Original article
https://doi.org/10.21683/1729-2646-2020-20-3-34-46

On the methods of qualitative estimation of the safety state of structurally complex systems

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

Alexander V. Bochkov

Abstract. Aim. *To show a method of overcoming the uncertainty in the requirements for the quality of data in non-standard situations and ways of formalizing the decision-making process aimed at ensuring safe operation of structurally complex systems. The paper proposes a method of axiomatic construction of integrated indicators that describe the properties of a system and its operational environment through the synthesis of the risk function.* **Methods.** *Methods of system analysis of the objective, Russman's methods of the difficulty in achieving the objectives and the Shewhart charts theory.* **Results.** *The author proposed methods of qualitative estimation of two types of safety state, i.e. "better than" (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or "not worse than" (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go), that imply certain ranges of deviation from the specified target or, respectively, the minimal allowable levels, within which the safety state evaluated with an integrated index is deemed to be acceptable.* **Conclusions.** *It is shown that, in respect to problems of safety and risk assessment of structurally complex systems, one should not try to work with specific safety-related events only. All such events are characterized by a set of properties and contributing factors with associated characteristics. One should try to identify each property and each characteristic of such property, which would later allow defining proactive and reactive control actions in response to changes in such characteristics and properties. Having worked out a property of a situation or an event, we work out a property of a risk, and it is of no significance in which specific risk this property manifests itself. Combinations of risk properties can be extremely numerous, therefore it is very difficult to predict specific situations. That causes the requirement for a proactive decision support system that ensures high-quality managerial decisions short before a critical event.*

Keywords: *structurally complex system, risk synthesis, safety, management, difficulty in achieving the objective, statistical reasoning.*

For citation: *Bochkov A.V. On the methods of qualitative estimation of the safety state of structurally complex systems. Dependability 2020;3: 34-46. https://doi.org/10.21683/1729-2646-2020-20-3-34-46*

Received on: *16.06.2020* / **Revised on:** *02.07.2020* / **For printing:** *21.09.2020*

Introduction

The problem of optimal decision making in system management under the condition of poor mathematical formulation that is characterized by, first, the uncertainty in the choice of the target function and definition of limitations associated with a large number of heteronymous and contradictory indicators of the possible current and future system state descriptions, and second, the non-standard decision-making situation that consists in the capability to only calculate for each option only the values of individual indicators, lack of knowledge on and difficulty to implement a number of important properties of the objective function, properties of the search domain, etc. In this context, decision-making is in general defined as the process of selection of the best out of all possible solutions. However, in practice, achieving optimal results may be difficult, as decision-makers (DM) and experts often have difficulties making decisions.

Risk analysis is essentially the only way of researching those aspects of safety that cannot be covered by statistics, like, for example, low-probability accidents with high potential consequences [1]. Certainly, risk analysis does not solve all safety problems, but its use is required to compare the consequences caused by various hazards, identify the most important among them, chose the most efficient and cost-effective safety systems, develop accident relief measures, etc. Risk as a dynamic characteristic that depends on the time, assets and information cannot be reduced to “two-dimensional estimates” of probability and damage. Additionally, there is a crucial difference between the stochastic factors that entail decisions in the presence of risk, and indefinite factors that entail decisions under uncertainty. Both cause varied outcomes of managerial actions, but stochastic factors are completely described by available stochastic information (such information is what allows choosing the optimal solution). In respect to uncertain factors such information is not available.

The problem of elimination of uncertainties in the context of safety assessment is of high practical significance and has not been completely resolved yet. Within the scientific community, even the interpretation of the concepts used by various researchers provoke discussions [2].

Many, if not most, methods in statistics use probabilities that comply with the classical Kolmogorov axioms (called “exact”, “classical” or “additive” probabilities). However, in the very early publications dedicated to quantitative estimation of uncertainty, among other things, foresight [3], non-additive probabilities [4] and convex sets of probabilities [5] were used. A clear emphasis on exact probabilities developed only after Laplace’s works [6], and today many statistics and probability theory researchers are still convinced that additive probabilities are the foundation of the quantitative definition of uncertainty that is rich enough to cope with all types of uncertainty and the information that is generated as part of practical tasks. However, the opinion is becoming commonplace that additive probabilities are too limited and the emerging alternative structures ensure the required flexibility for quantitative estimation of uncertainty, thus also providing new methods of addressing it as part of engineering risk, safety and dependability assessment.

The situation of uncertainty is characterized by the fact that the selection of a specific plan of actions may lead to any result out of a certain set of variants, but the probability of the effect of random factors is unknown. Normally, two cases are distinguished: in the first case, the probabilities are unknown due to the lack of required statistical information, while in the second case the situation is not statistical and objective probabilities are out of the question (the situation is the so-called “perfect” uncertainty). The “perfect” uncertainty is the most common, as decisions (specificity strategic ones) are normally taken under unique conditions. Decisions taken under uncertainty are strongly associated with risk.

Engineers usually addressed uncertainty using safety factors, requiring that the actual load capacity of a structure is above the design load by a certain coefficient. Nevertheless, the approach involving the safety factor does not provide any information on the actual time to failure and thus is not completely satisfactory. As a better analytical description of uncertainties was preferable, engineering evaluations were incorporated in the probabilistic basis since the 1950s in the innovative works of Freudenthal, Bolotin and others. This approach implied that each parameter of a model is considered as a random value, and instead of absolute safety the probability of failure is considered. Such probabilistic approach causes an explosive growth of the number of parameters: each physical parameter now has a probability distribution that, in turn, is described by distribution parameters (such as the average value, standard deviation, excess, etc.), not to speak of the description of correlations between variables. Unfortunately, that requires much more information than usually available. Thus, in practice, distribution parameters must be partially defined through normative assumptions, e.g. by simply limiting the type of distribution by the type that is common to technical literature, or naively presuming independence, if information on correlations is unavailable. In other words, it is required to introduce artificial information, that cannot be confirmed by available data.

The pursuance of uncertainty models that reflect the actual level of available information lead to the search for alternative models within the engineering community: probabilistic models were considered to be an excessively rigid concept, while engineering practice had sufficiently clearly shown that interval estimation of uncertainty is superior to pointwise estimation.

What is the solution? We must migrate towards risk synthesis in system management and conceptual design of management systems. Probability is not an additive value. The addition of the products of probability and damage only works for small probabilities. This matter was, for example, discussed in previous articles [7, 8]. The key idea expressed in those publications is that risk assessment shall be performed on the assumption of unachievable "ideal". As consequence, the development program (project, model) must include a description of such ideal in reference to all factors and threats. Solving this problem requires developing the structure of the management system that would reflect the correlations between such elements, threats, risks and vulnerabilities. By definition, the problem of such system's structure synthesis comes down to the definition of the set of correlations over the set of its elements.

