Original article
https://doi.org/10.21683/1729-2646-2020-20-1-57-67

On the method of risk synthesis in the safety management of structurally complex systems

Alexander V. Bochkov, *Gazprom Gaznadzor, Russian Federation, Moscow*
a.bochkov@gmail.com

Alexander V. Bochkov

Abstract. *The Aim of the paper is to show that the risk to critical infrastructure facilities (CIF) of structurally complex systems (SCS) should be considered as a multicomponent vector, whose set of parameters is subject to changes. Real safety estimation using the risk-oriented approach is impossible without a sufficient base of quantitative and qualitative characteristics of risk factors, as well as data on the status of facilities and processes that are exposed to such risk factors. Risk assessment always aims to estimate its quantitative indicators, which allows it to be used not only to assess industrial safety, but also to substantiate the economic efficiency of taken measures, conduct economic calculations of the required relief or compensation of lost health of workers and environmental damage.* **Method.** *The author suggests a method of risk synthesis (with game definition of the problem of countering possible external effects of various nature on CIF SCS) as one of the foundations of the design of advanced systems for monitoring safety threats to SCS. A special attention must be given to the effect of risk factors on the system of balanced safety and risk indicators, as prediction based on single indicators does not create a holistic image of the systems' status and development trends.* **Result.** *Key methodological premises were formulated: from general problem definition of safety management through the synthesis the model of a controlled facility and its external and internal connections, solution to the problem of selection of priority protection facilities in terms of assuring efficient operation and general safety of SCS. As the basis of advanced systems for monitoring safety threats and risks, the paper suggests the concept of risk management aiming to create the mechanism, method and tools for the synthesis, analysis and prediction of emergency risks.* **Conclusion.** *The proposed method can be applied to a wide range of tasks of primary analysis, synthesis and quantitative estimation of the CIF-related risks and safety management of SCS of various purpose.*

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

For citation: *Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. Dependability. 2020;1: 57-67. https://doi.org/10.21683/1729-2646-2020-20-1-57-67*

Received on: *13.12.2019* / **Revised on:** *23.01.2020* / **For printing:** *20.03.2020*

For psychological comfort some people would rather use the map of the Pyrenees while lost in the Alps than use nothing at all. They do not do so explicitly, but they actually do worse than that while dealing with the future and using risk measures. They would prefer a defective forecast to nothing.

Nassim Taleb

0. Introduction

Dependability and safety are key properties of critical and business-critical SCS, the requirements for which are on a constant rise. That is due to a number of factors.

First, the risks of emergencies and man-made catastrophes are increasing. For instance, according to the data announced at an ESREL conference, such accidents amount to 70% of the total number. Almost every tenth space launch results in an accident, causing economic and environmental consequences.

Second, the growing complexity of systems does not translate into improved reliability indicators of their components, which leads to reduced dependability and safety of SCS due to the absence of adequate structural solutions. Additionally, the diversity of components that can be used in a system design is growing as well, which, in turn, complicates the search for the ways of compensating for the above deficiency.

Third, the unique nature of such systems, be it with short or long periods of active use, causes a shortage of reliable information on the real values of reliability indicators reliability of the components and whole SCS. The gravity of this factor grows in proportion to the increasing complexity and stated reliability of components, e.g. large and ultra-large integration circuits. Additionally, the commercial nature of the manufacture of some elements and intense competition lead to the classification or unreliable information regarding their reliability.

On the other hand, the methods of today's complex technical systems dependability and risk theory, as well as the associated decision support technology, in the process of their development, operation and reengineering, do not provide suitable recommendations in terms of structural considerations, functionality and algorithms. The mathematical models of the classical dependability theory do not fully take into consideration the diversity of characteristics of components and therefore do not in fact allow obtaining exact solutions of optimization problems, which causes two types of risks. The risks associated with overstated dependability and safety indicators may cause an unacceptable growth of the actual value of failure and accident probability, while the risks of their understatement (as compared to the real ones) may lead to extra expenses at the stages of SCS development and operation, which is very important given the high cost of their manufacture and ownership.

The end of the XX century was marked by revolutionary changes in information processing that required a complete reconsideration of the basic principles of information management. Thus, while the information support of one or another type of activity used to revolve around the collection of rare data, today information is overabundant. In this context, the main problem consists in evaluating information by criteria of reliability, novelty, usefulness, as well as ensuring timely delivery of such information to the end user (decision-maker, DM) while observing the requirements for the specified scope and quality of data.

The tasks assigned to such entities of any company or nation due to their nature are beyond the capabilities of one person or even a whole team. Generating adequate managerial decisions requires complex, distributed among many employees procedures of search, storage and processing of required data, competent combination of scheduled activities and those imposed by the need for quick and effective reaction to the occurrence of unpredictable situations.

1. On the levels of system instability

The management of any organization follows the hierarchical principle. In a hierarchical management system, any subsystem of a certain level is subordinated to a higher-level system whose part it is and managed by. A management system is subdivided into subsystems until the resulting subsystem does not perform management functions, i.e. the bottom-level subsystem will be a subsystem that performs direct control of specific working tools, mechanism, device or processes. A higher-level management system controls manufacturing processes through lower-level subsystems (intermediate levels).

A company's management system also has a multilevel structure. Higher-level subsystems produce a flow of control information to lower-level subsystems. At the same time, lower-level subsystems send information on the current status of the controlled object to higher-level subsystems. The advantage of the hierarchical structure of company management consists in the fact that management problems are solved based on local decisions taken at the corresponding levels of the management hierarchy. The lower management level is the source of information for managerial decision-making at a higher level. The interlevel information flow gets smaller at each higher level, but at the same time, its semantic content increases.

