Chapter

Probabilistic Predictive Modelling for Complex System Risk Assessments

Andrey Kostogryzov, Nikolay Makhutov, Andrey Nistratov and Georgy Reznikov

Abstract

The risks assessment is described by the action of estimating the probability distribution functions of possible successes or failures of a system during a given prediction period. Typical probabilistic predictive models and methods for solving risks prediction problems are described, and their classification is given. Priority development directions for risks prediction in standard system processes and their implementation procedures are proposed. The reported examples demonstrate the effects and interpretation of the predictive results obtained. Notes: 1. System is a combination of interacting elements organized to achieve one or more stated purposes (according to ISO/IEC/IEEE 15288 “Systems and software engineering—System life cycle processes”). 2. Risk is defined as the effect of uncertainty on objectives considering consequences. An effect is a deviation from the expected — positive and/or negative (according to ISO Guide 73).

Keywords: prediction, method, model, probability, risk

1. Introduction

Systems are subject to various risks throughout their life cycles despite their successful design and effective operation. That is why mathematics and system performance prediction have been closely interrelated since the ancient times. There is no doubt in the design and the maintenance of the world-famous wonders, astonish modern man. The preservation of these wonders was entirely based on predictive methods using existing mathematical approaches by that time. With the advent of probability theory, this relationship has become even closer. Currently, various classical mathematics and probabilistic methods are often used to solve complex engineering problems.

If for the layman probability is still associated with divination on daisies, then for specialists these methods have long become powerful tools in predicting success or failure, proactive management, and achieving the desired effects. Risk predictive assessments are practiced in various industrial sectors, for example, fuel and energy, pharmaceutical, mining, metallurgical, chemical, communication and information, dispatch centers, etc. [1–32]. Hundreds of universities and other scientific organizations are involved in probabilistic research activities connected to risk prediction. By now it is possible to clearly trace the activities chain in a predictive approach: “From uncertainties formalization – to probabilistic modelling”, “From probabilistic modelling – to reasonable control”, “From reasonable control – to achievable effects” and “From achievable effects –to sustainable harmony”. It means that predictive probabilistic concepts meet the main analytical challenges in the eternal aspirations to go from uncertainties formalization” to “sustainable harmony”, see **Figure 1**.

Thousands of mathematicians are currently involved in risk prediction R&D activities. It is unfortunately impossible to mention all the running developments. This chapter will focus on:

- some generalizations and thoughts regarding the variety of the existing risk prediction probabilistic approaches;

- the formulation of the goals and objectives of the probabilistic methods throughout the life cycle of various systems;

WONDERS OF THE WORLD AS EXAMPLES OF RETROSPECTIVE PREDICTIVE METHODS
$P_{tim.i} \geq P_{req.i}$
From achievable effects – to sustainable harmony
$1 \ldots K$
$= V/(\nu \cdot T_{cont.}$
$\frac{d}{dt}p_j(t) = \sum_{k=1}$
$P_{infl.(1)} = 1 - \Omega_{penetr} *$
$P_{(1)}(T_{req}) = 1 - \int_0^{T_{reg}} dA$
$\tau_{part(2)} = V/N$
$P_{comp.} = exp\left\{-\lambda \int_0^\infty [1-\right.$
From reasonable control – to achievable effects
$\int_0^\infty C(t+\tau)dB(\tau) \bigg] dt$
From probabilistic modeling – to reasonable control
$P_{(2)}(T_{req}) = P^N_{(1)}(T_{betw} + T_{diag})P_{(1)}(T$
$P_{tim.i} \geq P_{req.i}$
EXAMPLES OF PROMISING SYSTEMS FOR PREDICTIVE MODELING
From uncertainties formalization – to probabilistic modeling
$P_{tim.i} = P(t_{full.i} \leq T_{req.i}) \geq P_{adm.i}$
$\tau_{part(2)} = T_{reg.}/N$
$ull.i \leq T_{req.i}$
$\int_0^\infty dt \int_t^\infty dF$

Figure 1.
The eternal aspirations: “From uncertainties formalization—to sustainable harmony.”

- the description of the general risk prediction probabilistic approach;
- the essence of the probabilistic concepts considering the acceptable risk notion;
- some original probabilistic models;
- the analytical methods of risks integrating for standard processes;
- some optimization problem statements for rational proactive actions;
- some examples of practical applications (illustrating some scientific and technical possibilities for solving real engineering problems);
- the expected achievable effects.

2. Goals and objectives

In general, risk prediction is associated with the achievement of pragmatic goals and solving the analytical problems of systems rational concept (conceptual design), development, utilization, and support. Pragmatic system goals may be:

- improving the efficiency of the implementation of the state and/or corporate strategy in the economy;
- improving the safety and sustainability of the region's development, ensuring socio-economic, pharmaceutical, medical, and biological safety of the region;
- ensuring the protection of the population and territories from natural and man-made risks, etc.

In turn, the following objectives require risk predictive capabilities:

- to predict the mean residual time before the next operational abnormality;
- to ensure the effective operation and development of complex engineering, energy, transport, and communication systems;
- to ensure the security of critical infrastructure, information, and information-psychological security;
- to ensure energy and industrial safety, technical diagnostics and resource management for critical facilities and systems;
- to ensure the safety of railway, aviation and water transport;
- to develop critical technologies (for example, information and cognitive technologies; energy technologies of the future; technologies for monitoring and predicting the state of the environment and equipment; technologies for

exploration and development of mineral deposits and their extraction; and technologies for preventing and eliminating natural and technogenic hazards), etc.

A review of the numerous existing mathematical approaches allows us to make the following generalization —the main goals of applying probabilistic prediction are connected with (see **Figure 2**):

- an analysis of opportunities, achievable quality, safety and efficiency;
- a rationale for achieving desirable characteristics and acceptable conditions;
- an optimization of systems performance and processes;
- exploring new ideas and innovative concepts.

The enlarged classification of methods, using the probabilistic risk predictive models (including the proposed models), is presented in **Table 1**. These methods are used for solving various objectives during system life cycle.

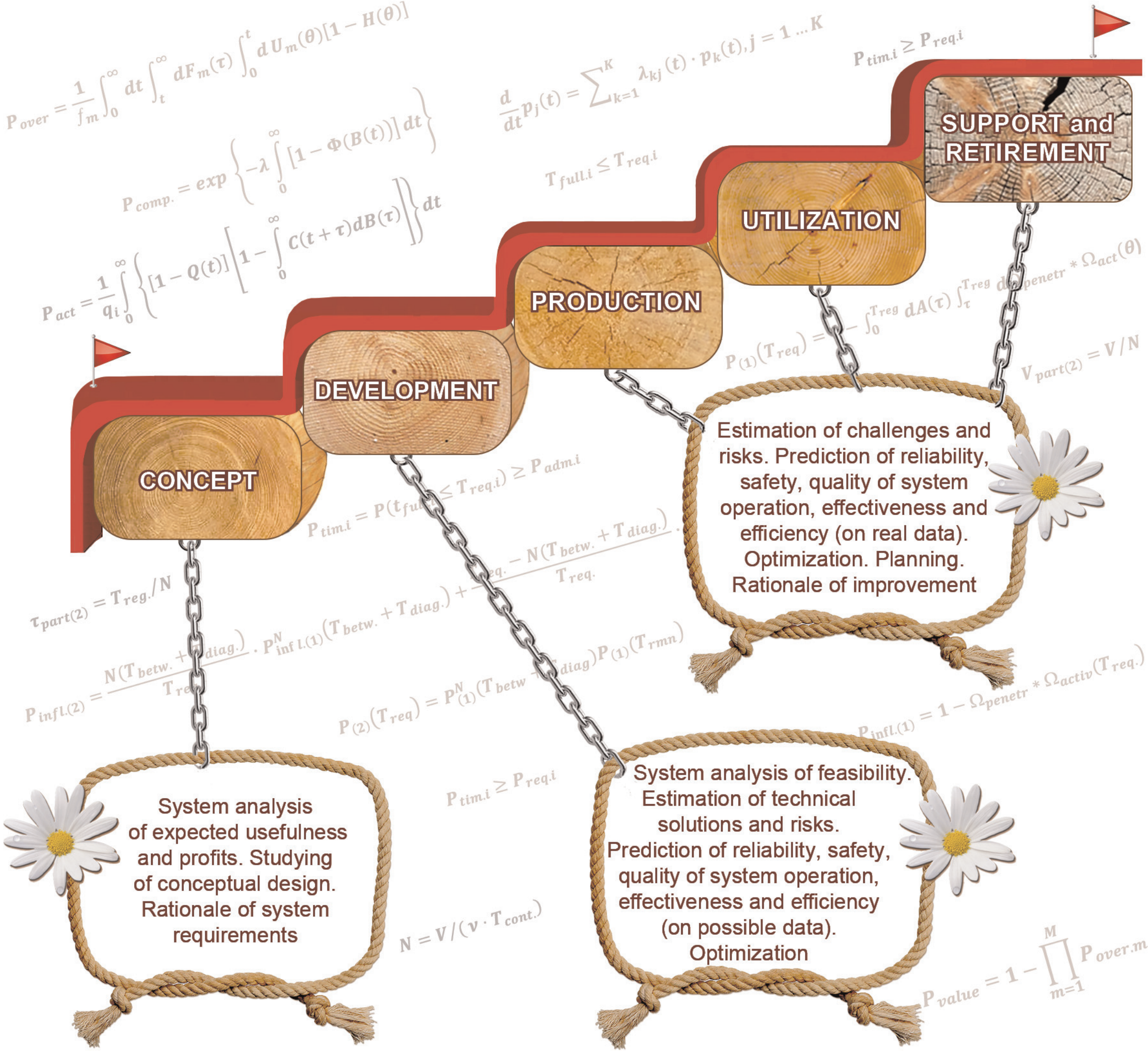

CONCEPT
DEVELOPMENT
PRODUCTION
UTILIZATION
SUPPORT and RETIREMENT
Estimation of challenges and risks. Prediction of reliability, safety, quality of system operation, effectiveness and efficiency (on real data). Optimization. Planning. Rationale of improvement
System analysis of expected usefulness and profits. Studying of conceptual design. Rationale of system requirements
System analysis of feasibility. Estimation of technical solutions and risks. Prediction of reliability, safety, quality of system operation, effectiveness and efficiency (on possible data). Optimization

Figure 2.
Generalization of goals and objectives throughout the system's life cycle that require risk probabilistic-predictive models.

Stages in life cycle (see, for example, ISO/IEC/IEEE 15288). The problems which are due to be solved by risks prediction	Methods, connected with:			
	an analysis of opportunities, achievable quality, safety, efficiency	a rationale of achieving desirable characteristics and acceptable conditions	optimization of systems and processes	finding and researching of new ideas and concepts
Concept stage. Problems connected with a system analysis of expected usefulness and profits, studying of system creation, the rationale of system requirements and acceptable conditions	Methods for estimating critical measures. Methods for probabilistic risk prediction	Methods for estimating critical measures. Methods for probabilistic risk prediction	Methods for optimization, considering risks prediction	Methods to analyze possible effects. Methods for probabilistic risk prediction.
Development stage. The problems connected with a system analysis of feasibility, the estimations of technical solutions and risks, the prediction of reliability, safety, a quality of system operation, effectiveness and efficiency (on possible data), optimization	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Methods for optimization, considering risks prediction	Methods to analyze possible effects. Methods for probabilistic risk prediction.
Production stage. The problems connected with an estimation of challenges and risks, the prediction of reliability, safety, quality of system operation, effectiveness and efficiency (on real data), optimization, planning, rationales for improvement	Measurements. Methods for estimating critical measures	Measurements. Methods for estimating critical measures	Methods for production optimization, considering risks prediction	Methods for estimating critical measures.
Utilization stage. The problems connected with an estimation of challenges and risks, the prediction of reliability, safety, a quality of system operation, effectiveness and efficiency (on real and possible data), optimization, planning, rationale of improvement	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Methods for optimization, considering risks prediction	Methods to analyze possible effects. Methods for estimating critical measures. Methods for probabilistic risk prediction.
Support and retirement stages. The problems connected with an estimation of challenges and risks, the predicting of reliability, safety, quality of system operation, effectiveness and efficiency (on real and possible data), optimization, planning, rationale of improvement (in part concerning)	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Measurements. Methods for estimating critical measures. Methods for probabilistic risk prediction	Methods for optimization, considering risks prediction	Methods for estimating critical measures. Methods for probabilistic risk prediction

Table 1.
The enlarged classification of methods, using risk probabilistic-predictive models.

3. Conceptual probabilistic-predictive approach

The solution of problems in the system life cycle [6–8, 9, 14] is considered by the example of a complex system, designated as (S-N-T)-system and covering: social sphere S (person, society, state and world community); natural sphere N (earth and space); techno-sphere T (man-made infrastructures and life support facilities).

In general, solving problems using a probabilistic-predictive approach includes:

- obtaining new knowledge about the fundamental laws of the operation and development of (S-N-T)-system in time and defining the probabilistic expressions and their parameters;
- formation of specific goals, concepts, and conditions in the system life cycle (with the construction of fault trees and event trees, as well as risk matrices for infrastructures and facilities), operation (including quality assurance, safety, efficiency) and development and their integration (taking into account certain priorities) for each of these areas (S, N, T) and (S-N-T)-system as a whole;
- rationalizing and building scientifically based predictions of the (S-N-T)-system development, as well as each of the constituent spheres (S, N, T), to achieve certain goals during the life cycle and to retain the critical parameters and measures within acceptable limits;
- rationalizing means, methods, and technologies for sustainable development of the (S-N-T)-system based on new knowledge and reasonable predictions;
- planning of rational (S-N-T)-system process management taking into account feedbacks;
- practical implementation and control (on-line and off-line) of the predictions and plans fulfillment for the operation and sustainable development of the (S-N-T) system, taking into account social, natural, and man-made hazard-exposure uncertainties.