In terms of perception, for instance, where the field of consciousness can be easily analyzed experimentally, it has been concluded that the so-called "elements" are always products of dissociation or extraction out of a whole within an initial set and no special correlation can be identified without the initial identification of the characteristic structural properties of the set. Eventually, that will lead to the realization of the requirement for a truly functional monitoring system that, in general, implies solving four interdependent problems [9, 10]:

– observation that consists in the acquisition and distribution of information, processing and delivery to users (this is the integration function and allows building a database for the purpose of analysis, estimation and prediction of the state of the monitoring object and its development);

– analysis and assessment involve the analysis of the collected information, identification of causal relationships, comparison of the adopted indicators with the specified standard ones;

– prediction that is associated with the feasibility to use high-quality monitoring information for the purpose of reliable representation of the general future development pattern of the observed phenomenon, object or system and thus scientifically substantiated development of short and long-term plans for the transformation and management of certain processes;

– supervision that consists in constant monitoring of the obtained results and their comparison with the input data, as well as organization and follow-up of the planned measures and tasks.

The inclusion of the analytical component into the monitoring system is justified and reasonable. Additionally, analysis is the most significant element of monitoring, since monitoring is not only about recording facts, mirror-image presentation of the occurring processes, but also analytics, assessment that enables conclusions and suggestions, predictions, planning, development scenario preparation, etc. The prognostic component is the basic one of the supervision, planning and management functions. If we imagine management as the transmission of information flows from one management entity to another, then management is the process of conditioning of the behaviour of the controlled object and ensuring its stable operation under risk and uncertainty by organizing internal and external information flows, as well as methods of its retrieval, processing and distribution that allow developing, selecting and implementing rational managerial decisions. In the context of limited flows of information on the state of the controlled object or the extreme scarcity of the safety-specific features of situation description, qualitative estimation may find widespread application.

1. On the qualitative assessments

There are two types of qualitative estimation of process safety: **"better than"** (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or **"not worse than"** (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go). Both estimates imply certain **ranges of deviation from the specified target or, respectively, the minimal allowable level**, within which the process safety state evaluated with an integrated index is deemed to be acceptable.

The advantage of qualitative estimation consists in the simplicity of application and use of a lesser amount of information, simplicity of perception and interpretation by the DM. Global experience shows that the application of qualitative methods of estimation often produces a higher number of safety recommendations than the quantitative method. Such methods have a number of characteristic features. Normally, qualitative indicators are expressed in points or ranks that are numbers, but such numbers cannot be subject to basic mathematical operations, they do not comply with general mathematical rules, i.e. if one of the indicators is assigned the rank of "1", while another is assigned the rank of "2", that does not mean that the former evaluates the hazard twice lower than the latter. In order to obtain an aggregate qualitative estimate of safety, logical rules and procedures are normally used.

2. On the assessment scale

For the purpose of indicator estimation, adequate numerical or ordinal scales must be developed. Indicator scoring, for instance, can be done using the nonlinear, nonuniform scale that has shown its efficiency as part of a number of practical tasks [11-13].

It is constructed on the basis of the knowledge of the range of values received by the indicators, i.e. the knowledge of the minimum x_{min} and maximum x_{max} estimates. It is adopted that the value 1 equals to x_{min}, while the value 9 equals to x_{max}, respectively (Fig. 1).

The average estimate 5 is to correspond with such value of indicator x_5 that meets the condition: relation x_{max}/x_5 is equal to x_5/x_{min}. Having solved equation $(x_{max}/x_5) = (x_5/x_{min})$ we deduce that x_5 is equal to the geometric mean of x_{min}, x_{max}. Value x_3 is defined similarly as $\sqrt{x_3 x_{min}}$; $x_5 = \sqrt{x_{max} x_{min}}$; $x_7 = \sqrt{x_5 x_{max}}$, respectively. Then, x_2 is the average compound $\sqrt{x_{min} x_3}$; $x_4 = \sqrt{x_3 x_5}$; $x_6 = \sqrt{x_4 x_7}$; $x_8 = \sqrt{x_7 x_9}$ and x_{min}, x_2, x_3,…, x_8, x_{max} are average values that correspond to 1, 2, 3, ..., 9 points.

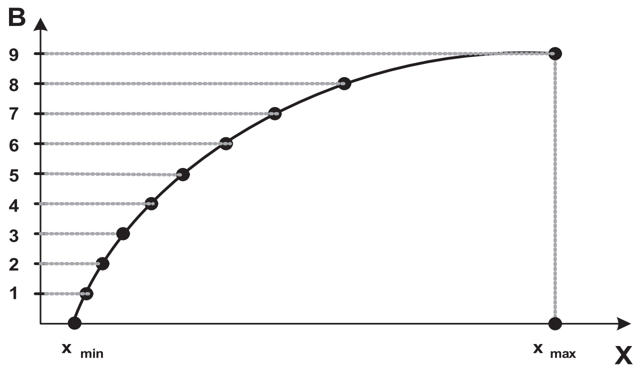

Fig. 1. Nonlinear, nonuniform scale of indicator estimation

The limit separating the values that correspond to one and two points is calculated as $\sqrt{x_{\min} x_2}$. Then, the limits between two and three points are defined as $\sqrt{x_2 x_3}$, etc. Finally, the limits between the eight-point and nine-point estimates are calculated as $\sqrt{x_8 x_{\max}}$. If there is no available information on an indicator, when transforming into point-based estimate, it is assigned the value of 5. The maximum and minimum values of features, relative to which the scale is calculated, are selected out of all data on the ranked objects of a certain object of evaluation.

For a random set of objects $\{O_j\}$ with dimension x_j, designating A the minimal out of all values x_j, and B the maximum value of all x_j, we have that in order to build a scale with K steps it is required to calculate K–1 values (i=1, ..., K–1). For instance, for K=9: $\tilde{x}_i = A\cdot\left(\frac{B}{A}\right)^{\frac{1}{2K-2}}\cdot\left(\frac{B}{A}\right)^{\frac{2(i-1)}{2K-2}}$ and, respectively:

$$\tilde{x}_1 = A\cdot\left(\frac{B}{A}\right)^{\frac{1}{16}};\ \tilde{x}_2 = A\cdot\left(\frac{B}{A}\right)^{\frac{3}{16}};\ \tilde{x}_3 = A\cdot\left(\frac{B}{A}\right)^{\frac{5}{16}};$$

$$\tilde{x}_4 = A\cdot\left(\frac{B}{A}\right)^{\frac{7}{16}};\ \tilde{x}_5 = A\cdot\left(\frac{B}{A}\right)^{\frac{9}{16}};\ \tilde{x}_6 = A\cdot\left(\frac{B}{A}\right)^{\frac{11}{16}};$$

$$\tilde{x}_7 = A\cdot\left(\frac{B}{A}\right)^{\frac{13}{16}};\ \tilde{x}_8 = A\cdot\left(\frac{B}{A}\right)^{\frac{15}{16}};$$

Next, all $x_j < \tilde{x}_1$ will be estimated as 1 point, all $\tilde{x}_i \le x_j < \tilde{x}_{2+1}$ $(i = 2,\ldots,K-1)$ will be rated i points and, finally, all $x_j \ge \tilde{x}_{K-1}$ will be rated (Fig. 2) $\tilde{x}_1$, maximum of K points.

Fig. 2. Table for conversion of actual object description parameter values into points

3. On the whole (minimally allowable) level

The target or, respectively, minimum safety status can be defined in two ways:

- statistically (based on the processing of a priori information on the changes of an indicator value that evaluates the safety status over a period of at least 5 years);

- expertly (based on consolidated opinions of safety experts on the allowable values of the appropriate indicators).

