Improvement of Existing Risks Control Concept for Complex Systems by
the Automatic Combination and Generation of Probabilistic Models and
Forming the Storehouse of Risks Predictions Knowledge

Andrey KOSTOGRYZOV1,2,3,*, Pavel STEPANOV1, Leonid GRIGORIEV2,
Oleg ATAKISHCHEV3, Andrey NISTRATOV4 and George NISTRATOV5

1Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences,
Vavilova Str. 44, Bld.2, Moscow, Russia, 119333
2The Gubkin Russian State University of Oil and Gas, Leninsky Pr. 65, Moscow, Russia, 119991
3Main Scientific Research Test Center (MSRTC) of the Russian Ministry of Defence,
Seriogina Str. 5, Moscow, Russia, 119001
4The Russian Power Agency of Ministry for the Power Generating Industry,
Schepkina Str .40, bl.1, Moscow, Russia, 129110
5The Research Institute of Applied Mathematics and Certification,
Krasnobogatyrskaja 2, Bld.2, Moscow, Russia, 107564
*Corresponding author

Keywords: Combination, Generation, Model, Optimization, Probability, Risk, System, Technology.

Abstract. The purposed approach to improve existing risks control concept includes: creation and
perfection of probabilistic models for problems decision; automatic combination and generation of
new probabilistic models; forming the storehouse of risks predictions knowledge; for storehouse -
dozens variants of the decision of typical industrial problems for risks control.

Introduction
In different areas the heterogeneous threats for complex systems are inevitable. The uncertainties
in system life cycle are usual. Different problems, connected with evaluations, comparisons,
selections, controls, system analysis and optimization, are due to be solved by the probabilistic
modelling of processes according to system engineering standards ISO/IEC/IEEE 15288, ISO 9001,
IEC 60300, IEC 61508, CMMI, some standards for use in the oil&gas industry (ISO 10418, 13702,
14224, 15544, ISO 15663, ISO 17776 etc.). An existing risks control concept tries to consider
different uncertainties. But in application for various areas the results of information gathering and
processing are not used purposefully for modeling, because of the used models of risks prediction,
that are used in majority of complex systems, are specific, results and interpretations are not
comparable. For heterogeneous threats an analytical rationale of the balanced preventive measures of
system integrity support at limitations on admissible risks and resources can’t be solved in many
cases. The storehouse of risks predictions knowledge is not formed.

These lacks define actuality of scientific efforts to improve existing risks control concept for
complex systems, because of this allows a customer to formulate better justified requirements and
specifications, a developer - to implement them rationally without wasted expenses, a user – to use
system potential in the most effective way [1-4].

Review of Universal Probabilistic Models to Improve Concept

General Propositions for Information Systems (IS)
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. 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 – see Figure 1.

The proposed analytical models and calculated measures are the next [1-2]: “The model of functions performance by a complex system in conditions of unreliability of its components” (the measures: \(T_{MTBF}\) - the mean time between failures; \(P_{MTBF}\) - the probability of reliable operation of IS, composed by subsystems and system elements, during the given period; \(P_{man}\) - the probability of providing faultless man’s actions during the given period); “The models complex of calls processing (the measures for the different dispatcher technologies (for unpriority calls processing in a consecutive order for singletasking processing mode, in a time-sharing order for multitasking processing mode; for priority technologies of consecutive calls processing with relative and absolute priorities; for batch calls processing; for combination of technologies above): the mean wait time in a queue; the mean full processing time, including the wait time; \(P_{tim}\) - the probability of well-timed processing during the given time; the relative portion of all well-timed processed calls; the relative portion of well-timed processed calls of those types for which the customer requirements are met); “The model of entering into IS current data concerning new objects of application domain” (the measure: \(P_{compl}\) - the probability that IS contains complete current information about states of all objects and events); “The model of information gathering” (the measure: \(P_{actual}\) - the probability of IS information actuality on the moment of its use); “The model of information analysis” (the measures: \(P_{check}\) is the probability of errors absence after checking; the fraction of errors in information after checking; \(P_{process}\) - the probability of correct analysis results obtaining; the fraction of unaccounted essential information); “The models complex of dangerous influences on a protected system” (the measures: \(P_{inf.l}\) - the probability of required counteraction to dangerous influences from threats during the given period); “The models complex of an authorized access to system resources” (the measures: \(P_{prot}\) - the probability of providing system protection from an unauthorized access by means of barriers; \(P_{conf.}\) - the probability of providing information confidentiality by means of all barriers during the given period).

These models, supported by different versions of software Complex for Evaluation of Information Systems Operation Quality, patented by Rospatent №200610272 (CEISOQ+), may be applied for predicting risks to lose system integrity in IS life cycle [2].

**General Propositions for “Black Box” System Before Integration**

There are proposed two general technologies of providing protection from critical influences on IS quality or/and safety: technology 1 - periodical diagnostics of system integrity (without the continuous monitoring between diagnostics) and technology 2 – continuous monitoring between periodical diagnostics is added to technology 1 – see Figure 2.

Technology 1 is based on periodical diagnostics of system integrity, that are carried out to detect danger sources penetration from threats (destabilizing factors) 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 from threats (destabilizing factors) is considered to be realized only after a danger source has influenced on a system.

Technology 2 = Technology 1 + monitoring between diagnostics

Figure 2. Some accident events for technology 2 (left – “correct operation”, right – “a loss of integrity” during Treq.).