When planning and implementing these actions, the following should be taken into account:

- the complexity and uncertainty of (S-N-T)-system probabilistic-predictive models, many challenges and threats leading to a deterioration of the system integrity, the effects of damaging factors, and the decrease in the survivability of the system;
- the time dependence of interrelations between spheres and components of the system, subsystems and significant elements, vulnerabilities and admissible limits for the (S-N-T)-system states in the conditions of possible challenges and threats;
- the need to categorize and classify (S-N-T)-system according to the level of importance and criticality in order to achieve goals throughout the life cycle and to retain critical parameters and measures within acceptable limits.

The random time variables τ considered in the predicted risk $R(\tau, t)$ does simultaneously take into account the probabilities $P(\tau, t)$ of the threats' occurrence and activation, and also the associated damages $U(\tau, t)$. For example, the random time variable τ may be defined as the time between successive losses of element integrity (see details in sections 4 and 5). Here the prediction period t (which in general is also subject to justification) is dependent on the basic measures, designed to characterize the uncertainties and complexity of (S-N-T)-system, and conditions for solving the analytical problems.

The source of risks regarding the (S-N-T) system has been and remains: human (human factor); nature with its own range of threats; and techno-sphere with its inherent hazards. They are the determinants of the reliability (including aging and degradation of technical means), other quality measures (including the quality of the information used), and the safety and efficiency of the system. This makes it possible to determine risk as functionals:

$$R(\tau, t) = F\{P(\tau,\ t), U(\tau,\ t)\} = F\{R_S(\tau,\ t), R_N(\tau,\ t), R_T(\tau,\ t)\}.$$

In practice, risks are estimated by the dimensionless probability of an elementary event during a period of time, comparing possible damage to it, or by the probabilistic expectation of damage (as the probabilistic multiplication of the possible damage on the probability of damage), or by the frequency of damage, etc. In turn, the magnitude of damages can be estimated in economic indicators (financial), areas of contamination, losses in case of accidents, etc.

For example, formalization of such limitations may be presented as follows:

$$R(\tau, t) \leq Radm(\tau, t), Radm(\tau, t) > 0.$$

Then a safety $S(\tau, t)$ for (S-N-T)-system can be expressed in terms of risks: $S(\tau, t) \leq Radm(\tau, t) - R(\tau, t)$. Safety is maintained if and only if $S(\tau, t) \geq 0$.

To ensure that the quality, safety and sustainable development of the (S-N-T)-system are in the acceptable risk zones. Thus, it is necessary to implement a set of actions with the economic costs expected to reduce risks to an acceptable level.

Examples of the applicability of this approach are proved in many industrial sectors such as nuclear, thermal and hydraulic power plants; the largest installations of oil and gas chemistry; the unique space station, aviation, sea and land transport; large-scale offshore energy resources development facilities [7], etc.

4. The essence of probabilistic concepts

The risk predictive approaches, used by system analysts, are based on classical probability theory. Generally, a probabilistic space (Ω, B, P) should be created per system (see for example [1–6, 9–14]), where: $\boldsymbol{\Omega}$ – is a finite space of elementary events; B – is a class of subspaces in $\boldsymbol{\Omega}$ -space with the properties of $\boldsymbol{\sigma}$-algebra; $\boldsymbol{P}$ – is a probability measure on a space of elementary events $\boldsymbol{\Omega}$. Because $\boldsymbol{\Omega} = \{\boldsymbol{\omega_k}\}$ is finite, there is enough to establish a correspondence $\boldsymbol{\omega_k} \rightarrow \boldsymbol{p_k} = \boldsymbol{P}(\boldsymbol{\omega}| \supset| \boldsymbol{k}|)$ in which $\boldsymbol{p_k} \geq \mathbf{0}$ and $\sum_k \boldsymbol{p_k} = \mathbf{1}$. Briefly, the initial formulas in mathematical form for original models (which are used in practice) are given in **Appendices A** and **B**.

Note. Some cases of a limited space of elementary events see in Section 6. The results of modelling are related only to introduced elementary events and specific interpretation, the results of the probabilistic prediction can not describe future exact events (place, time and other detailed characteristics).

The next interconnected concepts 1–7 are proposed for probabilistic predictive modelling.

Concept 1 is concerning the probability distribution function (PDF) $P(\tau \leq t)$ (see for example [1–6, 9–14] etc.) for a continuous random variable of time τ. $P(\tau \leq t)$ is a non-decreasing function $P(t)$ whose value for a given point $t \geq 0$ can be interpreted as the probability that the value of the random variable τ is less or equal to the given time t. Regarding risk prediction, the given time t indicates the prediction period. Additionally, $P(t) = 0$ for $t \leq 0$, and $P(t) \rightarrow 1$ for $t \rightarrow \infty$. From a decision-making standpoint, the problem is to determine the probability of system "success" and/or "unsuccess" during the given prediction period T_{req} (for example, a risk of "failure" considering consequences). This probability is a value for a point t = T_{req}, and a PDF is due to be built for modelling the system's operational states with the time.

Concept 2. The processes, connected with data processing should provide the required system operational quality (because the system performs functions by logical reasoning based on data processing). The corresponding probabilistic methods should be appropriate for the assessment of the quality of the used information [6–8, 9–14, 28–31].

Concept 3. The PDF should establish the analytical dependence between the input parameters to allow solving direct and inverse problems necessary for the rational management of the system operation. For example, the PDF P(t) describing the random time τ between successive losses of integrity of a system may be an analytical exponential approximation of a simple system element, i.e. $P(t) = 1 - exp\ (-\lambda t)$, where λ is the frequency of failures (losses of element integrity per unit of time). At the same time, the frequency of failures may be considered as a sum of frequencies of different types of failures because of various specific failure reasons—for example, failure from equipment λ_1, or from natural threats λ_2, or from "human factor" λ_3 and so on. For this use case, PDF may be presented as $P(t) = 1 - exp\ [-(\lambda_1 + \lambda_2 + \lambda_3 + \ \ldots)t]$, if and only if all the implied failures are independent. Then if the PDF $P(t)$ is built in dependence on different parameters and if an admissible probability level for acceptable risk is given then the inverse problem may be solved analytically—see also Section 7.

Notes. 1 System integrity is defined as such system state when system purposes are achieved with the required quality. 2. The rationale for exponential approximation choice in practice see for example in [6, 9, 14, 28–31].

Concept 4. Acceptable adequacy must be ensured. It means the consideration of several essential system parameters on which "success" or "failure" of the system operation is dependent. For example, today the way for risks prediction based on only one parameter − frequency of failures λ − is common. For this case, the exponential PDF can be used—see **Figure 3**. But the required acceptable adequacy is not always proven.

For exponential approximation the frequency of failures λ is connected with the hypothesis: "No failures during the given time with a probability less than the given admissible probability P_{adm}>0". This is always the case if the failure frequency is constant with time. For this case, the given prediction time must be no more than $t_{req} = 1/\lambda_{adm}$, here $\lambda_{adm} = \frac{-ln\ (1-P_{adm})}{t_{req}}$. That may not be often an accurate engineering estimation because many systems' capabilities and operation conditions are ignored [9, 14]. In **Figure 3**, this case is explained on the timeline. For

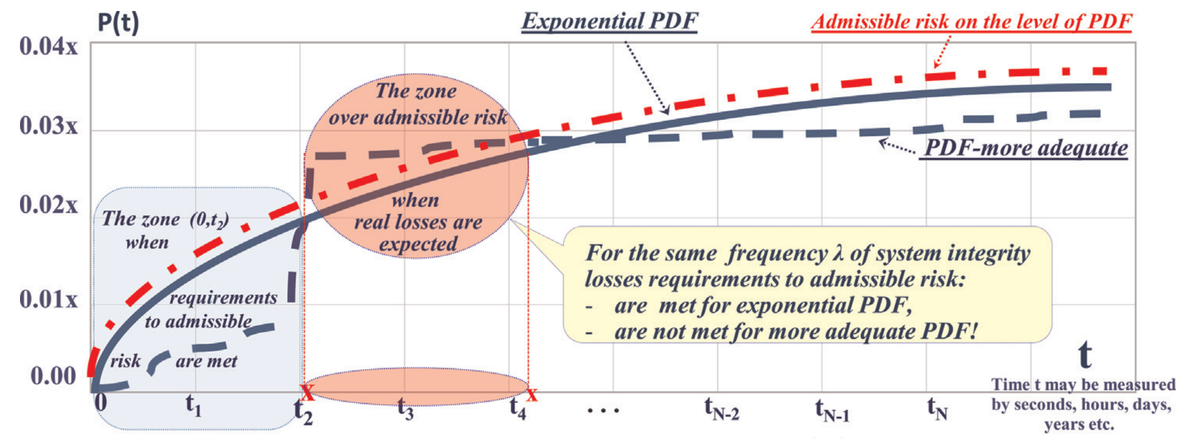


Figure 3.
Probabilistic risk, approximated by a more adequate PDF P(t), *in comparison with the existing representation of exponential PDF (both connected with the same* λ*), and admissible risk, imaginary by exponential PDF, connected with* λ_{adm}.

different approaches and discussions, devoted to adequacy, see for example the work in [33]. In that case, the diagnostic approach to evaluate the predictive performance is based on the paradigm of maximizing the sharpness of the predictive distributions. After calibration, one obtains an assessment and ranking of the probabilistic predictions of wind speed at the Stateline wind energy centre in the US Pacific Northwest. In [34], the approach is illustrated by examples connected with "human factors". For specific systems, the topic of improving the adequacy of the prediction will always remain relevant.

Concept 5. A complex system includes subsystems and/or components (system elements), the probabilistic approach must allow a generation of probabilistic predictive models to predict the system's operational performance and its dependence on different uncertainty conditions. In general, predictive models must consider system complexity, the diagnostics of system's integrity, the monitoring of the diagnostics, the recovery from loss integrity of every system component and the quality of the used information. The adequate PDF must be the output of the probabilistic-predictive models (see also **Appendix A**).

Concept 6. The input for the probabilistic-predictive models must be based on real and other possible data (subjective data, meta-data, etc.) considering the system operational specifications and the supporting actions. These may be also hypothetical data for research purposes.

Concept 7. The specific problems of optimization must be solved considering risks prediction results (including optimization in real time). The given time for prediction should be defined so to be in real system operation time to allow taking rational proactive actions.

5. The description of some original probabilistic models

For modelling modern and future systems, taking into account their specifications, it makes sense to distinguish between the intellectual part, where uncertainties are associated with information gathering, processing and production for decision-making, and the technical part, where there is no significant dependence on the high quality of the current information.

5.1 About system operational information quality

The created models [6–8, 9–14, 28–31] help to implement concepts 1 and 2. In general, operational information quality is connected with requirements for reliable and timely producing complete, valid and/or confidential information, if needed. The gathered information is used for proper system specificity. The abstract view of such quality is illustrated in **Figure 4**.

The proposed probabilistic predictive models to assess the information quality are described in **Appendix A**. The models cover the predictive measures according to the abstract information quality metrics in **Figure 4**. It may be applied for solving problems connected with decision-making on the base of information gathering, processing and production.

5.2 About "black box" formalization to predict "failure" risks

The models below help to implement concepts 1, 3 and 4 [6, 9, 14–31]. In general, successful system operation is connected with counteractions against various system integrity loss hazards (of social, natural and technogenic origins) throughout system operation timeline. There are considered two general technologies formalized to predict "failure" risks. Both technologies are briefly described below.

Technology 1 is based on a periodic diagnostic of system integrity policy. It is carried out to detect system functional abnormalities or degradations that may result in a system loss of integrity. The system loss of integrity can be detected only as a result of diagnostics. Dangerous influence on system is logically acted step-by-step: at first, a danger source penetrates into system and then after its activation begins to influence. System integrity can not be lost before penetrated danger source is activated. A danger is considered to be realized only after danger source has influenced on system.

Notes: 1. For example, for new steel structures, time before the appearance of critical erosion from rust can be considered as the source penetration time, activation time is the time before unacceptable structural damage occurs due to this rust. 2. Regarding a degradation of technical system the input time of danger source penetration tends to zero. 3. For special research cases of cyberattacks the term "Loss of Integrity" may be logically replaced by the term "functional abnormalities".

Technology 2, additionally to technology 1, implies that system integrity is monitored between diagnostics by operator. An operator may be a man or a special artificial

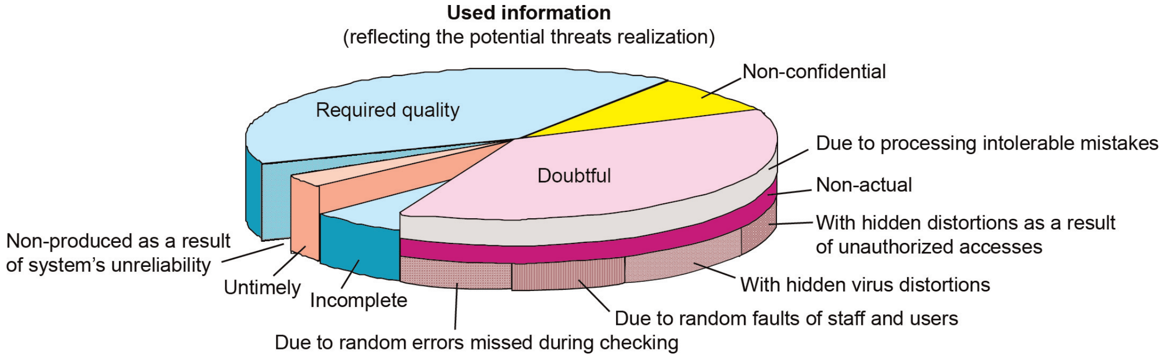


Figure 4.
The example of abstract information quality in the system.