For instance, according to 116-FZ, industrial safety is the state of protection of the vital interests of individuals and the society against accidents in hazardous industrial facilities and their consequences. Considering "accidents in hazardous industrial facilities and their consequences" as the result of realization of the threats to "vital interests of individuals and the society", the concept of "**safety**" – regardless of the application field – can be considered as the **acknowledged by individuals and the society allowable level of hazard to their vital interests**. That concept was defined in GOST R ISO 31000-2010 Risk management. Principles and guidelines as "risk": **risk is the effect of uncertainty on the objectives**.

If the objective of safety consists in achieving a subjective feeling of safety from hazards associated with any industrial activity that is sufficient to individuals and the society, then the measures aimed at achieving such objective are to reduce the effect (possible damage, losses) and uncertainty (of information, place, time) of an acknowledged hazard on safety.

Acknowledging the allowable level of hazard involves using the risk assessment procedure that is essentially the only possible way of researching those aspects of safety that cannot be answered by statistics, e.g. low-probability accidents with significant potential consequences, so-called Black Swan events (a term referring to events subjectively evaluated as impossible and, as consequence, not considered), etc. The irreplaceability of the approach based on the assessment of the risk associated with the existing options for the development of safety management systems is due to the fast-changing nature of the respective process, and therefore the corresponding data that describe the states of the system and its environment, that leads to a situation when models based on large amounts of statistical information soon become obsolete and do not reflect the reality. Given the above, the migration from point-wise assessment of the state of safety management system to interval integral estimates is inevitable.

4. On the integrated index

As an integral estimate of process safety, it is suggested using comprehensive target metric that is a convolution (weighted sum) of local safety indicators of the form [14]:

$$F = \sum_{v=1}^{h} \lambda_v F_v\left(\alpha^i\right),\ F = \prod_{v=1}^{h} F_v\left(\alpha^i\right)^{\beta_v} \quad (1)$$

where $\alpha^i \in D$; λ_v and β_v are the weight numbers obtained using certain additional assumptions on the operation of the model α^i; such numbers depend on the achieved particular indicators $F_v\left(\alpha^i\right)$; D is the allowable set of estimates.

The matter of selection of the type of convolution requires additional research. The initial premise of the convolution-based methods is that each individual alternative can be evaluated numerically. However, as each alternative depends on many variables, the problem of finding the best alternative becomes complicated, because points in a multidimensional space cannot be ordered naturally.

Hypothetically, we can imagine a case when one of the alternatives has the highest values of all compared criteria and, subsequently, is the best. However, in practice, such cases almost never occur. One of the most common and simple methods of comparing multicriteria alternatives consists in reducing a multicriteria problem to a unicriterial problem, i.e. replacing a vector argument function with a scalar function.

In specialized literature, this operation was named convolution calculation (construction of supercriterion, integrated indicator) that is the numerical measure that allows comparing it with the measures of the alternatives.

The following methods are currently the most commonly used:

- weighted summation;
- additive convolution;
- multiplicative convolution.

Weighted summation is based on the calculation of the mathematical average. A set of coefficients is to meet the normalization requirement, non-compliance with which makes the scales of individual criteria and, subsequently, the final estimates of the alternatives, incomparable. The only advantage of the weighted summation is the computational efficiency, while the shortcomings come down to the following: the computational result is the absolute values of criteria, which does not allow comparing heterogeneous criteria (e.g. cost, distance, weight); criteria values are not adjusted to the [0; 1] range of the absolute scale, which allows using only the properties of the "weaker" interval scale; the average, as an estimate of an alternative, does not contain the criterion's share of its maximum value, which does not allow comparing estimates obtained in different scales. The introduction of utility has an axiomatic substantiation in the form of the R. Keeney theorem, according to which the unicriterial utility may be either additive, or multiplicative [15].

Additive convolution. The characteristic property of the additive convolution is that it gives maximum estimates to those alternatives that have higher numbers of criteria whose values are close to maximum (given equal average values for all alternatives). If the direction of optimization changes, the priorities are reversed. The use of additive convolution instead of weighted summation has the following advantages: the convolution transforms absolute values into relative ones, which allows comparing heterogeneous qualities; the convolution reduces the criteria values to the range of [0; 1] of the absolute scale, which enables all permitted algebraic operations; specifying the criterion's share of its maximum value allows comparing estimates obtained in different scales.

Multiplicative convolution. The characteristic property of the multiplicative convolution is that it favours those alternatives that have a more even distribution on the absolute scale of criteria given equal average values for all alternatives. The advantages of the multiplicative convolution are similar to those of the additive convolution.

5. On the partial indices

The structure of indicators depends on the controlled object and regular availability of data on the values that describe the object and its environment in its features and characteristics. An example of such structure is the conventional structure of particular indicators of the process safety procedure of subsidiary operating companies and organizations (Fig. 3).

5.1. **Indicator of the quality of process safety of subsidiary operating companies and organizations** (F_{PS})

The generalized estimate of the state of process safety characterizes the overall level of the company's process safety accounting for the number, frequency, eliminability and severity of the inconsistencies.

5.2. **Indicator of the safety of subsidiary operating companies and organizations personnel** (F_{OT})

5.2.1. The **LTIF indicator**, the lost time injury frequency, i.e. the specific losses in manpower, cases of loss of productivity (including fatalities, as well as temporary and permanent incapacitation (disability) per 1 mil ppl/h of work. This number of cases of lost time incidents (LTI) taken relative to the total work hours in a business unit or company (WH) over a certain period of time (normally, a year) and normalized to 1 mil ppl/h. It characterizes the total work hours lost as the result of injuries.

5.2.2. The **TRCF indicator**, total recordable case frequency, i.e. the number of all recorded cases (TRC) taken relative to the total work hours (WH) and normalized to 1 mil ppl/h. It reflects the workplace injury situation in a timely and comprehensive manner.

5.3. **Indicator of subsidiary operating companies and organizations stability** (F_s)

5.3.1. **Process safety indicator** (Saf)

5.3.1.1. Number of accidents in the facility over five years.

5.3.1.2. Number of 1-st group incidents in the facility over five years.

5.3.1.3. Number of 2-nd group incidents in the facility over five years.

5.3.1.4. Integrity indicator (integral score of operability) calculated using the methods currently adopted in the industry. The indicator is calculated based on the logical and probabilistic evaluation of an object's probability of no-failure, significance of its engineering elements in term of their failure's effect on the operability, total technology-related risk of possible accidents.

