Estimations of "Smart" Engineering Systems Operation by Probabilistic Measures of Correctness And Reliability

Andrey Kostogryzov
•
Federal Research Center "Computer Science and Control"
of the Russian Academy of Sciences
Akostogr@gmail.com

Abstract

The estimations of critical operation quality deterioration for "Smart" Engineering Systems (SES) are analyzed considering impacts on SES operation correctness and reliability. Basic probabilistic models for the predictive analysis of SES operation are proposed. The effects are illustrated by examples that cover the comparisons of SES, acting as medium-level and skilled operators, the estimation of SES operation without and with considering correctness and reliability, rationale requirements to admissible level for the errors of analysis, predictions of the risks of critical SES operation quality deterioration, sensitivity estimation of predicted risks, the efficiency in practice applications. The novelty is formed from (1) the described methodology for risks of critical operation quality deterioration for SES, considering complexity and uncertainties for SES operation correctness and reliability, (2) the comparable impacts on SES operation quality from failures (reliability) and errors of the 1st and 2nd types (correctness), proved by probabilistic modeling, (3) the achievable levels about 0.999-0.9997 and more for probability of SES operation correctness and reliability and about 0.01 – 0.001 and less for probability of critical SES operation quality deterioration during 1 year, which characterizes risk for identical consequences.

Keywords: analysis, model, *estimation*, operation, prediction, probability, quality, system

I. Introduction

Operation of modern ad future SES in various areas of their applications is accompanied by a set of uncertainties. For general case the term "smart" is a mnemonic acronym, giving criteria of guiding on the set objectives. SES are defined as systems that incorporate functions of data sensing, information processing and transfer, monitoring of conditions, actuation and control of devices and other systems, improving their operation quality and/or safety. According to system engineering standards (see, for example, International standards ISO/IEC/IEEE 15288, ISO/IEC 16085, IEC 61508, etc.) the analysis of uncertainties should be carried out at all stages of system life cycle. Uncertainties are principal factors of risks. Today practice has shown: in the most cases from all properties of SES quality the main attention is paid to reliability of various systems. For an estimation of reliability there are created and used sets of standards, mathematical and methodical approaches [1-12] which can be applied for SES. At the same time, SES are differed from simple engineering systems that they are capable to carry out intellectual information processing based on formal modeling. Necessity of

considering SES possibilities of monitoring parameters and making control actions, and also increasing SES complexity prove an actuality of models development for risks predictions. The scientific probabilistic approaches for an estimation of SES information correctness are at the beginning stage yet, some approaches – see for example [1-2, 5-12 etc.].

The novelty of the manuscript is formed from (1) the described methodology for risks of critical operation quality deterioration for SES, considering complexity and uncertainties for SES operation correctness and reliability, (2) the comparable impacts on SES operation quality from failures (reliability) and errors of the 1st and 2nd types (correctness), proved by probabilistic modeling, (3) the achievable levels for probability of SES operation correctness and reliability for probability of critical SES operation quality deterioration which characterizes risk for identical consequences. Considering an importance of researches for all-round maintenance and improvement of SES operation quality here are proposed: the basic ideas for the risks prediction of critical operation quality deterioration and for the further uses of predictions; the improved models to estimate information correctness and operation reliability (for "black box»); the consecutive algorithm to predict risks, considering SES operation correctness and reliability (for "black box»); the integrated model to predict the risks of critical operation quality deterioration for SES, composed as complex structures; the statements of optimization problems in SES life cycle; the practical examples with interpretation of probabilistic modeling SES operation quality.

Note. The used definitions are: Risk – 1) effect of uncertainty on objectives (ISO Guide 73); 2) the combination of the probability of an event and its consequence (ISO/IEC 16085, IEC 61508 etc.); Reliability of SES operation - the property of SES to perform its required functions of data sensing, information processing, transfer, monitoring of conditions and actuation of devices and other systems under stated conditions for a specified period of time; Correctness of SES operation – the property of SES to provide the right results or the coordinated effects of information processing and control.

II. Basic Ideas

The next ideas are intended to explain the approaches for the risks prediction and the further uses of predictions.

