ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields

Andrey KOSTOGRYZOV, George NISTRATOV, Andrey NISTRATOV
Research Institute of Applied Mathematics and Certification, Moscow, Russia

Abstract - The paper is concerned with the development of the original probability models and supporting them software technologies to analyze and optimize system processes. Functionality and usability to analyze processes of threats development, information processing, situation control, system monitoring and integrity repairing are presented. Rational use of the proposed models and software technologies allows to predict effectiveness in system life cycle and optimize system operation. Effects are demonstrated by some examples of researches, applications and comparisons based on predicted quality and risks. The spectrum of the analyzed systems includes systems of government agencies, manufacturing structures (including enterprises, oil-and-gas and hazardous production systems), power generation, food storage, aviation and space industry, emergency services, municipal economy, military, etc.

***Index Terms*— Analysis, Effect, Optimization, Process, Quality, Risk, System.**

I. INTRODUCTION

For various application fields the system processes are the main objects for improvement of system operation. Existing practices for providing system quality and safety were reviewed and analyzed, including approaches of system standards of series ISO 9000, 14000, 18000, 22000, 27000, 31000, ISO/IEC 15288, IEC 60300, 61508, CMMI etc. In general case risk prediction should be founded on the probability modeling of system processes. Really, any process is a repeated sequence of consuming time and resources for outcome receiving. The moments for any activity beginning and ending are, as a rule, 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, analysis etc.) during system life cycle - for example see on Figure 1 the problems that are due to be and can be solved by the probability modelling of processes according to ISO/IEC 15288 "System engineering. Processes of system life cycle".

As a result of analyzing practice approaches to safety (to industrial, fire, radiating, nuclear, chemical, biological, transport, ecological systems, safety of buildings and constructions, information security etc.) we made the next conclusions. For the fields of industrial, fire, radiating, nuclear, aviation safety in which already there were numerous facts of tragedies - requirements to admissible risks are expressed quantitatively at probability level and qualitative at level of necessary requirements to the initial materials, used resources, protective technologies and operation conditions. GGenerally risk estimations from one field do not use in others fields because of methods and metrics for risk analysis are different, interpretations are not identical in spite of processes are logically similar. For the fields of chemical, biological, foods, transport, ecological safety, safety of buildings and constructions, information security etc. – requirements to admissible risks are set mainly at qualitative level in the form of requirements to performance. The analytical methods for quantitatively risk analysis are in creating yet. The term "Admissible risk" can't be defined because of one depend on methods. Experience from other fields is missing because of methodologies are different, interpretations are not identical. The methods for quantitative quality and risk analysis on probability level are in creating stage yet.

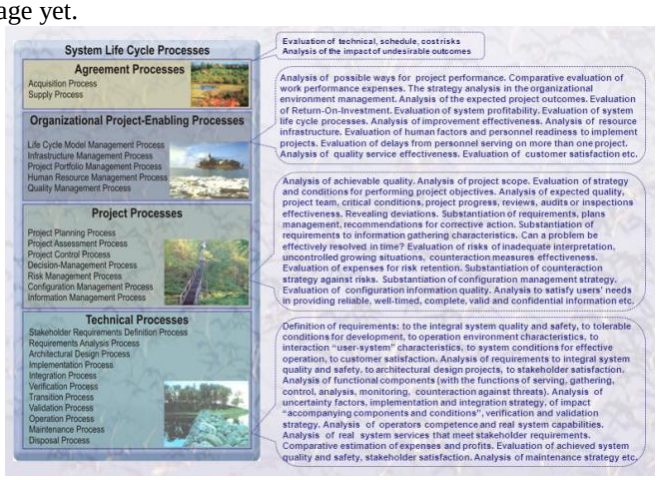

Fig. 1: The problems that are due to be and can be solved by probability modelling of processes (A.Kostogryzov [11])

To improve essentially this situation the offered way includes probability models and applicable technologies to predict, analyze and optimize different risks for complex systems. This work focuses on the way for using universal metrics in a system processes: 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 predicting risks on an uniform probability scale. The prediction of risks can use widely monitoring data and statistics. In general case a probabilistic space (Ω, B, P) to evaluate system operation processes should

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

be built, 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 $\omega_k \rightarrow p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$.