5.3.2. **Unplanned losses indicator** (insurance) LACE, loss of average capital employed, a dimensionless parameter (measured in %) defined as the ratio of the size of unplanned losses with allowance for insurance to the average capital employed [16]:

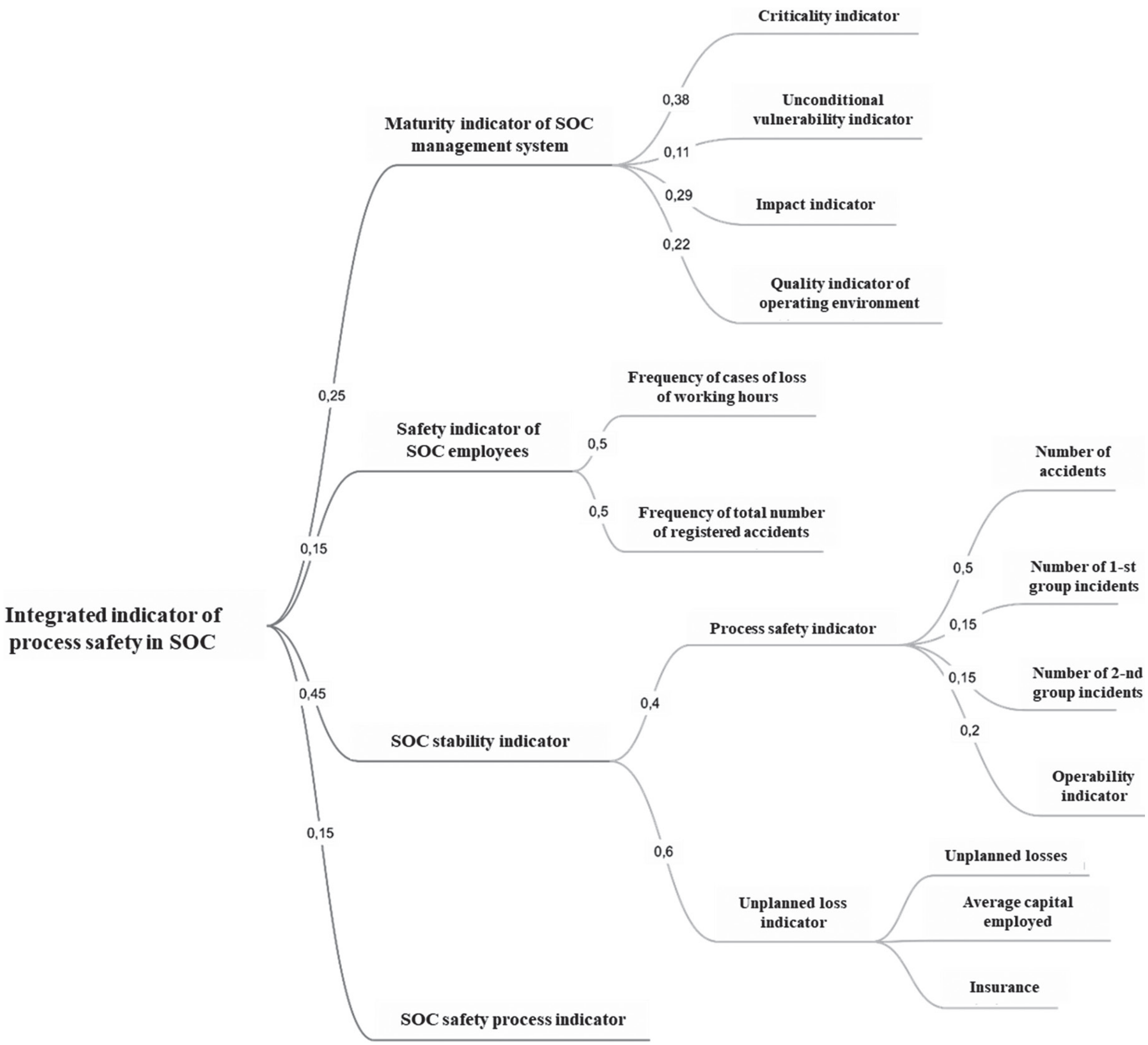

Figure 3. Structure of particular indicators of the process safety procedure of subsidiary operating companies and organizations (tentative example)

$$LACE = \frac{(1-M)\cdot UPL}{ACE},$$

where *UPL* is the unplanned losses (including the total money equivalent of material losses, human resource and financial losses, including compensation for losses from business interruption, compensation of damage to legal entities and property of citizens, compensations for environmental damage) that, through lower-level indicators is associated with industrial risk indicators: individual risk; social risk; economic risk; *M* is the indicator of unplanned losses insurance; *ACE* is the average capital employed.

As the "basis" of *LACE* calculation, the average employed capital is to be used (similarly to the definition of the first-level target indicator), the return on capital employed. In the Russian practice, operating costs are normally used as the "basis".

5.4. **Indicator of the maturity of the process safety management system of subsidiary operating companies and organizations' facilities evaluated based on a metric opposite of the risk of insufficient supervision** (F_{RIM})

The risk of insufficient supervision is a composite indicator that characterizes the hazard of a supervisory authority missing an object (business unit), that may potentially be affected by nonconformances and accidents. The risk of insufficient supervision defines the rank (place) of a subsidiary's business unit in the listing of supervised objects. The risk of insufficient supervision is calculated for various businesses (natural resources producers, gas transmission providers, processing companies, underground gas storage facilities, etc.) according to the same procedure [17].

The management system maturity indicator is defined as the value opposite of the weighted sum of the four indicators of risk of insufficient supervision (rated in points):

$$F_{RIM} = 1 - \sum_{i=1}^{4} \lambda_i F_i,$$

where λ_i is the weight indicator of the respective scale in units of the correction scale that are defined expertly;

supervision object criticality indicator (F_1) evaluates the specificity of the ranked subsidiary's business unit in terms of the aims of supervision (this indicator is used in calculations and is closely associated with the incident rate and inefficient gas utilization). It is calculated through the convolution of standardized description features of a business unit of the ranked type with appropriate weights;

indicator of unconditional "vulnerability" of the supervised object (F_2) evaluates the risk of imposition of sanctions by public supervisory bodies and the risk of undesirable consequences as the result of failure to eliminate the violations identified by corporate supervision. It is calculated through the convolution of standardized description features of a business unit of the ranked type with appropriate weights;

the indicator (coefficient) of the "effect" of the supervised object (F_3) for gas transmission (distribution) facilities is calculated using a flow-oriented model and statistical data on the structure of gas consumption in Russia's regions and characterizes the importance of performance by the object of a unit of commodity transport operation. For objects that are not gas transmission (distribution) facilities the value of this indicator is adopted as national-average;

the indicator (coefficient) of the "quality of the environment", in which the supervised object operates (F_4), a dimensionless value that is calculated based on fitted statistical data on the characteristics of subsidiaries in relation to their spatial location; for each territory, on account of geographical factors, specificity of the operating structure, sociocultural, ethnic, corruption-related and other differences, unique calculation models must be developed that would largely rely on subjective estimates by experts familiar with such specificity (the primary source of information for the calculation of the environment "quality" indicator of a ranked object is the Regiony Rossii. Sotsialno-ekonomicheskie pokazateli (Regions of Russia. Socioeconomic indicators) yearbook.

The weights of indicators shown in Fig. 3 as an example can be obtained by means of expert evaluation (e.g., Saaty's pairwise comparison). Detailed descriptions of the method can be found in literature [18].

6. On the methods of qualitative estimation

In order to obtain a qualitative estimate "better than", it is suggested using I. Russman's method [19-21] (estimation of the difficulty in achieving the target indicator value), while in order to obtain a qualitative estimate "not worse than", it is suggested to use Shewhart charts [22-24] (estimation of random and special causes of indicator value variation).

