About probabilistic risk prediction for system engineering. Models, applications, effects

Andrey Kostogryzov

Federal Research Center "Computer Science and Control"
of the Russian Academy of Sciences, Main Scientific Research Test Center of the Russian Ministry of Defence, Moscow, Russia,
Akostogr@gmail.com

Abstract. The paper is concerned with the development and application of the original probabilistic models of risks prediction for complex systems. The practical examples demonstrate possibilities to decide the different problems of analysis and optimization for system engineering. The pragmatic effects are viewed.

Keywords: Analysis, model, prediction, reliability, risk, safety, system, system engineering

1 Introduction

The knowledge and results of risk prediction for system engineering allows a customer to formulate substantiated requirements and specifications, a developer - to implement them rationally without wasted expenses, a user – to use system possibilities 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 general case system methods for analyzing and optimizing are founded completely on the mathematical modelling of system processes. As a rule process may be presented as 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 and risks prediction according to ISO/IEC 15288 (see also [1-7] in different applications).

This work focuses on using universal metrics in a systems life cycle (probability to lose system integrity considering possible damage as metric for risk prediction during

a given period for an element, subsystem, system or probabilities of success), applications and effects.

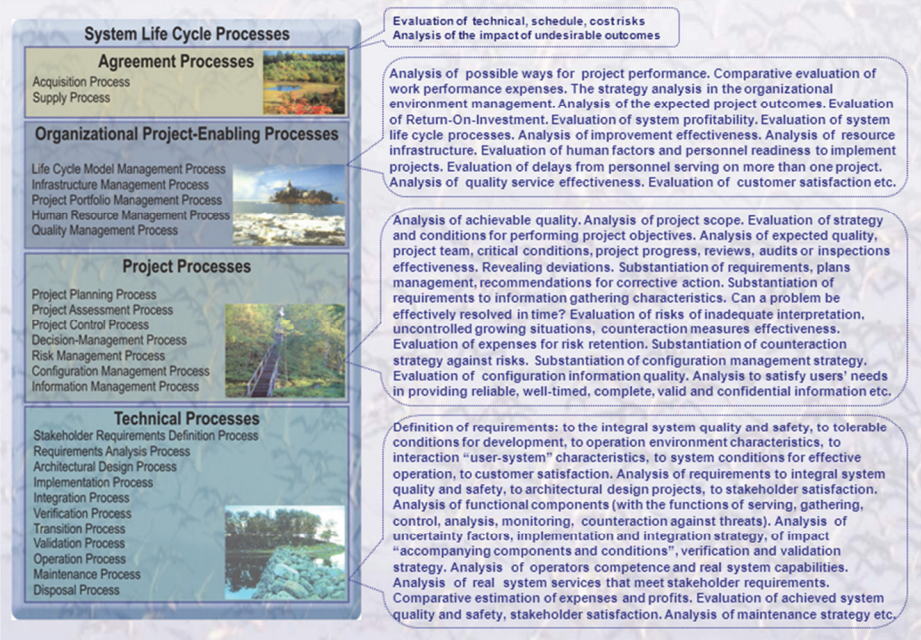

Fig. 1. The problems that are due to be solved by mathematical modelling of processes

2 Probabilistic models for risk prediction

Nowadays in system development and utilization an essential part of funds is spent on providing system protection from various dangerous influences on system integrity (these may be failures, defects events, "human factors" events etc). There are examined two general technologies of providing protection from critical influences: periodical diagnostics of system integrity (technology 1, without monitoring between diagnostics) and additionally monitoring between diagnostics (technology 2).

Technology 1 is based on periodical diagnostics of system integrity, that are carried out to detect danger sources penetration into a system or consequences of negative influences (see Figure 2). 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.

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 tools allow 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 functions (PDF) exist. Thus 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. Risk to lose integrity is an addition to 1 for probability of correct system operation ("probability of success") R=1 – P.

