Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling

A. Kostogryzov[1], P. Stepanov[1], A. Nistratov[2], G. Nistratov[3], O. Atakishchev[4] and V. Kiselev[5]
[1] Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia
[2] The Russian Energy Agency, Moscow, Russia
[3] The Research Institute of Applied Mathematics and Certification, Moscow, Russia
[4] Southwest State University, Kursk, Russia
[5] The Research Institute of Standardization and Unification, Moscow, Russia

***Abstract*—The probabilistic models and methods for risk prediction and processes optimization, considering characteristics of threats, the measures of control, monitoring and recovery for complex system are proposed. The way of generating new models to increase an accuracy of probabilistic modeling is described. Examples of applications cover detailed studying "human factor", some infrastructure, description of problems for risk analysis and optimization, implementation in the Complex of supporting technogenic safety on the objects of oil & gas distribution. The research is supported by the Russian Scientific Fund.**

keywords- model; optimization; probability; quality; resources; risk; system; technology

I. INTRODUCTION

Modeling procedures of risk prediction are an analytical core of effective control and preventive optimization for critical systems used in production, manufacturing, logistics and other applications. How to evaluate and compare the term "critical" by probability scale for complex systems of different applications? And what about the effectiveness of control? And how to use risks dependencies for preventive optimization? Generally these questions often have not correct analytical answers in practice [1-10 etc.]. But the logic views on processes are identical in time line. At first for different conditions of uncertainty the critical set of threats against quality and safety should be defined in system life cycle. Then taking into account available resources and possibilities the preventive measures for control should be chosen or developed. Technologies of system control, monitoring and recovery of lost system integrity are used as counteraction against the different threats (system integrity is defined as system state when system purposes are achieved with required quality and safety). The goal of this work is to propose the probabilistic models, considering the possibilities of control, monitoring and recovery of lost integrity, and the way of generating new models to increase an adequacy of probabilistic modeling, considering the complexity of the system. These can be used for risk prediction, effective control and preventive optimization for complex systems operating in different applications. The effectiveness of modeling is provided by using the main function of probability theory to research future- by the probability distribution functions (PDF) of time between integrity losses of system, subsystem and elements [11]. The practical effects are demonstrated by examples.

II. THE ANALYZED FEATURES OF PROBABILISTIC MODELING FOR COMPLEX SYSTEMS

A. ABOUT Risk Estimation for Simplified Cases

In general case risk may be estimated by a probability of danger threats influences, considering a damage. In general cases it is understandable how to estimate damages. Leaving an estimation of a possible damage, we will stop on researches of a probabilistic component of risk. The most difficulties from scientific point of view for anticipating dangerous development of events is to construct a PDF of time between losses of system integrity. What deviations in risk predictions are possible for system, presented as "black box"? To answer this question, it is necessary to understand typical metrics, engineering methods of risks predictions, definition and concept of use «admissible risk», and then to compare the various variants of estimations. In practice for simplified cases probabilistic estimations of system integrity losses quite often carry out by the frequency of emergencies or any adverse events. For example, with reference to safety it can be frequencies of different danger threats influences, leading to a damage. I.e. frequency replaces estimations of probability to lose integrity of system during prognostic period. Whether it is correct? From probability theory it is known, that for defined PDF one of its characteristics is the mathematical expectation (Texp.). In turn, for PDF of time between losses of system integrity the mathematical expectation is the mean time Texp. and moreover the frequency λ of system integrity losses is equal to 1/Texp.. If to be guided only by frequency λ (with ignoring PDF) in practice a large deviation may take place. Indeed, a probability that event has occurred till the moment Texp., can be equal 0.00 for approximation by deterministic (discrete) PDF and 0.36 for exponential approximation (PDF $R(t, \lambda)=1-\exp(-\lambda \cdot t)$, for $t=Texp=1/\lambda \rightarrow R(t, \lambda)=1-\exp(-1)\approx 0.36$). I.e. as a result of erroneous choice of PDF, characterized by

identical λ, the enormous difference may take place! On the one hand it means ambiguity of a probabilistic estimation of events, being guided only on frequency λ, and with another one – a necessity of search (or creations) more adequate PDF of time between losses of system integrity is very high. And we should consider – if for very long time (for example, t=1 year) to put λ about 10-3 times in a year or less, then under Taylor's approximation $R(t, \lambda) \approx \lambda \cdot t$ with accuracy $o(\lambda 2 \cdot t2)$. But if value $\lambda \cdot t$ increases, may exceed 1 and cannot be perceived as probability.

