Kostogryzov Andrey

Nistratov George

Nistratov Andrey

Research Institute of Applied Mathematics and Certification, Moscow, Russia

Applicable technologies to forecast, analyze and optimize reliability and risks for complex systems

Keywords

analysis, forecasting, model, quality, reliability, risk, safety, software tools, system engineering, technology

Abstract

The paper is concerned with the application of the original mathematical models and supporting them software technologies to forecast, analyze and optimize reliability and risks for complex systems (system is defined as a combination of interacting elements organized to achieve one or more stated purposes). Functionality and usability to analyze information system processes and standard processes in system life cycle are presented. Rational use of the proposed results allows to go «from a pragmatical filtration of information to generation of the proved ideas and effective decisions». Effects are demonstrated by examples.

1. Introduction

Today processes of system life cycle in different conditions and threats are the main objects for forecasting, analysis and optimization. For example, covering systems in different fields, the first system engineering standard ISO/IEC 15288 “System Engineering - System Life Cycle Processes" (since 2002) recommends to perform only the actions that were substantiated and not to act in the directions, which were not estimated and justified.

The goal of this work is to propose models and software tools covered in applicable technologies, well-tested in practice, to forecast, analyze and optimize quality (including reliability) and risks as applied to newly developed and currently operated manufacture, power generation, transport, engineering, information, control, security systems etc. Presented work covers logically closed contour: «system requirements of standards – supporting mathematical models to estimate probabilities of success, risks, profits and damages – ways of rational management». Thereby the reader can substantiate answers on system engineering questions: «Can be the system requirements met?», «What about the real risks, profits and possible damages?», «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?» and others. The answers may be received before critical events and proactive measures can be implemented in time.

The logic scheme everywhere in decisions of system engineering is identical: at first the set of destabilizing factors and/or threats against quality and safety is defined, then taking into account available resources the possible measures of neutralization should be chosen or developed. A vulnerability set of system comes to light. Technologies of system control and recovery of broken integrity should be used as counteraction against destabilizing factors and threats. Thus at every step of system life cycle the development of processes is supported by probabilistic forecasts, criteria of optimization are chosen in depending on the problem purposes. Rational decisions can be found on the base of mathematical modelling.

Note. System integrity is defined as such system state when system purposes are achieved with the required quality.

The offered models and software tools (patented in Russia by Rospatent) have been presented at seminars, conferences, ISO/IEC working groups and other forums in Russia, Australia, Canada, China, France, Germany, Poland, the USA, International Exhibitions in Germany. The technology of modelling through Internet has been acknowledged as the best project-2007 by the National Association of Innovations and Developments of Information Technologies of Russia.

2. Review of system processes to reveal general engineering problems that are due to be solved by the mathematical modelling

The knowledge and results of system analysis allows a customer to formulate substantiated requirements and specifications, a developer - to implement them rationally without wasted expenses, a user – to use system potential in the most effective way. Let's review some system standards - ISO 9001, ISO/IEC 15288, 12207, 17799, IEC 60300, 61508, CMMI, some standards for use in the oil&gas industry (ISO 10418, 13702, 14224, 15544, ISO 15663, ISO 17776 etc.) from the role of system analysis point of view. These are the representative part of the modern system engineering standards.

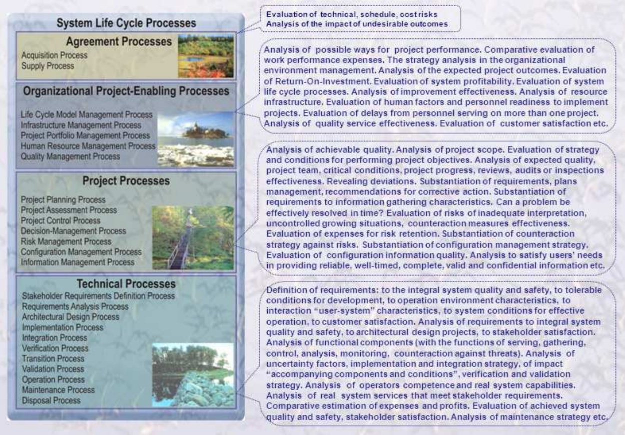
In compliance with ISO 9001 to all processes there can be applied methodology known as "Plan-Do-Check-Act" (PDCA). For any improvement a documented procedure shall be established to define requirements for determining potential nonconformities and their causes, evaluating the need for action to prevent occurrence of nonconformities, determining and implementing action needed. In compliance with ISO/IEC 15288, 12207 system analysis actions and optimization are the main actions for achievement system purposes in life cycle. The standard ISO/IEC 17799 and others like standards in security area (for example, ISO/IEC 15443, 13335 etc.) imply that high effectiveness of system protection measures should be evaluated and confirmed quantitatively. It means that any system security evaluations need in an adequate mathematical methodology. The standard IEC 60300 describes the approaches to the risk analysis of technological systems from system analysis point of view. The standard IEC 61508 includes Parts "Examples of methods for the determination of safety integrity levels" and "Overview of techniques and measures" that recommend to evaluate system risks. An application of CMMI allows selecting the order of improvement that best meets the organization's business objectives and mitigates the organization's areas of risk. And these results are also based on system analysis.

To understand the situation with requirements and applicable methods to analize and optimize system processes an existing practices for providing system quality and safety were reviewed. According to applicable mathematical models everyone (majority) solves the problems "how can", we can resume: all organizations need quantitative estimations, but only some part from them uses modelling complexes; used models are highly specialized, input and calculated metrics are adhered strongly to specificity of systems; existing modelling complexes have been created within the limits of concrete order for the systems and as a rule are very expensive. The summary of the analysis is the next.

1. Analysis of quality and risks is carried out mainly at qualitative level with assessments "better or worse". Independent quantitative estimations at probability level are carried out by special models.
2. Generally risk estimations from one sphere do not use in other spheres because of methodologies for risk analysis are different, interpretations are not identical. The methods for quantitatively risk analysis and quality analysis (on probability level) are in creating stage yet. The terms "Acceptable quality" and "Admissible risk" in use should be defined on probability scale level only in dependence on corresponding methods. As consequence probability estimations are not comparable for different areas, experience from other spheres is missing, comparisons for systems from different areas, as a rule, are not used, as universal objective scale of measurement is not established yet.
3. In all cases effective risk management for any system is based on: uses of materials, resources, protective technologies with best characteristics from the point of view of safety, including integrity recovery; rational use of situation analysis, effective ways of the control and monitoring of conditions and operative recovery of integrity; rational use of measures for risk counteraction.
4. It does not allow to solve the main problems of a substantiation of system requirements to parameters of information gathering and analysis, control, monitoring and counteraction measures at restrictions, and also to confirm about efficiency of the prevent measures to provide quality and safety!

In general case system methods for analyzing and optimizing are founded completely on the mathematical modelling of system processes. We understand that any process is a repeated sequence of consuming time and resources for outcome receiving. In general case the moments for any activity beginning and ending are, in mathematical words, random events on time line. Moreover, there exists the general property of all process architectures. It is a repeated performance for majority of timed activities (evaluations, comparisons, selections, controls, analysis etc.) during system life cycle - for example see on *Figure 1* the problems that are due to be solved by the mathematical modelling of processes according to ISO/IEC 15288.

This work focuses on the way for extracting latent effects by using universal metrics in a systems life cycle (see *Figure 2*): probabilities of success or failure during a given period for an element, subsystem, system. Calculation of these metrics within the limits of the offered probability space built on the basis of the theory for random processes, allows to forecast outcomes on an uniform scale, quantitatively to prove levels of acceptable quality (reliability) and admissible risks, to solve the problems of system engineering (see above).