All decisions taken as part of operations management are subdivided into routine and random. Routine decisions include those that are taken on the regular basis at certain intervals, so most procedures associated with the execution of such decisions can be automated. Random decisions are taken as the result of unforeseen circumstances and therefore are not subject to reliable information support.

For the top management of major industrial associations, specialized systems are created for execution supervision of higher-level directives and own decisions (indicative systems). That enables the managers to focus their attention on strategic matters, execution of long-term tasks and planned activities through quicker delivery of strategic information, wider and deeper analysis based on information grouping.

Thus, creating an optimal SCS safety management system requires the integration of research and development findings and information assets, as well as development of the method of comprehensive analysis of operational stability and basic procedures of a company's integrated risk management system. Such system will enable better substantiated decisions not only in terms of predicting emergencies and crises of various types and scale, but also as regards efficiency assessment of investment into safety and stable system operation. Comprehensive analysis of related risks will allow substantiating the required and sufficient safety levels of hazardous items and manufacturing facilities based on their importance in the context of a wide range of management problems.

Currently, there is a number of approaches to the assessment of critical (pre-critical) situations affecting a certain facility (system) that – from systems point of view – are based on the classification of the states of the examined partially-controllable dynamic facility (system) under risk and uncertainty or, in other words, the evaluation of the consequences of predicted scenarios of state development from the current to successor state.

From the point of view of systemology, the loss of stability of system development manifests itself at a number of hierarchically associated levels, each of which requires an individual and detailed analysis.

Level one is the "strength" level (a complex structure is to be composed of stable elements). It has to do with equipment ageing, personnel qualification lagging behind the development of modern technology and depletion of the resources the system's operation is based on.

Level two is the "dependability" level (retention of operability of the whole when some elements have failed). It is primarily ensured through element, unit and subsystem duplication.

Level three is the "survivability" level. It has to do with the system's ability to actively resist external threats.

Level four is the "self-organization" level. It is characterized by the adaptive properties of the system per "sublevels":

a) "homeostasis", meaning the retention of the "normal" system integrity and its vital functions;

b) "training", meaning the development of new methods of operation in order to ensure the ability to solve more complex tasks in the future;

c) "preadaptation" (prediction, intelligence), meaning the preventive development of optimized plans, mechanisms and resources for the purpose of resolving critical and pre-critical situations that have not occurred but may happen in the future;

d) "rebirth", meaning generation within the old system of a "new" system that operates according to "new" rules, in which the old system cannot exist.

Additionally, as it was noted above, a basic principle of situational management consists in the fact that a significant part of information is in the form of text messages in the mass media or other sources and is unplanned and unpredictable nature. As this information is unique and changes over time, a company's analytical units are often unable to evaluate its reliability, novelty and usefulness. For that reason, information in many cases is classified as "poorly formalized threats" (i.e. threats that are characterized by uncertainty and dynamic nature of input data and knowledge) that have the following properties:

– large amounts of symbolic information;

– the problem is not mathematically defined and lacks an algorithmic solution, or even if it does, the solution search space is too large and finding it within an allowable time and available resources is practically impossible;

– solving problems requires heuristics, i.e. affirmations based on experimental data, intuition. The aim of their application is to find a more rational solution, rather than the exact mathematical solution, by means of eliminating deliberately unsuitable solutions.

Despite the fact that, as of late, the proportion of poorly formalized threats (the advent of new information and social technologies, terrorist and war risks, changes in pricing policies, migration processes, etc.) has been growing, which inevitably reflects upon – among other things – integrated safety, assessment and analysis of such threats that are rather neglected.

However, we can observe growing experience with knowledge acquisition systems, models get developed that allow distinguishing between simple information noise and information attacks or designation of an incoming event. For instance, the vocabulary and frequency of messages before and after "critical" events. Information is normally multi-aspect, there are the so-called "problem classifiers", so, beside threat identification, knowledge of the fact which problems entail other problems as part of certain scenarios is accumulated and organized.

Only comprehensive analysis of related SCS and subsystem-related risks will allow substantiating the required and sufficient safety levels of hazardous items and manufacturing facilities based on their importance in the context of a wide range of management problems.

It should also be noted that the current practice of business mathematics is dominated by methods originating from the solution of certain physicotechnical problems. However, the "classical" science's postulate of impartiality of the laws of nature (their unconditional reproducibility in real life) doesn't hold up against criticism. Practical solutions are often "one-off", "unrepeatable", therefore the "life" mathematics are methodologically in principle more complex than the mathematics for "physics".

With all due respect to physicotechnical and other scientific problems, the phenomena they study are subject to natural laws and are not ruled by someone's subjective actions and interests. Conscious intervention into the development of the "physical world" comes down – in mathematical terms – to the definition of certain "parameters" subject to unchanging general laws. The study of physical processes aims to identify and analyze hidden causal relations and thus only pertains to the analytical level of knowledge.

System analysis does not include either the assessment of new knowledge, or examination of the cognizer's actions based on new information. True analysis is impartial. It cannot dictate what the object of study must be like (what it "should" become) and what actions should be taken to modify it in a certain way. Thus, the criterion of conclusion of the system analysis as a stage of systemic knowledge is the ascertainment of consistency of the data obtained after the formalization of facts and correctness of the conclusion procedure.

However, the research of the majority of phenomena of the real world is motivated by the need for active conscious "partial" modification by the cognizer of the object of cognition, for instance, by the need to design objects that never existed before. At the same time, one must be able to predict the activities and their results accounting for the fact that "the others are wide awake", i.e. working against competition in a constant search for optimal (acceptable) solutions.