B. *About "Admissible Risk"*

The matter is "admissible risk" should be a result of the consent of all parties involved in unsafe business on condition that it does not ruin business, it is unequivocally estimated and interpreted by all, and is scientifically proved. In practice frequently the «admissible risk» is interpreted as "border strip". It is supposed, that if do not cross this "border strip", the system integrity cannot be lost. But in reality it is not so! The residual risk always remains. In operation research the similar limitations are considered as a starting point for the decision of synthesis problems, connected with searching effective preventive measures of system integrity in life cycle. And rational use of these measures promotes to retaining the risk on admissible level. It is the typical approach which should work correctly.

And how it work in practice? Here quite pertinently to address to the developed form of the quantitative requirements, connected with the level of admissible risks. The elementary forms of requirements are: «A frequency λ of system integrity losses should not exceed admissible level λadm.»; and/or «probability to lose integrity of system during time Treq should not exceed admissible level Radm. (Treq)»; and/or their combination.

What engineering explanations occur in practice? – They are the next:

If the limitation on an admissible level of probability Radm. (Treq) is set. it means, that crossing "border strip" should not occur on an interval of time from 0 to Treq. For exponential PDF-approximation there is an unequivocal functional dependence: λadm. = - ln (1- Radm. (Treq)). I.e. this dependence means: a given point of admissible probability Radm. (Treq) corresponds unequivocally with a point of the maximum frequency of system integrity losses;

If the limitation on an admissible level of maximum frequency of system integrity losses λadm. is set, it means, that for exponential PDF-approximation probability from time t is considered: R(t, λadm.) = 1 – exp (-λadm.·t). I.e. this is the same "border strip", but in the form of function from t.

Despite obvious incompleteness of the elementary forms of requirements to «admissible risks» (in reality – only the limitations in one or several points) and absence of interrelations with a kind of real PDF of time between losses of system integrity (depending from many parameters: structure of system, heterogeneity of threats, different measures of counteraction to threats etc.), these forms are accepted by engineering Community. In the further statement of the work we will be guided by these elementary forms of requirements to "admissible risks».

C. *About Possible Dependence of Probability Distribution Function for Complex Systems*

On Figure 1 the limitations to admissible risks, fragment of exponential PDF and an adequate PDF of time between losses of system integrity with identical frequency of system integrity losses are demonstrated.

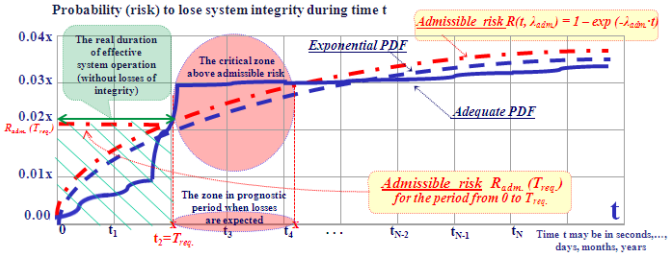

FIGURE I. FRAGMENT DEMONSTRATING THE POSSIBLE VARIANTS OF CORRELATIONS OF THE LIMITATIONS TO ADMISSIBLE RISKS, EXPONENTIAL AND AN ADEQUATE PDF OF TIME BETWEEN LOSSES OF SYSTEM INTEGRITY WITH IDENTICAL FREQUENCY OF SYSTEM INTEGRITY LOSSES λ

Using exponential approximation of PDF, it is possible to ascertain easily: are the requirements met to level of admissible risks? If it is below of "border strip" - the requirement is met, if it is above of "border strip" - the requirement isn't met! From "pluses" - only convenience of comparison. And it is all.

Using a more adequate PDF (for example, created by models from part 3, that considers frequency of occurrence and development of different threats, real protection processes against dangerous influences and the real complex structure of system), extraction of following knowledge is possible (see Figure 1) [12-14]:

To calculate more accurate the dependencies of the probability to lose system and subsystem integrity during time t from input characteristics;

To estimate accuracy of risk prediction in comparison with exponential approximation of PDF of time between losses of system integrity;

To define a real duration of effective system operation (i.e. without losses of integrity) considering real protection measures for making decision about predictive counteraction measures against threats in time;

To define critical zone above admissible risk when losses of system integrity are expected in prognostic period for making decision about predictive counteraction measures or justifying a revision of admissible risks for these zones (considering risk avoiding and mitigation);

To compare a real duration of effective system operation (i.e. without losses of integrity) considering real protection measures with the same period for exponential approximation of PDF of time between losses of system integrity.