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics (operator may be a man or special device or their combination). In case of detecting a danger source an operator recovers system integrity. The ways of integrity recovering are analogous to the ways of technology 1. Faultless operator’s actions provide a neutralization of a 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.

It is supposed for technologies 1 and 2 that the used diagnostic allows to provide necessary system integrity recovery after revealing danger sources penetration into a system or consequences of influences. Assumption: for all time input characteristic the probability distribution function (PDF) exists. Thus the probability of correct system operation within the given prognostic period (i.e. probability of success) may be computed as a result of use the models. For the identical damages risk to lose integrity is an addition to 1 for probability of correct system operation R=1-P [3-4].

There are possible the next variants for technology 1 and 2: variant 1 – the given prognostic period Treq is less than established period between neighboring diagnostics (Treq < Tbetw.+Tdiag); variant 2 – the assigned period Treq is more than or equals to established period between neighboring diagnostics (Treq ≥ Tbetw.+Tdiag). Here Tbetw. – is the time between the end of diagnostic and the beginning of the next diagnostic, Tdiag – is the diagnostic time.

Integration of Probabilistic Models

The main output of integration modelling for each element is probability of correct system operation or risk to lose system integrity during the given period of time. If probabilities for all points Treq from 0 to ∞ are computed, it means a trajectory of the PDF depending on characteristics of threats, periodic control, monitoring and recovery. And the building of PDF is the real base to prediction measures P and R for given time Treq. In analogy with reliability it is important to know a mean time between neighboring losses of integrity like mean time between neighboring failures in reliability (MTBF), but in application to quality, safety etc.

For complex systems with parallel or serial structure existing models with known PDF can be developed by usual methods of probability theory. Let’s consider the elementary structure from two independent parallel or series elements. Let’s PDF of time between losses of i-th element integrity is B_i(t), i.e. B_i(t) = P (τ_i ≤ t), then:
1) time between losses of integrity for system combined from series connected independent elements is equal to a minimum from two times $\tau_i$: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when either 1st, or 2nd element integrity is lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = \Pr(\min(\tau_1, \tau_2) \leq t) = 1 - \Pr(\min(\tau_1, \tau_2) > t) = 1 - \Pr(\tau_1 > t) \Pr(\tau_2 > t) = 1 - (1 - B_1(t))(1 - B_2(t));$$  \hspace{1cm} (1)

2) time between losses of integrity for system combined from parallel connected independent elements (hot reservation) is equal to a maximum from two times $\tau_i$: failure of 1st and 2nd elements (i.e. the system goes into a state of lost integrity when both 1st and 2nd elements have lost integrity). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = \Pr(\max(\tau_1, \tau_2) \leq t) = \Pr(\tau_1 \leq t) \Pr(\tau_2 \leq t) = B_1(t)B_2(t).$$  \hspace{1cm} (2)

Applying recurrently expressions (4) – (5), it is possible to build PDF of time between losses of integrity for any complex system with parallel and/or series structure.

All these ideas for analytical modelling operation processes are supported by the software tools “Mathematical modelling of system life cycle processes” – “know how” (registered by Rospatent №2004610858), “Complex for evaluating quality of production processes” (registered by Rospatent №2010614145) and others [1-4].

The Improvement of Existing Risks Control Concept

The purposed approach to improve existing risks control concept includes [4] (see Figure 3):

- creation and perfection of probabilistic models for problems decision;
- automatic combination and generation of new probabilistic models;
- forming the storehouse of risks predictions knowledge;
- for storehouse - dozens variants of the decision of typical industrial problems for risks control.

**Figure 3. The purposed approach to improve existing risks control concept.**

For example system, combined from complex interested system and IS (see Figure 4), can be analyzed by the formula (1) and probabilistic models. The correct operation of this system of system
during the given period means: during given period of prediction both the 1-st and the 2-nd complex systems should operate correctly. I.e. integrated system is in the state “Integrity (correct operation)” if “AND” the system left “AND” the system right are in the state “Integrity (correct operation)”. 

![Figure 4. System of two different complex systems (serial combination) for integration modelling.](image)

About pragmatic effect – rational application of the proposed automatic combination and generation of probabilistic models and forming the storehouse of risks predictions knowledge for Complex of supporting technogenic safety on the systems of oil&gas transportation and distribution, implemented in 200 systems in several regions of Russia during the period 2009-2014 have already provided economy about 8,5 Billions of Roubles [4].

Summary
The proposed improved risks control concept can be useful to do effectively: risks prediction; rationale 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 operation of complex systems; validation of system operation quality; rational optimization of system parameters; rationale of plans, projects and directions for effective system utilization, improvement and development. Expected pragmatic effect is the next: it is possible to provide essential system quality and security rise and/or avoid wasted expenses in system life cycle on the base of rational application of improved concept.

References
[1] A. Kostogryzov, and G. Nistratov, Standardization, mathematical modeling, rational management and certification in the field of system and software engineering (100 mathematical models, 35 software tools), Moscow: “Armament. Policy. Conversion”, 2004, 395 p.

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

[3] A. Kostogryzov, P. Stepanov, A. Nistratov, G. Nistratov, O. Atakishchev and V. Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling. Proceedings of the 2016 International Conference on AMSM, May 28-29, 2016, Beijing, China, pp. 186-192.

[4] V. Akimov, A. Kostogryzov, N. Mahutov, P. Stepanov at al. Security of Russia. Legal, Social & Economic and Scientific & Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of N. Mahutov N.A. – Moscow, “Znanie”, 2015, 936 p.