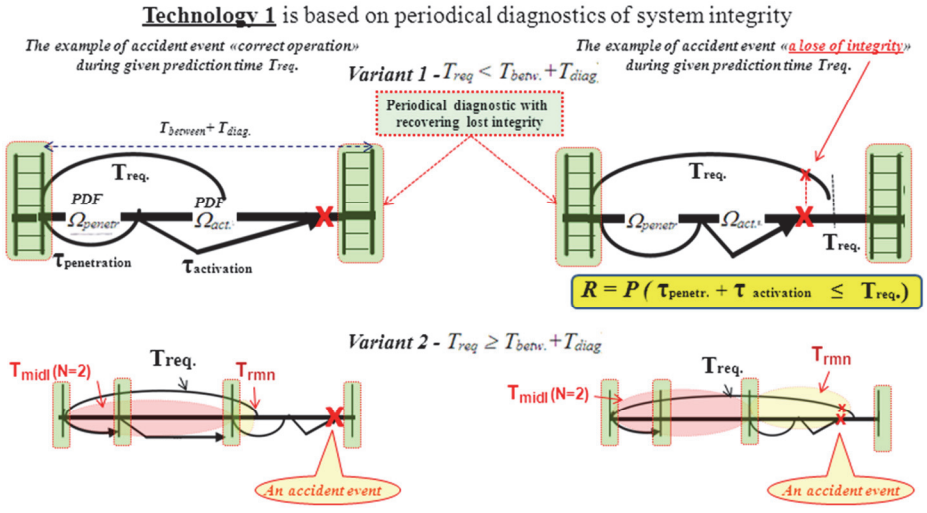

Fig. 2. Some accident events for technology 1 (left – correct operation, right – a lose of integrity during prognostic period $T_{req.}$)

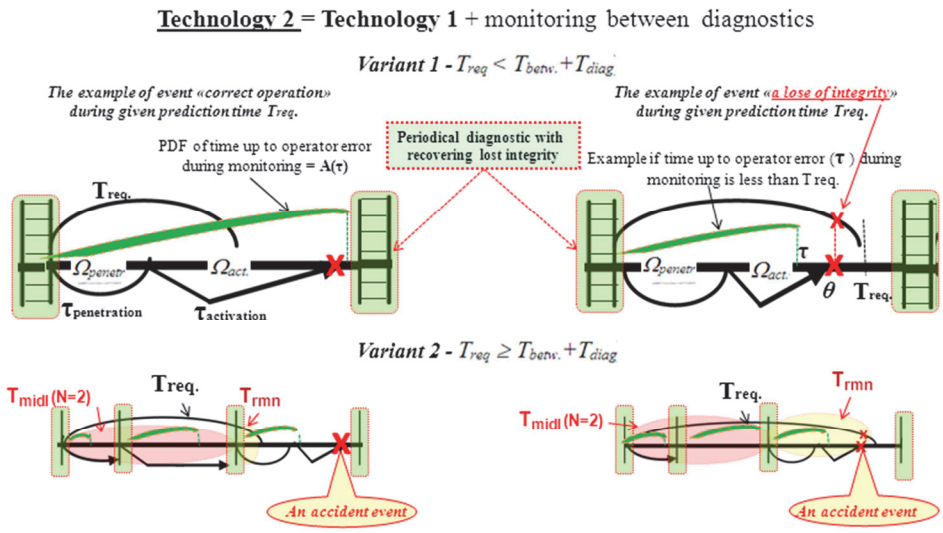

Fig. 3. Some accident events for technology 2 (left – correct operation, right – a lose of integrity during prognostic period $T_{req.}$)

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.

For the given period for prediction ($T_{req.}$) the next statements are proposed (see [6-7]).

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 Ωpenetr(t) – is the PDF of time between neighboring influences for penetrating a danger source; Ωactiv(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 may be equal to:

measure a)

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

where N=[Treq./(Tbetw.+ Tdiag.)] – is the integer part, Trmn = Treq - N(Tbetw +Tdiag);

measure b)

$$P_{(2)}(T_{req})=P_{(1)}^{N}(T_{betw}+T_{diag})P_{(1)}(T_{rmn}). \quad (3)$$

The probability of success within the given time P(1)(Tgiven) 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

$$P_{(1)}(T_{req})=1-\int_{0}^{T_{req.}} dA(\tau)\int_{\tau}^{T_{req.}} d\,\Omega_{penetr}*\Omega_{act.}(\theta) \quad (4)$$

Here A(t) is the PDF of time from the last finish of diagnostic time up to the first operator error.

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

measure a)

$$P_{(2)}(T_{req}) = N((T_{betw} + T_{diag})/T_{req})\, P_{(1)}^{N}(T_{betw} + T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (5)$$

measure b)

$$P_{(2)}(T_{req}) = P_{(1)}^{N}(T_{betw} + T_{diag})\, P_{(1)}(T_{rmn}), \quad \text{(see (3))},$$

where the probability of success within the given time P(1)(Treq) is defined by (4).

The final clear analytical formulas for modelling are received by Lebesque-integration of (4) expression with due regard to Statements 1-4.

The models are supported by software tools [3-7].

Comments: the measure a) allows to perform latent knowledge mining in the possibilities and impacts of every control because N is integer part. The measure b) allows to mine latent knowledge by average value of probability on the level of classical PDF.