2. Notes on the optimality

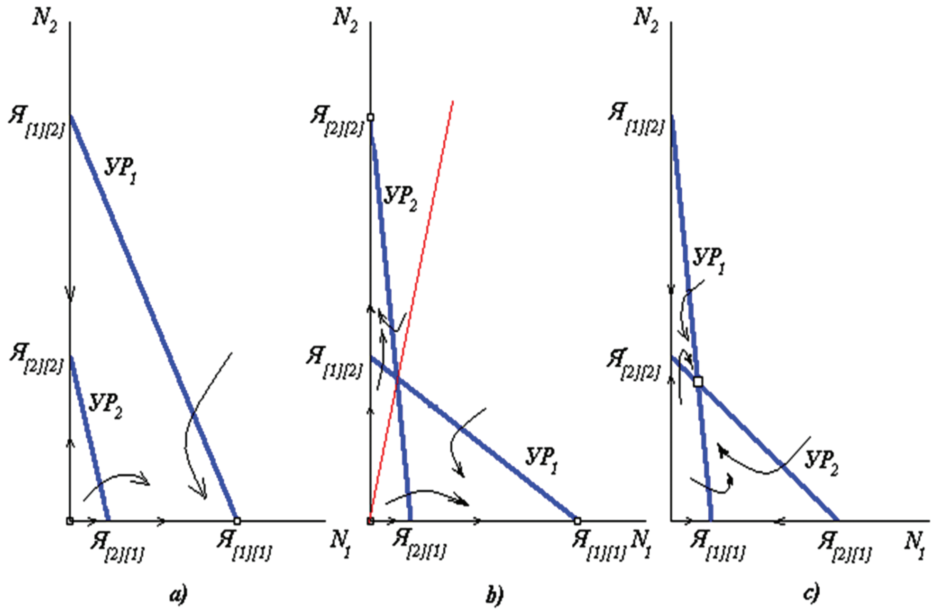
In order to answer the question of "What is optimal?", some methodological work is required. Ideas related to the meaning of optimality in conflicts (i.e. in the context of different interests) emerged and have been developing since a while. In many studies the concept of conflict and optimality in conflict is at the focus of attention in the sense that their non-consideration devoid the whole research of a subject matter. It is enough to mention such phenomena as military conflicts, political struggle, economic confrontations, etc. The presence of competition essentially modifies any predictions, including such regarding certain areas of business.

Let us elaborate on the above using the example of a system of Lotka–Volterra equations used in the research of "convergent evolution" (selection of the most promising directions of development), for instance:

$$\begin{cases} dN_1/dt=\varepsilon_1\times N_1-\gamma_{12}\times N_1\times N_2-\gamma_{11}\times N_1^2=УP_1(N_1,N_2)\times N_1; \\ dN_2/dt=\varepsilon_2\times N_2-\gamma_{21}\times N_2\times N_1-\gamma_{22}\times N_2^2=УP_2(N_1,N_2)\times N_2\,. \end{cases} \quad (1)$$

The first coefficients in the right members of the equations ε_1 and ε_2 are the rate of capital growth of two competing directions, the second ones γ_{12} and γ_{22} are the level of interspecific competition (effect of external competitors, or "them"); the third ones γ_{11} and γ_{22} are the indicators of intraspecific competition (effects of internal competitors, or "us"; the development of own production alleviates product shortage, i.e. reduces the commodity prices, thus reducing the rate of production). Here N_1 and N_2 are the dimensions of the competing capitals.

Let us designate as $Я_{[a][b]}$ the crossing coordinates of linear equations $УP_a(N_1,N_2)$ with the axes of variables $(0,N_b)$:



$УP_1$ and $УP_2$ are isoclinic lines of the vertical and horizontal tangents respectively
Figure 1- Phase portraits of Lotka–Volterra equation.

$$Я_{[1][1]} = \frac{\varepsilon_1}{\gamma_{11}},\ Я_{[1][2]} = \frac{\varepsilon_1}{\gamma_{12}},\ Я_{[2][1]} = \frac{\varepsilon_2}{\gamma_{21}},\ Я_{[2][2]} = \frac{\varepsilon_2}{\gamma_{22}}. \quad (2)$$

Depending on the value of those four coefficients and initial values of capital $N_1(0)$ and $N_2(0)$, system (1) allows for three types of solutions that describe three different outcomes of competitive activity (Fig. 1).

Case (a). If $Я_{[1][1]} \succ Я_{[2][1]}$ and $Я_{[1][2]} \succ Я_{[2][2]}$ are simultaneously true, then the first type of business certainly outcompetes its opponent regardless of the "starting" conditions (see. Fig. 1a). The scenario of "selection" of the strongest is realized, the weakest party has no chance to survive.

Case (b). If $Я_{[1][1]} \succ Я_{[2][1]}$ and $Я_{[2][2]} \succ Я_{[1][2]}$, again there is only one winner, but which of the two is the matter of the initial conditions (see. Fig. 1b).

In this case the antagonism between the competitors is so intense that self-restraint does not play a significant role. Case (b) is different from the previous one in that the "weakest" party gets a chance to win through "numerical superiority": a certain "startup capital" that places the winner on the preferable side relative to the separatrix that passes through the point on the phase plain (0,0) and point of intersection of the isoclinic lines of the vertical and horizontal tangents. This case describes a market situation when the key factor consists in the sufficiency of the "critical mass" of the startup capital to nip the competitor in the bud, not allow it to grow up to the level when it has to be dealt with (by sharing the market).

Case (c). The intraspecific competition for both competitors is so intense (each one is preoccupied with the problem of slowing capital expansion due to "internal problems") that the competition among "us" is higher than the pressure of "them" (if $Я_{[2][2]} \prec Я_{[1][2]}$ and $Я_{[1][1]} \prec Я_{[2][1]}$).