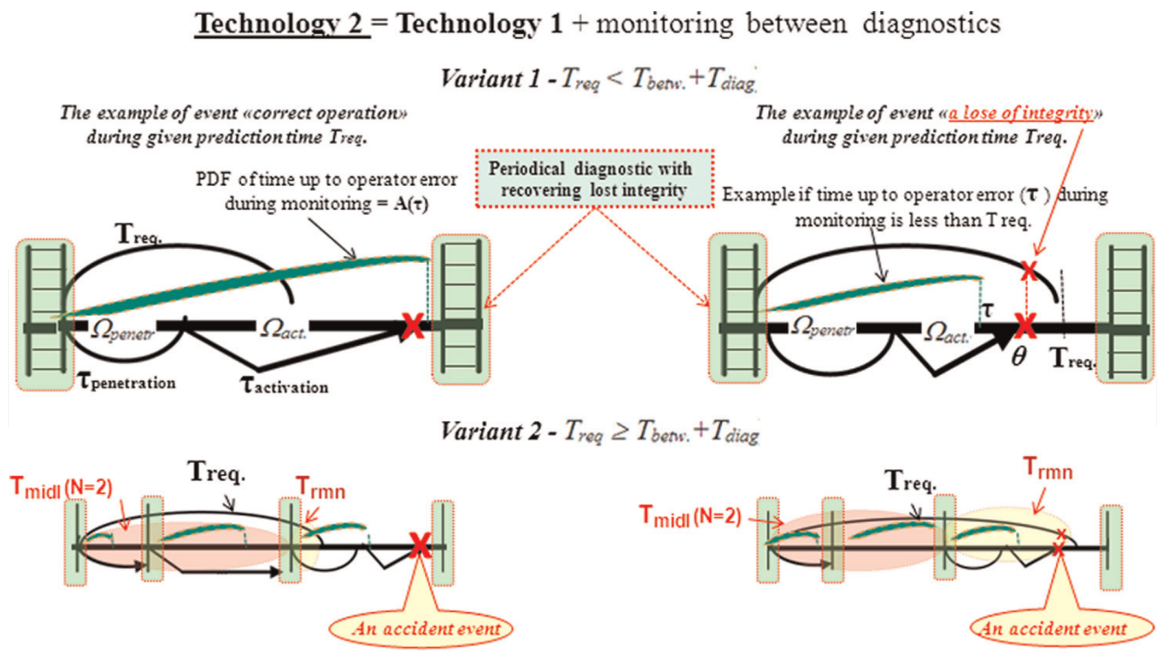

Technology 2 = Technology 1 + monitoring between diagnostics
Variant 1 - $T_{req} < T_{betw.} + T_{diag}$
The example of event «correct operation» during given prediction time Treq.
PDF of time up to operator error during monitoring = A(τ)
Periodical diagnostic with recovering lost integrity
The example of event «a lose of integrity» during given prediction time Treq.
Example if time up to operator error (τ) during monitoring is less than T req.
Treq.
Ωpenetr
Ωact.
τpenetration
τactivation
τ
θ
Treq.
Variant 2 - $T_{req} \geq T_{betw.} + T_{diag}$
Tmidl (N=2)
Treq.
Trmn
An accident event
Treq.
Trmn
Tmidl (N=2)
An accident event

Figure 5.
Some accident events for technology 2, left—successful (correct) operation, right—a lose of integrity during given time T_{req}.

intelligence system or a system of support or their combination. The operator repairs the system after having detected the loss of integrity hazard—see **Figure 5**. Accordingly, the model assumption of operator's faultless action can do the full neutralization of the active hazard. Penetration is only possible if an operator makes an error. A dangerous influence occurs if the danger is activated before the next diagnostic. Otherwise, the source will be detected and neutralized during the next diagnostic.

The probability of a successful operation within a given period of time, i.e. the probability of "success" (P) may be estimated using the models presented in **Appendix B**. The risk to lose integrity (R) is an addition to 1 of the probability of successful operation, i.e. $R = 1 - P$ considering consequences. Damage from the consequences for the given period is taken into account as an additional characteristic of the calculated probability.

5.3 Algorithm to generate probabilistic models for complex system

The algorithm helps to implement concepts 1 and 5 for complex systems with parallel or serial structure [9–31] with the assumption of random variables independence. Let us consider the elementary structure for two independent parallel or series elements. Let us PDF of time between losses of the i-th element integrity is $B_i(t) = P(\tau_i \leq t)$, then the time between successive integrity losses will be determined as follows:

1. for a system composed of serial independent elements is equal to the minimum of the two times τ_i: failure of 1st or 2nd elements. The PDF $B_{sys}(t)$ is defined by expression

$$B_{sys}(t) = P = [1 - B_1(t)] \bullet [1 - B_2(t)]; \tag{1}$$

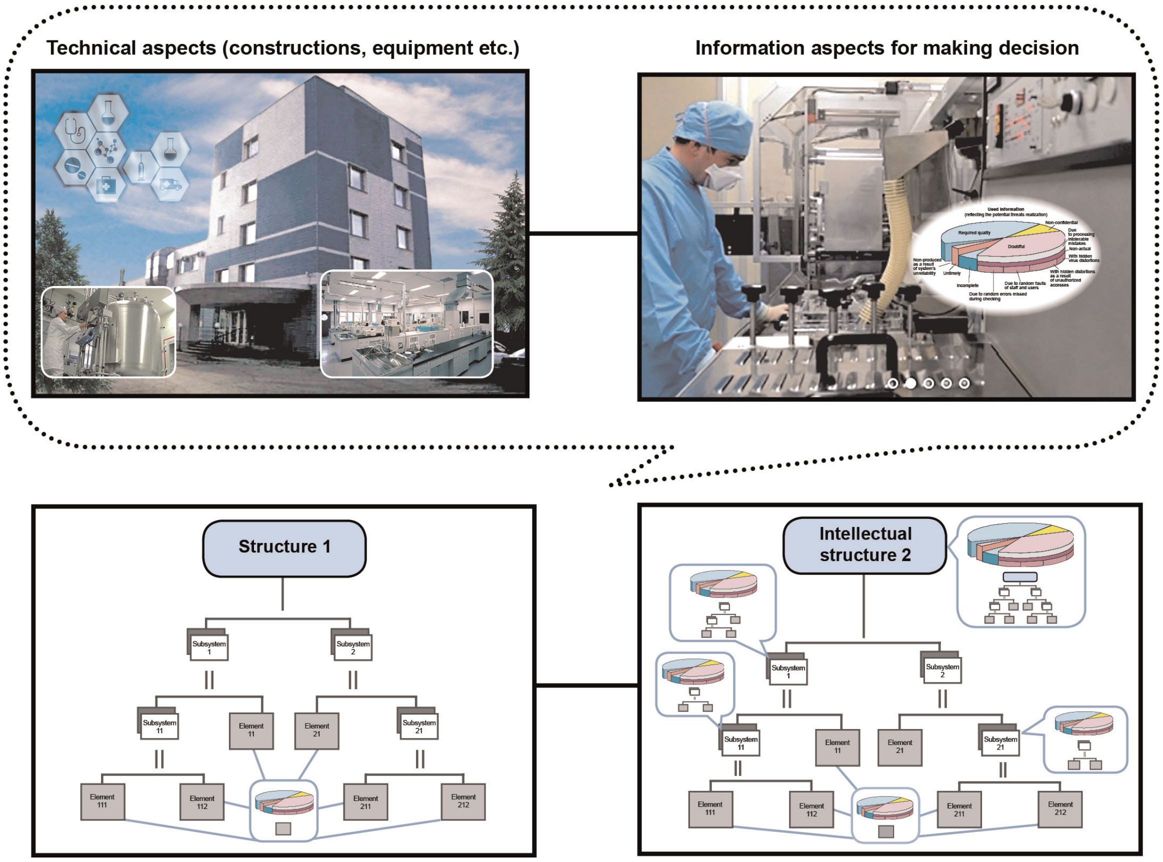


Figure 6.
An example of a complex system integrating two serial complex structures, which also are complex subsystems (abstraction).

2. for a system composed of parallel independent elements is equal to the maximum of the two timesτ_i, i.e. the system goes into the state of integrity loss when both elements lose integrity. The PDF $B_{sys}(t)$ is

$$B_{sys}(t) = P = [1 - B_1(t) \bullet B_2(t)]. \qquad (2)$$

Applying expressions (1–2), the PDF of the time interval between successive losses of integrity for any complex system with parallel and/or serial structure and their combinations can be built. An example of a complex system integrating two serial complex subsystems is presented in **Figure 6**, see also Examples 2—4. For this system the following interpretation of elementary events is used: complex system integrating serial components "structures 1 and 2" is in the state of "successful operation" during a given period T_{req} if during this period component "structure 1" "AND" component "structure 2" are in the state of "successful operation". Note that both components are in their turn complex subsystems including subsystems and components, as well.

6. Risks prediction for standard processes

6.1 About standard processes

All actions in the timeline may be characterized as the performance of some system processes. The main system processes according to ISO/IEC/IEEE 15288 "System and software engineering—System life cycle processes" include 30 standard processes—agreement processes (acquisition and supply processes), organizational project-enabling processes (life cycle model management, infrastructure management, portfolio management, human resource management, quality management and knowledge management processes), technical management processes (project planning, project assessment and control, decision management, risk management, configuration management, information management, measurement and quality assurance processes), technical processes (business or mission analysis, stakeholder needs and requirements definition, system requirements definition, architecture definition, design definition, system analysis, implementation, integration, verification, transition, validation, operation, maintenance and disposal processes).

The focus on standard processes is justified by the fact that the life cycle of any complex system is woven from a variety of standard processes deployed in time, and for them, possible purposes, outcomes and typical actions are defined. Considering that for many critical systems, the potential damage and costs of eliminating the consequences in the conditions of heterogeneous threats can exceed the costs of preventive measures by an order of magnitude, it is necessary to find effective solutions to counter threats and ensure effective risk management for each of the processes performed. Despite many works on risk management for different areas theproblems of this chapter continue to be relevant (of course in practice developing new processes may be considered, not only from ISO/IEC/IEEE 15288 standpoint).

6.2 The example about input for probabilistic modelling

The proposed practical way to input forming helps to implement concept 6 for any monitored system (including real time system). For each critical parameter (for which prognostic estimations are needed to do proactive actions) the ranges of acceptable conditions can be established. The traced conditions of monitored parameters are data on a timeline. For example, the ranges of possible values of conditions may be established: "Working range within the norm", "Out of working range, but within the norm" and "Abnormality" for each traced separate critical parameter. If the parameter ranges of acceptable conditions are not established in explicit form, then for modelling purpose they may be impleaded and can be expressed in the form of average time value. These time values are

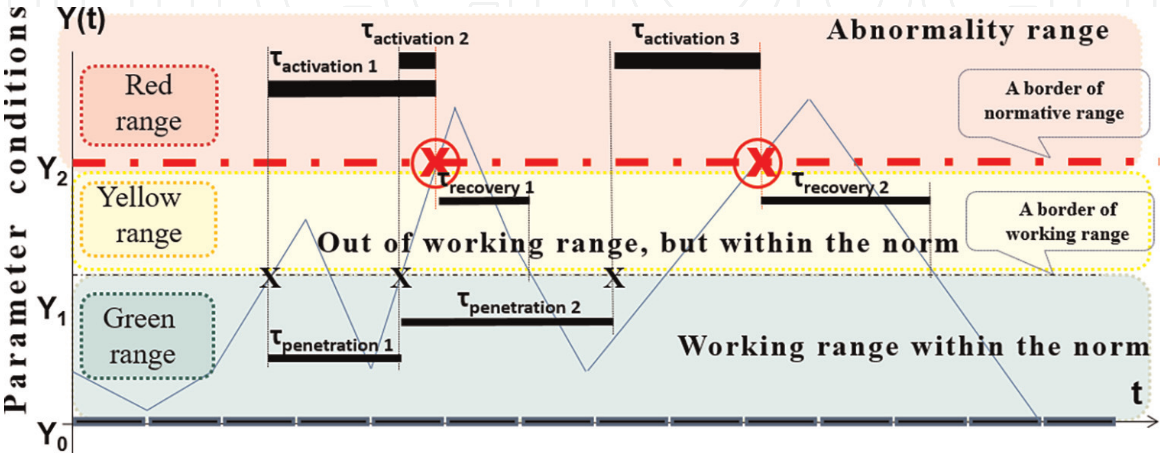


Figure 7.
An example of universal ranges for data about events and conditions. Note. In general case, the ranges may be established by subjective mode if a reasonable and objective one is impossible.

used as input for probabilistic models (see **Appendices A** and **B**). For example, for coal mine some of many dozens heterogeneous parameters may be compression, temperature, etc. It may be interpreted similarly by light signals “green”, “yellow” and “red” [18, 25, 28–31]—see **Figure** 7 and following Example 1.

6.3 The considerations

For the estimation of reliability of standard process performance, there may be two cases to estimate the probabilistic measure: the case of observed repeatability and the case of assumed repeatability of random events influencing reliability without the consideration of additional specific threats (for example, threats to operational information quality). For the estimation, the probabilistic measure repeatability of threats activation is assumed. For estimation of the assumption of independence of events connected with reliability of standard process performance and additional specific threats activations (for example, threats to information security) is used.