Besides, after creating more adequate PDF, it is possible to extract additional knowledge by usual methods of probability theory (see, for example, [3-4,7]) - to calculate from known PDF the mean time between neighboring losses of integrity Tmean , and the frequency λ of system and subsystem integrity losses (λ = 1/ Tmean) considering real protection processes and conditions of dangerous influences.

Resume: existing approach of modeling for system, presented as "black box" using exponential PDF of time between losses of system integrity, is rather simplified case with low accuracy. More adequate analytical probabilistic models for risks prediction and processes optimization in application to complex systems, considering measures of control, monitoring and recovery, are needed.

III. The Generated Probabilistic Models for Adequate Risks Prediction

We present some ways to increase an adequacy of probabilistic modeling by the examples of different consideration of the complexity of the system, real protection processes against dangerous influences and the creation algorithm of integration PDF for complex systems [5-14]. Nowadays at system development and utilization an essential part of funds is spent on providing system protection from different dangerous influences able to violate system integrity (these may be failures, incidents events, capable to lead to failures, "human factors", information security events, terrorists attacks, etc). There are described 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 [12-14]. These models allow to create more adequate PDF of time between losses of system integrity.

A. The Models for the Systems that are Presented as One Element ("Black Box")

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 the recovery of integrity 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 activated and influenced on a system. Otherwise the source will be detected and neutralized during the next diagnostic. Note: it is supposed that used diagnostic tools allow to provide 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 and system recovery are the same as for technology 1). Faultless operator's actions provide a neutralization of a danger source trying to penetrate into a system. When a complex diagnostic is periodically made, this time operators are alternated. 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.

The probability of system operation with required safety and quality within the given prognostic period (i.e. probability of success) may be estimated as a result of use the next models for technologies 1 and 2. Assumption: for all time input characteristic the probability distribution functions exist. Risk R to lose integrity (safety, quality or separate property, for example – reliability) is an addition to 1 for probability P of providing system integrity ("probability of success") R=1-P.

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.

The next formulas for PDF of time between the losses of system integrity are proposed.

PDF for the model of technology 1, variant 1: Under the condition of independence for 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 penetrations of a danger source; Ωactiv(t) – is the PDF of activation time of a penetrated danger source. These PDF Ωpenetr(t) and Ωactiv(t) may be exponential PDF. For different danger threats a frequency λ for these PDF is the sum of frequencies of every kind of threats.

PDF for the model of technology 1, variant 2. Under the condition of independence for characteristics the probability of providing system integrity for variant 2 is equal to

$$P(2)(Treq) = N((Tbetw + Tdiag)/Treq)\, P(1)N(Tbetw + Tdiag) + (Trmn/Treq)\, P(1)(Trmn), \quad (2)$$

Where N= [Treq./(Tbetw.+ Tdiag.)] – may be real (for PDF) or the integer part (for estimation of deviations),

Trmn = Treq - N(Tbetw +Tdiag)).

The probability of providing system integrity within the given time P(1)(Tgiven) is defined by (1).

PDF for the model of technology 2, variant 1. Under the condition of independence for characteristics the probability of providing system integrity 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.

PDF for the model of technology 2, variant 2. Under the condition of independence of characteristics the probability of providing system integrity for variant 2 is equal to

$$P(2)(Treq) = N((Tbetw + Tdiag)/Treq)\, P(1)N(Tbetw + Tdiag) + (Trmn/Treq)\, P(1)(Trmn), \quad (4)$$

where the probability of providing system integrity within the given time P(1)(Tgiven) is defined by (3).

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

The models are applicable to the system presented as one element. The main result of such system modeling is probability of providing system integrity or of losses of system integrity during the given period of time. If a probability for all points Treq. 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.

B. The Way of Generating New Models for Complex Systems

The basic ideas of correct integration of probabilistic metrics are based on a combination and development of the offered models [1-10]. For a complex system estimation with parallel or serial structure new models can be generated by methods of probability theory. For this purpose in analogy with reliability it is necessary to know a mean time between losses of integrity for each element. Let's consider the elementary structure from two independent parallel elements that means logic connection "OR" or series elements that means logic connection "AND" – see Figure 2.