The offered probability models can be used in system life cycle to form system requirements on probability level, compare different processes, substantiate system engineering decisions, carrying out tests, adjust technological parameters, estimate quality and risks and provide system effects. The idea is based on probability modeling standard processes and 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 risks. And conditions are characterized by set of the random destabilizing 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 large, and theoretically we can speak about probability of events which can occur in time line. Time characteristics of processes, frequency characteristics of any events and characteristics, connected in due course are general for any application fields and used as input. As final or intermediate result probabilities of "success" during a given time or risks to lose system integrity are used as evaluated output. It allows to analyze and optimize processes for system in various fields.

II. Development of Probability Models for Risk Prediction

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

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 is the next [1]-[3]. Requirements to Information Systems (IS) operation depend on SYSTEM purposes and general purpose of IS operation, real conditions, available resources, information sources facilities and communication requirements. This offered approach was implemented in standard GOST RV 51987 "Information technology. Set of standards for automated system. The typical requirements and metrics for information systems operation quality. General provisions". The models to predict quality and risks is supported by software Complex for Evaluation of IS Operation Quality, patented by Rospatent №2000610272 (CEISOQ+) [2]-[3]. Since 2000 the CEISOQ+ supports the next probability models in sytem life cycle: 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 - see Figure 2.

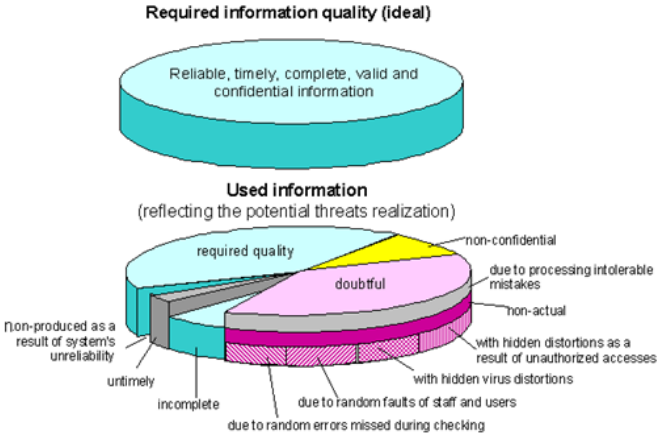

Fig. 2: Potential threats to output information according to general purpose of IS operation in a SYSTEM (A.Kostogryzov [1]-[4], [9]-[11])

B. Examples of modeling 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 (these may be failures, defects events, "human factors" events, terrorist's attacks, etc). There are examined two general technologies of providing protection in different spheres: proactive periodical diagnostics of system integrity (technology 1) and additionally monitoring between diagnostics (technology 2), researches are in [4]-[7], [9]-[12]. Technology 1 is based on proactive diagnostics of system integrity, that are carried out periodically to detect danger sources penetration into a system or consequences of negative influences. The lost system integrity can be detect only as a result of diagnostics, after which system recovery is started. Dangerous influence on system is acted step-by step: at first a danger source penetrates into a system and then after its activation begins to influence. System integrity can't be lost before a penetrated danger source is activated. A danger is considered to be realized only after a danger source has influenced on a system.

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. 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 recovers system integrity (ways of danger sources removing are analogous to the ways of technology 1). Faultless operator's actions provide a neutralization of a

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

danger source trying to penetrate into a system. When operators alternate a complex diagnostic 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 during the next diagnostic.

The probability of correct system operation within the given prognostic period (i.e. probability of success) may be estimated as a result of use the next models (assumption: for all time input characteristic the probability distribution functions (PDF) exist). Risk to lose integrity (safety, quality or separate property, for example – reliability) is an addition to 1 for probability of providing system integrity (correct system operation or "probability of success") R=1-P.

There are possible the next variants for technology 1 and 2: variant 1 – the given prognostic 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.

The next statements are proposed (Author – A. Kostogryzov [1]-[7], [9]-[12]).

Statement 1 (for technology 1). Under the condition of independence of considered characteristics the probability of providing system integrity for variant 1 is equal to

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

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.

Statement 2 (for technology 1). Under the condition of independence for considered characteristics the probability of providing system integrity for variant 2 is equal to

$$P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\, P_{(1)}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (2)$$

where $N=[\, T_{req.}/(T_{betw.}+T_{diag.})]$ – is the integer part, $T_{rmn} = T_{req} - N(T_{betw}+T_{diag})$. The probability of success within the given time $P_{(1)}(T_{given})$ is defined by (1).

Statement 3 (for technology 2). Under the condition of independence for considered characteristics the probability of correct system operation for variant 1 is equal to

$$P_{(1)}(T_{req}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{\tau}^{T_{req.}} d\,\Omega_{penetr} * \Omega_{act.}(\theta), \quad (3)$$

Here $A(t)$ is the PDF of time between operator's error.