6.1. Estimation of the difficulty in achieving the target indicator value

The method is applicable if there is a specified (required) value of the integrated indicator, whose quantitative expression is the value in point C (Fig. 4). Information is available that allows evaluating the minimum and

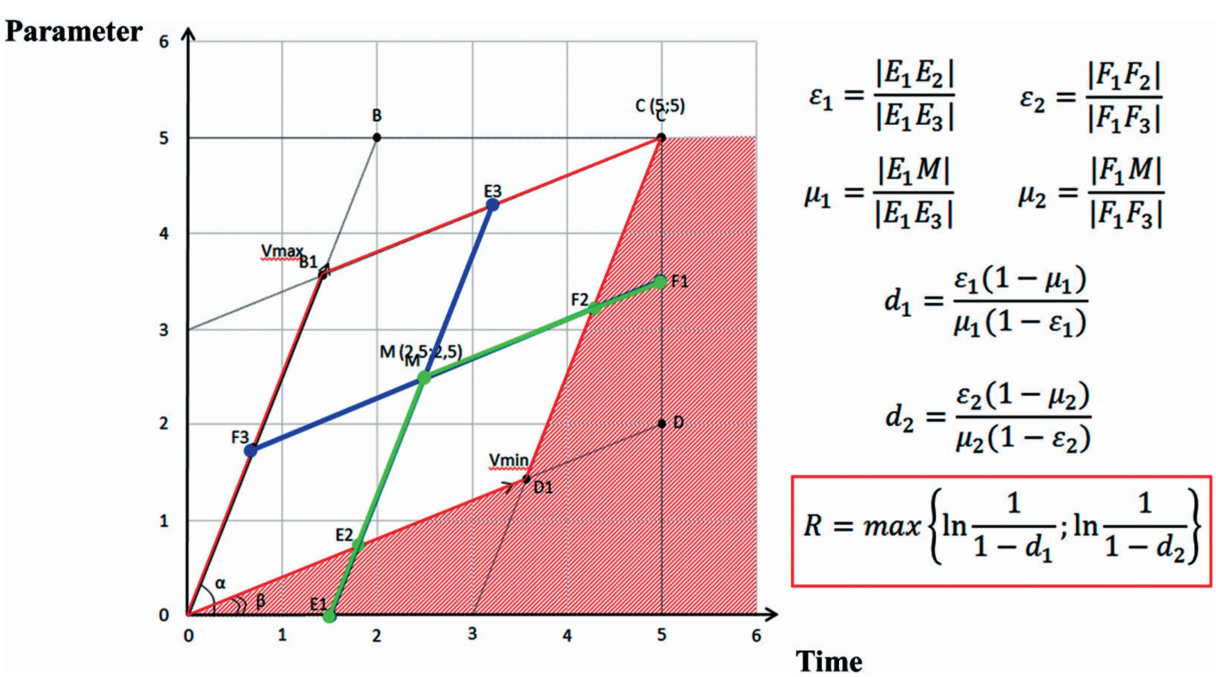

Fig. 4. Russman's basic calculation formulas

maximum rate of change of the indicator over the previous observation periods.

If, over time, the integrated indicator falls within the dashed area (Fig. 4), achieving the target within the specified time will become impossible, therefore this area becomes forbidden and proximity to it should be considered as potential mission failure and, consequently, unsatisfactory assessment of the process safety.

For the purpose of qualitative estimation of process safety of subsidiary operating companies and organizations, let us define the difficulty in achieving the specified target indicator values as the hazard of non-achievement of the specified target value of the integrated safety indicator. The difficulty consists in the variable value that is a function relative to the current position of the indicator: it grows as the indicator value approaches certain allowable limits, upon crossing which achieving the target value is practically impossible.

Under the adopted assumption the difficulty qualitatively characterizes the probability of non-achievement of the target. Graphically, this probability is taken as the ratio between the length of the segment of possible velocities to the length of the segment of allowable velocities (maintaining which the target indicator value can be achieved within the given time).

The **"better than" estimation criteria** of process safety of subsidiary operating companies and organizations impose limitations on the rate of change of the integrated indicator, namely:

Criterion 1. *The rate of change of the integrated indicator of process safety of subsidiary operating companies and organizations cannot be lower than the minimum rate over the whole preceding measurement interval.*

Criterion 2. *The rate of change of the integrated indicator of process safety of subsidiary operating companies and organizations cannot be negative.*

In case those two conditions (criteria) are met, the state of process safety of subsidiary operating companies and organizations is recognized as satisfactory, as under any current indicator value there remains a nonzero probability of the specified target value being reached. The method allows ranking subsidiary operating companies and organizations depending on the quantitative estimation of the integrated indicator.

Let us illustrate the practical application of Russman's method using the example of conventional integrated indicator dynamics analysis. The value of indicator Ψ^k over the current year, when the estimation is performed, and the preceding year are shown in Table 1.

The rate of change of the indicator value is calculated according to formula $V = \frac{\Psi^k_{t+1}}{\Psi^k_t}$, whereby $V_{\max} = 1,8500$ and $V_{\min} = 0,6507$. Respectively, the rate vector inclination angles to the speed to the axis of X are equal to 61.60 and 330. Let the value 0.96 be defined as the target value of indicator

Table 1.

No.	Performance target values		Rate of change of performance target
	Ψ^k_t	Ψ^k_{t+1}	
1	0.950	0.940	1.0106
2	0.954	0.960	0.9938
3	0.950	0.910	1.0440
4	0.960	0.850	1.1294
5	0.980	0.982	0.9980
6	0.965	0.980	0.9847
7	0.982	0.930	1.0559
8	0.940	0.840	1.1190
9	0.968	0.974	0.9938
10	0.985	0.940	1.0479
11	0.991	0.990	1.0010
12	0.650	0.999	0.6507
13	0.999	0.890	1.1225
14	0.920	0.840	1.0952
15	0.925	0.500	1.8500

Ψ^k after t+2 years from the starting moment of evaluation. The current average value Ψ^k is equal to 0.941. Let us now assume that a year later, in the year t+1, one of the companies obtained the value of integrated indicator Ψ^k equal to 0.946. The situation is illustrated in Fig. 5.