System Life Cycle Processes

Agreement Processes
Acquisition Process
Supply Process

Organizational Project-Enabling Processes
Life Cycle Model Management Process
Infrastructure Management Process
Project Portfolio Management Process
Human Resource Management Process
Quality Management Process

Project Processes
Project Planning Process
Project Assessment Process
Project Control Process
Decision-Management Process
Risk Management Process
Configuration Management Process
Information Management Process

Technical Processes
Stakeholder Requirements Definition Process
Requirements Analysis Process
Architectural Design Process
Implementation Process
Integration Process
Verification Process
Transition Process
Validation Process
Operation Process
Maintenance Process
Disposal Process

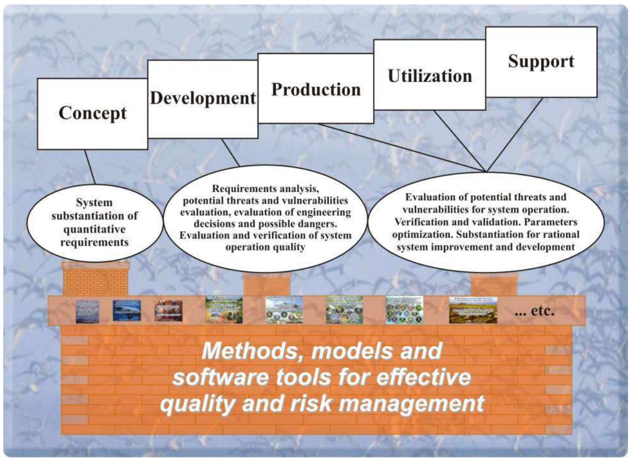
Evaluation of technical, schedule, cost risks
Analysis of the impact of undesirable outcomes

Analysis of possible ways for project performance. Comparative evaluation of work performance expenses. The strategy analysis in the organizational environment management. Analysis of the expected project outcomes. Evaluation of Return-On-Investment. Evaluation of system profitability. Evaluation of system life cycle processes. Analysis of improvement effectiveness. Analysis of resource infrastructure. Evaluation of human factors and personnel readiness to implement projects. Evaluation of delays from personnel serving on more than one project. Analysis of quality service effectiveness. Evaluation of customer satisfaction etc.

Analysis of achievable quality. Analysis of project scope. Evaluation of strategy and conditions for performing project objectives. Analysis of expected quality, project team, critical conditions, project progress, reviews, audits or inspections effectiveness. Revealing deviations. Substantiation of requirements, plans management, recommendations for corrective action. Substantiation of requirements to information gathering characteristics. Can a problem be effectively resolved in time? Evaluation of risks of inadequate interpretation, uncontrolled growing situations, counteraction measures effectiveness. Evaluation of expenses for risk retention. Substantiation of counteraction strategy against risks. Substantiation of configuration management strategy. Evaluation of configuration information quality. Analysis to satisfy users' needs in providing reliable, well-timed, complete, valid and confidential information etc.

Definition of requirements: to the integral system quality and safety, to tolerable conditions for development, to operation environment characteristics, to interaction "user-system" characteristics, to system conditions for effective operation, to customer satisfaction. Analysis of requirements to integral system quality and safety, to architectural design projects, to stakeholder satisfaction. Analysis of functional components (with the functions of serving, gathering, control, analysis, monitoring, counteraction against threats). Analysis of uncertainty factors, implementation and integration strategy, of impact "accompanying components and conditions", verification and validation strategy. Analysis of operators competence and real system capabilities. Analysis of real system services that meet stakeholder requirements. Comparative estimation of expenses and profits. Evaluation of achieved system quality and safety, stakeholder satisfaction. Analysis of maintenance strategy etc.

Figure 1. The problems that are due to be solved by mathematical modelling of processes



System substantiation of quantitative requirements

Requirements analysis, potential threats and vulnerabilities evaluation, evaluation of engineering decisions and possible dangers. Evaluation and verification of system operation quality

Evaluation of potential threats and vulnerabilities for system operation. Verification and validation. Parameters optimization. Substantiation for rational system improvement and development

Methods, models and software tools for effective quality and risk management

Figure 2. System engineering problems which are solved on the base of system analysis

Below the original approaches, based on the probability theory, theory of regenerative processes (see, for example [1-5] etc.) are described. As the first objects for demonstrating the offered technologies information systems (IS) are selected.

3. The models and software tools to analyze information system processes

3.1. General propositions

Requirements to IS operation depend on SYSTEM purposes and general purpose of IS operation, real conditions (including potential threats), available resources, information sources facilities and communication requirements (see *Figure 3*). This is the logical basis to create universal mathematical models to estimate the reliability and timeliness of information producing, the completeness, validity and confidentiality of the used information from users' point of view [3].

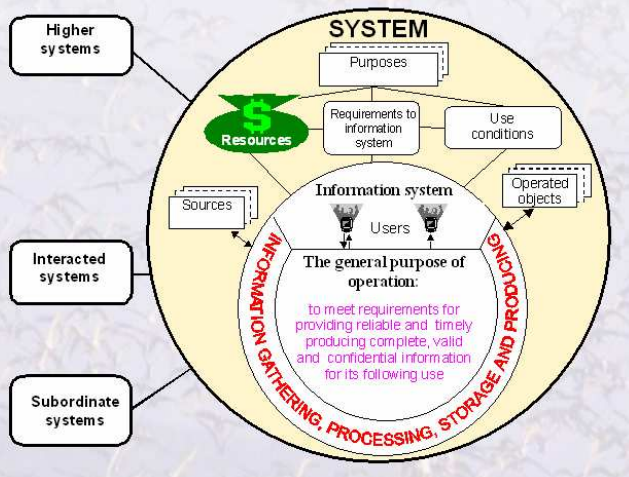

Higher systems
Interacted systems
Subordinate systems
SYSTEM
Purposes
Resources
Requirements to information system
Use conditions
Sources
Operated objects
Information system
Users
The general purpose of operation:
to meet requirements for providing reliable and timely producing complete, valid and confidential information for its following use
INFORMATION GATHERING, PROCESSING, STORAGE AND PRODUCING

Figure 3. The place and the purpose of information system in a SYSTEM

The idea of estimating IS operation quality appeared as a result of studying potential threats to output information (see *Figure 4* and example of modeling protection processes against dangerous influences in subsection 3.2). The created modeling software Complex for Evaluation of Information Systems Operation Quality, patented by Rospatent №2000610272 (CEISOQ+), allows to simplify and to spread the use of the next mathematical models: of functions performance by a system in conditions of unreliability of components; complex of calls processing; of entering into IS current data concerning new objects of application domain; complex of information gathering from sources; of information analysis; of dangerous influences on a protected system; of an unauthorized access to system resources [4]-[10].

The software tools CEISOQ+ may be applied for solving such system problems appearing in IS life cycle as: substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis; estimation of project engineering decisions and possible danger; detection of bottle-necks; investigation of problems concerning potential threats to system operation and information security; testing, verification and validation of IS operation quality; rational optimization of IS technological parameters; substantiation of plans, projects and directions for effective system utilization, improvement and development.

In general case a probabilistic space (Ω, B, P) for the evaluation of system operation processes is proposed, where: Ω - is a limited space of elementary events; B – a class of all subspace of Ω-space, satisfied to the properties of σ-algebra; P – a probability measure on a space of elementary events Ω. Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \to p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$. The proofs of the mathematical formulas used by the CEISOQ+, see in [3-10].

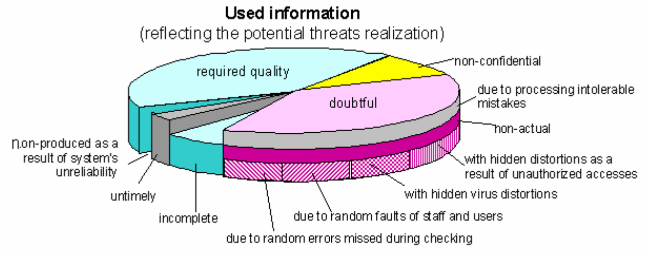


Figure 4. Potential threats to output information according to general purpose of IS operation

3.2. Example of modelling protection processes against dangerous influences

Nowadays at system development and utilization an essential part of funds is spent on providing system protection from various dangerous influences able to violate system integrity. Such dangerous influences on IS are program defects events, virus influences, influences of software bugs, violators' influences, terrorists attacks, psychological influences etc.