In this case both competing parties can coexist on a market for long periods of time (see. Fig. 1c). There is only one stable solution, under which the reproduction rates of new elements in the competing parties offsets the suppression created by the cumulative effect of the factors of internal and external competition.

Such models are, for instance, used for predicting the future development of relatively uniform competing technologies (for instance, due to them having different owners) that have a common "enemy". For instance, for the gas industry such is the nuclear energy, possibly other alternative types of energy, chemical industry that produces materials that substitute gas that is used in synthesis processes, etc.

As we can conclude from the analysis of even the above simplified analytical model, using the tools of "technical analysis" of economic data is not always correct. At least when the dominating factor is not the dynamics of the preceding success, but rather the factors that define the competitive advantage of old (proven) technology as compared to the developing new technology (belonging to both "us" and "them"), when they compete for the same consumer, whose capabilities are limited, methods are required for analyzing competing systems.

3. Algorithm of risk function synthesis

In [2], the author proposed an algorithm for solving the task of resources allocation for critical infrastructure protection against terrorist attacks based on subjective expert estimates. Let us show how quality expert estimates can enable quantitative estimation of a threat by using an algorithm that was previously designated risk synthesis.

So, let us examine a certain (k-th) SCS facility.

As the result of a supposed effect of certain intensity the facility will be damaged by being completely or partially disabled. Let us denote it as X.

Given that not each effect inevitably causes destruction, the protection profile of the k-th facility can be described with an interval representation by defining four matrices:

$$Q^{[k]}_{\min}(i,j),\ Q^{[k]}_{\max}(i,j),\ X^{[k]}_{\min}(i,j),\ X^{[k]}_{\max}(i,j), \quad (3)$$

where $i(i=0,1,\ldots,I^{[k]})$ is the level of protection of the k-th facility (zero level ($i=0$) corresponds to the current protection status).

The matrix elements are to be interpreted as: if the above facility k with protection level i is subject to an effect with the intensity level j, then with the probability of $Q^{[k]}_{\min}(i,j)$ to $Q^{[k]}_{\max}(i,j)$ the SCS will sustain damage with the magnitude of $X^{[k]}_{\min}(i,j)$ to $X^{[k]}_{\max}(i,j)$.

It is clear that values (3) will be growing as the level of effect j is on the rise and will decrease as the facility's protection level i is growing.

It is obvious that protection at any level requires certain material expenditure both on the part of the item's owner, and the Government. Let us designate the cost of achieving and maintaining the protection of facility k at the i-th level as $Y^{[k]}(i^{[k]})$.

As the total funds allocated for the protection of all facilities are limited, the following inequality must be fulfilled:

$$\sum_k Y^{[k]}\left(i^{[k]}\right) \le Y, \quad (4)$$

where Y is the sum of all costs of protecting a facility, provided that for each facility k protection system variant $i^{[k]}$ is chosen.

In case of natural effects, that unlike man-made effects do not have the benefit of aim and type, i.e. the nature is indiscriminate (like technology failures), the "optimal" protection profile of facilities could be achieved through the sequential execution of the following algorithm:

Step 1. Evaluation of probability $\lambda^{[k]}(j)$ of effect on each k-th facility of the j-th intensity level;

Step 2. Calculation of the median level of the risk effect on the k-th facility of the -th intensity level under the $i^{[k]}$-th protection facility variant:

$$R\left[k;i^{[k]}\right]=\sum_{j=0}^{J}\left\{\begin{array}{c}\lambda^{[k]}(j)\times\left(\dfrac{Q_{\min}^{[k]}\left(i^{[k]},j\right)+Q_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\times\\ \times\left(\dfrac{X_{\min}^{[k]}\left(i^{[k]},j\right)+\ X_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\end{array}\right\};\quad(5)$$

Step 3. Identification of the magnitude of the prevented risk per unit of protection investment, $\theta[k,i^{[k]}]$:

$$\theta\left[k,i^{[k]}\right]=\frac{R\left[k,i^{[k]}\right]}{Y^{[k]}(i^{[k]})};\quad(6)$$

Step 4. selection for each k-th facility of the maximum value of $\theta[k,i^{[k]}]$:

$$\theta\left[k,i^{*[k]}\right]=\max_{i^{[k]}}\left\{\theta\left[k,i^{[k]}\right]\right\},\quad(7)$$

i.e. the selection of variant $i^{*[k]}$ ensures the maximum reduction of the risk per unit of investment for the k-th facility.

Step 5. Ranking the facilities placing them in the descending order per the value of indicator $\theta[k,i^{*[k]}]$ and counting out the first $\tilde{K}$ facilities with the total costs of protection within the allocated sum Y with the ($\tilde{K}$+1)-th facility falling short of funds.

The essence of the above procedure is simple and clear: there is no point in funding additional protection of the assets that are not threatened (threat values $\lambda^{[k]}(j)$ are low). It is also unnecessary to additionally protect a facility, whose temporary inoperability has practically no effect on the overall losses of the facility's owner ($X_{\max}^{[k]}\left(i^{[k]},j\right)$ are low). And finally, additional protection is unnecessary in facilities that are already protected so well, that losses can be reduces, but that would require unreasonably high costs (i.e. values of $\theta[k,i^{*[k]}]$ are low).

The key factor of the above algorithm is the ranking facilities by the criterion of minimization of the mathematical expectation of losses per unit of funds invested in their protection (their stable operation).

Formula (5) clearly suggests the need for collection and assessment of data per three components:

- values of loss caused by the effects $X_{\min}^{[k]}\left(i,j\right)$, $X_{\max}^{[k]}\left(i,j\right)$;
- indicator of "aggressiveness of the operating environment" $\lambda^{[k]}(j)$;
- dependence of risks on the types of facilities k.