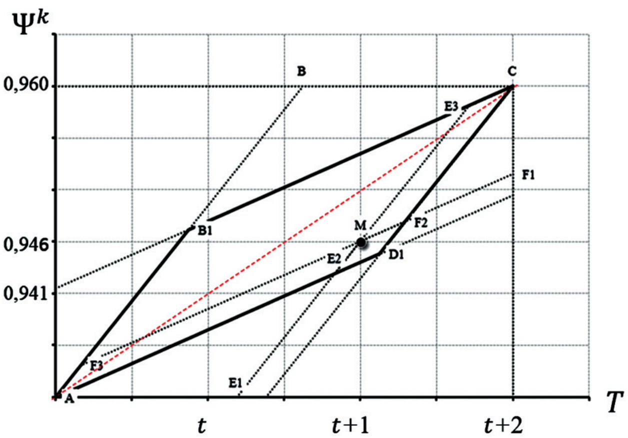

Fig. 5. Example of calculation. Critical system state

For this situation, in accordance with Russman's method, we have:

$$\varepsilon_1 = \frac{|E_1E_2|}{|E_1E_3|} = 0,4247;\ \varepsilon_2 = \frac{|F_1F_2|}{|F_1F_3|} = 0,2499;$$

$$\mu_1 = \frac{|E_1M|}{|E_1E_3|} = 0,5338;\quad \mu_2 = \frac{|F_1M|}{|F_1F_3|} = 0,3528;$$

$$d_1 = \frac{\varepsilon_1(1-\mu_1)}{\mu_1(1-\varepsilon_1)} = 0,6448;\ d_2 = \frac{\varepsilon_2(1-\mu_2)}{\mu_2(1-\varepsilon_2)} = 0,6110,$$

and, consequently,

$$R_{t+1} = \max\left\{\ln\frac{1}{1-d_1};\ln\frac{1}{1-d_2}\right\} \cong 1.$$

The value $R_{t+1} \cong 1$ show that if the indicator's rate of change remains the same, in a year the target value will not be able to be achieved. It can be seen (Fig. 5) that point M that denotes the current position of the indicator was approaching the hazardous limits AD$_1$C, beyond which there was a high probability of loss of control and non-fulfillment of mission. The current situation requires attention and corrective measures. For comparison, let us examine the integrated indicator estimate for another company that the same year t+2 achieved a higher estimate (Fig. 6).

For this situation, respectively:

$$\varepsilon_1 = \frac{|E_1E_2|}{|E_1E_3|} = 0,3633;\ \varepsilon_2 = \frac{|F_1F_2|}{|F_1F_3|} = 0,1205;$$

$$\mu_1 = \frac{|E_1M|}{|E_1E_3|} = 0,7878;\quad \mu_2 = \frac{|F_1M|}{|F_1F_3|} = 0,4137;$$

$$d_1 = \frac{\varepsilon_1(1-\mu_1)}{\mu_1(1-\varepsilon_1)} = 0,1537;\ d_2 = \frac{\varepsilon_2(1-\mu_2)}{\mu_2(1-\varepsilon_2)} = 0,1942;$$

$$R_{t+1} = \max\left\{\ln\frac{1}{1-d_1};\ln\frac{1}{1-d_2}\right\} = 0,2159.$$

The value R_{t+1}=0.2159 under this scenario (again, it is assumed that the indicator's rate of change remained the same) shows that if the parameter's rate of change remains as before, in a year the target value will well be able to be achieved. The risk is not high, the point that characterizes the location of the indicator is practically on the optimal trajectory.

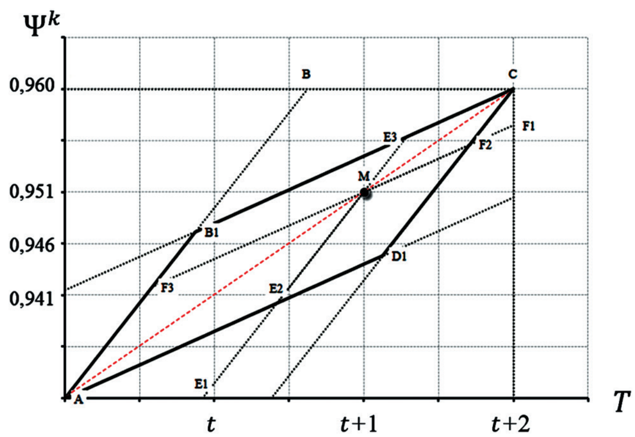

Fig. 6. Example of calculation. Controllable system state

Both values of the integrated indicator meet the above criteria and in both subsidiary operating companies the state of process safety is satisfactory. However, compared to the target value of the safety indicator, the second company shows qualitatively better results.

6.2. Estimation of random and special causes of indicator variations

A control chart is a graphical tool for decision making regarding the stability or predictability of any process, which defines the methods of managing such processes.

The control chart theory distinguishes two types of variability. The first type is random variability caused by "common" or "random" causes. It is due to a wide range of permanent causes, whose identification at the moment is complicated or economically unviable, and among which none is dominant. However, as a whole, the sum of all such causes creates something that can be considered systemic variability of a process. Preventing or reducing the effect of common causes requires managerial decisions aimed primarily at modifying the system. The second type of variability consists in the effect of such causes that are not inherent to the process, do not belong to the system and can be identified and eliminated, at least in theory. Such causes of variability are conventionally called "special". Those include insufficient material homogeneity, tool breakdown, personnel error, non-performance of procedures, etc.

As long as a process is affected by special causes of variability, it, according to the definition suggested by Shewhart, is unstable, or uncontrollable.

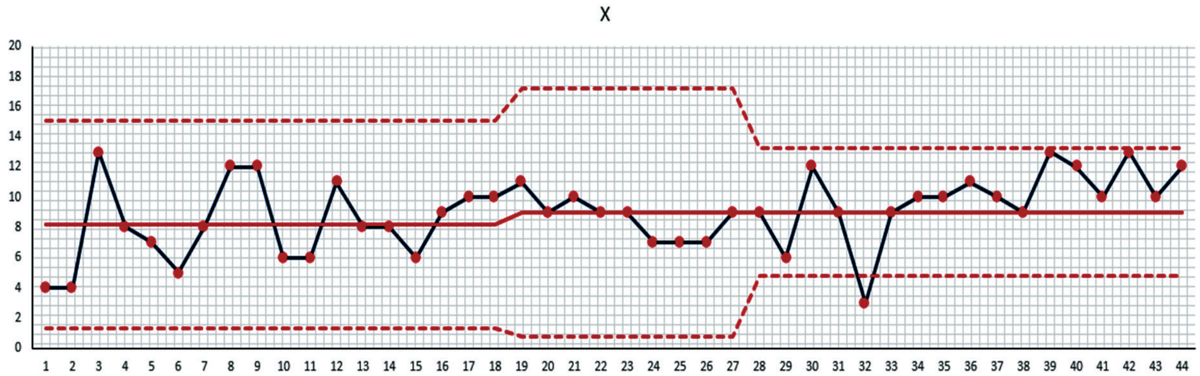

Fig. 7. Chart of outliers of the conventional integrated index of process safety of subsidiary operating companies and organizations

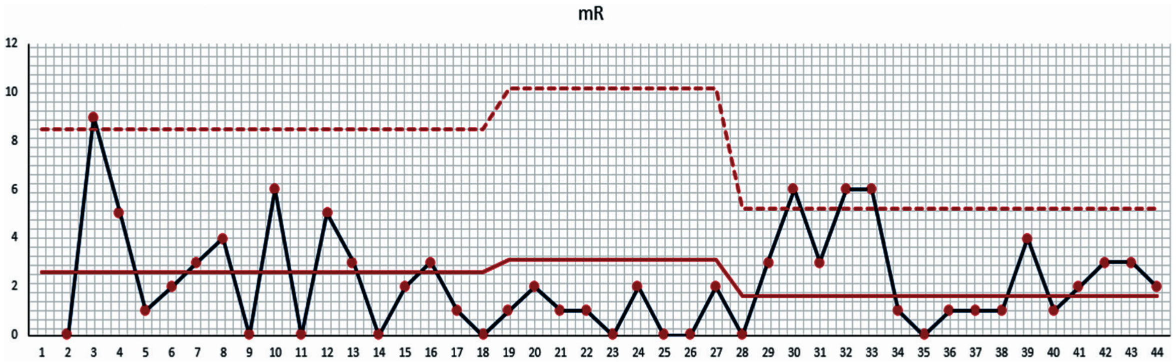

Fig. 8. Chart of value ranges of the conventional integrated index of process safety of subsidiary operating companies and organizations

Therefore, the purpose of control charts is to identify whether a process is stable. If not, the main task is to stabilize the process, which requires finding the root causes of intervention in the system and eliminate them. If the process involves only common causes of variability, it is in the statistically controllable state.