There are examined two technologies of providing protection from dangerous influences: proactive diagnostic of system integrity (technology 1) and security monitoring when system integrity is checked at every shift change of operators (technology 2).

Technology 1 is based on proactive diagnostics of system integrity. Diagnostics are carried out periodically. It is assumed that except diagnostics means there are also included means of necessary integrity recovery after revealing of danger sources penetration into a system or consequences of negative influences. Integrity violations detecting is possible only as a result of diagnostics, after which system recovery is started. Dangerous influences on system are acted step-by step: at first a danger source penetrates into a system and then after its activation begins to influence. System integrity is not considered to be violated before a penetrated danger source is activated. A danger is considered to be realized only after a danger source has influenced on a system. If to compare an IS with a man technology 1 reminds a periodical diagnostics of a man's health state. If diagnostics results have revealed symptoms of health worsening a man is cured (integrity is recovered). Between diagnostics an infection penetrated into a man's body brings a man into an unhealthy state (a dangerous influence is realized). The essence of protecting process architecture for the first technology is illustrated by *Figure 5*. The cases 1, 4 illustrate dangerous influences. The cases 2, 3, 5 illustrate secure system operation during period T_{req}.

Note. It is supposed that used diagnostic tools allow to provide necessary system integrity recovery after revealing of danger sources penetration into a system or consequences of influences.

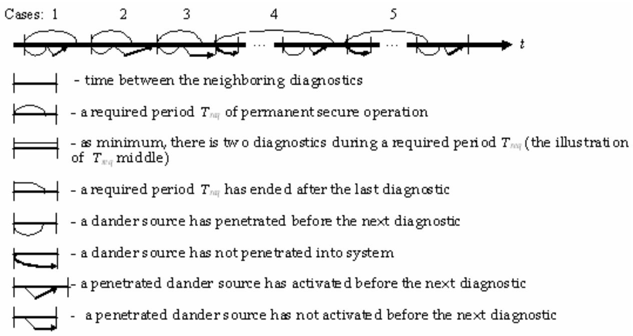

Cases: 1
2
3
4
5
t
- time between the neighboring diagnostics
- a required period T_{req} of permanent secure operation
- as minimum, there is two diagnostics during a required period T_{req} (the illustration of T_{req} middle)
- a required period T_{req} has ended after the last diagnostic
- a dander source has penetrated before the next diagnostic
- a dander source has not penetrated into system
- a penetrated dander source has activated before the next diagnostic
- a penetrated dander source has not activated before the next diagnostic

Figure 5. Abstract formalization for technology 1

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics. In case of detecting a danger source an operator is supposed to remove it recovering system integrity (ways of danger sources removing are analogous to the ways of technology 1. A penetration of a danger source into a system and its activation is possible only if an operator makes an error. Faultless operator's actions provide a neutralization of a danger source trying to penetrate into a system. When operators alternate a complex diagnostics is held. A penetration of a danger source is possible only if an operator makes an error but a dangerous influence occurs if the danger is activated before the next diagnostic. Otherwise the source will be detected and neutralized. Thus in comparison with a man technology 2 reminds a continuous staying in a hospital when between rare diagnostics a patient is permanently under medical observation of operator. A dangerous infection penetrates into a man's body only because of a doctor's fault while it may be discovered later as a result of either an exacerbation of a latent illness or the next diagnostic.

For all technologies availability of means of danger sources total-lot detecting and existence of ways of violated system integrity total-lot recovery may seem to be a very high requirement. Nonetheless, a system which can’t check and recover its integrity is a very vulnerable and knowingly doomed system.

The probability of secure system operation within the assigned period may be estimated as a result of use the next mathematical models (assumption: for all time input characteristic the probability distribution functions (PDF) exist).

There are possible the next variants for technology 1: variant 1 – the assigned period T_{req} is less than established period between neighboring diagnostics ($T_{req} < T_{betw.}+T_{diag}$); variant 2 – the assigned period T_{req} is more than or equals to established period between neighboring diagnostics ($T_{req} \geq T_{betw.}+T_{diag}$). Here $T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, T_{diag} – is the diagnostic time.

Statement 1. Under the condition of independence of considered characteristics the probability of dangerous influence absence for variant 1 is equal to

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

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source; $\boldsymbol{T_{req}}$ – is the required period of permanent secure system operation.

Statement 2. Under the condition of independence for considered characteristics the probability of dangerous influence absence for variant 2 is equal to

$$P_{\inf l.(2)} = \frac{N(T_{betw.}+T_{diag.})}{T_{req.}} \cdot P_{\inf l.(1)}{}^{N}(T_{betw.}+T_{diag.}) + \frac{T_{req.} - N(T_{betw.}+T_{diag.})}{T_{req.}} P_{\inf l.}(T_{betw.}+T_{diag.}),$$

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

*Statement 3***.** Under the condition of independence for considered characteristics the probability of dangerous influence absence for variant 1 is equal to

$$P_{\inf .(1)}(T_{req.}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{0}^{T_{req.}-\tau} d\,\Omega_{penetr.} * \Omega_{act.}(\theta). \qquad (1)$$

Here $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source; $T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic ($T_{betw.}$=*const*); $A(t)$ is the PDF of time between operator’s error; T_{diag} – is the diagnostic time ($T_{diag.}$=*const*); T_{req} – is the required period of permanent secure system operation.

Statement 4. Under the condition of independence of considered characteristics the probability of dangerous influence absence for variant 2 is equal to

$$P_{\inf .(2)}(T_{req.}) = \frac{N(T_{betw.}+T_{diag.})}{T_{req.}}$$

$$\cdot P_{wholly}{}^{N} + \frac{T_{rmn}}{T_{req.}} \cdot P_{\inf l.(1)}(T_{rmn}),$$

P_{wholly} – is the probability of dangerous influence absence within the assigned period $T_{req.}$:

$$P_{wholly} = 1 - \int_{0}^{T_{betw.}+T_{req.}} dA(\tau) \int_{0}^{T_{betw.}+T_{req.}-\tau} d\,\Omega_{penetr.} * \Omega_{activ.}(\theta), \qquad (2)$$

and $P_{infl.(1)}(T_{rmn})$ is defined above, but one is calculated not for all period T_{req}, only for the remainder time $T_{rmn} = T_{req}\text{-}N(T_{betw} + T_{diag})$.

The final clear analytical formulas for modelling are received by Lebesque-integration of (1), (2) expressions with due regard to Statements (1)-(4) [3].

4. Models, software tools and methods to analyze and optimize system processes

4.1. General approach to mathematical modelling standard processes

The idea of mathematical modelling standard processes consists in the following. Any process represents a set of the works which are carried out with any productivity at limitations for resources and conditions. This amount of works is characterized by expenses of resources (cost, material, human), accordingly works can be executed for different time with various quality. And conditions are characterized by set of the random factors influencing processes. From the point of view of probability theory and the theory of regenerating processes it is possible to put formally, that all processes on macro-and micro-levels are cyclically repeated. If to assume, that number of recurrences of such processes is very large it is theoretically we can speak about probability of any events which can occur. Time characteristics of processes, frequency characteristics of any events and characteristics, connected in due course are used as input. As final or intermediate result probabilities of "success" during a given time of forecasting or risks of failures as an addition to 1. They are used as evaluated output.

Thus the main proposition, implemented in the offered models, concludes the next: all amounts of works, characteristics of their performance, possible events and other inputs are interpreted as expense of time which can be reflected on a timeline. Probability metrics on the introduced limited space of elementary events are calculated by the rule of the probability theory [1]-[2].

The basic ideas of correct integration of probability metrics are based on a combination and development of models and consist in the following.

1st idea. As models are mathematical, the use of the same mathematical models is possible by a semantic redefinition of input and output of modelling. The idea is mentioned only for understanding the further logic in construction of modeled system, subsystems, elements and corresponding metrics on the basis of integrated modules.