Statement 4 (for technology 2). Under the condition of independence of considered characteristics the probability of providing system integrity for variant 2 is equal to

$$P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\, P_{(1)}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (4)$$

where the probability of success within the given time $P_{(1)}(T_{given})$ is defined by (3).

The final clear analytical formulas for modelling are received by Lebesque-integration of (3) expression.

Note. There may be another measure to estimate $P_{(2)}(T_{req})$ for both technologies 1 and 2, for example $P_{(2)}(T_{req}) = P_{(1)}^{N}(T_{betw}+T_{diag})\, P_{(1)}(T_{rmn})$.

Many models are applicable to the system presented as one element. The main result of such system modelling is probability of providing system integrity (correct system operation) or of losing 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 time is automatically synthesized. The known kind of this PDF allows to define mean time of providing integrity or between losing of system integrity for every element by traditional methods of mathematical statistics. It is the analog of mean time between failures (MTBF) from reliability theory. Thus, there is input for calculating metrics on the level of a PDF of time of providing system integrity (or time between neighboring losses of integrity). And it is the real theoretical foundation for risk prediction on PDF-level.

C. The idea of modelling complex system operation

The basic ideas of correct integration of probability metrics are based on a combination and development of the offered models [4]-[7], [9]-[12]. For a complex system estimation with parallel or serial 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 losing integrity for each element (similarly mean time between neighbouring failures (MTBF) from reliability theory, but in application to lose quality, safety etc. For unrenowal objects this is mean time to the first failure). Let's consider the elementary structure from two independent parallel elements that means logic connection "OR" or series elements that means logic connection "AND".

Let's PDF of time between losses of i-th element integrity is $B_i(t) = P(\tau_i \leq t)$, then:

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

$$B(t) = P(\min(\tau_1,\tau_2) \leq t) = 1 - P(\min(\tau_1,\tau_2) > t) = 1 - P(\tau_1 > t)P(\tau_2 > t) = 1 - [1-B_1(t)]\,[1-B_2(t)]. \quad (5)$$

2) Time between losses 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 broken integrity when both 1st and 2nd element integrity will be broken). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\max(\tau_1,\tau_2) \leq t) = P(\tau_1 \leq t)P(\tau_2 \leq t) = B_1(t)B_2(t). \quad (6)$$

Applying recurrently expressions (5) – (6), it is possible to receive distribution of time between losses of integrity for any complex system with parallel and/or series structure.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

Note. The same approach is developed by Prof. K.Kolowrocki [8].

III. SOFTWARE TECHNOLOGIES

More than 100 probability models of system processes and their proof are presented on www.mathmodels.net . Software technologies, based on complex "Modelling of processes" (Rospatent №2004610858), "Complex for evaluating quality of production processes" (Rospatent №2010614145), supporting offered models, including above models, are used to analyze and optimize processes for system in various fields [5]-[6] – see Figures 3-7 (A.Kostogryzov [4], [9]-[12]).

Fig. 3: Software Complexes for modelling system operation

For example the next complex "MODELLING OF PROCESSES" includes multi-functional software tools for evaluation of various standard processes: Agreement processes (models and software tools "ACQUISITION", "SUPPLY"), Enterprise processes (models and software tools "ENVIRONMENT MANAGEMENT", "INVESTMENT MANAGEMENT", "LIFE CYCLE MANAGEMENT", "RESOURCE MANAGEMENT", "QUALITY MANAGEMENT"), Project processes (models and software tools "PROJECT PLANNING", "PROJECT ASSESSMENT", "PROJECT CONTROL", "DECISION-MAKING", "RISK MANAGEMENT", "CONFIGURATION MANAGEMENT", "INFORMATION MANAGEMENT") and Technical processes Modelling (models and software tools "REQUIREMENTS DEFINITION", "REQUIREMENTS ANALYSIS", "ARCHITECTURAL DESIGN", "HUMAN FACTOR ", "IMPLEMENTATION", "INTEGRATION", "VERIFICATION", "TRANSITION", "VALIDATION", "OPERATION", "MAINTENANCE", "DISPOSAL" tools) – see Figures 4-7 (one separate box is an implementation of one or more original probability models [1]-[7]). And all models allows answer engineering questions from Figure 1.