One must bear in mind that the boundaries of Shewhart's control charts are calculated based on data on the process itself, are not associated with tolerances and are not lines of certain probabilities. Constructing a Shewhart's control chart requires data obtained from the process with certain time intervals using samples (data subsets). Time intervals may be defined by either time, or be associated with the moment a certain number of supervised items has been checked. Normally, each sample consists of same-type supervised items with the same supervised quality indicators. All samples (subsets) in most cases have the same size. For each sample (subset) one or more statistical characteristics are defined, such as the total number of inconsistencies, share of inconsistent products, arithmetic mean value, range of sample, etc.

A Shewhart's control chart has a center line (CL), Fig. 7, 8.

For the purpose of studying the process and estimating whether the process is statistically controllable, the center line is the arithmetic mean value of the examined data. For the purpose of process management, the center line is the target value of the quality characteristic of products defined in the specifications. A Shewhart's control chart also has two statistically defined control limits that are usually symmetrical in relation to the center line and are the upper control limit (UCL) and lower control limit (LCL). Control limits are 3σ above and below the center line (± 3σ), where σ is the standard deviation of random variations of the used statistical characteristic (statistic) in the entire assembly. The variability within samples (subsets) is the measure of such random variations and does not include the value of between-groups variance.

The center line and the regulation boundaries reflect the laws of variation of the supervised characteristic under normal process realization, i.e. in the absence of special causes. The ordinate of the center line corresponds to the statistical estimate of the position, and the control limits correspond to the highest and the lowest limits of the intrinsic variability interval. In terms of the quantitative indicator, charts reflect the variability of quality both in terms of dispersion and position.

Therefore, in terms of the quantitative indicator, control charts should be analyzed in pairs, one chart for dispersion and one for position. The pair of the chart X and mR is the most commonly used (Fig. 7, 8). X is the average value of a small subset (measure of position), mR is the range of values within each subset (measure of dispersion).

An example of indicators of special causes appearing in a chart (points that require a closer attention and additional research in order to identify the causes of such deviations):

- points above the UCL or below the LCL;
- a long series of points (7 and more) above or below the CL;
- ascending or descending long series of points (trend);
- other manifestations of "non-randomness":

a) significantly more than 2/3 of points are situated within the middle third of the area between the UCL and the LCL (concentrated around the CL);

b) significantly less than 2/3 of the points are situated around the CL;

c) obvious trends within short series;

d) repeating differences in the results within individual samples (e.g., the first is always higher than the rest).

For the purpose of defining control limits, Shewhart chose the number 3 for other (not normal) types of distribution as well. That was done in order to keep from considering and calculating exact probabilities, as for other distributions under number 3 such probabilities are close to one as well. Therefore, for the range and reject charts, limits with the distance of ±3σ are also used instead of exact probabilistic limits, which simplifies the understanding and interpretation of such control charts. In this context, the calculation of control limits is "approximate", qualitative in its nature.

The **"not worse than" estimation criterion** of process safety of subsidiary operating companies and organizations imposes limitations on the variations (deviations) of the integrated indicator from the average value:

Criterion. *Deviations from the average value of the integrated indicator are not to exceed three standard deviations (± 3σ).*

The probability of control limits violation is very low (0.3%). Therefore, the emergence of a point outside the control limits (onset of a rare event) should be considered as the effect of non-random (special) causes on the process.

The use of control charts involves two types of possible errors: the errors of the first and second kind.

An error of the first kind occurs when the process is a statistically controllable (stable) state, and the point crosses the control limits accidentally. As the result, an incorrect decision is taken implying that the process has gone beyond the stable, i.e. statistically controllable state, and an attempt is made to find and eliminate the cause of a non-existent problem. The probability of such error is 0.3%, or three cases per thousand (0.003). In case an error of the first kind occurs, no special cause of stability disruption will be found, as the process is in fact in a statistically controllable state. The fact of the point going beyond a control limit in such case shows the onset of a rare random event.

An error of the second kind occurs when the examined process goes beyond the statistically controllable state, but all points of the control chart are within the control limits.

7. On the construction of supercriterion

In case the two above approaches are employed simultaneously, the state of safety may yield varying estimates.

It becomes necessary to develop an integrated supercriterion $F = F\left(F_1(\alpha),\ldots,F_k(\alpha)\right)$ for the purpose of selecting the optimal estimate over the allowable set. As it was shown above, the most usable integrated criteria are formulas (1) (see [14]).

If we introduce designation $\lambda_v F_v = F_v^{'}$ into (1), the first of the above estimates becomes the sum of the values of local criteria, and if we substitute $F_v^{\beta_v} = F_v^{''}$, the second integral estimate becomes the product of the local criteria taken as dimensionless value-based numbers. In both cases integrated criterion F can be constructed through repetitive use of a binary associative and communicative operation and is an integer analytical function of local criteria $F_v, v = 1,\ldots,k$. As it was shown by Russman, the class of such operations is sufficiently narrow and there are only three (accurate to constant parameters) binary operations that meet the condition of commutativity, associativity and integral analyticity. They are defined by the following three functions: a) c; b) $F_1 + F_2 + c$; c) $a\left(F_1 + F_2\right) + bF_1F_2 + \frac{a(a-1)}{b}; a, b, c - const, b \neq 0.$

He also showed (see [14]) that the third of the estimates provided by the theorem (under certain values of the coefficients that are part of it) is to be used for the purpose of obtaining the integrated criterion of quality, provided there is interaction between subsystems and criterial limitations F_v^{**} of the ranges of variation of local estimates.

Convolution of difficulties for k criteria

$$d = 1 - \prod_{v=1}^{k}\left(1 - d_v\right).$$

Russman notes that other types of convolution can be used that meet the conditions of commutativity, associativity, but are not integral analytical functions. He cites the example of the convolution of type $F = \max(F_1, F_2)$ that is exactly like that. Such convolutions are often used when the quality of the whole system is defined by the performance of its weakest subsystem.

Conclusion

As the final observation, let us note that the main conclusion of the above arguments and reasonings consists in the obvious idea: you should not try to operate with specific security events only. All such events are characterized by a set of properties and contributing factors with associated characteristics. One should try to identify each property and each characteristic of such property, which would later allow defining proactive and reactive control actions in response to changes in such characteristics and properties. Thus, having worked out a property of a situation or an event, we work out a property of a risk, and it is of no significance in which specific risk this property will manifests itself. Combinations of risk properties can be extremely numerous; therefore, it is very difficult to predict specific situations. That causes the requirement for a proactive decision support system that ensures qualitative DM support short before a critical event. Along with that, it is completely unimportant what cataclysm triggers such critical event. What matters is that it will be feasible to clearly identify what level of a property's characteristic is critical for a company (project, facility) and what the company (project manager, operator) should do in order to put off this critical level.