2nd idea. For a complex estimation of the systems with parallel or consecutive structure existing models can be developed by usual methods of probability theory. For this purpose in analogy with reliability it is necessary to know a mean time between violations of integrity for each of element (similarly mean time between neighboring failures in reliability (MTBF), but in application to violation of quality, safety etc. For unrenowal objects this is mean time to the first failure). Further taking into account idea 1 concept of a mean time between violations of an element integrity may be logically connected (for example, redefined) in concepts of a frequency of influences for penetrating into an element and a mean activation time of a penetrated danger source. The last concepts mean characteristics of threats.

Let's consider the elementary structure from two independent series elements that means logic connection "AND" (Figure 6, left), or parallel elements that means logic connection "OR" (*Figure 6*, right).

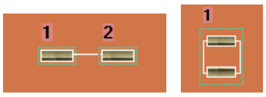


Figure 6. Illustration of system, combined from series (left) or parallel (right) elements

Let’s designate PDF of time between violations of i-th element integrity as $B_i(t) = P(\tau_i \leq t)$, then:

1) time between violations of integrity for system combined from consecutively connected independent elements is equal to a minimum from two times τ_i: failure of 1st or 2 nd elements (i.e. the system goes into a state of violated integrity when either 1st, or 2nd element integrity will be violated). For this case the PDF of time between violations of system integrity is defined by expression

$$B(t) = P(\min(\tau_1,\tau_2)\leq t)=1- P(\min(\tau_1,\tau_2)>t)$$

$$=1-P(\tau_1>t)P(\tau_2 > t)= 1 – [1-B_1(t)]\,[1- B_2(t)]. \quad (3)$$

Note. For exponential approximations:

$$B(t)=1–[1-B_1(t)][1-B_2(t)]$$

$$=1-\exp(-t/T_{MTBF1})\exp(-t/T_{MTBF2}).$$

2) time between violations of integrity for system combined from parallel connected independent elements (hot reservation) is equal to a maximum from two times τ_i: failure of 1st or 2nd elements (i.e. the system goes into a state of violated integrity when both 1st and 2nd element integrity will be violated). For this case the PDF of time between violations of system integrity is defined by expression

$$B(t)=P(\max(\tau_1,\tau_2)\leq t)$$

$$=P(\tau_1 \leq t)P(\tau_2 \leq t)=B_1(t)B_2(t) \quad (4)$$

Note. For exponential approximations:

$$B(t)=B_1(t)B_2(t)$$

$$=[1-\exp(-t/T_{MTBF1})]\,[1-\exp(-t/T_{MTBF2})].$$

Applying recurrently expressions (3) – (4), it is possible to receive PDF of time between violations of integrity for any complex system with parallel and/or consecutive structure. The illustration of threats, periodic control, monitoring and recovery of integrity for combined subsystems of estimated system is reflected on *Figure 7*.

3rd idea. Mean recovery time for system combined from consecutively connected independent elements may be calculated by expression

$$T_{rec.} = T_{rec.1}\,((1/T_{MTBF1})/\,(1/T_{MTBF1}+ 1/T_{MTBF2}))$$

$$+T_{rec.2}\,((1/T_{MTBF2})/\,(1/T_{MTBF1}+ 1/T_{MTBF2})),$$

for system combined from parallel connected independent elements

$$T_{rec.} = T_{rec.1}\,((1/T_{MTBF2})/\,(1/T_{MTBF1}+ 1/T_{MTBF2}))$$

$$+T_{rec.2}\,((1/T_{MTBF1})/\,(1/T_{MTBF1}+ 1/T_{MTBF2})).$$

Applying recurrently these expressions, it is possible to receive mean recovery time for any complex system with parallel and/or consecutive structure.

4th idea. If integrity violations are absent then diagnostic time for each element is equal on the average $T_{diag.}$. At the same time, if results of diagnostics require additional measures of integrity recovery this time increases. Thus mean time of diagnostics can be calculated iteratively with the given accuracy ε: 1-st iteration: $T_{diag.}^{(1)} = T_{diag.}$ that is given by input for modelling. I.e. for 1st iteration at detection of violation it is supposed instant recovery of integrity. Risk to lose required integrity $R^{(1)}$ is calculated (for example, by the models of subsection 3.2). Here recovery time is not considered; 2-nd iteration: $T_{diag.}^{(2)} = T_{diag.}^{(1)} (1 – R^{(1)}) + T_{rec.} R^{(1)}$, where $R_{.}^{(1)}$ is risk to lose required integrity for input $T_{diag.}^{(1)}$. Optimistic risk to lose required integrity $R^{(2)}$ is calculated; …, n-th iteration is carried out after calculating risk $R_{.}^{(n-1)}$ for input $T_{diag.}^{(n-1)}$: $T_{diag.}^{(n)} = T_{diag.}^{(n-1)} (1 – R^{(n-1)}) + T_{rec.} R^{(n-1)}$, where $R_{.}^{(n-1)}$ is risk to lose required integrity for input $T_{diag.}^{(n-1)}$. Here recovery time is considering with the frequency aspiring to real, hence risk $R_{.}^{(n-1)\,)}$ will aspire to the real. The last iteration is when the given condition is satisfied: $\left| R^{(n)} - R^{(n-1)} \right| \le ε$.

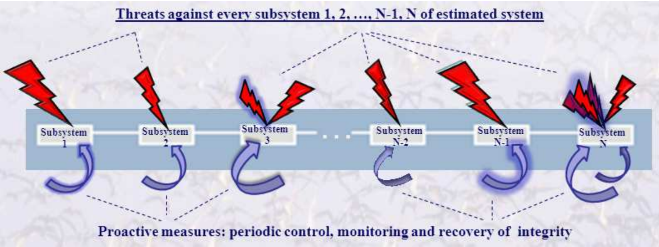

Threats against every subsystem 1, 2, …, N-1, N of estimated system
Subsystem 1
Subsystem 2
Subsystem 3
Subsystem N-2
Subsystem N-1
Subsystem N
Proactive measures: periodic control, monitoring and recovery of integrity

Figure 7. Threats, control, monitoring and recovery for combined subsystems (series elements)

5th idea. Mentioned models are applicable to the system presented as one element. The main output of such system modelling is probability of providing system integrity or violation of system integrity during the given period of time. If a probability for all points $T_{given.}$ from 0 to ∞ will be calculated, a trajectory of the PDF for each combined element depending on threats, periodic control, monitoring and recovery of integrity is automatically synthesized. The known kind of this PDF allows to define mean time of providing integrity or between violations of system integrity for every system element by traditional methods of mathematical statistics. And taking into account ideas 2-4 it gives necessary initial input for integration.

Thus, applying ideas 1-5, there is possible an integration of metrics on the level of a PDF of time of providing system integrity or violation of system integrity. And it is the base to forecast quality and risks.

Note. Ideas 2-5 are implemented in the supporting software tools [9] - see, for example, the "Complex for evaluating quality of production processes" (patented by Rospatent №2010614145).

The next complex for modelling system life cycle processes "MODELLING OF PROCESSES", patented by Rospatent №2004610858, supports more than 100 models and includes multi-functional software tools for evaluation of Agreement, Enterprise, Project and Technical Processes Modelling – see *Figure 8* [5-10].