The values of losses X caused by the fact that SCS are not autonomous business entities must reflect the systemic impact (or socio-economic multieffect) that significantly grows depending on which of the affected facility's product consumers will be most harmed by its inoperability.

Subsequently, one must consider not the medium, but the upper boundaries of the damage indicators and additionally examine a fourth component, i.e. the indicator of importance of continuous operation of the facility due to the cascading increment of the consequences of the facility's lost operability to other businesses.

And finally, a fifth component needs to introduced in order to ensure correct ranking of facilities affected by terrorist attacks. This requirement is due to the fact that if an effect is active and targeted, has values and priorities unknown to security experts and governmental agencies that shift the values of $\lambda^{[k]}(j)$ away from the "industry average". Sometimes, such "additional" values are peculiar. Terrorists, for instance, have a tendency for excessive bloodshed, hostage-taking, ritualized murders, etc. The systemic importance of protecting certain facilities often increases when they are visited by top public officials, Government members, especially attending the inaugurations of politically-significant industrial facilities of not only international, but also regional importance within the country. One can spend a lot of time analyzing the factors that require taking into consideration the specificity of certain criminal activities, but what matters is the fact that criminals act out of their own ideas regarding the effectiveness and feasibility of attacks. Thus, the priorities of target selection shift. What matters to terrorists is not only and not so much the economic warfare, the damage to the facility's owner (as a competitor, as a "tool" to influence the authorities of another nation, etc.), but other aims to be reached by doing damage to a specific SCS' facilities.

The fifth component will help take those circumstances into consideration. Coefficient $\mu^{[k]}$ that initially equals one for all facilities and that, in the DM's or experts' opinion, may be increases in such a way as to increase the priority of exactly the k-th facility for inclusion on the list of facilities equipped with additional measures of protection for reasons that are not taken into consideration according to the common rules. To some extent, the significance of the new indicator $\mu^{[k]}$ is made clearer by the following integration diagram of models.

So, let $\tilde{Z}$ be the estimate of the total resources at the disposal of the forces interested in disrupting SCS facilities safety. If $\tilde{Z}<Z$, then the defending party underestimates the potential effects, if $\tilde{Z}>Z$, then, on the contrary, the effect is being overestimated.

Further, let us examine active intrusion as the most unpredictable case. Let us assume that at the moment of attack planning the intruder has his/her own idea of the amount of resources allocated by the system's owner to the protection of own facilities, i.e. he/she aware of how the "zero option" he/she knows could change.

Intruders are able to choose targets and sets of facilities they will attack. Let the choice be based on their own model of expected damage, i.e., they have at their disposal four similar (3) matrices for each facility: $\tilde{Q}_{\min}^{[k]}\left(i,j\right)$, $\tilde{Q}_{\max}^{[k]}\left(i,j\right)$, $\tilde{X}_{\min}^{[k]}\left(i,j\right)$, $\tilde{X}_{\max}^{[k]}\left(i,j\right)$ and own idea of the amount of resources $\tilde{Y}$ been invested by the owner into SCS facilities protection. Similarly, if $\tilde{Y}<Y$, then the

adversary underestimates the facility protection capabilities, if $\tilde{Y}>Y$, then he/she overestimates them. Obviously, an intruder can also either overstate or understate estimate $\tilde{Q}_{\min}^{[k]}(i,j)$, $\tilde{Q}_{\max}^{[k]}(i,j)$, $\tilde{X}_{\min}^{[k]}(i,j)$, $\tilde{X}_{\max}^{[k]}(i,j)$, however, using their freedom of choice they select such set of target facilities and such preparations for attacking specific facilities that would do maximum possible damage.

Let us designate as $\delta^{[k]}(i,j)$ the characteristic function that means that against the k-th facility with expected level of protection $i(i=0,1,\ldots,I^{[k]})$ an attack of level $j(j=0,1,\ldots,J^{[k]})$ has been chosen. If for all $i(i=0,1,\ldots,I^{[k]})$ the values of $\delta^{[k]}(i,j)$ are equal to zero, the -th facility will not be exposed to an attack of level j. If for all j and all i the values of $\delta^{[k]}(i,j)$ are equal to zero, the k-th facility under the intruder's assumed objectives definitely drops out of the list of targets.

If for some $\tilde{i}$ value $\delta^{[k]}\left(\tilde{i}, j\left(\tilde{i}\right)\right)=1$, we assume that facility k with the level of protection 0 has been chosen as the target with level of competence $j\left(\tilde{i}\right)$.

The above properties are written with a set of equations:

$$\begin{cases} \forall k \forall i \forall j\, \delta^{[k]}(i,j)\times\left(1-\delta^{[k]}(i,j)\right)=0, \\ \forall k\left(\sum_{i=0}^{I_k}\sum_{j=0}^{J}\delta^{[k]}(i,j)-1\right)\times\left(\sum_{i=0}^{I_k}\sum_{j=0}^{J}\delta^{[k]}(i,j)\right)=0. \end{cases} \quad (8)$$

Given that

$$\forall j \sum_{i=0}^{I_k}\sum_{k}\delta^{[k]}(i,j)=N_j \quad (9)$$

and complementing (8), (9) with a set of constraints we obtain the estimate of the total damage sustained by the facility:

$$\tilde{R}=\sum_{k}\sum_{i=0}^{I_k}\sum_{j=0}^{J}\left\{\begin{array}{c}\delta^{[k]}(i,j)\times\left(\dfrac{Q_{\min}^{[k]}\left(i^{[k]},j\right)+Q_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\times \\ \times\left(\dfrac{X_{\min}^{[k]}\left(i^{[k]},j\right)+X_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\end{array}\right\}. \quad (10)$$