6.4 The case of the observed repeatability

The inputs for calculations use statistical data according to some observed repeatability. For standard process, the reliability of process performance and expected results in time are required. Failure to perform the necessary actions of the process is a threat of possible damage. From the different points of view, all varieties of the standard process can be divided into K groups, $K \geq 1$ (if necessary). Based on the use of statistical data, the probability $R_{\text{act }k}(T_k)$ of failure to perform the actions of the process for the k-th group for a given time $T_{\boldsymbol{k}}$ is proposed to be calculated by the formula:

$$R_{\text{act }k}(T_k) = G_{\text{failure }k}(T_{\boldsymbol{k}})/G_k(T_{\boldsymbol{k}}), \tag{3}$$

where $G_{\text{failure }k}(T_{\boldsymbol{k}})$,$G_k(T_{\boldsymbol{k}})$—are accordingly the number of cases of failures when performing the necessary actions of the process and the total quantity of necessary actions from the k-th group to be performed in a given time T_k.

The probability $R_{\text{rel}}(T)$ of failure to perform the necessary actions of a standard process without consideration of additional specific threats activations (for example, threats to operational information quality) is proposed to be estimated for the option when only those cases are taken into account for which the actions were not performed properly (they are the real cause of the failure)

$$R_{\text{rel}}(T) = 1 - \sum_{k=1}^{K} W_k[1 - R_{\text{act }k}(T_k)]\, Ind(\upalpha_k)/\sum_{k=1}^{K} W_k, \tag{4}$$

where T is the specified total time for a process performance for the entire set of actions from different groups, including all particular values T_k, taking into account their overlaps; theW_k is the number of actions taken into account from the k-th group for multiple performances of the process.

For the k-th group, the requirement to perform the process actions using the indicator function $Ind_k(\alpha_k)$is taken into account

$$Ind(\alpha) = \begin{cases} 1, \textit{ifthe specified requirements} \wedge \textit{conditions are met}, \textit{i.e.}\alpha \textit{ is true}, \\ 0, \textit{otherwise}, \textit{i.e.if the condition } \alpha \textit{ is false}. \end{cases} \tag{5}$$

The condition α used in the indicator function is determined by the analysis of different specific conditions, proper to the process. It is to allow take into account the consequences associated with the failure of the process—see (3) and (4). Condition α_k means a set of conditions for all process actions required from the k-th group.

6.5 The case of the assumed repeatability

There may be recommended the models from Section 5 and **Appendices A** and **B**, which do not exhaust the whole set of possible probabilistic models.

6.6 About estimation of generalized measure

The generalized probability $R_{\text{gener}}(T)$ of failure to perform standard process considering additional specific threats $R_{\text{add}}(T)$ for the given period T may be calculated by the formula:

$$R_{\text{gener}}(T) = 1 - [1 - R_{\text{rel}}(T)] \cdot [1 - R_{\text{add}}(T)]. \tag{6}$$

Here the probabilistic measure $R_{\text{gener}}(T)$ of failure to perform reliable process considering specific threats are estimated according to proposition of section 5, subsections 6.1–6.5 and **Appendices A** and **B** considering the possible consequences.

6.7 Approach for risks integration from different processes

The integral risk of violation of the acceptable performance of standard processes set is proposed to be evaluated depending on the real or hypothetical initial data characterizing each process (see subsections 6.1–6.4), from the possible scenarios of using each process during the given prediction period. The prediction period can cover any period during the system life cycle, including at least 1 complete process of each of the types involved in the specified set of standard processes in the scenario under consideration. An example of the standard processes performed on the time axis is shown in **Figure 8**. In general, the scenario of using standard processes i_1, i_2, … , i_k is proposed to be determined by the real or hypothetical frequency of these

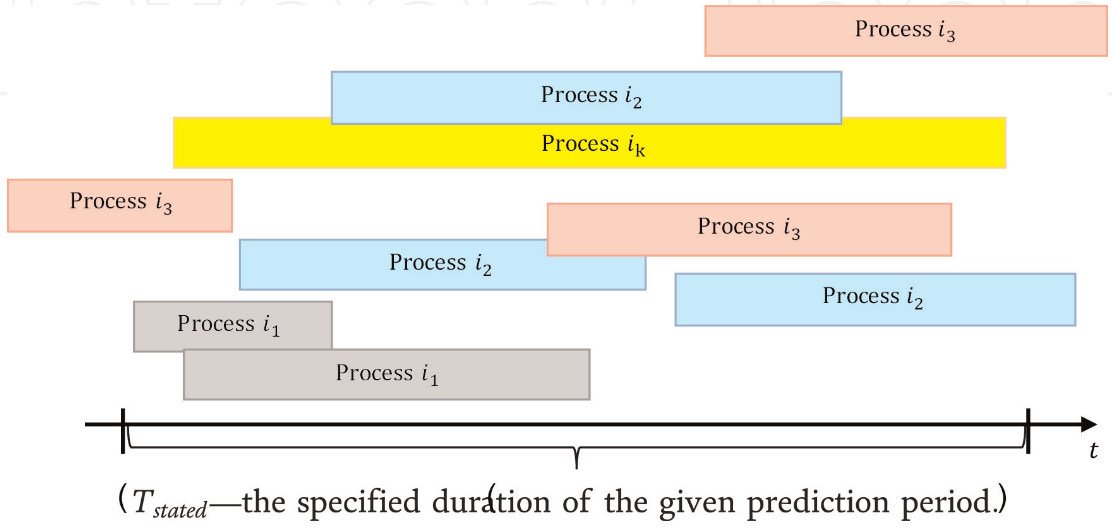


Figure 8.
An example of standard processes performed on the time axis.

processes (taking into account the typical actions performed at the same time that affect the time characteristics of the implementation of the processes). This approach allows us to take into account such opportunities when one process can be part of the work performed within other standard processes in the system lifecycle and, if necessary, include*s* other processes.

The integral risk of violation of the acceptable performance of standard processes set $R_{\int}(T_{stated})$ for given prediction period T_{stated} is proposed to be estimated by the formula

$$R_{\int}(T_{stated}) = 1 - \sum_{i=1}^{I} \lambda_i \{1 - R_i(T_{stated\ i}) \bullet [Ind(\alpha_i)]\} / \sum_{i=1}^{I} \lambda_i, \qquad (7)$$

where λ_i is the expected frequency of execution of standard processes of the i-th type for the prediction period. If the duration of the executed process can go beyond the prediction period (which depends on the actions performed and their time characteristics), this frequency can be a fractional number that characterizes the number of executions of each type of process, greater than one;

$T_{stated\ i}$ – the expected period specified in the source data for modeling for the acceptable execution of standard type i process;

T_{stated} – the given prediction period that covers the duration of all the specified periods $T_{stated\ i}$ of each from standard processes involved in the scenario. The assumption about a partially completed process that can start at the end of the prediction period and not finish (if the total number of processes of each type is greater than one) can be satisfied by setting the fractional value λ_i.

At the same time, the criterion for meeting the requirements and conditions (α_i) for each type of process, including the requirements for acceptable risks and damages, is set using the indicator function (5).

Note. The expression (6) is a special case of expression (7).

The proposed in Section 6 models and methods are applicable for solving practical problems related to risk prediction and the justification of effective proactive measures to reduce risks or their prevention within acceptable limits.

7. Optimization of problem statements for rationale proactive actions

The proposed optimization problem statements for rationale actions help to implement concept 7. The matter is the metrics calculated in sections 5 and 6, in the models from **Appendixes A** and **B** depend on many parameters. The values of some parameters may be given and often variated within system life cycle. These values of some parameters may be specified or selected to achieve pragmatic goals and solve the different analytical problems of systems rational concept, development, utilization and support (described in Section 2). They are impacting the values of the estimated probabilistic risks. It means many optimization problems may be solved by rationale proactive actions connected with providing rational values of these parameters. For example, such parameters for optimization may be the duration of prediction period, parameters, impact on the information quality (see **Appendix A**), system structure, for the compound components: time between the end of diagnostic and the beginning of the next diagnostic, diagnostic time (see **Appendix B**) etc.

The proposed concepts 2–6 may be supported by the following typical optimization problem statements for various systems [9, 14, 28–31]:

1. on the stages of the system conceptual design, development, production and support: system parameters, software, technical and control measures (they are described by a set $\mathbf{Q}$ of parameters, which may be optimized) are the most rational for the given prediction period if the minimum of expenses $Z(\mathbf{Q})$ can be reached

$$Z(\mathbf{Q}_{rational}) = \min_{\text{parameters of } \mathbf{Q}} Z(\mathbf{Q}), \tag{8}$$

   a. with limitations on probability of an admissible level of quality $P_{quality}(\mathbf{Q}) \geq P_{adm}$ and expenses for development, production, and support $C(\mathbf{Q}) \leq C_{adm}$ and under other development, operation or maintenance conditions; or

   b. with limitations on admissible risk to lose system integrity $R(\mathbf{Q}) \leq R_{adm}$ and expenses for development, production and support $C(\mathbf{Q}) \leq C_{adm}$ and under other development, operation or maintenance conditions; or

   c. with limitations based on a combination between 1a) and 1b);

2. utilization stage:

- System parameters, software, technical and control measures $(\mathbf{Q})$ are the most rational for the given period of system operation if the maximum of the probability of successful operation can be reached

$$P_{quality}(\mathbf{Q}_{rational}) = \max_{\text{parameters of } \mathbf{Q}} P_{quality}(\mathbf{Q}), \tag{9}$$

   a. with limitations on probability of an admissible level of quality $P_{quality}(\mathbf{Q}) \geq P_{adm}$ and expenses for operation $C(\mathbf{Q}) \leq C_{adm}$ and under other operation or maintenance conditions; or

   b. with limitations on the admissible risk to lose system integrity $R(\mathbf{Q}) \leq R_{adm}$ and expenses for operation $C(\mathbf{Q}) \leq C_{adm}$ and under other operation or maintenance conditions; or

   c. with limitations based on a combination between 2.1a)and 2.1b);

- System parameters, software, technical and control measures $(\mathbf{Q})$ are the most rational for the given period of system operation if the minimum of the risk to lose system integrity can be reached

$$R(\mathbf{Q}_{rational}) = \min_{\text{parameters of } \mathbf{Q}} R(\mathbf{Q}), \tag{10}$$

   a. with limitations on the quality $P_{quality}(\mathbf{Q}) \geq P_{adm}$ and expenses $C(\mathbf{Q}) \leq C_{adm}$ and under other operation or maintenance conditions; or

b. with limitations on the admissible risk to lose system integrity$R(\mathbf{Q}) \leq R_{adm}$ and expenses $C(\mathbf{Q}) \leq C_{adm}$ and under other operation or maintenance conditions; or

c. with limitations based on a combination between 2.2a) and 2.2b).

These statements may be retransformed into the other problems statements of expenses minimization for different limitations.

In system life cycle, there may be a combination of these formal statements.

Note. There may be another applicable variants of optimization.

8. Examples

The applications of the proposed approach cover: the analysis of the reliability of complex systems built from unreliable components; the estimation of the expected reliability and safety for complex constructions and intelligent manufacturing, the modelling of robotic and automated systems operating in cosmic space, the optimization of a centralized heat supply system, the analysis of the possibilities to keep "organism integrity" by continuous monitoring, the risk analysis during longtime grain storage, the control of timeliness, the completeness and validity of used information; the comparison between information security processes in networks; resources management and predicting quality for information systems operation; the estimation of human factor, the research of mutual monitoring operators actions for transport systems, rational dispatching of a sequence of heterogeneous repair works, the analysis of sea oil and gas systems vulnerabilities in conditions of different threats, the development of recommendations to reduce risks for the important land use planning (including Arctic region), the rationales of preventive measures by using "smart systems" etc.—see [9, 14–31]. Here the examples are intended to demonstrate some probabilistic risk prediction sectorial applications.

8.1 Example 1 of predicting the mean residual time before the next parameter abnormality

The example demonstrates system possibility on the base of solving the inverse problem by models described in subsection 5.2 and **Appendix B**. The research results are applied to rationale actions in real time for coal companies.

The conditions of parameters, traced by dispatcher intelligence centre, are data about a condition before and after the current moment of time. But always the scientifically justified predictions open new possibilities in the prevention of risks. With the use of predicted residual time, the responsible staff (mechanics, technologists, engineers, etc.) can determine the admissible time for rational changing of system operational regime to prevent negative events after expected parameter abnormality. For monitored critical parameters, the probabilistic approach to predict the mean residual time before the next parameter abnormality is proposed.

For every subsystem (element) monitored parameter, the ranges of possible values of conditions are established—see **Figures 7** and **9**. The condition "Abnormality" means system (element) integrity loss (it may simply mean "system failure" that includes also “functional failure”). To prevent the possible cross-border abnormalities propagation, through the prediction of the residual time on the base of the data about parameter condition fluctuations. Given that the information quality also is estimated and provided (by using models from **Appendix A**).