The probability is not to be subject to subjective assessment. At the exact moment when subjective probability estimates come into use, an objective concept of an impossible event (like Nasim Taleb's Black Swan) is substituted with a subjective one. In the subjective understanding, a Black Swan can be any unusual or even ordinary event. It is important to draw a clear line.

The application of the most efficient security management methods is inseparable from an active use of the external and internal information space, whose state is defined by a special type of resource allocation, the information resources.

The concept of a control systems' information resources provision comprises a set of methods and procedures of information process management within production systems that allow selecting and using a required IT solution for the purpose of acquiring information on the manufacturing situation.

Consequently, the following management problems are identified:

– problem of objective definition, i.e. the required state or behaviour of the system;

– problem of stabilization, i.e. maintaining the system in the current state in the presence of disturbing effects;

– problem of task performance, i.e. taking the system into the required state, when the values of the controlled variables vary according to known deterministic laws;

– problem of supervision, i.e. ensuring the required system behaviour, when the laws of variation of the controlled variables are unknown or not constant;

– problem of optimization, i.e. retention or bringing the system into a state with extreme characteristic values under the given conditions and limitations.

One might say that security should be researched using the methods common to cybernetics that use the information approach to the research of managerial processes that involves identifying and examining, within the test objects, various types of information flows, methods of their processing, analysis, transformation, transmission procedures, etc. Under this approach, management is very broadly understood as the process of conditioning of a goal-oriented system behaviour through controlling information action by a person or a device.

References

[1] Bochkov A.V. Safonov V.S. Special analysis and assessment of risk indicators for rare events in regard to dangerous industrial facilities. *Vesti Gazovoy Nauki* 2020;1(42):84-95. (in Russ.)

[2] Kolesnikov E.Yu. A topic of uncertainty in the publications of the journal "Issues of Risk analysis". *Issues of Risk Analysis* 2019;16(3):78-93. (In Russ.) DOI:10.32686/1812-5220-2019-16-3-78-93.

[3] Huygens C. (1657). De calcul dans les jeux de hazard. Oeitvr. Comply t. 14. La Haye; 1920.

[4] Bernoulli J. Ars conjectandi, opus posthumum. Accedit Tractatus de seriebus infinitis, et epistola gallicé scripta de ludo pilae reticularis. Basel: Thurneysen Brothers; 1713.

[5] Boole G. An Investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities. New York: Dover; 1957.

[6] Laplace P.S. Le Systeme du Monde. Leningrad: Nauka; 1982.

[7] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. *Dependability* 2019;4:53-64. DOI:10.21683/1729-2646-2019-19-4-53-64.

[8] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. *Dependability* 2020;1:57-67. DOI:10.21683/1729-2646-2019-19-4-53-64.

[9] Bochkov A.V., Ponomarenko D.V. [Methodological foundations of monitoring and prediction of process safety in PAO Gazprom]. *Gas Industry Magazine*. 2017;3(749):20-30. (in Russ.)

[10] Ponomarenko D.V., Lesnykh V.V., Bochkov A.V. Modern approach to monitoring of industrial safety for hazardous production facilities. *Issues of Risk Analysis* 2018;15(1):6-17. (In Russ.)

[11] Bochkov A. Ram M., Davim J., editors. Hazard and Risk Assessment and Mitigation for Objects of Critical Infrastructure. Diagnostic Techniques in Industrial Engineering. Management and Industrial Engineering. Springer, Cham; 2017. DOI:10.1007/978-3-319-65497-3_3.

[12] Bochkov A., Zhigirev N. 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; 121-154.

[13] Bochkov A., Lesnykh V., Lukyanchikov M. Problem of Creation of Integrated Index of Assessment of Production Safety Condition at Hazardous Production Facilities. In: Beer M., Zio E., editors. Proceedings of the 29th European Safety and Reliability Conference. Research Publishing, Singapore; 2019; 1643-1650. DOI:10.3850/978-981-11-2724-3 0077-cd.

[14] Artobolevsky I.I. [On some methods of selection of integral criteria of quality in respect to optimal design of machines]. *Proceedings of the Academy of Sciences of the USSR* 1978;2:3-10. (in Russ.)

[15] Keeney R.L., Raiffa H. Decisions with multiple objectives: preferences and value tradeoffs. Moscow: Radio i sviaz; 1981.

[16] Barsukov A.N., Bykov A.A., Lesnykh V.V. [Development of a system of indicators of emergency situations and crises]. [Industrial and environmental safety of gas industry facilities: Collection of studies]. Moscow: VNIIGAZ LLC;2008:76–86. (in Russ.)

[17] Lukianchikov M.I. et al. [On the specificity of application of the risk-oriented approach as part of some types of inspection and oversight activities in Gazprom]. *Gas Industry Magazine* 2020;1(107):21-27. (in Russ.)

[18] Saaty T.L. Decision making with dependence and feedback: The analytic network process. Moscow: Izdatelstvo LKI; 2008.

[19] Gayday A.A., Russman I.B. [Continuous supervision of the process of meeting a goal]. *UBS* 2004;7:106-113. (in Russ.)

[20] Berkolayko M.Z., Dolgikh Yu.V., Ivanova K.G. [Difficulties in the sense of I.B. Russman and dependability estimation of control]. Proceedings of Voronezh State University. Series: Systems analysis and information technologies. 2008;2:7-9. (in Russ.)

[21] Berkolayko M.Z., Dolgikh Yu.V. [Application of the difficulties apparatus to dependability estimation of organizational systems management]. Proceedings of the X International Research and Practice Conference System Analysis in the Design and Management. Saint Petersburg. 2006. 126-144. (in Russ.)

[22] Cowden D. Statistical Methods in Quality Control. Moscow: Gosudarstvennoe izdatelstvo fiziko-matematicheskoy literatury; 1961.

[23] Adler Yu., Shper V. [Practical guidelines for statistical process control]. Moscow: Alpina Publisher; 2019. (in Russ.)

[24] GOST R 50779.42-99 (ISO 8258-91) Statistical methods. Shewhart control charts. Moscow: IPK Izdatelstvo standartov; 2002. (in Russ.)

About the author

Alexander V. Bochkov, Doctor of Engineering, 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

Within the scope of the unified concept of the system for monitoring the safety state of structurally complex systems and facilities the author has generalized the methods of qualitative estimation of the safety state of two types, i.e. “better than” (for the purpose of defining a certain target level that characterizes the safety state that is to be ideally achieved) or “not worse than” (for the purpose of defining a certain maximum allowable level that characterizes the safety state, below which it is not allowed to go), that imply certain ranges of deviation from the specified target or, respectively, the minimal allowable levels, within which the safety status evaluated with an integrated index is deemed to be acceptable.

Conflict of interests

The author declares the absence of a conflict of interests.