The idea 1 is: to focus on operation correctness and reliability as the main critical properties characterizing SES quality in use for conditions of uncertainties.

Note. SES quality in use also may be characterized additionally by other properties, for example – by the timeliness of information producing, the completeness, actuality, faultlessness, confidentiality of information etc. [1, 2, 12].

The idea 2 is: to improve created earlier probabilistic models for the correctness analysis and reliability prediction [1-2, 8-11] at mathematical SES description by a "black box»; to create the consecutive algorithm for prediction the risks of critical SES operation quality deterioration by the consecutive input of the results of the correctness modeling into the improved model for reliability prediction.

The idea 3 is: to create integrated probabilistic model for prediction the risks of critical operation quality deterioration of SES, composed as complex in the form of parallel-serial structures.

The idea 4 is: to use the risks of critical SES operation quality deterioration for rationale preventing measures by solving the problems of optimization in SES life cycle.

The idea 5 is: on the basis of application of the proposed models to demonstrate results of ideas 1-4 implementation by the examples devoted to:

-a comparison of possibilities of SES, acting as operators of medium-level and skilled operators;

- an estimation of SES operation reliability (without considering correctness of information processing) and SES operation considering correctness and reliability;

- rationale requirements to admissible level for the errors of analysis (of 1st and 2nd types) during SES information processing;
- predictions of the risks of critical SES operation quality deterioration during 1 month and 1 year;
- sensitivity estimation of predicted risks in dependence on changing initial data of probabilistic modeling of SES operation in diapason -50%+100%;
- reference on efficiency in practice applications.

III. The Proposed Probabilistic Models as "Black Box" for probabilistic estimations

I. The Improved Model of Items Content Analysis

Problems of item (text, forms, events) content analysis are inherent to SES operation. It may be identification of items, recognition of images, manuscripts, speech or signals, nondestructive control, hardware or software testing, information analysis for making decision etc. In any case there exist latent or suspicious objects for revealing and their following analysis by SES. Item content analysis depends on SES specificity and methods of content analysis. In general case methods of content analysis and SES decision-making may contain elements of guessing. Nonetheless, any analysis is based on logical positions. Logic implies argumentation based on essential items use. The way of logical approach is an algorithm of given items analysis by SES. Such algorithm is implemented by an operator (operator may be a SES-device or a SES, combined by a man, or their combination). See the core of formalization on Figure 1 (for information checking). The formalization core of item analysis is illustrated by Figure 1.