The predicted residual time T_{resid} is the solution t_0 of the following equation:

$$R\left(T_{penetr}, t, T_{betw}, T_{diag}, T_{req.}\right) = R_{adm.}\left(T_{req}\right) \qquad (11)$$

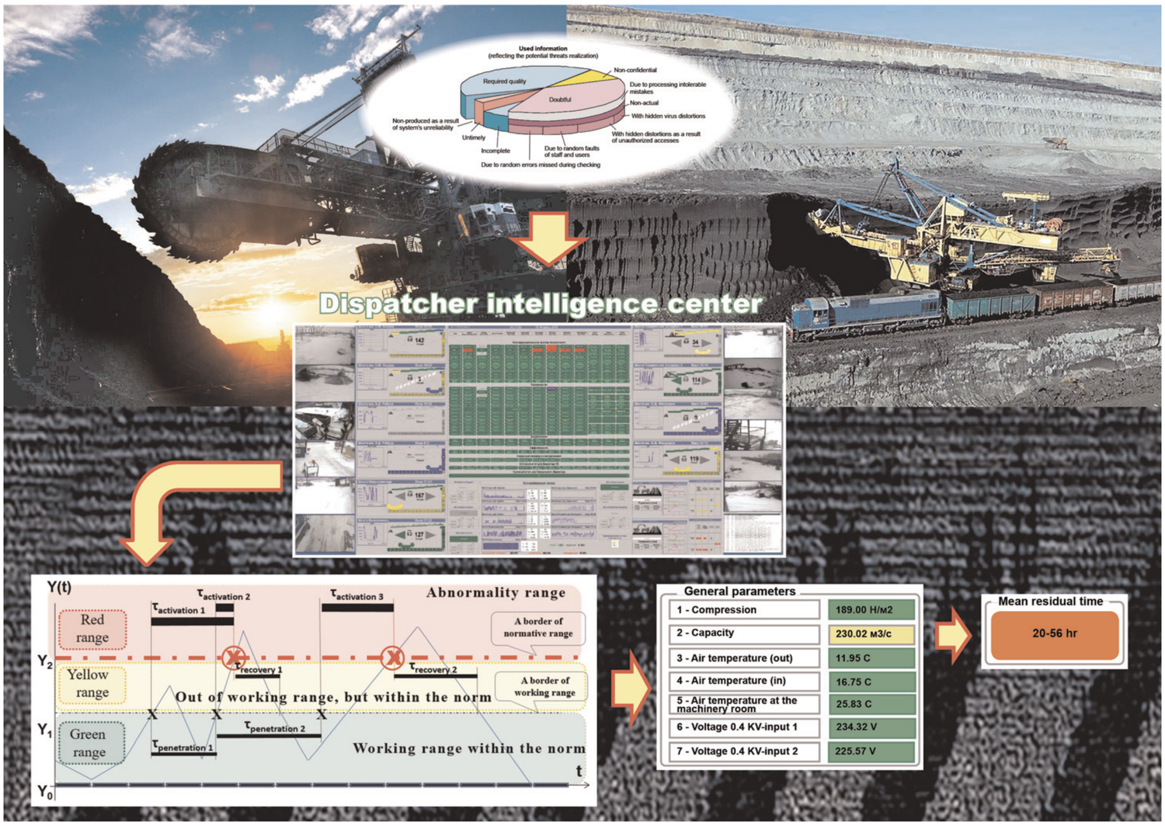
concerning of unknown parameter t, i.e. T_{resid} = t_0.

Here $R(T_{penetr}, t, T_{betw}, T_{diag}, T_{req.})$ is the risk to lose integrity, calculated according to the model of **Appendix B**. T_{penetr} is the probabilistic expectation of PDF Ω_{penetr} (τ), defined by the transition statistical parameter from “green” to “yellow”—see **Figures 7** and **9**. The other parameters T_{betw} and T_{diag} in (11) are known—see **Appendix B**. The example explains a method to rationally estimate the value of prediction time T_{req}.

The properties of the function R(Tpenetr, t, Tbetw, Tdiag, Treq.) are the next:

- if t increases from 0 to ∞, for the same another parameter, the function R(… , t, …) is monotonously decreasing from 1 to 0;

- if parameter T_{req} increases, from 0 to ∞ for the same another parameter, the function R(… , T_{req}) is monotonously increasing from 0 to 1,i.e. for large T_{req}, the risk approaches to 1. It means that the such maximal x exists when t = x and $T_{req.}$ = x and 0 < $R(T_{penetr}, x, T_{betw}, T_{diag}, x)$ < 1, i.e. the mean residual time


Used information
(reflecting the potential threats realization)
Required quality
Non-confidential
Due to processing intolerable mistakes
Doubtful
Non-actual
With hidden virus distortions
With hidden distortions as a result of unauthorized accesses
Due to random faults of staff and users
Due to random errors missed during checking
Incomplete
Untimely
Non-produced as a result of system's unreliability
Dispatcher intelligence center
Y(t)
$\tau_{activation\ 1}$
$\tau_{activation\ 2}$
$\tau_{activation\ 3}$
Abnormality range
Red range
A border of normative range
Y_2
$\tau_{recovery\ 1}$
$\tau_{recovery\ 2}$
Yellow range
Out of working range, but within the norm
A border of working range
X
X
X
Y_1
Green range
$\tau_{penetration\ 1}$
$\tau_{penetration\ 2}$
Working range within the norm
t
Y_0

General parameters

1 - Compression	189.00 Н/м2
2 - Capacity	230.02 м3/с
3 - Air temperature (out)	11.95 C
4 - Air temperature (in)	16.75 C
5 - Air temperature at the machinery room	25.83 C
6 - Voltage 0.4 KV-input 1	234.32 V
7 - Voltage 0.4 KV-input 2	225.57 V

Mean residual time

20-56 hr

Figure 9.
Example of predicted residual time before the next parameter abnormality.

before the next abnormality is equal to “x” with the confidence level of the admissible risk R(T_{penetr}, x, T_{betw}, T_{diag}, x). See details in [18].

The proposed ideas, probabilistic methods, models and justified normative requirements are implemented in Russia at the level of the national standard for system engineering—see for example GOST R 58494–2019 regarding the multifunctional safety systems of the coal mines (in the part of a remote monitoring system of critical industrial systems).

8.2 Examples related to socio-economic and pharmaceutical safety in a region

Examples 2—4 below demonstrate some analytical capabilities of the proposed approach for infrastructure management process related to socio-economic and pharmaceutical safety in a region of Russia. It concerns some problems in the creation and application of enterprise (S-N-T)-system — the manufacturer of pharmaceuticals denoted further as (S-N-T)-ESMP. Let the purposes of S-N-T-ESMP are to solve the following tasks:

- for the development of socio-economic infrastructure (tasks of the 1st type): ensuring the population with high-quality medications in a low-cost range (more than a hundred items); providing the emergence of new jobs; increasing tax revenues to the region; making profit from economic activities in the interests of strengthening and expanding business and stakeholders satisfaction;

- for the development of production and transport infrastructure (tasks of the 2nd type): ensuring strict compliance with the rules of production of good practice (GMP); development of a laboratory complex for ensuring and controlling the quality of products as part of microbiological, physical–chemical laboratories and air-liquid chromatography laboratories; expansion of the composition of manufacturers of substances and excipients, their suppliers and consumers of finished products; increasing the stability of the parameters of the production processes in order to ensure the reproducibility of the properties of finished medications;

- for the development of information and communication infrastructure (tasks of the 3rd type), providing the creation of an effective control system for ensuring the safety and quality, information security, integration of the enterprise into the state information system for monitoring the movement of medications.

In relation to the mentioned tasks, which allows achieving the demonstration goals of the examples, the application of methodological approach illustrates predicting on probability level: the risk of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts (see example 2); the risk of unacceptable damage because of abnormal impacts; the integral risk of failure to reliable perform system infrastructure management process considering specific abnormal impacts (see example 4). Assuming the commensurability of possible damages, a system analysis using probabilistic risk measures is carried out in the examples.

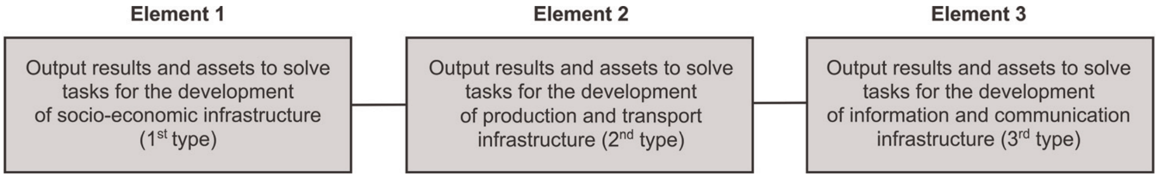

Element 1
Output results and assets to solve tasks for the development of socio-economic infrastructure (1st type)
Element 2
Output results and assets to solve tasks for the development of production and transport infrastructure (2nd type)
Element 3
Output results and assets to solve tasks for the development of information and communication infrastructure (3rd type)

Figure 10.
The abstract complex structure for modelling (example 2).

Taking into account possible damages, the objectives of risk prediction are formulated as follows. In the conditions of existing uncertainty, to carry out: a quantitative predicting of the risks of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts; a quantitative predicting of the risks of unacceptable damage because of abnormal impacts on (S-N-T)-ESMP (both piecemeal for each type of infrastructure tasks and for the entire set of tasks); identification of critical factors affecting risks; determination of such a period in which guarantees of risks retention within admissible limits are maintained; a quantitative predicting of the integral risk of failure to reliable perform system infrastructure management process considering specific abnormal impacts.

Example 2. Here, the infrastructure model without consideration of specific abnormal impacts is focused on a set of output results and assets for solving tasks of the 1st, 2nd and 3rd types—see system structure in **Figure 10**. The following interpretation is applicable: During the given prediction period, the modeled complex structure is in an elementary state “the integrity of the infrastructure is maintained” if an implementation of the system infrastructure management process is reliable to solve the tasks “AND” for socio-economic, “AND” for production and transport “AND” for information and communication infrastructure. Many possible threats affecting the reliability of output results for each of the structural elements have been identified. Without delving into the numerous technical aspects of setting and solving the tasks of developing socio-economic, production and transport, information and communication infrastructure in a region, **Table 2** reflects hypothetical averaged input data for research by the models (see sections 5, 6 and **Appendix B** considering application of **Appendix A** models).

Input for every element (see model in Appendix B)	**Values**		
	for 1st element	**for 2nd element**	**for 3rd element**
σ—frequency of the occurrences of potential threats	2 times in a year	1 time in a year	1 time in a month
β—mean activation time of threats up to unacceptable damage	6 months	2 months	2 weeks
T_{betw} – time between the end of diagnostics and the beginning of the next diagnostics	1 week	1 week	1 hour
T_{diag} – diagnostics time of element integrity	1 hour	1 hour	1 minute
T_{recov} – recovery time after integrity violation	3 days	1 week	30 minutes
T – given prediction period	From 1 to 4 years		

Table 2.
Input for probabilistic modelling (example 2).

For modelling a period from 1 to 4 years was chosen because it is a typical period for short- and medium-term plans according to an infrastructure project. Analysis of the calculation results showed that in probabilistic terms the risk of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts for 2 years will be 0.282 totally for all elements (see **Figure 11**). In turn, for 1 year the risk will not fall below 0.150 (see **Figure 12**), and for 4 years with weekly diagnostics, the probabilities of "success" and "failure" will almost equal (0.51 vs. 0.49). In practice, such a level of risks is inadmissible, i.e. it is necessary to identify the critical factors (affecting risks) and effective ways to reduce risks.

Additional calculations have shown that one of the critical factors is the parameter "time between the end of diagnostics and the beginning of the next diagnostics" (that can also be called "Mean Time Before Diagnosis-MTBD" because of "diagnostics time of element integrity" is much less—see **Table 2**) for the 1st and 2nd elements (T_{betw}). Due to the management decision, expressed in changing the frequency of diagnostics from weekly to daily and the adoption of the appropriate measures to counter threats, with other conditions unchanged, it is possible to reduce risks several times. It is enough to compare the risks in **Figures 11** and **13**. About 2.1-fold reduction in risk has been achieved totally for all elements. That is, due to the most simply implemented

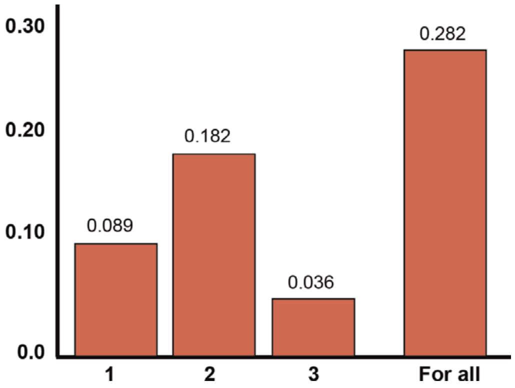


Figure 11.
The risks of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts on elements 1–3 for 2 years (for weekly diagnostics).

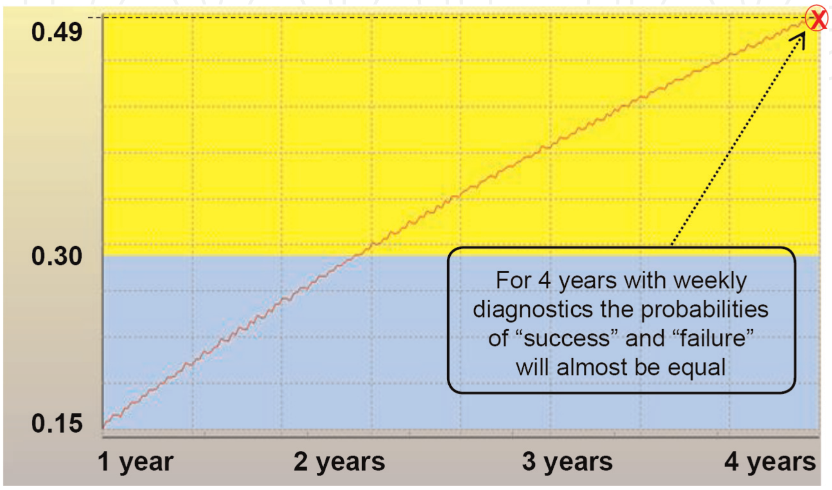


Figure 12.
The dependence of total risk of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts from duration of prediction period (for weekly diagnostics).

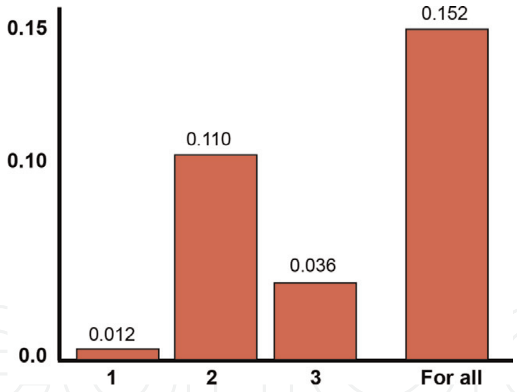


Figure 13.
The risks of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts on elements for 2 years.