3 The generation of new probabilistic models for risk prediction

The basic ideas of correct integration of probability metrics are based on a combination and development of models [3-7]. For a complex systems with parallel or serial structure existing models 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 Bi(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 τi: 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

$$B(t) = P(\min(\tau_1,\tau_2) \le t) = 1 - P(\min(\tau_1,\tau_2) > t) = 1 - P(\tau_1 > t)P(\tau_2 > t) = \\ = 1 - [1 - B_1(t)]\,[1 - B_2(t)], \quad (6)$$

2) time between losses of integrity for system combined from parallel connected independent elements (hot reservation) is equal to a maximum from two times τi: 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

$$B(t) = P(\max(\tau_1,\tau_2) \le t) = P(\tau_1 \le t)P(\tau_2 \le t) = B_1(t)B_2(t). \quad (7)$$

Applying recurrently expressions (6) – (7), it is possible to build PDF of time between losses of integrity for any complex system with parallel and/or series structure.

4 The examples of applications and effects

The presented approach of risk prediction allows to solve problems of system analysis and optimization. Expected pragmatic benefit from its application 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.

Example 1. Let's analyze a fragment of the main gas pipeline Bovanenkovo-Ukhta (more than 1200 km) by probabilistic modelling of natural and technogenic processes. It constructed over an earth surface. Subfragments between compressor stations (9 stations - Bajdaratsky, Jarynsky, Gagaratsky, Vorkuta, Usinsk, Intinsky, Syninsky, Chikshinsky, Maloperansky) are allocated. There are serial subsystems and every subsystem has parallel structure of elements (pipeline) - see Figure 4.

About 75-90% from the pipelines are under natural threats, including ice drift (threats for constructions). It is required to estimate risk to lose integrity (quality of operation) of fragment Bovanenkovo-Ukhta in 2023-2043.

The solving of a problem is the next [8]. According to estimations of experts, in 20-30 years there will be considerable changes of climatic conditions which will cause rise in temperature of frozen thicknesses, increase in depth seasonal thawing and, as consequence, decrease in stability and bearing ability of the bases for a gas pipeline and other engineering constructions.

Technical characteristics of elements between compressor stations are considered as identical, except for the first subfragment (between stations Bajdaratsky and Jarynsky) which is underwater transition (reservation by 4 elements-pipelines) – see Figure 5. Initial data for modelling have been generated depending on conditions of concrete sites and specificity of a territorial arrangement of a line.

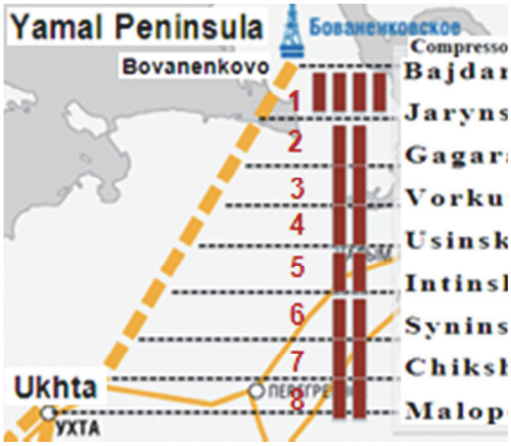

Fig. 4. The analyzed fragment of the main gas pipeline

Fig. 5. The serial-parallel structure for modelling processes

Results of modelling processes have shown, that risk to lose integrity (quality of operation) for 20 prognostic years during the period 2023-2043 is equal to 0,6-0,8. In comparison with other precedents these figures speak about expediency of undertaking of preventive measures, and also about necessity of working out of the Plan of emergencies liquidation.

If period between system controls will be reduced from 6 to 3 months the risk to lose integrity in 2023-2043 is nearby 0,16-0,44. It is twice more low, rather than for an existing mode of maintenance and repair. On the basis of these results the following recommendations are scientifically proved:

- to establish a risk level to lose integrity (quality of operation) 0,38 within 10 years of operation as admissible (on the base of «precedent principle»);
- to pass to the quarterly control of a condition of system after 10 years of operation (i.e. since 2024);
- to use annual planning of maintenance measures service on the basis of modelling processes for rational risk management in admissible limits.

Example 2. The Complex (as a part of global system) of risks predictions for technogenic safety support on the objects of oil&gas distribution has been awarded by Award of the Government of the Russian Federation in the field of a science and technics for 2014. The created peripheral posts are equipped additionally by means of Complex to feel vibration, a fire, the flooding, unauthorized access, hurricane, and also intellectual means of the reaction, capable to recognize, identify and predict a development of extreme situations – see engineering decisions on Figure 6.