Fig. 4. Ssoftware tools for evaluation of Agreement Processes

Fig. 5. Software tools for evaluation of Enterprise Processes

Fig. 6. Software tools for evaluation of Project Processes

Fig. 7. Software tools for evaluation of Technical Processes

The first approach of risk prediction is based on usual technology, supported by the offered probability models and software tools.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

The another offered innovative technology is based on modified software tools applications using Internet. When analyst uses this technology 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 some mathematical modelling by the Internet versions of the offered models – see Figure 8 (A. Kostogryzov [9]-[12]). User 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, analysis of system processes behavior 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.

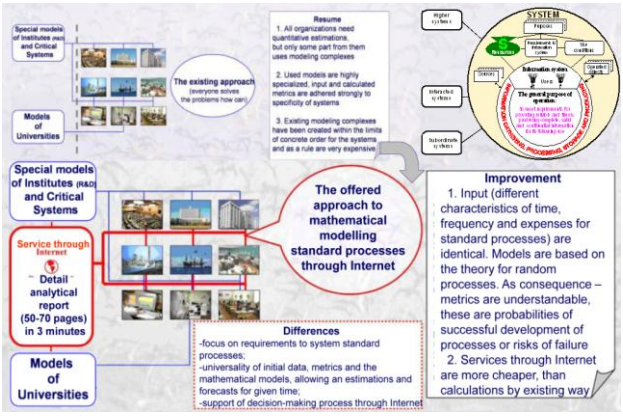

Fig. 8: Mathematical modelling by the Internet

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, reduce risks and/or avoid wasted expenses in system life cycle on the base of modelling system processes by the offered mathematical models.

IV. THE FORMAL STATEMENT OF PROBLEMS FOR SYSTEM ANALYSIS AND OPTIMIZATION

Classical examples of optimization 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 acceptable level of risk or admissible level of quality, reliability and/or safety in some limitations. For example, 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 (A. Kostogryzov [3]-[7]):

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 for them the minimum of expenses ($Z_{dev.}$) is reached

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

at limitations on risks to lose integrity $R \le R_{accept}$, the probability of correct system operation (on admissible level of quality) $P_{quality}(Q) \ge P_{adm.}$ and expenses for operation $C_{oper.}(Q) \le C_{adm.}$ 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 for them the minimum of risks to lose integrity or/and the maximum of probability of correct system operation (on admissible level of quality) is reached at limitations on acceptable risks to lose integrity R_{accept}, probability of an admissible level of quality $P_{quality}(Q) \ge P_{adm.}$ and expenses for operation $C_{oper.}(Q) \le C_{adm.}$ and under other operation or maintenance conditions.

$$R(Q_{rational}) = \min_{Q} R(Q),$$

or/and

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

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 models of part 2 and 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 (A. Kostogryzov [9]-[12]).

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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

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.

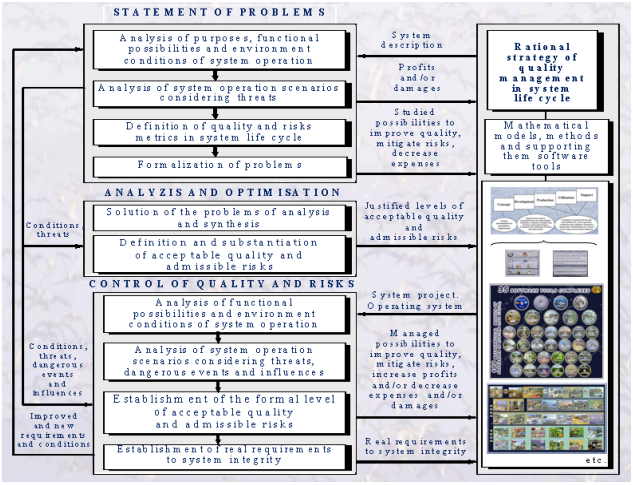

Fig. 9: The purposed approach to analyze and optimize system processes

As a matter of fact traditional approaches for system analysis and optimization consist 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.

V. EXAMPLES OF APPLICATIONS AND COMPARISONS FOR SYSTEM OPERATING IN VARIOUS FIELDS

Example 1 concerns estimation of the possibilities of dispatcher performing control and monitoring operations for a system element. Let a frequency of critical situations is 3 events per year, the mean time of situation evolution before damaging is 1 hour. The system integrity is confirmed on a central control center once in a day while the dispatcher shifts are changed. Duration of integrity control is 1 hour on average, the mean time between mistakes for the shift of monitoring to be 1 week or more.

What about the risk to lose system element integrity during 1 month (columns 1, 4), 1 year (columns 2, 5), 10 years (columns 3, 6); integrity control and recovery time 1 hour (columns 1-3) and 10 days (columns 4-6)?