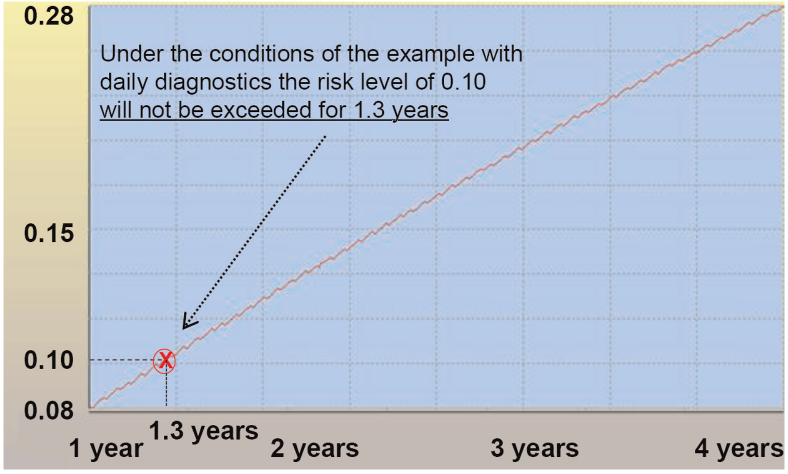


Figure 14.
The dependence of total risk of failure to reliable perform system infrastructure management process without consideration of specific abnormal impacts from duration of prediction period (for daily diagnostics).

organizational measures related to the introduction of more frequent diagnostics of work on the development of socio-economic and production and transport infrastructure, a significant risk reduction is achievable. This finding is the result of the used models. Despite the high value of this logical finding for example conditions, frequent diagnosis generates higher running costs and lower services supply capacity. Diagnosis costs money and time. It should be considered in other optimization problems (see Section 7).

For 1 year, the risk of failure of the infrastructure management process without considering the specific abnormal impacts will be about 0.08 (see **Figure 14**). In turn, as a result of the analysis of the risk dependence on the prediction period (from 1 to 4 years), it is additionally revealed that under the conditions of the example with daily diagnostics the risk level of 0.10 will not be exceeded for 1.3 years. Accordingly, and for infrastructure management process during development, focusing on admissible risk at the level of 0.10, in the conditions of the example, guarantees risks prevention within the admissible limits for about 1.3 years. Recommended measures to reduce risks are to increase the stability of the mechanical properties of the critical areas of structures, to timely carry on preventive and repair maintenance, to perform statistical analysis of emergency situations, and to predict critical unacceptable values of critical parameters inherent in the unacceptable risks.

Example 3. In contrast with Example 2, the model of specific abnormal impacts covers a set of actions related to the maintenance of buildings and constructions (element 1), ensuring the operation of engineering and technical systems (element 2), ensuring the operation of engineering networks (element 3), solving development problems of socio-economic infrastructure (element 4), production and transport infrastructure (element 5) and information and communication infrastructure (element 6)—see model on **Figure 15**. The following interpretation is applicable: during the given prediction period, the modeled complex structure is in an elementary state "the integrity of the system in case of abnormal impacts is maintained", if all the system elements are taken into account during the entire prediction period are in the state "the integrity of the system element in case of specific abnormal impacts is maintained".

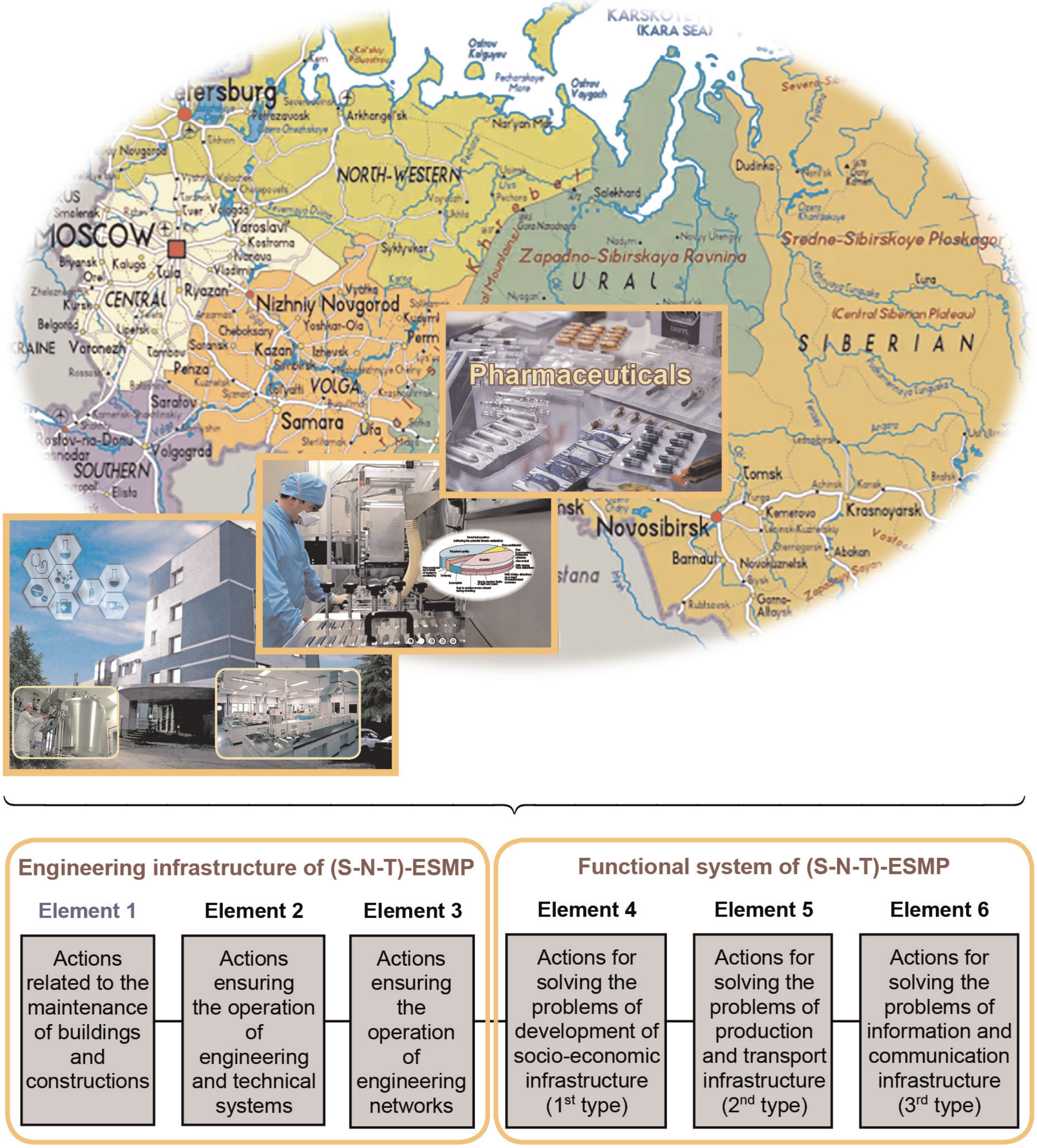

KARSKOYE (KARA SEA)
Petersburg
MOSCOW
NORTH-WESTERN
CENTRAL
VOLGA
SOUTHERN
URAL
SIBERIAN
Nizhniy Novgorod
Samara
Volgograd
Novosibirsk
Tomsk
Krasnoyarsk
Zapadno-Sibirskaya Ravnina
Sredne-Sibirskoye Ploskogor
(Central Siberian Plateau)
Pharmaceuticals
Engineering infrastructure of (S-N-T)-ESMP
Functional system of (S-N-T)-ESMP
Element 1
Element 2
Element 3
Element 4
Element 5
Element 6
Actions related to the maintenance of buildings and constructions
Actions ensuring the operation of engineering and technical systems
Actions ensuring the operation of engineering networks
Actions for solving the problems of development of socio-economic infrastructure (1st type)
Actions for solving the problems of production and transport infrastructure (2nd type)
Actions for solving the problems of information and communication infrastructure (3rd type)

Figure 15.
The abstract complex structure for modelling specific abnormal impacts.

Input for every element (see model in [1–7])	Elements	Values
σ – frequency of the occurrences of potential threats	Element 1	4 times a year
	Element 2	2 times a year
	Element 3	1 time in a year
	Element 4	1 time in 2 years
	Element 5	1 time in 2 years
	Element 6	2 times a year
β – mean activation time of threats up to unacceptable damage	For all elements 1–6	1 month
T_{betw} – time between the end of diagnostics and the beginning of the next diagnostics	Element 1	24 hours
	Element 2	24 hours
	Element 3	24 hours
	Element 4	8 hours
	Element 5	8 hours
	Element 6	1 hour
T_{diag} – diagnostics time of element integrity	For all elements 1–6	30 seconds
T_{recov} – recovery time after integrity violation	For all elements 1–6	10 minutes
T – given prediction period	For all elements 1–6	From 1 to 4 years

Table 3.
Input for probabilistic modelling (example 3).

Without delving into the numerous technical, engineering and functional aspects of (S-N-T)-ESMP, **Table 3** reflects hypothetical averaged input data for research by models, described in sections 5–7, **Appendices A, B** and [1–7]. Input values for element 1 consider additional factors leading to degradation and destruction of techno-sphere systems (seismic, wind, snow, corrosion and other natural impacts). For element 6, proper impacts may be from "human factor" and/or from "cyber threats". For elements 2–5, input values have usual explanation.

Analysis of the results showed that in probabilistic terms the risk of unacceptable damage due to specific abnormal impacts for 2 years will be about 0.219 totally for all elements (see **Figure 16**). In turn, for the predict for 4 years with daily monitoring of the state of the engineering infrastructure of the (S-N-T)-ESMP (i.e. elements 1, 2, 3), the risk of unacceptable damage from specific impacts for all elements 1–6 will be about 0.39, and for the predict 1, this probability is about 0.12 (see **Figure 17**). In general, the results are comparable with the results of Example 2 (**Figures 18** and **19**).

Moreover, due to the management decision, expressed in changing the frequency of diagnostics from daily to 1 time every 8 hours it is possible to reduce total risk from 0.219 to 0.091 (see **Figure 18**). And owing to diagnostics every 8 hours the admissible risk level of 0.10 will not be exceeded about 2.3 years (see **Figure 19**).

Example 4. In continuation of Examples 2 and 3, the integral probability $\boldsymbol{R}_{\int}(\boldsymbol{T})$ of failure of the infrastructure management process considering specific system abnormal impacts for the prediction period T = 1 year is calculated using the recommendations of Section 6. It depends on probabilities $\boldsymbol{R}_{\mathbf{rel}}(\boldsymbol{T})$ and $\boldsymbol{R}_{\mathbf{add}}(\boldsymbol{T})$ – see formula (6). Considering that $\boldsymbol{R}_{\mathbf{rel}}(\mathbf{1year}) = 0{,}08$ and $\boldsymbol{R}_{\mathbf{add}}(\mathbf{1year}) = 0{,}05$,

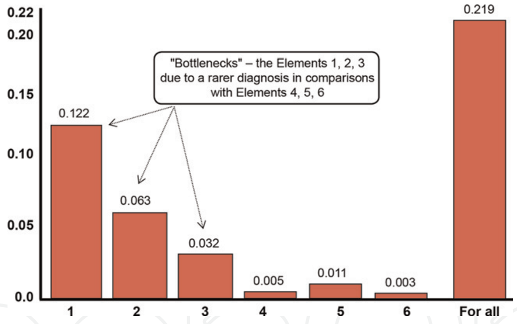


Figure 16.
The risks of unacceptable damage because of specific abnormal impacts on elements 1–6 for 2 years (for daily diagnostics).

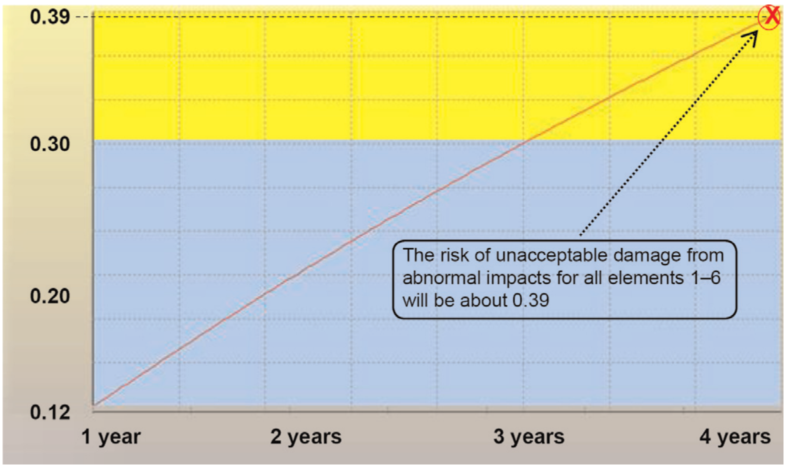


Figure 17.
The dependence of total risk of unacceptable damage because of specific abnormal impacts on elements 1 –6 from duration of prediction period (for daily diagnostics).