Let us denote $\tilde{R}$ by $\tilde{R}(Var_I, Var_J)$ and emphasize that $\tilde{R}$ depends on both the facility protection solution Var_I, and the type of attack Var_J. Let us find the maximum of $\tilde{R}$ for all types of attack that comply with the restrictions provided that all additional protection solutions are considered as parameters:

$$\tilde{R}^{*}\left(Var_I\right)=\max_{Var_J}\left\{\tilde{R}(Var_I,Var_J)\right\}. \quad (11)$$

Thus, we postulate that the adversary (nature) choses the option that is the worst for the defending party. Subsequently, the problem of protection comes down to limiting the attack options. Such measures of facility protection strengthening are found that minimize $\tilde{R}^{*}\left(Var_I\right)$. In other words, the problem of safety management comes down to finding the equilibrium values of $\tilde{R}^{**}$:

$$\tilde{R}^{**}=\min_{Var_I}\left\{\tilde{R}^{*}(Var_I)\right\}. \quad (12)$$

The proposed problem definition is typical for the games theory. The solution is a Nash equilibrium, saddle value (Var_{I*}, Var_{J*}):

$$\tilde{R}^{**}=\tilde{R}\left(Var_{I^*},Var_{J^*}\right). \quad (13)$$

In this point the defending party is not interested in modifying its equipment strategy Var_{I*}, as outside this strategy the adversary becomes able to perform more "sensitive" attacks. An active attacker is also not interested in modifying its plan $Var_{J*}(Var_{I*})$, as any changes reduces the potential total damage to the SCS facilities and, indirectly, to the nation.

In theory, this definition of the problem has very large dimension and combinatorial complexity, but is quite solvable due to the monotonicity of the criteria and linear nature of the sets of constraints.

The main difficulties of this problem are more about information technology that mathematics:

- for each k-th facility it is required to have estimates of the potential consequences of attacks of varied intensity j, which is often practically impossible;
- for the whole SCS, it is required to consider risks for the facilities along with other possible, if poorly formalized threats. Optimization of protection is more efficient, the more accurate is the assessment of the potential attack capabilities (those are not uniform both in terms of technology and geographical distribution).

In the light of the above problem definition that takes into consideration the integrated effect the understanding of the efficiency estimation of protection systems changes radically. For cases of active attacks, due to the limited resources at the disposal of the criminal underworld, it should be expected that attacks will be retargeted from well-protected facilities (with low expected effectiveness) to less protected facilities (with high effectiveness, but lower immediate damage). It is obvious that it is not rational to additionally protect facilities that noone attacks. It is possible that there are no attacks exactly because the protection measures are regularly enhanced.

Another key element of the problem under consideration is that the search for effective solutions on both sides is largely about the availability of information:

- a criminal, while preparing for an attack, theoretically looks for accomplices that would help choose a target, that would be attainable given the available competences and equipment;
- the protection system would be able to perform greater concentrated countermeasures if it was aware of the criminals' intentions.

For that reason, in the description of the above procedure for the case of active attack it is repeatedly emphasized that this only refers to assessments on both sides. Due to the inevitable uncertainty of the assessments, the problem of definition of the strategy and tactics of enhancement of SCS facilities protection against possible unlawful acts, including terrorist attacks and sabotage, should be solved by "coarsening" the game formulation [3]. While doing so, the adversary's capabilities are to be "idealized", possible losses are to be overstated by means of, for instance, using median instead of maximum estimates.

In conclusion, let us note that the risk assessment must involve the identification of the relations between the analyzed safety indicators and the high-level indicators (for instance, strategic target indicators) and their effect on the attainment of the target values of such indicators. The supervision of the monitored facility is to be organized in such a way as to enable timely execution of managerial decisions, if facility status is approaching hazard. This problem comprises several tasks, as in vertically integrated companies there are several centers of decision-making at various levels of management. This problem may be efficiently solved by means of methods for the estimation of reliability of target indicator attainment and methods of cluster analysis [3, 4].

4. On the indicators of pre-critical situations

The calculation of the parameters that describe the levels of competition, aside from strategy coded forecasts, require the creation of a monitoring system for "poorly formalized" threats to stable operation and development of SCS, i.e. development of the indicators of pre-critical situations.

Obviously, the development of pre-critical situation indicators is a most complex multilevel task, for which there is no single comprehensive solution, therefore further development of the system for standardization and methodological support of SCS safety management would involve the consideration of a number of additional areas of research in pre-critical situation indicators that is to be conducted within "particular" research paradigms using various theoretical approaches and models:

– datalogical approach;

– energy (balance sheet) approach;

– balance sheet approach (program-based planning);

– system status indication based on group behaviour models of system elements;

– system status indication based on the measurement of the correlations within the dynamics of system component indicators;

– system status indication based on "gray box" models (neural network, support vector machines, etc.).

Let us provide brief descriptions of the above approaches.

Datalogical approach. As part of this approach, the "critical situation" entity C is described as a logical function, the integration of possible "reference" implementations with the "OR" operator:

$$C = \bigcup_{n} C^{[n]}. \tag{14}$$

Each critical situation $C^{[n]}$ is described with a certain sufficiently large subset of datalogical characteristics (similarly to keywords in a text). Such descriptions, in general, are ambiguous; "synonyms", omissions of "implied" characteristics, etc. are possible. Normally, characteristics are subdivided into three categories: indicators of the status of the investigated system X, indicators of the "neutral" (natural) environment p and indicators of the potential adversary's ("competitor"'s) activities Y:

$$C^{[n]} = F^{[n]} \left\{ \begin{matrix} X^{[n,1]},..., X^{[n,K(n)]}; p^{[n,1]},..., \\ p^{[n,L(n)]}; Y^{[n,1]},..., X^{[n,M(n)]} \end{matrix} \right\}. \tag{15}$$

A pre-critical situation (threat of critical situation) is diagnosed as an incomplete set of indicators close to one or several "reference" sets of function arguments $F^{[n]}$. At the same time, it is assumed that the solving system is able to estimate the probability of threat escalation into critical situations. That requires models of natural phenomena and models of competitor behaviour in response to the implementation of certain managerial decisions.