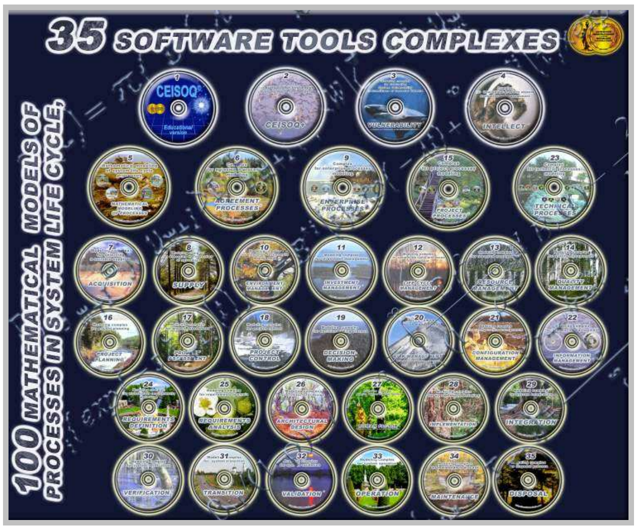


Figure 8. Complexes for modelling system processes

An application of the offered methodology uses to evaluate probabilities of "success", risks and related profitability and expenses. This helps to solve well-reasonly the next problems in system life cycle:
analysis of system use expediency and profitability, selecting a suitable suppliers, substantiation of quality management systems for enterprises, substantiation of quantitative system requirements to hardware, software, users, staff, technologies;
requirements analysis, evaluation of project engineering decisions, substantiation of plans, projects and directions for effective system utilization, improvement and development;
evaluation of customer satisfaction in system design&development and possible dangers, detection of bottle-necks;
investigation of problems concerning potential threats to system operation including protection against terrorists and information security;
verification and validation system operation quality, investigation rational conditions for system use and ways for optimization etc.

4.2. The formal statement of problems for system analysis and optimization

Classical examples of optimization generally are maximization of a prize (profit, a degree of quality or safety, etc.) at limitations on expenses or minimization of expenses at limitations on a admissible level of quality, reliability and/or safety. It is clear, that in life cycle of systems criteria and limitations vary. For security services it is necessary to provide safety of object, process or system up to the mark. In this case the criterion of a minimum of expenses at limitations on an admissible risk level of dangerous influence on system contrary to counteraction measures or a minimum of risk of dangerous influence at limitations on expenses are possible. The statement of problems for system analysis includes definition of conditions, threats and estimation a level of critical measures. As probability parameters give higher guarantees in estimations of a degree of achieving purposes in comparison with average value at a choice it is recommended to use probability as the cores. And evaluated mean time characteristics (for example the mean time between violations of admissible system operation reliability) are auxiliary. For example, there are applicable the next general formal statements of problems for system optimization:

1) on the stages of system concept, development, production and support: system parameters, software, technical and management measures (Q) are the most rational for the given period if on them the minimum of expenses ($Z_{dev.}$) for creation of system is reached

$$Z_{dev.}\,(Q_{\,rational}) = \min_{Q} Z_{\,dev.}\,(Q),$$

at limitations on probability of an admissible level of quality (reliability) $P_{quality}\ (Q) \geq\ \ P_{adm.}$ and expenses for operation $C_{oper.}\ (Q) \leq\ C_{\,adm.}$ and under other development, operation or maintenance conditions;

2) on operation stage: system parameters, software, technical and management measures (Q) are the most rational for the given period of operation if on them the maximum of probability of providing admissible system operation quality (reliability) is reached

$$P_{quality}\,(Q_{\,rational}) = \max_{Q} P_{quality}\,(Q),$$

at limitations on probability of an admissible level of quality (reliability) $P_{quality}\ (Q) \geq\ \ P_{adm.}$ and expenses for operation $C_{oper.}\ (Q) \leq\ C_{\,adm.}$ and under other operation or maintenance conditions.

Of course these statements may be identically transformed into problems of expenses or risk minimization in different limitations. System parameters, software, technical and management measures (Q) is a rule a vector of input – see examples. There may be combination of these formal statements in system life cycle.

The purposed order for use the developed formal approach to analyze and optimize system processes is illustrated by *Figure 9*.

When analyst use this approach he'd like for several minutes to formalize a problem, perform mathematical modeling, analyze system processes in different conditions, choose the most rational variant and prepare analytical report. Such possibilities exist: an analyst should perform mathematical modelling by the Internet versions of the offered models – see *Figure 10*. He prepares input and receives analytical report in Word or pdf-file about 50-100 sheets as a result of interaction. This report will be formed automatically and include a formalization of analyst's problem, input, results of mathematical modeling in pictures (as demonstrated above in examples), analysis of system processes behaviour for different conditions, choice of the most rational variant and recommendations." It means that any analyst, understanding the used mathematical model, can receive during 1-3 minutes scientifically proved analytical report after interaction with an Internet version of model.

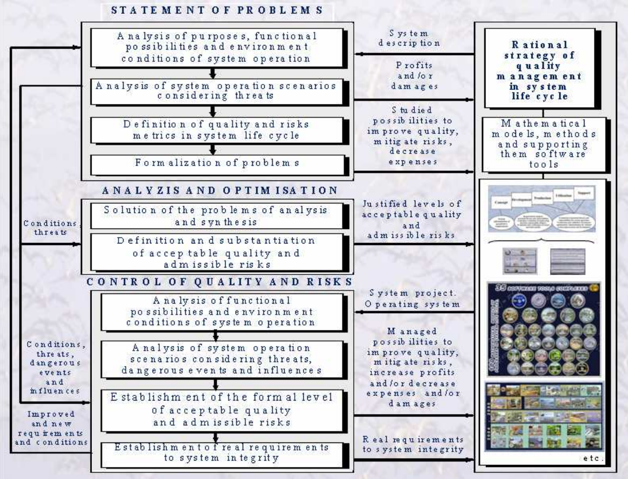
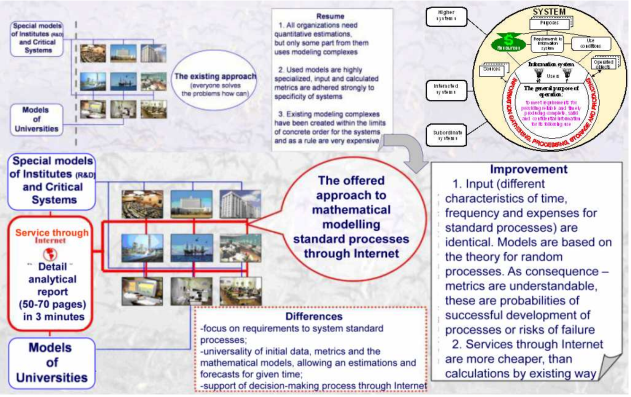

STATEMENT OF PROBLEMS
Analysis of purposes, functional possibilities and environment conditions of system operation
Analysis of system operation scenarios considering threats
Definition of quality and risks metrics in system life cycle
Formalization of problems
ANALYZIS AND OPTIMISATION
Solution of the problems of analysis and synthesis
Definition and substantiation of acceptable quality and admissible risks
CONTROL OF QUALITY AND RISKS
Analysis of functional possibilities and environment conditions of system operation
Analysis of system operation scenarios considering threats, dangerous events and influences
Establishment of the formal level of acceptable quality and admissible risks
Establishment of real requirements to system integrity
Conditions, threats
Conditions, threats, dangerous events and influences
Improved and new requirements and conditions
System description
Profits and/or damages
Studied possibilities to improve quality, mitigate risks, decrease expenses
Justified levels of acceptable quality and admissible risks
System project. Operating system
Managed possibilities to improve quality, mitigate risks, increase profits and/or decrease expenses and/or damages
Real requirements to system integrity
Rational strategy of quality management in system life cycle
Mathematical models, methods and supporting them software tools
35 SOFTWARE TOOLS COMPLEXES
etc.

Figure 9. The purposed approach to analyze and optimize system processes

It is virtual outsourcing of high system analysis on the base of the offered mathematical models. The purpose is to give to analysts an opportunity of accessible and cheap high technology of studying standard processes in life cycle of estimated systems. This work has begun, the first models are accessible (see www.mathmodels.net). Expected pragmatic effect from an application of the presented software tools is the next: it is possible to provide essential system quality rise and/or avoid wasted expenses in system life cycle on the base of modelling system processes by the offered mathematical models.