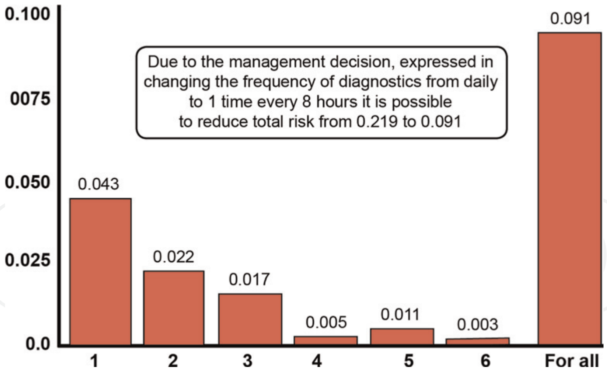


Figure 18.
The risks of unacceptable damage because of abnormal impacts on elements 1–6 for 2 years (for diagnostics every 8 hours).

$$R_{\int}(\mathbf{1year}) = 1-(1-0,\ 08)\cdot(1-0,\ 05)\approx 0{,}126.$$

Interpretation: the integral risk for the prediction period of 1 year is about 0.126 considering possible damage. In general, such risk is considered elevated. It can be considered acceptable only in exceptional cases when there are no real possibilities of any counteraction to threats. As measures to improve the process, additional control systems for damaging natural factors, emergency protection systems for

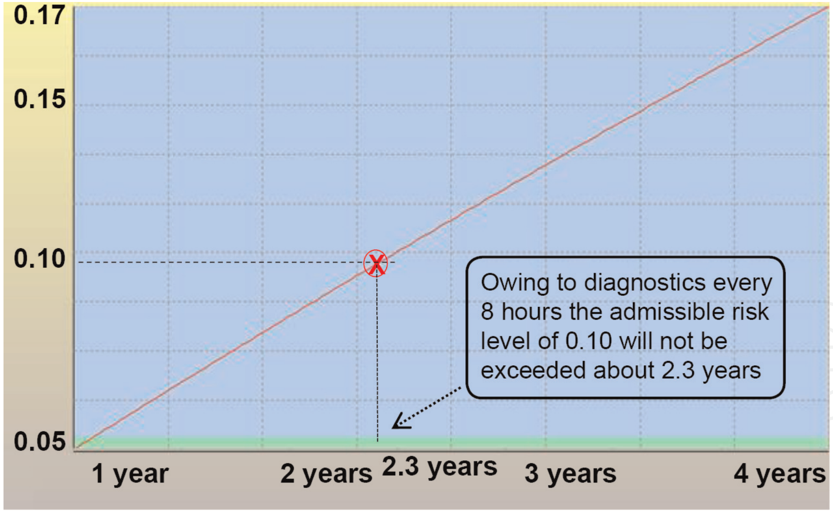


Figure 19.
The dependence of total risk of unacceptable damage because of abnormal impacts on elements 1—6 from duration of prediction period (for diagnostics every 8 hours).

techno-sphere systems, operators and personnel under extreme natural hazards, and measures to increase safety against specific system threats (the sources of specific abnormal impacts) can be used. Since such opportunities are far from being exhausted, an additional search for measures to reduce the integral risk is necessary. Decision-making on ways to reduce risks may be quantitatively justified using the proposed models and methods.

8.3 What about the possible pragmatic effects?

In general pragmatic effects are connected with achieving pragmatic goals (see Section 2). It may characterize the efficiency of the implementation of the state and/or corporate strategy in the economy, effects from improving the safety and sustainability of the region's development, from ensuring the protection of the population and territories from natural and man-made hazards, etc. For example, the authors of this chapter took part in the creation of the complex of supporting technogenic safety in the systems of oil and gas transportation and distribution and have been awarded for it by the award of the Government of the Russian Federation in the field of a science and technic. Through the Complex intellectual means, it is possible to detect remote-sensing technology: vibrations, fire, flood, unauthorized access, hurricane; and to recognize, identify and predict the development of extreme hazardous situations, and to make decisions in real-time. The applications of this Complex for 200 objects in several regions of Russia during the period 5 years have already provided economy about 8,5 Billion Roubles (reached at the expense of effective risks prediction and processes optimization [7]).

9. About directions for development

It is proposed to focus on scientific and technical efforts on the meta-level of system engineering, which allows, by universal probabilistic models, to set and analytically solve the problems of rational development and efficient operation of complex systems of various functionalities and purposes.

The proposed prioritization of development directions for predicting are: 1 – focusing on scientific and technical efforts on achieving the goals of ensuring the required safety, quality, balanced effects, sustainable operation and development of complex systems; 2 – providing capabilities for predicting and rational risk managing in standard processes of the system life cycle, improving and accumulating knowledge, patterns discovery; 3 – expansion of the functionality of the created models and methods, software and technological and methodological solutions (for predicting and rational risk managing) to all spheres of human activity, cross-application of knowledge bases; 4 – transformation of the existing approach to the creation and use of models and methods into artificial intelligence technology to support logical decision-making (based on proactive research with traceability of logic from the idea to the achieved effect).

The proposed steps to implement these directions are 1st step: from pragmatic filtering of information → to promising ideas and purposeful conceptions; 2nd step: from promising ideas and purposeful conceptions → to the formalization of uncertainties; 3rd step: from the formalization of uncertainties → to the knowledge of patterns and logical solutions; 4th step: from the knowledge of patterns and logical solutions → to rational risk management; 5th step: from rational risk management → to achieving the required safety, quality, balanced effects and sustainable operation and development.

The expected results will equally be understood at the level of probabilistic risk predictions, identically interpreted and comparable, the traceability of the effectiveness of scientific and technical system efforts from the conceptions to the results obtained will also be ensured. The purposeful aspirations "From uncertainties formalization – to sustainable harmony" (see Section 1) may be really supported.

10. Conclusion

On the generalizations of goals and objectives throughout the system's life cycle and existing approaches to risks prediction, there are proposed main goals of applying probabilistic methods. The goals of probabilistic concepts of risks prediction are connected with: an analysis of opportunities, achievable quality, safety and efficiency; a rationale for achieving desirable characteristics and acceptable conditions; an optimization of systems and processes; and finding and developing new ideas and concepts.

The enlarged classification of probabilistic methods for solving various objectives is explained for all stages of the system life cycle: concept, development, production, utilization, support and retirement.

The conceptual approach, proposed to risk prediction, covers social sphere (person, society, state and world community), natural sphere (earth and space) and techno-sphere (man-made infrastructures and life support facilities).

The essence of the proposed probabilistic concepts of risks prediction for the system is described on the level of probability distribution function. The described methods of risks prediction for complex systems include probabilistic models, methods for risks prediction and integration, optimization methods for rationale actions and examples for solving the problems of system analysis and rationale proactive actions in uncertain conditions. The achievable practical effects are explained.

The prioritization of development directions for risk prediction in standard system processes and targeted steps for their implementation are proposed. They support the purposeful aspirations "From uncertainties formalization – to sustainable harmony" in application to the life cycle of various systems.

Appendix A. The recommended models to predict information system operation quality

The proposed models are presented in **Table A.1**.

Appendix B. The models to predict risks for "Black box"

B.1. The model for technology 1 ("Black box") – see 5.2, [9, 14, 15].

Input:

$\Omega_{penetr}(t)$—is the PDF of time between neighboring influences for penetrating a danger source;

$\Omega_{activ}(t)$– is the PDF of activation time up to "accident event";

$T_{betw.}$—is time between the end of diagnostic and the beginning of the next diagnostic,

T_{diag}—is diagnostic time.

$R = 1 - P$ considering consequences.

Variant 1—$(T_{req.} < T_{betw.} + T_{diag})$:

$$P_{(1)}(T_{req.}) = 1 - \Omega_{penetr} * \Omega_{activ}(T_{req.}). \tag{12}$$

Variant 2—the assigned period $T_{req.}$ is more than or equals to an established period between neighboring diagnostics $(T_{req.} \geq T_{betw.} + T_{diag})$:

measure a)

$$P_{(2)}(T_{req.}) = N((T_{betw.} + T_{diag})/T_{req.})\bullet P^{N}_{(1)}(T_{betw.} + T_{diag}) + (T_{rmn}/T_{req.})\bullet P_{(1)}(T_{rmn}), \tag{13}$$

where $N = [T_{given}/(T_{betw.} + T_{diag})]$ is the integer part,

$$T_{rmn} = T_{given} - N(T_{betw.} + T_{diag});$$

measure b)

$$P_{(2)}(T_{req.}) = P^{N}_{(1)}(T_{betw.} + T_{diag})\bullet P_{(1)}(T_{rmn}), \tag{14}$$

where the probability of success within the given time $P_{(1)}(T_{req.})$ is defined by (B.1).

B.2. The model for technology 2 ("Black box")—see 5.2, [9, 14, 15].

Input:

Additionally to Input for technology 1: $A(t)$—is the PDF of time from the last finish of diagnostic time up to the first operator error.

Evaluated measures:

Risk to lose system integrity (R). Probability of providing system integrity (P).

$R = 1 - P$ considering consequences.

Models. Input	Evaluated measures
The model of functions performance by a complex system in conditions of unreliability of its components. Input: $N(t)$—is the PDF of time between neighboring failures; $W(t)$—is the PDF of repair time; and $V(t)$—is the PDF of given time if this time is a random value	Probability P_{rel} of providing reliable function performance during given time $P_{rel} = \int_0^\infty \left\{ \int_t^\infty V(\tau - t)dN(\tau) \right\} dt / \int_0^\infty td[N * W(t)]$, (A.1) *—is the convolution sign.
The model of calls processing for the different dispatcher technologies. Input for M/G/1/∞: λ_i– frequency of the i-th type calls for processing; β_i—mean processing time of the i-th type calls (without queue).	Probability $P_{tim.i}$ of well-timed processing of i-type calls during the required term $T_{req.i}$ $P_{tim.i} = P\left(t_{full.i} \le T_{req.i}\right) = \frac{\int_0^{\gamma_i^2 T_{req.i}/T_{full.i}} t^{\gamma_i^{-1}} e^{-t} dt}{\int_0^\infty t^{\gamma_i^{-1}} e^{-t} dt}$, (A.2) $\gamma_i = \frac{T_{full.i}}{\sqrt{T_{full.i2} - T_{full.i}^2}}.$ Relative portion of all well-timed processed calls—S and relative portion of well-timed processed calls of those types for which the customer requirements are met—C: $S = \frac{\sum_{i=1}^I \lambda_i P_{tim.i}}{\sum_{i=1}^I \lambda_i}, C = \frac{\sum_{i=1}^I \lambda_i P_{tim.i}[Ind(\alpha_1) + Ind(\alpha_2)]}{\sum_{i=1}^I \lambda_i},$ $Ind(\alpha) = \begin{cases} 0, if\ \alpha = true \\ 1, if\ \alpha = false \end{cases},$ $\alpha_1 =$(criterion 1); $\alpha_2 =$(criterion 2). Criterion 1 is requirement to mean processing time $T_{full.i} \le T_{req.i}$, which means that i-type calls must be processed in time (in average), criterion 2 is requirement on the level of PDF $P_{tim.i} = P\left(t_{full.i} \le T_{req.i}\right) \ge P_{adm.i}$, which means hard processing in real time, $P_{adm.i}$—is admissible level for well-timed processing of i-type calls during the required term $T_{req.i}$.
The model of entering into system current data concerning new objects of application domain. Input: q_m—the probability that m new objects appear in random moment, intervals between these moments are exponentially distributed with parameter λ. $\Phi(z) = \sum_{m>0} q_m z^m$—is productive (generating) function; $B(t)$ —is the PDF of time for new information revealing and preparing, transfer and entering into database	Probability $P_{comp.}$ that system contains information about states of all real objects and coincides $P_{comp.} = exp\left\{ -\lambda \int_0^\infty [1 - \Phi(B(t))] \right\}$, (A.3)

The model of information gathering. Input: $C(t)$ is the PDF of time between essential changes of monitored object states, ξ_i—is the mean time for this PDF; $B(t)$ is the PDF of time for information gathering, preparing, transfer and entering into system; $Q(t)$ is the PDF of time between information updating, q is mean time; the mode D_1 of gathering: information is gathered in order "immediately after an essential object state change; the mode D_2 of gathering: information is gathered without any dependencies on changes in objects' current states (including regulated information gathering).	Probability P_{act} of information actuality on the moment of its use: 1) for the mode D_1 when information is gathered in order "immediately after an essential object state change: $P_{act} = \frac{1}{\xi_i}\int\limits_0^{\infty} B(t)[1 - C(t)]dt$, (A.4) 2) for the mode D_2 when information is gathered without any dependencies on changes in objects' current states (periodical gathering) $P_{act} = \frac{1}{q}\int\limits_0^{\infty}\left\{[1 - Q(t)]\left[1 - \int\limits_0^{\infty} C(t+\tau)dB(\tau)\right]\right\}dt$, (A.5)
The model of information analysis. Input: $T_{req.}$—assigned term for analysis; $N(t)$ − is the PDF of time between operator error ("false" instead of "true" (on time line), i.e. type I errors, η^{-1} is the mean time; $M(t)$ is the PDF of time between the neighboring errors in analyzed information (on timeline); $A(t)$ is the PDF of time between skipping an error (type II errors on timeline), T_{MTBF} is mean time; μ is the possible relative fraction of errors in information content (destined for problems of checking) or the possible relative fraction of information, which is essential for analysis (destined for problems of analysis); $T_{real} = V/\nu$—is the real time for complete information analysis; V—is a content of analyzed information; ν—is an analyzed speed; $T_{cont.}$—is time of continuous analyst's work. $T_{req.}$– is given term for analysis (deadline)	Probability P_{after} to be without errors after checking (or probability P_{after} of correct analysis): Variant 1—($T_{real} \le T_{req.}$) and ($T_{real} \le T_{cont.}$): $P_{after(1)}\left(V, \mu, \nu, n, T_{MTBF}, T_{cont.}, T_{req.}\right) =$ $= \left[1 - \hat{N}(V/\nu)\right] \cdot \left\{\int\limits_0^{V/\nu} dA(\tau)[1 - M(V/\nu - \tau)] + \int\limits_{V/\nu}^{\infty} dA(t)\right\}$ (A.6) Variant 2—($T_{real} \le T_{req.}$) and ($T_{real} > T_{cont.}$): $P_{after(2)} = \left\{P_{after(1)}\left(V_{part(2)},\ \mu,\ \nu,\ \eta,\ T_{MTBF},\ T_{cont.},\ \tau_{part(2)}\right)\right\}^N$, (A.7) $N = V/(\nu \cdot T_{cont.}), V_{part(2)} = V/N,\ \tau_{part(2)} = T_{req.}/N.$ Variant 3—($T_{real} > T_{req.}$) and ($T_{real} \le T_{cont.}$): $P_{after(3)} = \left(V_{part(3)}/V\right) \cdot P_{after(1)} \cdot V_{part(3)},\mu,\nu,\eta,T_{MTBF},T_{cont.},$ $+\left[\left(V - V_{part(3)}\right)/V\right] \cdot P_{without}$, (A.8) where $V_{part(3)} = \nu \cdot T_{req.}, P_{without} = e^{-\mu\cdot\left(V - V_{part(3)}\right)}$. Variant 4—($T_{real} > T_{req.}$) and $T_{real} > T_{cont.}$. $P_{after} =$ $= \begin{cases} \left[V_{part(4)}/V\right] \cdot P_{after(1)} \cdot \left(V_{part(4)},\ \mu,\ \nu,\ \eta,\ T_{MTBF},\ T_{cont.},\ T_{req.}\right) + \\ +\left[\left(V - V_{part(4)}\right)/V \cdot e^{-\mu\cdot\left(V - V_{part(4)}\right)}, \text{if} T_{req.} \le T_{cont.}; \end{cases}$ $\left[V_{part(4)}/V\right] \cdot \left\{P_{after(1)} \cdot \left(V_{part(4.2)},\ \mu,\ \nu,\ \eta,\ T_{MTBF},\ T_{cont.},\ \tau_{part(4.2)}\right)\right\}^N +$ $+\left[\left(V - V_{part(4)}\right)/\mathrm{V}\right] \cdot e^{-\mu\cdot\left(V - V_{part(4)}\right)}, \text{if} T_{req.} > T_{cont.},$ (A.9)