FIGURE II. ILLUSTRATION OF SYSTEM, COMBINED FROM SERIES (LEFT) OR PARALLEL (RIGHT) ELEMENTS

Let's PDF of time between neighboring losses of i-th element integrity is $Bi(t) = P(\tau i \le t)$, 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 will be lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\min(\tau 1,\tau 2) \le t) = 1 - P(\min(\tau 1,\tau 2) > t) =$$

$$= 1 - P(\tau 1 > t)P(\tau 2 > t) = 1 - [1 - B1(t)]\,[1 - B2(t)], \quad (5)$$

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

$$B(t) = P(\max(\tau 1,\tau 2) \le t) = P(\tau 1 \le t)P(\tau 2 \le t) = B1(t)B2(t). \quad (6)$$

Note. The same approach is studied also by Prof. E.Ventcel (Russia) in 80th who has formulated the trying tasks for students.

Thus an adequacy of probabilistic models is reached by the consideration of real processes of control, monitoring, element recovery for complex structure. Applying recurrently expressions (5) – (6), it is possible to create PDF of time between losses of integrity for any complex system with parallel and/or series structure.

The known kind of the more adequate PDF allows to define accordingly mean time between neighboring losses of system integrity Texp. (may be calculated from this PDF by traditional methods of mathematical statistics), and a frequency λ of system integrity losses $\lambda = 1/Texp$..

All these ideas are implemented in the software technologies of risk prediction for complex systems, for example, the "Complex for evaluating quality of production processes" (patented by Rospatent №2010614145) [12-14].

IV. SOME METHODS FOR PROCESSES OPTIMIZATION

The results of modeling processes can and should be used for optimization of complex systems operation on the base of risk prediction. 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 an admissible level of quality and/or safety. In a life cycle of systems criteria and limitations vary. 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 [5, 8, 14] - system parameters, software, technical and management measures (Q) are the most rational for the given period if on them:

The minimum of expenses Zdev. (Q rational) for creation of system is reached at limitations on probability of an admissible level of risks $R(Q) \le R\,adm$, quality and expenses for operation and under other development, operation or maintenance conditions (on the stages of system concept, development, production and support);

the minimum of risks R (Q rational) is reachedat limitations on probability of an admissible level of quality and expenses for operation and under other operation or maintenance conditions (on operation stage).

There may be combination of these formal statements in system life cycle.

V. THE EXAMPLES OF APPLICATIONS AND EFFECTS

The next examples demonstrate some pragmatic effects from risks prediction, preventive optimization and control in application to complex systems [5, 8, 14].

Example 1 allowed to estimate operation of object as “black box”. Dangerous manufacture is a complex of diverse processes, in each of which «the human factor» is the bottleneck. Let a frequency of occurrence of the latent or obvious threats is equal to once a month, an average time of development of threats (from occurrence of the first signs of a critical situation up to failure) – 1 days. A work shift is equal to 8 hours. The system control is used once for work shift, a mean duration of the system control is about 10 minutes (it is supposed, that recovery of object integrity is expected also for 10 minutes). The workers of medium-level and skilled workers are capable to revealing signs of a critical situation after their occurrence, and workers of initial level of proficiency – are incapable. Medium-level workers can commit errors on the average not more often 1 time a month and skilled workers – not more often once a year. How consideration of the qualification level influences on risks to lose object safety for a year and for 10 years?

The results of modeling are: for workers of initial level of proficiency risks to lose object safety are near 1 (losses of integrity are inevitable). For workers of medium-level risk to lose object safety for a year is about 0.007, for 10 years – 0.067, and for skilled workers risk equals to 0.0006 for a year and 0.0058 for 10 years.

Example 2. Critical operations on dangerous manufacture are carried out by skilled workers in interaction (including reservation and supports of another). Formally they operate as parallel elements with hot reservation. Thereby the consideration of such complex interaction allows to increase adequacy of modeling. Let's estimate risk to lose object safety for this variant (all input data for each from 2 parallel elements are the same,that in an example 1, but the mean recovery time of the lost integrity of object equals to 1 days instead of 10 minutes).

