first kind – an incorrect classification of objects belonging to *C* class. Accuracy coefficient corresponds to the mistakes of the second kind, i.e. with classifications of false objects as belonging to the *C* class.

The good classification method should allow fewer mistakes, i.e. has great values of *ComplMcl* and *ExactMcl*. However, the 100% result is achieved with the specified prepared "reference" data array. In practice, both *ComplMcl* and *ExactMcl* values seldom exceed 70% [19, 20].

Improving the reliability of estimates for the preparation of training samples requires explanatory components, which follows from the analytical nature of the activity.

In practice, we in fact observe two types of estimates:

• Estimates of experts (sources);

• Estimates calculated according to the similarity of text publications, which are acquired from the experts in similar professions.

That is, a final estimate of the sources' quality should be carried out according to the "final result". The following indicators are proposed as integral criteria of trust to the information source:

• Mean time to a critical number of mistakes in the source;

• Mean time to a critical ratio of mistakes of the first and second types made on the basis of the data source.

Conclusion

Therefore, for the purpose of the construction of a safety monitoring and risk prediction system of SCS, we should consider the possibility of simultaneous application of two basic indicators: risks of development (in this capacity we can use quantitative indicators that identify unfavorable combination of probabilities of occurrence of dangerous processes and their consequences (harms) in the economic and scientific development of a company at the specified forecasted period of time) and efficiency of comprehensive measures in the development process (quantitative indicator that determines the increase of strategic levels of economic and scientific development of a company at the forecasted period of time owing to the development and implementation of corporate policy on basic priority directions, methods, criteria and systems of prediction implementation taking into account the strategic risks of development).

For the appropriate assessment of the current status of a system, it is necessary to have:

• Complete system of indicators of the status of the system and environment (competitive environment) (description of the position);

• Generator of the finite possible number of scenarios of the system development (moves of "your own figures", "neutral" moves of "nature" and "antagonistic" moves of "competitor's figures");

• Functions of status assessment (win – improvement of the position – deterioration of the position – lose).

At the same time, without waiting for "lose" happening (in the case of the deterioration of the assessment of the current state, or competitors take moves not forecasted before), it is necessary to search for new development scenarios, since all the previously reviewed options result in loss or the probability of favorable consequences is extremely small. Since in the development of any system there are active opponents (competitors), partially controlled internal factors (technological and human accidents) or uncontrolled factors (natural disasters and accidents), all scenarios have a probabilistic nature. Therefore, even with a smooth change of the system's status (in which it is impossible to result in a huge loss in a short time), it is necessary to take into account the factor of accumulation of accidents and to develop the indicators for assessing the proximity of a tested system to the limits of the loss of sustainable development.

References

[1] Aksyonov GP. Vernadsky. Moscow: Molodaya gvardia; 2015 [in Russian].

[2] Michel J-B, Shen YK, Aiden AP, Veres A, Gray MK, The Google Books Team, Pickett JP, Hoiberg D, Clancy D, Norvig P, Orwant J, Pinker S, Nowak MA, Aiden EL. Word frequency history based on a Google Books sample of one million books in English. Quantitative Analysis of Culture Using Millions of Digitized Books. Science 2011;331.

[3] Kuznetsov AS. K ponimaniyu edinstva analiza i sinteza [Towards the understanding of the unity of analysis and synthesis], <http://www.smyrnyh.com/?page_id=686>; 2019 [accessed 18.08.2019] [in Russian].

[4] Flammini F, editor. Critical Infrastructure Security. Assessment, Prevention, Detection, Response. WIT Transactions on State-of-the-art in Science and Engineering 2012;54. ISBN 978-1-84564-562-5.

[5] National Infrastructure Protection Plan. U.S. Department of Homeland Security; 2009, <

[6] National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. U.S. Department of Homeland Security; 2003, <.

[7] Dudenhoeffer DD, Permann MR, Manic M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In: Perronc LF, Wieland FP, Liu J, Lawson BG, Nicol DM, Fujimoto RM, editors. Proceedings of the 2006 Winter Simulation Conference. Piscataway (New Jersey, USA): Institute of Electrical and Electronics Engineers; 2006. p. 478-485.

[8] Perrow C. Normal Accidents. Princeton (New Jersey, USA): Princeton University Press; 1999.

[9] Ramo JC. The Age of the Unthinkable. New York: Little, Brown & Company; 2009.

[10] National Research Council, The Internet Under Crisis Conditions: Learning from September 11. Washington, DC: National Academics Press; 2003, <

[11] August 14th Blackout: Causes and Recommendations. U.S.-Canada Power System Outage Task Force; 2004, <https://reports.energy.gov>.

[12] Riabinin IA. Nadezhnost i bezopasnost strukturnoslozhnykh sistem [Dependability and safety of structurally complex systems]. Saint Petersburg: Saint Petersburg University Publishing; 2007 [in Russian].

[13] Taleb NN. Antifragile: Things That Gain from Disorder. Random House Trade Paperbacks: Reprint edition; 2014.

[14] Radaiev NN, Lesnykh VV, Bochkov AV**.** Metodicheskie aspekty zadaniya trebovaniya, otsenki i obespecheniya zashchishchennosti obektov gazovoy otrasli ot protivopravnykh deystviy. Monogrfia [Methodology aspects of requirements specification, assessment and assurance of gas facilities protection against unlawful activities. A monograph]. Moscow: VNIIGAZ; 2009 [in Russian].

[15] Bochkov AV, Zhigirev NN. Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty. In: Ram M, Davim J, editors. Advanced Mathematical Techniques in Engineering Science. Series: Science, Technology and Management 2018; May 17, p. 121-154.

[16] Bochkov AV, Zhigirev NN. Ispolzovanie metoda opornykh vektorov dlya poiska skrytykh zakonomernostey v zadachakh klassifikatsii situatsiy, opisyvaemykh otsenennymi voprosnikami [Use of the method of reference vectors

in data mining as part of classification of questionnaire-described situations]. Proceedings of the 8th DQM International Conference Life Circle Engineering and Management ICDQM-2017; 2017 [in Russian].

[17] Korenev VV, Gareev AF et al. Intellektualnaya obrabotka dannykh [Intelligent data processing]. Moscow: Nolidzh; 1999 [in Russian].

[18] Salton G. Automatic Text Processing. Reading (Massachusetts, USA): Addison-Wesley Publishing Company, Inc.; 1989.

[19] Gareev AF. Reshenie problemy razmernosti slovarya pri ispolzovanii veroyatnostnoy neyronnoy seti dlya zadach informatsionnogo poiska [Solution to the problem of directory size in the context of application of probabilistic neural networks in information search]. Neyrokompyutery: razrabotka, primenenie 2000;1:60-63 [in Russian].

[20] Global Trends 2015: A Dialogue About the Future With Nongovernment Experts. This paper was approved for publication by the National Foreign Intelligence Board under the authority of the Director of Central Intelligence. Prepared under the direction of the National Intelligence Council. NIC 2000-02; December 2000, http://infowar.net/cia/publications/globaltrends2015/ <http://www.futurebrief.com /globaltrend2015.pdf>.

About the author

Alexander V. Bochkov, Candidate of Engineering, Deputy Head of Unit for Analysis and Ranking of Controlled Facilities, Gazprom Gaznadzor, Russian Federation, Moscow, e-mail: a.bochkov@gmail.com

The author's contribution

The author has compared the primary concepts of risk management and shown it is to be developed and improved. A type of risk functional is proposed that allows defining a safety solution with the value of mathematical expectation of losses, subject to corrections. The author introduces the concept of "risk synthesis" and sets forth the prerequisites for the development of the corresponding method.