Dependency of the risk for 1 year as input data varying in the range of -50% +100% (variant 5: period of integrity control and recovery =10days) is reflected on Figure 6. Serrated and nonmonotonic character of dependence on Figure 10 (A. Kostogryzov [12]) is explained by the periodic diagnostics of elements, monitoring presence or absence and their quantitative values (because of $N=[\ T_{req.}/(T_{betw.}+\ T_{diag.})]$ – is the integer part).

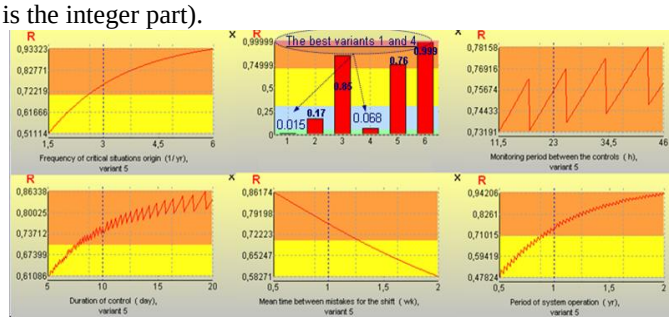

Fig. 10: Predicted risk for 1 year in dependences of input data varying in the range of -50% +100%

Analysis of modeling results show: to decrease risks the mean time between mistakes for the dispatcher personnel should be increased, the time of carrying out control and repairing damages should be shorten to several days or even hours.

Example 2 (Reliability of engineering equipment for enterprise object fragment). Prediction of operation reliability of computer-aided engineering equipment against usual non-automated one is needed for the stages “Concept”, “Development” and “Utilization” of system life cycle. Let the analyzed object (for instance, the center of information processing and storage) includes a power supply subsystem (PSS), an air conditioning subsystem (ACS), supported by 2 sources of uninterrupted supply (SUS) and a server, supported by 1 SUS and disks for information storage, supported also by 2 SUS. In turn, PSS includes the switchboards, supporting by 2 SUS. All listed above engineering equipment is supported by 2 engine-generating installations (EGI). What about the comparison of variants?

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

The solution is based on the modelling complex processes, considering against existing models the possibilities of monitoring, periodic control and recovering the lost integrity - see Figures 11, 12.

The analysis of modelling results 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 MTBF that is equal to 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 (see Figure 12, A. Kostogryzov [11]-[12])).

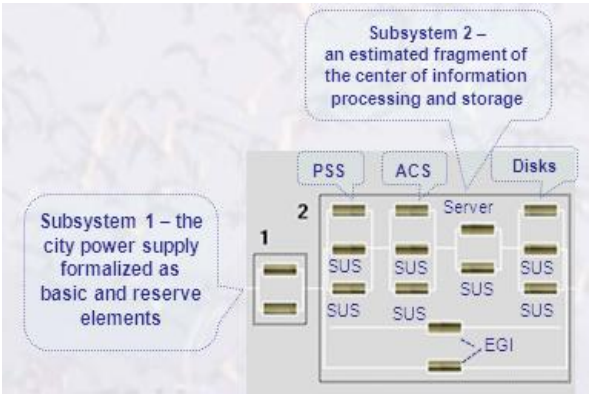

Fig. 11: Logic structure of analyzed system

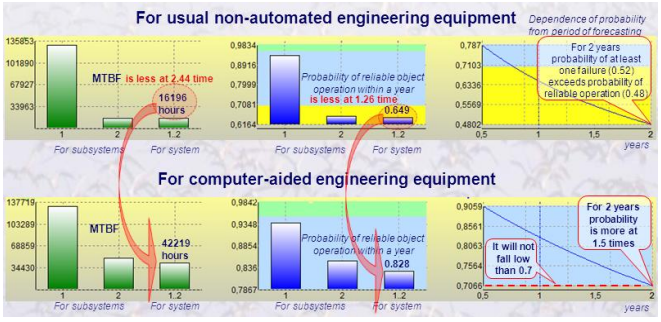

Fig. 12: Probability of correct operation within 1 year

Example 3 (flights safety in conditions of terrorist threats). We understand that a system component of the global terrorism problems can't be fully studied within any monograph. Nevertheless, we'll offer an approach, which allows to estimate quantitatively and compare some organizational and technical ways of its solution within quality management (safety aspect). From the modelling point of view a flying airplane is a protected system operating in conditions of threats to its integrity during the flight. We'll try to answer the next questions: "How effective was the existing before 09/11 system of flights safety provision in Russia and the USA from the point of view of opposing to terrorists?" and "How this level of the safety may be increased and by what measures?"