The results of modeling are: risk to lose object safety increases from 0.0000003 (for a year) to 0.00014 (for 20 years). Thus the mean time between neighboring losses of object safety Tmean, calculated from known PDF, equals to 663 years. I.e. the frequency λ of system safety losses is about 0.0015 times a year. It is 8000 times less (!) in comparison with a primary frequency of occurrence of the latent or obvious threats (once a month). If to compare with exponential approximation of PDF with the same frequency λ, the risk to lose object safety will grow from level 0.0015 (for a year) to 0.03 (for 20 years). Difference is in 200 – 5000 times more against adequate PDF. The border of admissible risk 0.0015 will be reached for 195 years, not for 1.3 year as for exponential PDF. I.e. the real duration of effective object operation (i.e. without losses of safety) is 150 times more! Such effect can be reached at the expense of mutual aid (reservation and supports) of skilled workers. This knowledge is mined owing to consideration of details of complex system (skill workers in interaction as a complex)

Example 3. The larger enterprise the risks higher. Let’s analyze a system of complex gas preparation at an enterprise of a gas craft. The typical processes are: 1) processes, connected with operation of entrance threads; 2) processes of low temperature gas separations; 3) process of gas measuring; 4) processes of gas heating and reduction, candle and torch separation; 5) processes, connected with methanol storage and using, storage, giving and drainage dumps of condensate and diesel fuel; 6) processes of management in a service of Chief engineer; 7) processes of management in a service of the Chief of production; 8) processes of shop divisions; 9) processes of control system operation. Let's put, the interacted workers are involved in each of processes (for reservation). Their activity is modelled by the models of part 3. The high adequacy is reached by decomposition of system structure of worker’s “human factor” to 9 logical subsystems, each of which implements corresponding typical processes 1)-9), i.e. every subsystem consists 2 parallel elements. Safety of system is provided, if safety is provided "And" for the 1st subsystem, “And" for the 2nd, “And" for the 9th subsystem – see Figure 3.

FIGURE III. COMBINATION OF PARALLEL AND SERIES SUBSYSTEMS

Those input data for every element are the same as in example 2. Question: what risks are possible because of «human factor» during term from one to 20 years of operation of the enterprise?

Computed PDF shows: risk to lose object safety increases from 0.000003 (for a year) to 0.0013 (for 20 years). The mean time between neighboring losses of object safety Tmean equals to 283 years. I.e. the frequency λ of system safety losses is about 0.0035 times a year. It is 2.3 times more often against the results of Example 2. In comparison with a primary frequency of occurrence of the latent or obvious threats (once a month) the frequency λ is 3430 times lower! For exponential approximation of PDF with the same frequency λ the risk to lose object safety will grow from level 0.0035 (for a year) to 0.07 (for 20 years). Difference is in 54 – 1167 times more against created adequate PDF for complex system. The border of admissible risk 0.002 will be reached for 24 years, not for 7 months as for exponential PDF. I.e. the real duration of effective object operation is 41 times more!

Example 4. How much risks will increase, if in a system of the example 3 only medium-level workers are used?

The pragmatic results from risk prediction (see fragment PDF on Figure 4) are: risk to lose object safety increases from 0.0009 (for a year) to 0.25 (for 20 years). Thus the mean time between neighboring losses of object safety Tmean equals to

24 years. I.e. the frequency λ of system safety losses is about 0.04 times a year. It is 11.4 times less often against the results of Example 3 for skilled workers. In comparison with a primary frequency of occurrence of the latent or obvious threats (once a month) the frequency λ is 21 times lower!

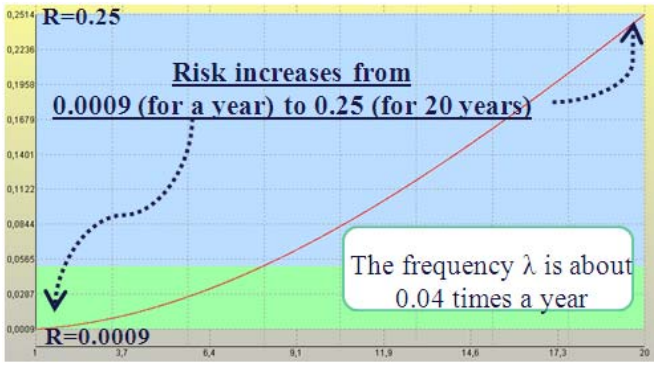

FIGURE IV. CALCALATED PDF FRAGMENT FOR EXAMPLE 4

For exponential approximation of PDF with the same frequency λ the risk to lose object safety will grow from level 0.04 (for a year) to 0.55 (for 20 years). Difference is 2.2 – 44.4 times more against adequate PDF. The border of admissible risk 0.002 will be reached for 2 years, not for one month as for exponential PDF. I.e. the real duration of effective object operation (i.e. without losses of safety) is 24 times more! The results of examples 1-4 and like them can be used to mitigate risks and as "precedents" for rationale of "Admissible risk" in applications of "human factor".