A similar approach is developed within the theory of conflicting structures and theory of heuristics in multi-step position games [5], in the decision theory [6], in some areas of artificial intelligence application [7] (medical diagnostic systems and other pattern recognition systems). In any case, this approach implements a certain automation of hypothesis formation [8] and some mechanisms of "reference" pattern "smearing" [9].

The descriptions of the pre-critical situation models are formalized as event/failure trees/networks that illustrate the logic of scenario development [10]. The synonymy (competition or replacement of risks) is simulated in the form of mutually nested contraction functions of information features $F^{[n]}$, from the contractions of primary features to larger aggregative features [6]. In case of large numbers of primary features, the feature dictionaries are often organized hierarchically [11].

The description of event trees is the prerogative of experts, however, interest has been growing lately in describing complex poorly formalized expert decisions using "genetic" algorithms and other heuristic methods that combine the search for the best description of a complex system (pre-critical situation) and limited logic of evolutionary selection [12].

Energy (balance sheet) approach. The activities of any company include three components: the resource-related component, the science and technology (manufacturing) component and the foreign economic (market) component.

Given the above, the amount of sold goods can be evaluated using the following formula

$$C=E \times C_{eff} \times C_{plan}, \quad (16)$$

where E is the energy required for manufacturing the goods; efficiency coefficient (C_{eff}) ($0\leq C_{\mathrm{eff}} \leq 1$) reflects the efficiency of the manufacturing process (scientific and technological level of the manufacturer); plan quality coefficient (C_{plan}) lower than one indicates that the product has been manufactured but found no demand (or sold at a lower price), for instance, due to competitors' actions (emergence of alternative sources of energy), or foreign political (economic) circumstances (nonpayment risk, relocation of energy-intensive, polluting industrial facilities to developing countries, etc.).

This approach allows developing indicators of critical situation threats in terms of the probability of production capacity disruption. In this approach, a special attention is given to identifying the "bottlenecks" that define the top rates of goods flow (Gause's principle, Powell's bottleneck, etc.), whose indicators are used in the performance analysis of autopoietic systems accounting for "intraspecific" and "interspecific" competition [13].

Balance sheet approach (program-based planning). Methods of project management (scheduling) can help calculate the dependencies of the probabilities of certain activities completion from the amounts of allocated resources R and time T. Due to physical reasons there are minimal values T_{min} and R_{min}, below which activities cannot be completed in principle. For that reason, in order to improve the probability of activity completion, time and resource margins are created that are assumed to enable work performance in accordance with the approved schedule and within the allocated funds depending on the remaining work effort.

While analyzing the dynamics of time and funds consumption, it is advisable to employ as indicators the data that attest to the approach of the work completion indicators not situated on the "critical" paths in the activity charts to the critical activity indicators. The threat of overabundance of new critical paths for resources and/or time may indicate a pre-critical situation.

All the above approaches imply increasing level of detail of the description of system dynamics within the adaptive control paradigm. In other words, the level of deviation from the chosen work schedule of the considered system are analyzed as if only "external" factors (nature, competition) put the system out of balance, and it is required to measure the probability of crossing a certain barrier of stability.

However, situations may arise when maintaining the balance is impossible or unnecessary, and the system structure is to be reorganized in search of a "new way of living".

System status indication based on group behaviour models of system elements. As of late, prediction of the behaviour of economic system often involves "field" models based on Langevin and Fokker-Plank equations. Such equations describe the dynamics of system elements as a certain "particle hive" that is affected by two types of factors, i.e. factors of drift that shift the center by the action of external forces, and diffusion factors that reflect the freedom of particle migration with the hive. Within the models, hive disintegration or deterioration indicators are developed. Model indicators are estimative in their nature, as they are primarily based on the validity of the law of large numbers (theory of large deflection under random walks).

We can note a close relationship between the "field" models and applied catastrophe theory [14]. For instance, the work shows the proximity between such indicators as "increased large deviations – reduction of time of controlled indicator deviation outside the "corridor", reduction of the "rate of system relaxation to equilibrium states", "deterioration of the Hessian stability matrix".

System status indication based on the measurement of the correlations within the dynamics of system component indicators. Under this definition, critical situations are classified based on the variation of stable (for instance, correlation, causal, associative, information) relations between system elements. The analysis of interconnected economic behaviour of large subsystems (subsidiaries) can be enhanced by the application of findings of gender (family) relations analysis, as well as Gumilyov's mathematical theory of complementarity of ethnic groups [15].

System status indication based on "gray box" models (neural networks).Neural network classification of complex system states is based on the identification of information features and connections between them that correspond to the most common structures of critical situations. Decision rules are obtained by means of programming by example.

As the distribution laws of critical situations are unknown, a large number of parameters and examples are required for their description, therefore the "critical situation – non-critical situation" classification involves certain simplifications.

The following neural network solutions are most efficient for stochastic process simulation: probabilistic neural networks [16], Kohonen self-organizing maps [17] and algorithms with dynamic adaptation to modifiable statistics that describe the coordinates of the "reference" critical situations in the form of growing neural gas that propagates across the description space of examples [18].

Conclusion

All of the above, as well as the requirements of the systems approach to the study of the problems identified in the paper, naturally leads to the requirement to simulate the safety system of SCS as an evolutionary system [19].