Special models of Institutes (R&D) and Critical Systems
Models of Universities
The existing approach (everyone solves the problems how can)
Higher systems
SYSTEM
Purposes
Resources
Requirement to information system
Use conditions
Sources
Information system
Uses
Operated objects
Interacted systems
Subordinate systems
The general purpose of operation:
to meet requirements for providing reliable and timely producing complete, valid and confidential information for its following use
INFORMATION GATHERING, PROCESSING, STORAGE AND PRODUCING
Special models of Institutes (R&D) and Critical Systems
Service through Internet
" Detail " analytical report (50-70 pages) in 3 minutes
Models of Universities
The offered approach to mathematical modelling standard processes through Internet

Resume
1. All organizations need quantitative estimations, but only some part from them uses modeling complexes
2. Used models are highly specialized, input and calculated metrics are adhered strongly to specificity of systems
3. Existing modeling complexes have been created within the limits of concrete order for the systems and as a rule are very expensive

Improvement
1. Input (different characteristics of time, frequency and expenses for standard processes) are identical. Models are based on the theory for random processes. As consequence – metrics are understandable, these are probabilities of successful development of processes or risks of failure
2. Services through Internet are more cheaper, than calculations by existing way

Differences
-focus on requirements to system standard processes;
-universality of initial data, metrics and the mathematical models, allowing an estimations and forecasts for given time;
-support of decision-making process through Internet

Figure 10. Mathematical modelling by the Internet versions of the offered models

Thereby necessary attributes of the offered innovative approach to control of system processes in quality management are above formed. Traditional approaches consist as a matter of fact in a pragmatical filtration of the information. In the decisions the responsible person, making decision, is guided firstly by the own experience and the knowledge and the advices of those persons of a command to whom trusts. Intuitively forming ideas which seem correct, this person chooses only that information which proves idea. The denying information is often ignored and more rare – leads to change of initial idea. This approach can be explained from the facts that at absence or limitation of used models it is difficult to investigate at once many ideas for given time. The presented models, methods and software tools, reducing long time of modelling (from several days, weeks and months to few minutes) change this situation cardinally.

The offered innovative approach is at the beginning substantiation of the system requirements, purposefully capable to lead to a success. Further, the responsible person, equipped by a set of necessary mathematical models and their software tools possibilities to forecasting quality and risks, is powered for generation of the proved ideas and effective decisions. These decisions are physically clear because of using accessible and operative analysis and optimization of processes in system life cycle. The offered approach allows to go «from a pragmatical filtration of information to generation of the proved ideas and effective decisions». The effect from implementation in system life cycle is commensurable with expenses for system creation.

5. Examples

Examples 1-5 are presented from simply to complex and based on real input for some operating systems. Example 6 is artificial hypothetic system as a combination of the systems from examples 1-5.

Example 1 («Human factor»). Let the problem solution depends on joint but independent actions of 5 people. Let each of 4 specialists make 1 error a month and the 5th inexperienced person makes 1 error a day. System recovery time after an error equals to 30 minutes. It is required to evaluate faultlessness of such group's actions within a week.

Solution. Integral computation results by CEISOQ+ reveal that the probability of faultless joint actions of the first 4 skilled specialists within a 40-hours workweek equals to 0.80 but the low-quality work of the 5th unexperienced member mocks the whole group work. Indeed, the probability of faultless actions decreases to 0.15 (see *Figure 11*).

The question is lawful - what MTBF an worker should possess to provide a faultlessness of the actions with probability 0.99 within 8 hours of the working day? According to calculations the MTBF not less than 850 working hours is acceptable. It is more than 8-hours working day in 106 times (!).

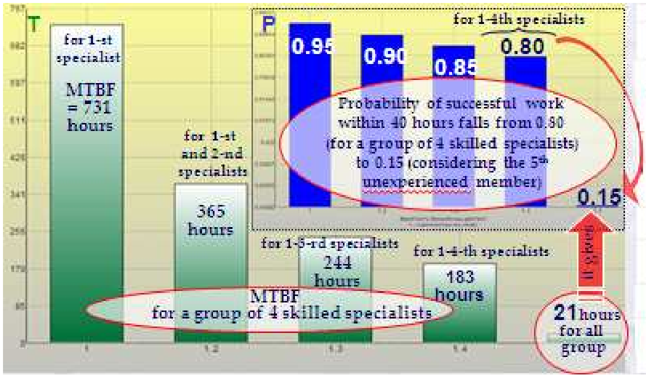


Figure 11. An estimation of human factor

Example 2 (Errors during a use of SCADA system). The control towers use SCADA system (Supervisory Control And Data Acquisition) for making decision. Wrong interpretation may be caused by errors of dispatcher personnel, which can miss important information or turn harmless information into dangerous one, fails of SCADA system. Let's consider a control station receiving information from the SCADA system. The information flow is measured in some conventional units and the information flow is of 100 units per hour. The total information contains not more than 1% of data related to potentially dangerous events. Taking into account automatic data analysis we suppose the speed of event interpretation to be near 30 sec per information unit. In this case 100 information units will be processed during 50 min. At that the frequency of errors for the whole dispatcher shift on duty, including fails of the SCADA system itself is about 1 error per year according to statistical data. The task is to estimate the risk of of mistaken analytical conclusion for a time period of 1 hour, during one dispatcher shift turn of 8 hours, 1 month, 1 year, and 10 years.

Solution. The analysis of modeling by the software tools "Complex for evaluating quality of production processes" shows (see Figure 12) that for short time periods such as one shift turn or even for a month the risk of mistaken analytical conclusion is small enough (0.00076 and 0.07 accordingly). But when the time period grows the risk increases and becomes 0.565 for a year and almost unity (0.9998) during time period of 10 years. This means that during a month the probability for errors of dispatcher personal or SCADA system fails to occur is very small and their operation will be almost faultless. But for a more long time period such as a year is considered 1-2 errors of dispatcher personal or system SCADA fails will occur for certain. Considering high reliability of SCADA system and according to "precedent" principle the level 0.07 for the risk of mistaken analytical conclusion during a month can be defined as acceptable.

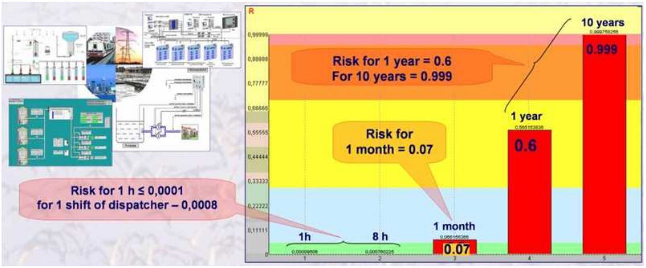


Figure 12. A results of modelling a SCADA-system

Example 3 (Fire extinguishing). An automatic system of fire extinguishing for an enterprise of dangerous manufacture operates, as a rule, on following principles: provision of multilevel protection, which highest level means a stop of all servers operation; use of diagnostic results of devices and technological equipment. The next measures are carried out for system availability to provide operation and fault tolerance: reservation of input for signals to acting; duplication of data transfer for switching-off equipment; consideration of switching-off only at the command of the safety officer (from the button); the voltage control in chains for executive mechanisms; implementation of intellectual devices with self-diagnostics; reservation of power supplies; reservation of safety control and emergency stop in conditions of failure of the basic system means. To avoid false operation after detecting a fire-dangerous situation, the automatic system of fire extinguishing starts with delay 0,5 seconds. Control from the panel of the safety officer is blocked for the period of operating the automatic system of fire extinguishing. Duration of diagnostics with possible actions of fire-prevention protection is about 8.5 seconds. Control comes back to safety officer after end of automatic system act.

Solution. Analysis of real situations allowed to form approximately the next input for modelling: frequency of occurrence of a danger source = 1 time a day, activation time of a danger source = 1 minute, the period between integrity diagnostics = 0.5c, duration of diagnostics with performance of actions of fire-prevention protection = 8.5c, MTBF for system = 2000 hours (it is commensurable with MTBF for complex technical systems and also with the period between maintenance service). Mean time to system recovery is about 1 hour. Results of modelling show the next (see *Figure 13*). At the expense of automatic monitoring and fire-prevention protection the risk of occurrence an emergency within a year equals to 0. 065, and within 2 years is nearby 0.125. The mean time between possible emergencies will be about 131590 hours (these results characterize effectiveness of the whole technology (!) of the control, monitoring and integrity recovery in the given conditions of threats).