Example 5. Let's system formalization covers subsystem 1 (logically reflecting a human resource of transport station as one element of system), subsystem 2 (considering vehicles in a control zone of station as one element of system), subsystem 3 (considering transportation infrastructure as one element of system), subsystem 4 (central power supply as the main and reserve elements), subsystem 5 (a center of information processing and storage as combination of power supply subsystem, air conditioning subsystem, source of an uninterrupted supply, engine-generating installation), subsystem 6 (10 barriers against unauthorized access to valuable resources of station) – see Figure 5 right.

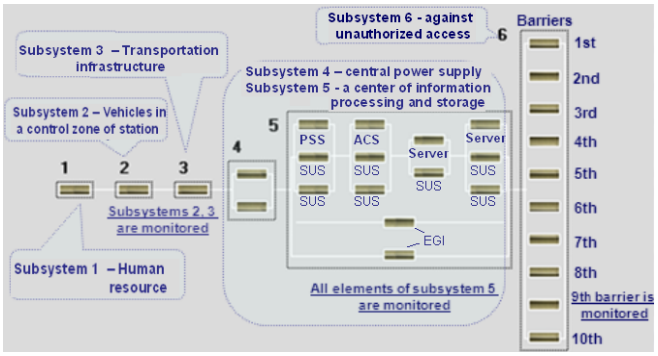

FIGURE V. LOGIC MODEL OF TRANSPORT STATION FRAGMENT

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

We will not go deeply into details of input and the results of modeling (input has been formed from statistic data for abstract fragment of transport station). We concentrate your attention only on knowledge mining from some integral distribution of risk to lose complex integrity depending on control, monitoring, counteraction, recovery measures and prediction time – see Figure 6.

Comments: correctly a trajectory on Figure 6 is not fragment of PDF, because N= [Treq/ (Tbetw.+Tdiag.)] is integer. It allows to feel on time line the possibilities of control, monitoring, counteraction, recovery measures used for different elements. If to use N=Treq/ (Tbetw.+Tdiag.) – real, monotonic increasing trajectory of PDF can be built.

Dependability of integrated risk to lose system integrity during operational 1 – 4 years is demonstrated by Figure 6.

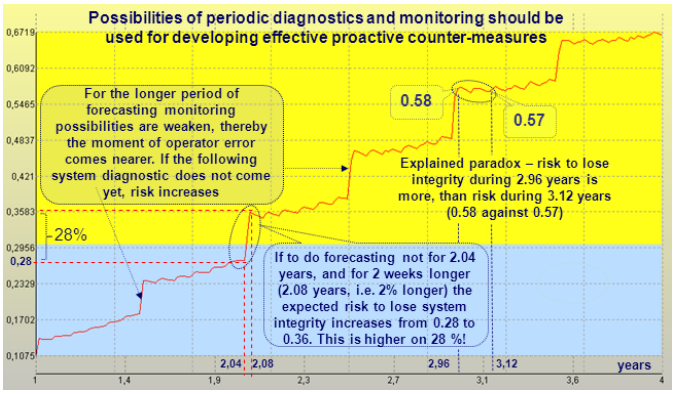

FIGURE VI. THE DEPENDABILITY OF INTEGRATED RISK TO LOSE SYSTEM INTEGRITY DURING OPERATIONAL 1 – 4 YEARS

Analysis of results shows, that integrated risk to lose integrity of system is changing from 0.11 (prognostic period = 1 year) to 0.67 (4 years). It is traditional understandable that the risk to lose system integrity increases in depending on increasing time period of prediction. But in practice it often is not so because of system periodic control, continuing monitoring and recovery measures. There are the features demanding a logic explanation. Serrated and nonmonotonic character of risk dependence on is explained by the periodic diagnostics of every elements, monitoring presence or absence and their quantitative values.

Immediately after 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. 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 prediction the possibilities of monitoring 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 modeling: if to predict 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 (higher on 28 % (!)). These results of knowledge mining should serve to developing preventive counter-measures concerning possibilities of control in time.