The answers are based on the use of software tools "Complex for evaluating quality of production processes" [3]-[7].

To gather necessary input data for modelling let's recall pictures of the some acts of terrorism. One of these is a high jacking of the Russian airliner Tu-154 (the company "Vnukovo" airlines) on March 15, 2001. And it is a terrorist attack on the USA committed on September 11 with the help of several passenger airliners.

The passenger airliner Tu-154 was flying from Istanbul to Moscow with 162 passengers on board. Three terrorists armed with cold steel captured the airliner and threatening with a bomb blowing-up made the pilots fly to Medina (Saudi Arabia). All terrorist attempts to break open the door to the cockpit failed. The pilots not controlled by the terrorists explained the situation on board, terrorists' maneuvers, necessary details concerning the airliner arrangement before the start of a rescue operation. Moreover, they secretly communicated with stewardesses situated in the plane cabin. On March 16 Arabian troops of special purposes made an attempt to capture the airliner. A Russian stewardess, Julia Fomina, who was fatally wounded during that storm, opened a ramp. At the cost of her life she rescued lives of the passengers. From the moment of high jacking till the moment of capturing there passed about 24 hours.

In September an unprecedented attack was committed on the USA. That attack killed thousands of people. Two skyscrapers of the World Trade Center were rammed by two passenger airliners "Boeing-767" and "Boeing-757" (the company American Airlines), captured by terrorists on their flights from Boston to Los Angeles (92 people on board) and from Washington to Los Angeles (64 people on board). The Pentagon was attacked by " Boeing-76" (the company "United Airlines") flying from Newark (New Jersey) to San Francisco (45 people on board).

Now we go to modelling of unauthorized access to airliner resources. From the point of view of terrorists opposing formalization the existing system of security provision represents a sequence of technological barriers, which should be overcome. What are the barriers?

For the existing before 09/11 safety system it is: the 1st barrier is pass and inter-object modes in aerodromes and centers of air traffic control; the 2nd barrier is a preflight examination and control of passengers and their luggage during the registration; the 3rd barrier is a preflight examination before boarding; the 4th barrier is a lock-up door to the cockpit; the 5th barrier is an on-line warning about a high jacking (this barrier is critical if terrorists try to hide the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

fact of high jacking). It is clear that the first three barriers if a passenger behaves well are conditional because terrorists reveal their criminal nature only on board an aircraft. Moreover, the character of the last terrorism acts proves that among terrorists there are trained executors. The terrorist actions are worked out in details.

Taking the above considerations into account we'll form input data for modelling. At first we'll discuss time of barriers overcoming. For a trained terrorist (not "wanted", having valid documents and luggage) both in Russia and in the USA mean time of the 1st barrier overcoming equals to 10 minutes necessary for identification (m=1). For an untrained terrorist the main task is not to be taken into those who are checked by security service of the aerodrome. Let only 0.5% of passengers be checked. This check may result in imprisonment during 10 days. This means that mean time of a barrier overcoming equals to ≈ 1.36 hours.

To evaluate input characteristics of the 2nd and the 3rd barriers we'll analyze the existing facts and specialists' reports. On one hand prevention of guns and explosives carrying through customs in the USA seems to be rather reliable. From the other hand carrying of penknives with blade length up to 8 centimeters had been officially allowed before September 11. On September 11 the terrorists were armed with knives for cutting of thick carton ("cutters"). Moreover, American specialists in terrorism-fighting cite facts when in 2000 employees of the USA Department of Transport decided to check 8 American airports for their vigilance. They could carry bags with guns in 68 cases of 100 ones. Finally in several shops of airports there were sold knives-souvenirs, which are brought right to the airline ladder, i.e. without any control. In Russia the situation was not better. It was worsened by the fact that in some airports modern systems of electronic examination are not used. Let's assume that a fraction of such airports mounts to 30%. The above-mentioned allows to state that for a trained terrorist overcoming of the 2nd and 3rd barriers in the USA takes about 2 hours (for each barrier) and in Russia – 1 hour. The same actions will take an untrained terrorist 10 days appeared as a result of his/her imprisonment. Then in the USA mean time of a barrier overcoming equals to ≈ 3.3 days and in Russia it equals to ≈ 2.6 days. Mean time of pass and examination in the airport is not less than a year before any essential change happens (usually before a next serious incident and start of an appropriate fight for providing airports security). The authors of the monograph know about real control service on local airlines of the USA and Russia not through hearsay. Thus the input data necessary for computations concerning the first three barriers may be considered to be formed.