The model of authorized access to system resources during objective period. Input: M is the conditional quantity of security barriers in counteraction to unauthorized access; $F_m(t)$ is the PDF of time between changes of m-th barrier parameters, f_{m} is mean time for this PDF; $U_m(t)$ is the PDF of parameters decoding time of the m-th security system barrier, $H(t)$—is the PDF of objective period, when resources value is high. If the mean objective period, when resources value is high → ∞, this he model is transformed into the model of an authorized access to system resources (see below)	Probability P_{value} of system protection against unauthorized access during objective period $P_{value} = 1 - \prod_{m=1}^{M} P_{over.m}$, (A.10) where $P_{over.m}$—is the risk of overcoming the m-th barrier by violator during objective period when resources value is high, $P_{over} = \frac{1}{f_m}\int_0^\infty dt \int_t^\infty dF_m(\tau)\int_0^t dU_m(\theta)[1-H(\theta)].$
The model of dangerous influences on a protected system. Input: $\Omega_{penetr}(t)$—is the PDF of time between neighboring influences for penetrating danger source; $\Omega_{activ}(t)$—is the PDF of activation time of penetrated danger source; $T_{req.}$—is the required period of permanent secure system operation; $T_{betw.}$ is time between the end of diagnostic and the beginning of the next diagnostic, $T_{diag.}$—is diagnostic time; $A(t)$—is the PDF of time from the last finish of diagnostic time up to the first operator error.	Probability P_{infl} of faultless (correct) operation during given time: Variant 1—$\left(T_{req.} < T_{betw.} + T_{diag}\right)$: $P_{(1)}\left(T_{req.}\right) = 1 - \int_0^{T_{req.}} dA(\tau) \int_\tau^{T_{req.}} d\Omega_{penetr}\ {}^{*}\Omega_{activ}(\theta)$. (A.11) Variant 2—$\left(T_{req.} \geq T_{betw.} + T_{diag}\right)$: measure a) $P_{(2)}\left(T_{req.}\right) = N\left(\left(T_{betw.} + T_{diag}\right)/T_{req.}\right) \cdot P_{(1)}^{N}\left(T_{betw.} + T_{diag}\right) +$ $+\left(T_{rmn}/T_{req.}\right) \cdot P_{(1)}(T_{rmn})$, (A.12) measure b) $P_{(2)}\left(T_{req.}\right) = P_{(1)}^{N}\left(T_{betw.} + T_{diag}\right) \cdot P_{(1)}(T_{rmn})$, (A.13) where N is the same and the probability of success within the given time $P_{(1)}\left(T_{req.}\right)$, which is defined by (A.11)
The model of authorized access to system resources. Input (for estimation of confidentiality): M is the conditional quantity of a barriers against an unauthorized access; $F_m(t)$ is the PDF of time between changes of the m-th barrier parameters, f_{m} is the mean time for this PDF; $U_m(t)$ is the PDF of parameters decoding time of the m-th security system barrier	Probability P_{prot} of system protection against unauthorized access: $P_{prot} = 1 - \prod_{m=1}^{M} P_{over.m}$, (A.14) where $P_{over.m}$—is the probability of overcoming the m-th barrier by violator, $P_{over.m} = \frac{1}{f_m}\int_0^\infty [1 - F_m(t)] \bullet U_m(t)dt$. (A.15)
Note. The final clear analytical formulas are received by Lebesque-integration of (A.1), (A.3)–(A.6), (A.10), (A.11), and (A.15).	

Table A.1.
The proposed models (for the details—See [7–9, 14, 15]).

For variant 1 $\left(T_{req.} < T_{betw.} + T_{diag}\right)$: see (A.11).

For variant 2 $\left(T_{req.} \geq T_{betw.} + T_{diag}\right)$: see (A.12), (A.13), and the same (B.2), (B.3).

Evaluated measures:

Risk to lose system integrity (R). Probability of providing system integrity (P).

Acknowledgements

The authors would like to thank the Russian Academy of Sciences for supporting the work presented in this Chapter.

The authors much obliged to Dr. Mohamed Eid, President of ESReDA (European Safety, Reliability & Data Association) for meaningful advices regarding Chapter.

And also thanks a lot to Ms. Olga Kostogryzova for some artistic Figures design.

Author details

Andrey Kostogryzov[1]*, Nikolay Makhutov[2], Andrey Nistratov[1] and Georgy Reznikov[3]

1 Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, Moscow, Russia

2 The A.A. Blagonravov Institute for Machine Sciences of the Russian Academy of Sciences, Moscow, Russia

3 Company “Regional Engineering Consulting Firm” Ltd., Samara, Russia

*Address all correspondence to: akostogr@gmail.com

References

[1] Feller W. An Introduction to Probability Theory and Its Applications. New York: Jhon Wiley & Sons; 1971;**2**

[2] Martin J. System Analysis for Data Transmission. Englewood Cliffs; New Jersey: Prentice Hall, Inc; 1972

[3] Gnedenko BV et al. Priority Queueing Systems. Moscow: MSU; 1973

[4] Kleinrock L. Queueing Systems, V.2: Computer Applications. New York: John Wiley & Sons; 1976

[5] Matweev VF, Ushakov VG. Queuing Systems. Moscow: MSU; 1984

[6] Kostogryzov AI, Petuhov AV, Scherbina AM. Foundations of Evaluation, Providing and Increasing Output Information Quality for Automatized System. Moscow: Armament. Policy. Conversion; 1994

[7] Security of Russia. Legal, Social& Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of Makhutov N.A. Moscow: Znanie. Volumes 1–63; 1998-2021

[8] Kostogryzov AI. Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). In: Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium. Dallas; 2000. pp. 63-70

[9] Kostogryzov A, Nistratov G. Standardization, Probabilistic Modelling, Rational Management and Certification in the Field of System and Sengineering (80 Standards, 100 Probabilistic Models, 35 Software Tools, More than 50 Practical Examples). Moscow: Armament. Policy. Conversion; 2005

[10] Zio En. An Introduction to the Basics of Reliability and Risk Analysis. Singapore: World Scientific Publishing Co.Pte. Ltd; 2006

[11] Makhutov NA. Strength and Safety. Fundamental and Applied Research. Novosibirsk: Nauka; 2008

[12] Kolowrocki K, Soszynska-Budny J. Reliability and Safety of Complex Technical Systems and Processes. London: Springer-Verlag; 2011

[13] Eid M, Rosato V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach. New York: Springer Open; 2016:43-62

[14] Kostogryzov AI, Stepanov PV. Innovative Management of Quality and Risks in Systems Life Cycle. Moscow: Armament. Policy. Conversion; 2008

[15] Kostogryzov A, Nistratov G, Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma. Rijeka, Croatia: InTech; 2012; 127-196

[16] Kostogryzov A, Nistratov G, Nistratov A. The innovative probability models and software technologies of risks prediction for systems operating in various fields. International Journal of Engineering and Innovative Technology (IJEIT). 2013;**3**(3):146-155

[17] Grigoriev L, Guseinov C, Kershenbaum V, Kostogryzov A. The methodological approach, based on the risks analysis and optimization, to research variants for developing hydrocarbon deposits of Arctic regions.

Journal of Polish Safety and Reliability Association. 2014;**5**:1-2

[18] Artemyev V, Kostogryzov A, Rudenko J, Kurpatov O, Nistratov G, Nistratov A. Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. In: Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS). Milan, Italy; 2017. pp. 368-373

[19] Kostogryzov A, Stepanov P, Nistratov A, Atakishchev O. About Probabilistic Risks Analysis During Longtime Grain Storage. Proceedings of the 2nd Internationale Conference on the Social Science and Teaching Research (ACSS-SSTR), Volume 18 of Advances in Social and Behavioral Science. Singapore: Singapore Management and Sports Science Institute, PTE.Ltd; 2017: 3-8

[20] Kostogryzov A, Stepanov P, Nistratov A, Nistratov G, Klimov S, Grigoriev L. The method of rational dispatching a sequence of heterogeneous repair works. Energetica. 2017;**63**(4): 154-162

[21] Kostogryzov A, Stepanov P, Grigoriev L, Atakishchev O, Nistratov A, Nistratov G. Improvement of existing risks control concept for complex systems by the automatic combination and generation of probabilistic models and forming the storehouse of risks predictions knowledge. In: Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM). Phuket, Thailand: DEStech Publications; 2017. pp. 279-283

[22] Kostogryzov A, Panov V, Stepanov P, Grigoriev L, Nistratov A, Nistratov G. Optimization of sequence of performing heterogeneous repair work for transport systems by criteria of timeliness. In: Proceedings of the 4th International Conference on Transportation Information and Safety (ICTIS). Canada; 2017. pp. 872-876

[23] Kostogryzov A, Grigoriev L, Golovin S, Nistratov A, Nistratov G, Klimov S. Probabilistic modeling of robotic and automated systems operating in cosmic space. In: Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI). Beijing, China: DEStech Publications; 2018. pp. 298-303

[24] Kostogryzov A, Grigoriev L, Kanygin P, Golovin S, Nistratov A, Nistratov G. The experience of probabilistic modeling and optimization of a centralized heat supply system which is an object for modernization. In: International Conference on Physics, Computing and Probabilistic Modeling (PCMM). Shanghai: DEStech Publications, Inc; 2018. pp. 93-97

[25] Artemyev V, Rudenko J, Nistratov G. Probabilistic modeling in system engineering. Chapter 2. Probabilistic methods and technologies of risks prediction and rationale of preventive measures by using “smart systems”. Applications to coal branch for increasing Industrial safety of enterprises. IntechOpen. 2018:23-51

[26] Kershenbaum V, Grigoriev L, Nistratov A. Probabilistic modeling in system engineering. Chapter 3. Probabilistic modeling processes for oil and gas systems. IntechOpen. 2018:55-79

[27] Kostogryzov A, Nistratov A, Nistratov G, Atakishchev O, Golovin S, Grigoriev L. The probabilistic analysis of the possibilities to keep “organism integrity” by continuous monitoring. In: Proceedings of the International Conference on Mathematics, Modelling,

Simulation and Algorithms (MMSA). Chengdu, China: Atlantis Press; 2018. pp. 432-435

[28] Kostogryzov A, Korolev V. Probability, combinatorics and control. Chapter 1. Probabilistic methods for cognitive solving problems of artificial intelligence systems operating in specific conditions of uncertainties. IntechOpen. 2020:3-34

[29] Kostogryzov A, Kanygin P, Nistratov A. Probabilistic comparisons of systems operation quality for uncertainty conditions. RTA&A. 2020; **15**:63-73

[30] Kostogryzov A, Nistratov A, Nistratov G. Analytical risks prediction. Rationale of system preventive measures for solving quality and safety problems. In: Sukhomlin V, Zubareva E, editors. Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science. Cham: Springer; 2020. pp. 352-364. DOI: 10.1007/978-3-030-46895-8_27

[31] Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In: Safety and Reliability of Systems and Processes. Poland: Gdynia Maritime University; 2020. pp. 153-174

[32] Moskvichev VV, Makhutov NA, Shokin YM, Gadenin MM. Applied Problems of Structural Strength and Mechanics of Destruction of Technical Systems. Novosibirsk: Nauka; 2021

[33] Gneiting T, Balabdaoui F, Raferty AE. Probabilistic forecasts, calibration and sharpness. Journal of the Royal Statistical Society, Series B (Statistical Methodology). 2007;**68**:243-268

[34] Kostogryzov A, Nistratov A, Zubarev I, Stepanov P, Grigoriev L. About accuracy of risks prediction and importance of increasing adequacy of used probabilistic models. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars. 2015;**6**:71-80