Any object of research complimented, if necessary, with some connections to other evolving items, for instance, subjects of research, can be interpreted as such system. The realization of this fact stimulates a more and more active development of this line of research in a variety of fields of study [19-23].

Expert estimates show that the cumulative effect of the application of all available means of situational analysis (identification of hazardous activity, safety declaration, emergency action planning, community awareness of possible emergencies) in terms of reduction of accident rate and unplanned losses may be as high as 10 to 15 %. For instance, the speedy adoption by the European Union of the primary provisions of the Seveso Directive (1982) [24] allowed reducing the accident rate in developed countries 4 to 8 times (from 400 accident, including 75 major ones, in 1983 to 70, including 21 major ones, in 1989). The proposed information and organization measures will become more efficient if all components of the process safety management system responsible for the prediction, prevention and localization of negative consequences are in compliance with single regulations and standards. Subsequently, a process is required of gradual updating of the information, regulatory, predictive and analytical support of process safety activities both at the corporate and institutional levels.

In general, monitoring of the operation of the complex system that is a corporation is a key task of safety management. This monitoring can be compared to preventive therapeutic measures. Unlike in supervisory control that aims to quickly react to the ever-evolving situation, localize the occurring emergencies, sometimes perform (again, using a medical analogy) “surgical” intervention, the monitoring center (in the future, a network of centers for collection of reliable information on the changes occurring within SCS) is to predict the onset of negative trends in the SCS environment, in its internal processes in order to suggest remedial actions that could prevent the transformation of the identified threats into emergencies and crises.

References

[1] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. Dependability. 2019;4:54-66. URL: https://doi.org/:10.21683/1729-2646-2019-19-4-54-66.

[2] Bochkov A.V., Ushakov I.A. Solving the task of resources allocation for critical infrastructure protection against terrorist attacks based on subjective expert estimate. *Dependability*. 2015;1:88-96. Available at: https://doi.org/10.21683/1729-2646-2015-0-1-88-96

[3] Bochkov A.V., Zhigirev N.N., Lesnykh V.V. Dynamic Multi Criteria Decision Making Method for Sustainability Risk Analysis of Structurally Complex Techno-Economic Systems. Reliability: Theory & Applications. 2012;1;2(25):36-42.

[4] Bochkov A.V., Zhigirev N.N. Ram M., Davim J., editors. Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty. Advanced Mathematical Techniques in Engineering Science. CRC Press. Series: Science, Technology and Management. 2018;May, 17:121-154.

[5] Lefebvre V.A. Conflicting structures. Moscow: Sovietskoie radio; 1973.

[6] Muschick E., Muller P. Methods of engineering decision-making. Moscow: Mir; 1990.

[7] Popov E.V., Fomin I.B., Kisel E.B. et al. [Statistical and dynamic expert systems]. Moscow: Finansy i statistika; 1996. (in Russ.)

[8] Hajek P., Havranek T. Mechanizing hypothesis formation. Moscow: Nauka; 1984.

[9] [Fuzzy sets and possibility theory]. Moscow: Radio i sviaz; 1986. (in Russ.)

[10] Podinovsky V.V., Nogin V.D. [Pareto-optimal solutions of multicriterion problems]. Moscow: Nauka; 1982. (in Russ.)

[11] Jambu M. Classification automatique pour l’analyse des données. Moscow: Finansy i statistika; 1988.

[12] Price K.V. Genetic Annealing. Dr. Dobb’s Journal. 1994;19(11):117.

[13] Ebeling W., Engel A., Feistel R. Physik der Evolutionsprozesse. Moscow: Editorial URSS; 2001.

[14] Gilmore R. Catastrophe theory for scientists and engineers. Moscow: Mir; 1984.

[15] Guts A.K., Korobitsyn V.V. [Mathematical models of social systems: Study guide in 2 volumes]. Omsk: OmSU; 2000. (in Russ.)

[16] Specht D. Probabilistic Neural Networks. Neural Networks;1990:1.

[17] Kohonen T. Self-Organizing Maps. Springer-Verlag; 1995.

[18] Fritzke B. Tessauro G., Touretsky D.S., Leen T.K., editors. A growing neural gas network learns topologies. Advanced in Neural Information Processing Systems 7. Cambridge (MA): MIT Press; 1995.

[19] Glushkov V.V., Ivanov V.V., Yanenko V.M. [Simulation of evolutionary systems]. Moscow: Nauka. Main office of physics and mathematics; 1983. (in Russ.)

[20] Nikolis G., Prigozhin I. Chizmazhev Yu.A., editor. [Self-organization in nonequilibrium systems]. Moscow: Mir; 1979. (in Russ.)

[21] Reutov A.P., Savchenko R.G., Suslov R.M. [System model as a relation of generalized properties: order, dependability and efficiency]. In: [Matters of cybernetics (system development management)]. Moscow: 1979. (in Russ.) Moscow: 1979. 26 – 34.

[22] Romanovsky Yu.M. [Self-organization processes in physics, chemistry and biology]. Moscow: Znanie; 1981. (in Russ.)

[23] Ganti T. A theory of Biomedical supersystems and its application to problems of natural and artificial biogenesis. Budapest: Akademiai; 1979.

[24] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major accident hazards involving dangerous substances. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018&from=en (accessed 17.02.2017).

About the author

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

The author's contribution

The author suggested a method of risk synthesis (with game problem definition of countering possible external effects of various nature on critical infrastructure facilities) as one of the foundations of the design of advanced systems for monitoring safety threats to structurally complex systems. Key methodological premises were formulated: from general problem definition of safety management through the synthesis of a model of a controlled facility and its external and internal connections, solution to the problem of selection of priority protection facilities in terms of assuring efficient operation and general safety of structurally complex systems.