The 4th and 5th barriers are the only barriers on board an airliner. A cockpit door in American Airlines "Boeing" is usual. It can be broken within a few minutes. This was done to rescue pilots in case of a catastrophe. For the same purpose some airliners take off and land with open doors. To make it clear let's set mean time of the "Boeing" 4th barrier overcoming equal to 15 minutes. A door of a Russian airliner is armored. Impossibility of such a door breaking within a few hours allowed avoiding more grave consequences on March 15. Nonetheless, according to the specialists' opinion it is not a great difficulty to blow it up or open it with the help of a fire extinguishing ax or a forcer. Let's assume that using additional improvised means it takes not more than 2 hours to overcome this barrier.

Russian aircraft are furnished with a special button of reporting about a high jacking. Not all foreign airliners are furnished with such a button and terrorists may cut off the communication with the Earth. According to specialists it is possible to escape radars by reducing height to its critical point and sharp changing of an airliner's course. On Earth it is possible to guess that an airliner is high-jacked only on the basis of indirect signs: a disappeared communication, a change of course, strange maneuvers. Sometimes passengers may use mobile phones what happened on September 11 in the USA. So, let's set time of preventing a warning about the highjacking equal to flight time. Results of modelling are on Figure 13 (A. Kostogryzov [3]-[6], [11]-[12]).

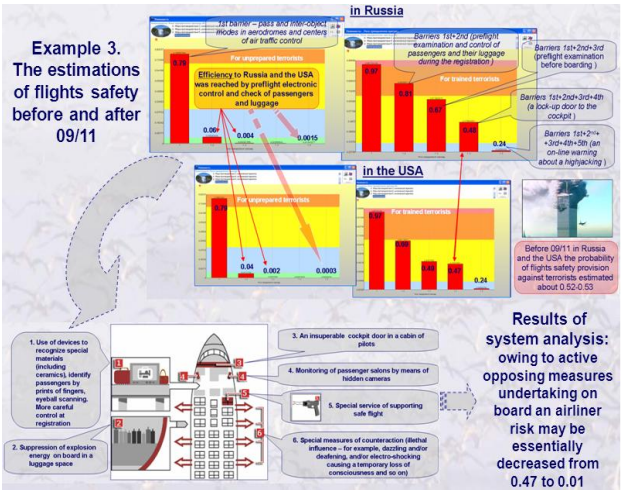

Fig. 13: Results of modeling for example 3

An analysis of computation results reveals the following: both in Russia and the USA the existing systems of flights safety provision are very effective against inexperienced or untrained terrorists (the probability of security provision is not less than 0.99). It is achieved owing to preflight electronic examination and control of passengers and their luggage; the probability of flights safety provision in Russia and in the USA consisting in preventing of trained terrorists' penetration into a cockpit is practically the same: it equals to 0.52-0.53. In case of on-line warning about a high jacking and owing to this warning a possibility of essential opposing to terrorists this probability increases to 0.76. In Russia an armored door is the essential obstacle and in the USA it is a modern electronic examination system. According to the computations both in Russia and the USA the probability of terrorist's goals achievement in case of a thorough preliminary training is unacceptably high.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

The drawn frightening figures (0.52-0.53) mean that the time of "single terrorists" has passed. They may act only on local airlines of developing countries where are no means of electronic examination and control of passengers. The computations allow with a high degree of confidence to come to the conclusion that all the taken place terrorist acts were committed after their thorough preliminary planning and preparing.

Applications of the offered probability models and software technologies cover systems in various fields: systems operated by government agencies, manufacturing structures (including enterprises, oil&gas and transport facilities, and hazardous production systems), food storage, power generation, financial and business, aviation and space industry, emergency services, municipal economy etc. (www.mathmodels.net).

VI. Conclusion

The innovative probability models and software technologies of risks prediction are offered. Their applications in Russia (for systems operated by government agencies, manufacturing structures (including enterprises, oil&gas and transport facilities, and hazardous production systems), food storage, power generation, financial and business, aviation and space industry, emergency services, municipal economy etc.) show: they are real levers to analyze and optimize system processes and improve complex systems in various fields. It allows to the customer to formulate well-reasoned system requirements, and to developer - to execute them without excessive expenses of resources, and to the user – as much as possible effectively to implement in practice the incorporated power of system. The offered results help to go «from a pragmatical filtration of information (traditional approach) to generation of the proved ideas and effective decisions (innovative approach) » for solving complex engineering problems.