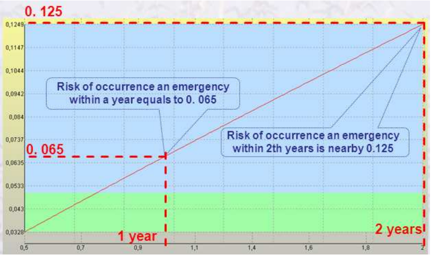


Figure 13. Dependence from the forecasting period

The reached level of risk (not above 0.065 within a year) can be de facto recognized as admissible according to "precedent" principle. At the same time, the risk of occurrence an emergency within 3 years will already exceed 0.6. This means, that at daily threats of a fire within the next 3-5 years at least one potentially emergency will be real. And moreover it can't be prevented by the operating automatic system. Here the additional measures of fire-prevention protection should be provided.

Example 4 (Reliability of engineering equipment for enterprise objects). Prediction of operation reliability of computer-aided engineering equipment against usual non-automated engineering equipment is needed for the stages "Concept" and "Development". Let the estimated object (for instance, the center of information processing and storage) includes power supply subsystem, an air conditioning subsystem, supported by 2 sources of an uninterrupted supply and a server, supported by 1 source of an uninterrupted supply and disks for information storage, supported also by 2 sources of an uninterrupted supply. In turn, the power supply subsystem includes the switchboards, supporting by 2 sources of an uninterrupted supply. All listed above engineering equipment is supported by 2 engine-generating installations.

Solution. Within the example two subsystems are allocated (see *Figure 14*): subsystem 1 – the city power supply formalized as basic and reserve subsystems; subsystem 2 – an object fragment. It is supposed, that reliability of the object operation during given period is provided, if "AND" in 1st subsystem "AND" in 2nd subsystem there will be no power supply infringements.

The analysis of modelling shows, that, at estimated technology of the control, monitoring and integrity recovery the MTBF for computer-aided engineering equipment will equal to 42219 hours. The probability of reliable object operation within a year equals to 0.828. In turn, for usual non-automated engineering equipment (there is no the monitoring implemented for computer-aided engineering equipment) efficiency characterized by estimations on *Figure 15*.

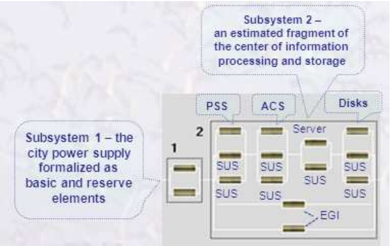

Subsystem 2 – an estimated fragment of the center of information processing and storage
Subsystem 1 – the city power supply formalized as basic and reserve elements
1
2
PSS
ACS
Disks
Server
SUS
SUS
SUS
SUS
SUS
SUS
SUS
EGI

Figure 14. Logic model (PSS - power supply subsystem, ACS - air conditioning subsystem, SUS - source of an uninterrupted supply, EGI - engine-generating installation)

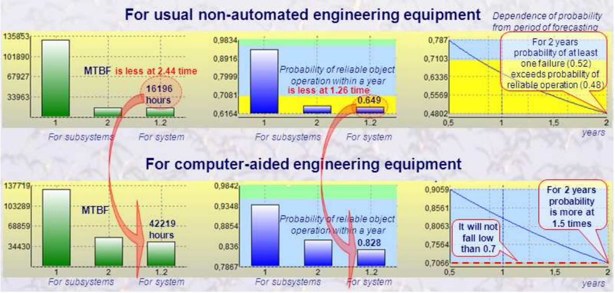


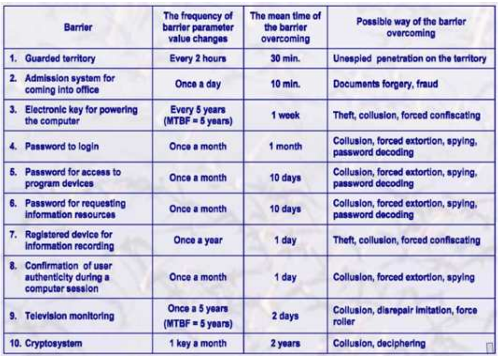
Figure 15. Results of modelling for example 4

For usual non-automated engineering equipment the MTBF will make 16196 hours (it is at 2.44 time less, than for computer-aided engineering equipment that uses monitoring), and the probability of reliable object operation within a year equals to 0.649 (at 1.26 time less, than for computer-aided engineering equipment). Moreover, without automation for 2 years the probability of at least one failure (0.52) exceeds probability of reliable operation (0.48). Against this the probability of reliable object operation within 2 years for computer-aided engineering equipment is more at 1.5 times and will not fall low than 0.7 .

Example 5 (Information security). We will consider the approach to an estimation of IS security from an unauthorized access (UAA) and information confidentiality. A resources protection from UAA is a sequence of barriers. If a violator overcomes these barriers he gets access to IS information and/or software resources. In the *Table 2* there are shown supposed characteristics of barriers and mean time of their overcoming by a specially trained violator (real values of such characteristics may be drawn as a result of actual tests or use of other models). It is required to estimate IS protection against UAA.

Solution. The analysis of computed dependencies (see *Figure 16* left) shows the next. The barriers 1,2,3 will be overcome with the probability equal to 0.63. However, monthly password changing for barriers 4, 5, 6 allows to increase the protection probability from 0.37 to 0.94 but the level of IS protection (the first six barriers) is still low. The introducing of 7,8,9 barriers is useless because it does not practically increase the level of IS protection. The use of cryptography allows to increase the level of IS protection to 0.999. This is probability for all time of IS operation (i.e. about 20-30 years). It is possible to establish a conclusion, that with the use of cryptographic devices the achieved protection level exceeds similar level of reliability and safety for processes from examples above. But according to "precedent" principle this level of protection can't be recommended as high for every cases.

Table 2. Input for modeling



Barrier	The frequency of barrier parameter value changes	The mean time of the barrier overcoming	Possible way of the barrier overcoming
1. Guarded territory	Every 2 hours	30 min.	Unespied penetration on the territory
2. Admission system for coming into office	Once a day	10 min.	Documents forgery, fraud
3. Electronic key for powering the computer	Every 5 years (MTBF = 5 years)	1 week	Theft, collusion, forced confiscating
4. Password to login	Once a month	1 month	Collusion, forced extortion, spying, password decoding
5. Password for access to program devices	Once a month	10 days	Collusion, forced extortion, spying, password decoding
6. Password for requesting information resources	Once a month	10 days	Collusion, forced extortion, spying, password decoding
7. Registered device for information recording	Once a year	1 day	Theft, collusion, forced confiscating
8. Confirmation of user authenticity during a computer session	Once a month	1 day	Collusion, forced extortion, spying
9. Television monitoring	Once a 5 years (MTBF = 5 years)	2 days	Collusion, disrepair imitation, force roller
10. Cryptosystem	1 key a month	2 years	Collusion, deciphering

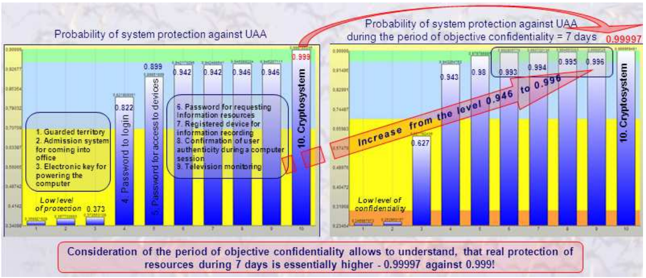


Figure 16. Comparison of protection levels

Let's look on example condition more widely. The violator is interested in a certain IS resources during a certain period of time. This period is called the period of objective confidentiality. Unlike UAA information confidentiality should be provided within these lasting 7 days. *Figure 16* (right) shows how this period influences on protection:

in comparison with the results above the use of the first 5 barriers provides confidentiality during 7 days on the level 0.98 which is more higher than protection by the 9 barriers (0.946 – see *Figure 16* left);

the use of all the 10 barriers provides the required confidentiality on the level 0.99997. It eliminates the customer's risk in providing system protection. It explains the role of a considered period of objective confidentiality – its consideration allows to understand, that real protection of resources during 7 days is essentially higher - 0.99997 against 0.999!