Example 6. What about the fields of models application? The proposed models are used in system engineering and education to provide and increase system quality and safety. Applications in Russia cover systems in various fields: information and transportation systems, manufacturing structures (including enterprises, oil&gas facilities, and hazardous production systems), power generation etc. So, for researching some variants of development of hydrocarbons deposits from Arctic ocean many scientific and technical problems should be solved [13].

Example 7. What about the possible pragmatic effects? Authors of this article took part in creation of the Complex of supporting technogenic safety on the objects of oil&gas distribution and have been awarded for it by Award of the Government of the Russian Federation in the field of a science and technics for 2014. Here peripheral posts are equipped additionally by means of monitoring 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 7.

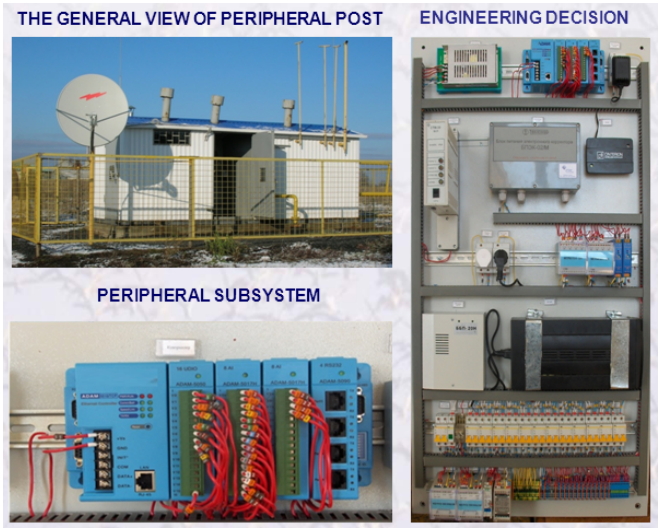

FIGURE VII. THE COMPLEX OF SUPPORTING TECHNOGENIC SAFETY ON THE OBJECTS OF OIL&GAS DISTRIBUTION

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 [14].

REFERENCES

[1] 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, 2000, pp.63-70.

[2] 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, 395p.

[3] A. Kostogryzov., and G. Nistratov "100 Mathematical Models of System Processes According International Standards Requirements". Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models. Maiority, Italy, September 20-24, 2005, University of Solerno, Italy pp. 196-201.

[4] Enrico Zio An Introduction to the Basics of Reliability and Risk Analysis, World Scientific, 2006, 222p.

[5] A. Kostogryzov, and P. Stepanov, Innovative management of quality and risks in systems life cycle, Moscow, "Armament. Policy. Conversion", 2008 404p.

[6] L. Grigoriev, V. Kershenbaum, and A. Kostogryzov System foundations of the management of competitiveness in oil and gas complex. Moscow: National Institute of oil and gas, 2010, 374p.

[7] K.Kolowrocki and J.Soszynska-Budny Reliability and Safety of Complex Technical Systems and Processes, Springer-Verlag London Limited, 2011, 405p.

[8] Kostogryzov A., Nistratov G. and Nistratov A., "Some Applicable Methods to Analyze and Optimize System Processes in Quality Management", Total Quality Management and Six Sigma, InTech, 2012, pp. 127-196, 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

[9] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. "Prediction and Optimization of System Quality and Risks on the Base of Modeling Processes", American Journal of Operations Research, Special Issue, Volume 3, Number 1A, January 2013, pp.217-244,Kostogryzov A., Nistratov G. and Nistratov A., The Innovative "Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields". International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. http://www.ijeit.com/archive.php

[11] W. Feller, An Introduction to Probability Theory and Its Applications. Vol. II, Willy, 1971.

[12] A.I. Kostogryzov & P.V.Stepanov, G.A.Nistratov & A.A.Nistratov, L.I.Grigoriev, O.I.Atakishchev "Innovative Management Based on Risks Prediction. Information Engineering and Education Science". Taylor & Francis Group, London, 2015, pp. 159-166.

[13] A. Kostogryzov, L.Grigoriev, V. Kershenbaum, Ch. Guseinov, O. Atakishchev, P. Stepanov "The probabilistic approach to solve analytical problems in a life cycle of complex systems for developing and transportation hydrocarbon deposits of Arctic regions". The 3rd International Conference on Transportation Information and Safety, June 25 – June 28, 2015, Wuhan, P. R. China. pp.682-688

[14] 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, 936p.