REFERENCES

[1] Kostogryzov A.I., Petuhov A.V. and Scherbina A.M. "Foundations of evaluation, providing and increasing output information quality for automatized system", Moscow, "Armament. Policy. Conversion", 1994, 278p. (in Russian).

[2] Kostogryzov A.I. "Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)." Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.

[3] Bezkorovainy M.M., Kostogryzov A.I. and Lvov V.M., "Modelling Software Complex for Evaluation of Information Systems Operation Quality CEISOQ. 150 problems of analysis and synthesis and examples for their solutions", Moscow, "Armament.Policy.Conversion", 2002, 305p. (in Russian).

[4] Kostogryzov A., Nistratov G. "Standardization, mathematical modelling, rational management and certification in the field of system and software engineering", Moscow, "Armament.Policy.Conversion", 2004, 395p. (in Russian).

[5] Kostogryzov A.I., Nistratov G.A., "100 Mathematical Models of System Processes According International Standards Requirements". Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models. Majority, Italy, University of Solerno, Italy, pp. 196-201, 2005.

[6] Kostogryzov A.I., Stepanov P.V., Innovative management of quality and risks in systems life cycle, Moscow, "Armament. Policy. Conversion", 2008 , 404p. (in Russian).

[7] Grigoriev L.I., Kershenbaum V.Ya. and Kostogryzov A.I. "System foundations of the management of competitiveness in oil and gas complex, Moscow, National Institute of oil and gas", 2010, 374p. (in Russian).

[8] K.Kolowrocki and J.Soszynska-Budny "Reliability and Safety of Complex Technical Systems and Processes", DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited, 2011, 405p.

[9] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. "Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems", Proceedings of the 1st International Conference on Transportation Information and Safety（ICTIS 2011), Wuhan, China, pp. 845-854, June 2011

[10] Kostogryzov A., Nistratov A., Nistratov G. "Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems" // Proceedings of the 6st International Summer Safety and Reliability Seminar, Poland, Volume 3, Number 1, pp. 1-14, September 2012

[11] Andrey Kostogryzov, George Nistratov and Andrey Nistratov, "Some Applicable Methods to Analyze and Optimize System Processes in Quality Management", Total Quality Management and Six Sigma, InTech, pp. 127-196, August 2012. Available from: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[12] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. "Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes", American Journal of Operations Research, Special Issue, Volume 3, Number 1A, pp.217-244, January 2013, Available from: http://www.scirp.org/journal/ajor/

AUTHOR'S PROFILE

Andrey Kostogryzov - Honored Science Worker of the Russian Federation, Dr. of Engineering Science, Professor, Corresponding Member of the Russian Academy of Rockets and Artillery Sciences, Russian Academy of Natural Sciences, Full Member of Russian Academy of Informatization in Education. Lenin Komsomol Prize Winner in the Field of Science and Engineering. The Winner of Research Award from the Russian President for Scientific School in system quality and safety (2004-2005).

Director and Scientific leader of the Research Institute of Applied Mathematics and Certification (RIAMC), General Director of the Center of Standardization, Design and Development for Information-Communication Technologies and Systems ("INFOSTANDARD"), the Main Researcher of the Institute of Informatics Problems of the Russian Academy of Sciences, Professor of the Gubkin Russian State University of Oil and Gas and the Moscow State Technical University of Radio engineering, Electronics and Automatics. The Member of the Expert Council of Russian Higher Attestation Committee, Chairman of Subcommittee "Information Security" of the Chamber of Commerce and Industry of the Russian Federation, Chairman of Subcommittee "System and Software Engineering" and Deputy

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 3, September 2013

Chief of the National Russian Technical Committee "Information Technologies", Member of Interbranch Council of the Russian Union of Industrialists and Enterpreneurs (RUIE) for Technical Regulation, Standardization and Conformity Estimation in Information Technology, Certified Expert of Gosstandard of Russia.

The author more than 100 mathematical models and dozens effective software tools complexes for analyzing and prediction quality and risks and more than 150 scientific proceedings, including 16 books.

George NISTRATOV - PhD of Engineering Science. Chief of the Software Department of the Research Institute of Applied Mathematics and Certification. The co- author of dozens effective software tools complexes for analyzing and prediction quality and risks and more than 30 scientific proceedings, including 2 books.

Andrey NISTRATOV - PhD of Engineering Science. The Main Researcher of the Software Department of the Research Institute of Applied Mathematics and Certification. The co- author of effective software tools complexes for analyzing and prediction quality and risks and more than 20 scientific proceedings, including 1 book.