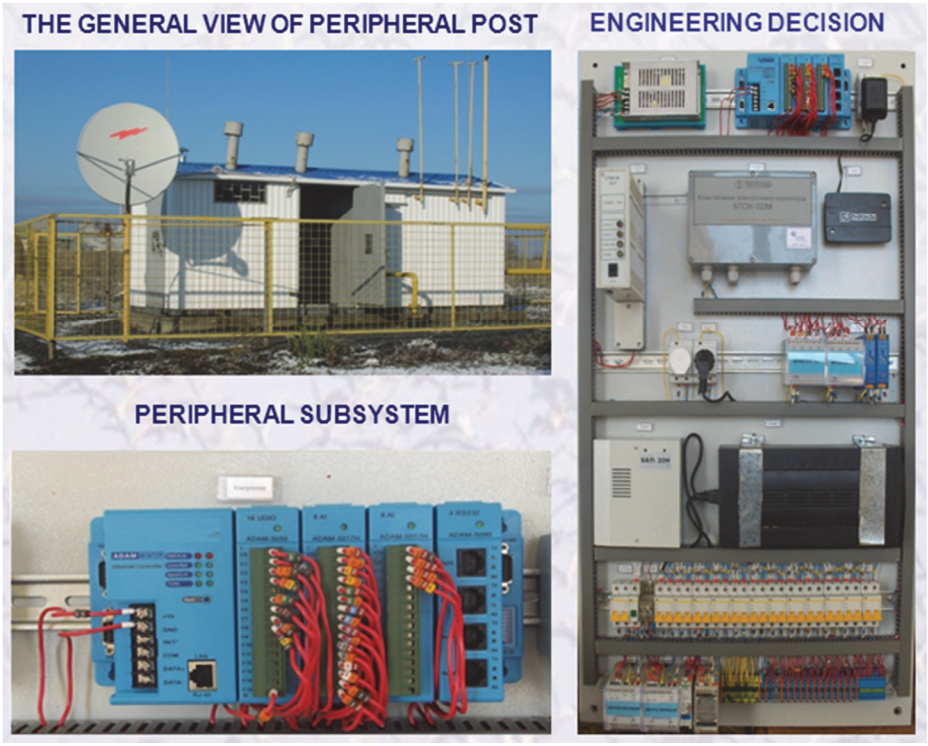

Fig. 6. The Complex of supporting technogenic safety on the objects of oil&gas distribution

The applications of Complex for 200 objects in several regions of Russia during the period 2009-2014 have already provided economy about 8,5 Billions of Roubles. The economy is reached at the expense of effective implementation of the functions of risks prediction and processes optimization [9].

5 Conclusion

An application of the proposed approach allows to solve well-reasonly the next problems in system life cycle: analysis of quality and safety level, substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis, evaluation of engineering decisions, system utilization, improvement and development; analysis of problems concerning potential destabilizing factors and/or threats against quality and safety; prediction of bottle-necks; verification and validation system operation quality, definition of rational conditions for system use and ways for optimization, evaluation of customer satisfaction.

The efficiency from implementation in system life cycle is commensurable with expenses for its creation [1-9].

References

1. Kostogryzov, A.I., Petuhov, A.V. & Scherbina, A.M. 1994. Foundations of evaluation, providing and increasing output information quality for automatized system. Moscow: "Armament. Policy. Conversion"
2. Kostogryzov, A.I. 2000. 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: 63-70. USA: Dallas.
3. Kostogryzov, A.I. & Nistratov, G.A. 2005. 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"
4. Kostogryzov, A.I. & Stepanov, P.V. 2008. Innovative management of quality and risks in systems life cycle. Moscow: "Armament. Policy. Conversion"
5. Kostogryzov, A., Krylov, V., Nistratov, A., Nistratov, G., Popov, V. & Stepanov P. 2011. Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, Proceedings of the 1st Internatinal Conference on Transportation Information and Safety, ICTIS, 30 June – 2 July 2011: 845-854. China: Wuhan.
6. Kostogryzov, A., Nistratov, G. & Nistratov, A. 2012. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, Total Quality Management and Six Sigma: 127-196. InTech. http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
7. Kostogryzov, A., Nistratov, A. & Nistratov, G. 2013. The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields: 146-155. International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, http://www.ijeit.com/archive.php
8. Burtseva, A. 2013. Quality management of operation of the gas transportation system in conditions of Yamal Peninsula. The dissertation on a scientific degree PhD. Scientific supervisor - Kostogryzov A.I., The Gubkin Russian State University of Oil and Gas
9. Kostogryzov A.I. etc. (2015) Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety / Edited by N.Machutov – Moscow: «Znanie», 2015, – 936 p.