__Example 6__ (Forecasts of risks for complex multipurpose system). Let's consider a hypothetic multipurpose system which formally composed from a functional subsystem 1 (similar, for instance, a system mentioned in sections 2-3), gathering and data processing subsystem 2 (similar to SCADA system from example 2), subsystem 3 of fire extinguishing (from example 3), subsystems 4-5 of engineering equipment for enterprise object (from example 4), information security subsystem 6 (from example 5). «The human factor» is considered in the parameters of control, monitoring and integrity recovery measures for corresponding elements. It is supposed, that a required integrity of system is not lost, if during given time a required integrity is not lost by all subsystems: "And" by 1st subsystem, "And" by 2nd subsystem, … "And" by the last 6th subsystem. It is required to estimate the measures of risk management, including the periodic control and, where it is possible, continuous monitoring of integrity of each components – see *Figure 17*.

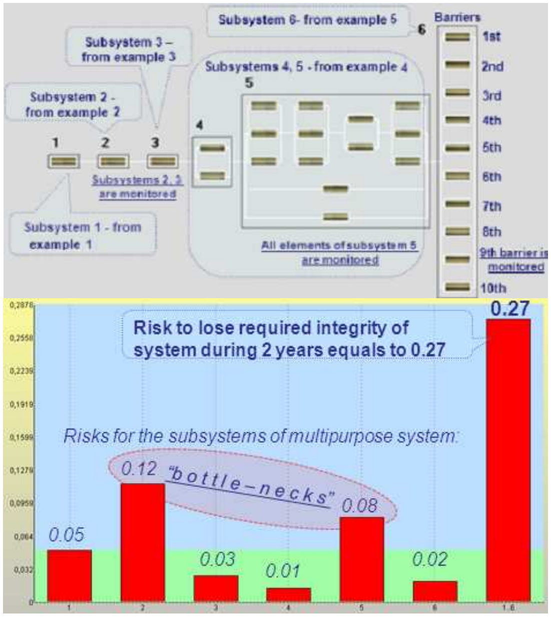

Subsystem 6- from example 5
6
Barriers
1st
2nd
3rd
4th
5th
6th
7th
8th
9th barrier is monitored
10th
Subsystem 3 – from example 3
Subsystems 4, 5 - from example 4
5
4
Subsystem 2 - from example 2
1
2
3
Subsystems 2, 3 are monitored
Subsystem 1 - from example 1
All elements of subsystem 5 are monitored
0.27
Risk to lose required integrity of system during 2 years equals to 0.27
Risks for the subsystems of multipurpose system:
0.12
"bottle–necks"
0.08
0.05
0.03
0.01
0.02

Figure 17. The formal scheme of multipurpose system, and the results of complex risks evaluation

The input for subsystem 1-6 is used from examples 1-5. The general results of risk forecasting are reflected by *Figure 18*. Analysis of results shows, that the integrated risk to lose integrity of system during operational 1 – 4 years is changing from 0.11 to 0.67 (with using of measures of the periodic control and where it is possible, monitoring of elements operation).

The general logic proposition is right for a given period of forecasting: as a rule, the risk to lose system integrity increases in depending on increasing time period. But there are the features demanding a logic explanation. Serrated and nonmonotonic character of dependence on Figure 18 is explained by the periodic diagnostics of elements, monitoring presence or absence and their quantitative values.

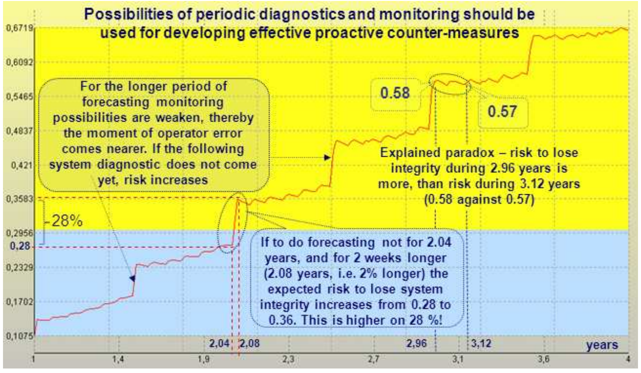


Figure 18. Integrated risk to lose integrity of system during operational 1 – 4 years

Let's remind: for every monitored element a penetration of a danger source and its activation is possible only if an operator-monitor makes an error but a dangerous influence occurs if the danger is activated before the next diagnostic. Otherwise the source will be detected and neutralized. Immediately after element diagnostic the risk decreases because during diagnostic all dangers are detected and neutralized and at the beginning of a period after diagnostic dangerous influences don't have enough time to accumulate and be activated. Nonetheless, there is a lack of protection accumulated for the previous full periods that's why the risk doesn't decrease to 0 for every element. By the middle of a period between neighboring diagnostics there is an increase of the calculated risk because new danger sources can begin to influence. Moreover, for the longer period of forecasting monitoring possibilities are weaken, thereby the moment of operator error comes nearer. And, if on timeline the following diagnostic does not come yet, risk increases. Similar effects paradoxes are explained – for example, that risk to lose integrity during 2.96 years (0.58) is more, than risk during more long time - 3.12 years, 58 days longer (0.57). One more effect of modelling: if to do forecasting not for 2.04 years, and for 2 weeks longer (2.08 years, i.e. 2% longer period) the expected risk to lose system integrity increases from 0.28 to 0.36. This is higher on 28 %! These results should serve as a substantiation for developing counter-measures, for example, by solving the problems for system analysis and optimization (see subsection 4.2).

6. Conclusion

The presented models, methods and software tools, allowing to forecast quality and risks according to system requirements of standards, are real levers to analyze and optimize system processes. The investigated practical examples demonstrated their functionality and possibilities to use "precedent principle» for definition the justified levels of acceptable quality (reliability) and admissible risks. For complex systems the proposed results helps to answer the question «What rational measures should lead to estimated effect without waste expenses, when, by which controllable and uncontrollable conditions and costs?» and allows to go «from a pragmatical filtration of information to generation of the proved ideas and effective decisions». The effect from implementation in system life cycle is commensurable with expenses for system creation.

7. References

[1] Gnedenko, B.V. et al. (1973). *Priority queueing systems*, MSU, Moscow, 448p.

[2] Klimov, G.P. (1983). *Probability theory and mathematical statistics*. MSU, Moscow.

[3] Kostogryzov, A.I., Petuhov, A.V. & Scherbina, A.M. (1994). *Foundations of evaluation, providing and increasing output information quality for automatized system*. Moscow: Moscow: Armament. Policy. Conversion (APC).

[4] Bezkorovainy, M.M., Kostogryzov, A.I. & Lvov, V.M. (2001). *Modelling Software Complex for Evaluation of Information Systems Operation Quality CEISOQ*. Moscow APC.

[5] Kostogryzov, A. & Nistratov, G. (2004). *Standardization, mathematical modelling, rational management and certification in the field of system and software engineering*. Moscow APC.

[6] Kostogryzov, A. & Stoiljković, V. (2007). *Applicable methods to analyze and optimize system processes*. Moscow APC.

[7] Kostogryzov, A.I. & Stepanov, P.V. (2008). *Innovative management of quality and risks in systems life cycle*. Moscow. APC.

[8] Grigoriev, L.I., Kershenbaum, V.Ya. & Kostogryzov, A.I. (2010). *System foundations of the management of competitiveness in oil and gas complex*. Moscow: National Inst. of oil & gas.

[9] Kostogryzov, A. et al. (2011). Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems. *Proceedings of the 1st Intern. Conf. on Transportation Information and Safety (ICTIS),* Wuhan, China, Vol. 2, 845-854.

[10] Kostogryzov, A. et al. (2012). *Some applicable methods to analyze and optimize system processes in quality management*. InTech, ISBN979-953-307-778-8.