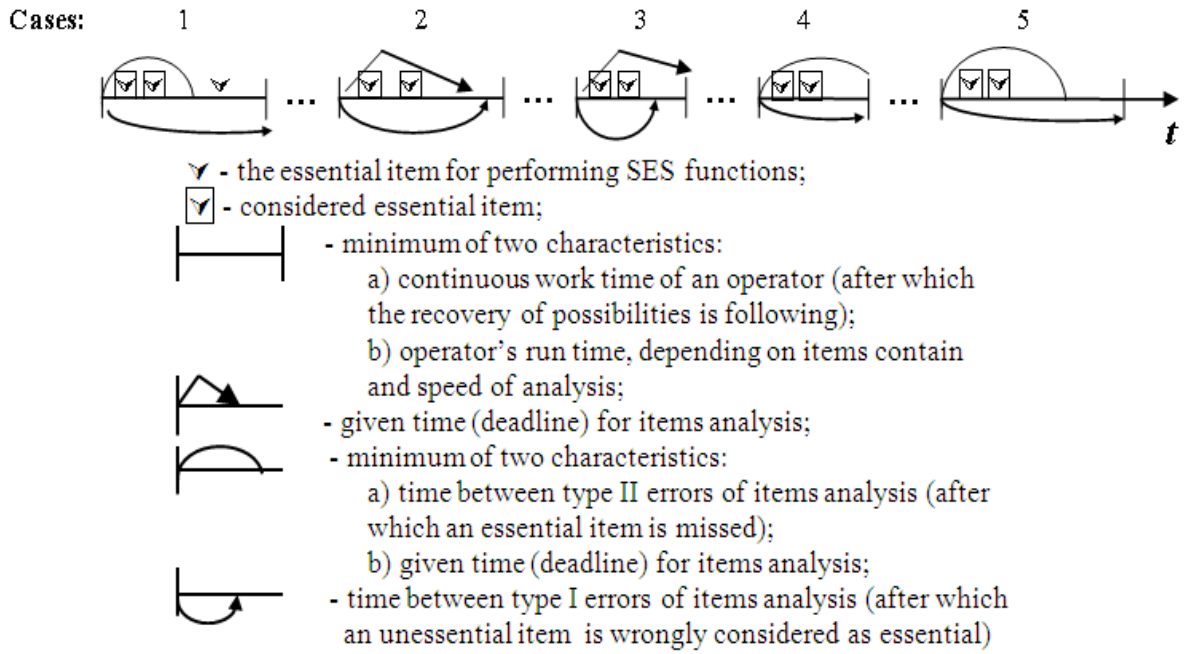

Figure 1: *Some possible cases in items analysis*

The case 1 illustrates error of the 2nd type (essential item is missed), the case 2 illustrates error of the 1st type after deadline, the case 3 illustrates error of the 1st type before deadline (unessential item is wrongly considered as essential), the cases 4 and 5 characterize correctness of items analysis during SES operation.

Because of uncertainties now and in future it may not always possible to distinguish a formal bound between essential and unessential items for performing some SES functions. A problem of a balance between input items content and quality of their analysis by SES within the given time should be solved. If input items content is big the number of errors increases what may cause a control action time waste. It is necessary to optimize the items content and to develop more rational technologies of SES operation.

Definition. SES operation is considered as correct during given time if all essential items are analyzed rightly and no an unessential item is wrongly considered as essential. Because of uncertainties SES operation correctness may be estimated by probabilistic modeling.

There are possible the four variants of correlations between the input characteristics for modeling.

Variant 1. The given time for items content analysis is no less than the real analysis time ($T_{real} \le T_{req.}$) and the content of analyzed items is such small that it is required only one continuous operator's work period ($T_{real} \le T_{cont.}$).

The next Statements 1-4 are used.

Statement 1. Under the condition of independence for considered input characteristics the probability of SES operation correctness during the given time is equal to:

$$P_{after(1)}(V, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, T_{req.}) = [1 - N(V/\nu)]\left\{\int_0^{V/\nu} dA(t)[1 - M(V/\nu - t)] + \int_{V/\nu}^{\infty} dA(t)\right\}, \quad (1)$$

where V is an analyzed content of items;

μ is a relative fraction of essential items in items content, dimensionless ($\mu \cdot 100\%$ characterizes a relative fraction of essential items in percentage);

ν is a speed of items analysis;

N(t) is a probability distribution function (PDF) of time between errors of 1st type (when unessential item is wrongly considered as essential), η^{-1} is mean time, $N(t) = 1 - exp(-t \cdot \eta)$;

$M(t)$ is a PDF of time between real neighboring essential items in analyzed content for the given speed of items analysis and relative fraction of essential items in items content, $M(t) = 1 - exp(-t \cdot \mu \cdot \nu)$;

$A(t)$ is a PDF of time between errors of 2nd type (when essential item is missed), T_{MTBF} is mean time;

$T_{cont.}$ is a time of continuous operator's work;

$T_{req.}$ is a given time for items content analysis.

V, ν, $T_{cont.}$ and $T_{req.}$ are assigned as deterministic values.

The probability of operation correctness without items content analysis is $P_{no}(V) = e^{-\mu V}$. If μ=0%, $P_{no}(V)$ =1 (no comments for no essential items).

The final clear analytical formula for modeling is received by Lebesque-integration of expression (1).

Variant 2. The given time for items content analysis is no less than the real analysis time (i.e. $T_{real} \le T_{req.}$). But the content of analyzed items is comparatively large, i.e. $T_{real} > T_{cont.}$.

Statement 2. Under the condition of independence for considered characteristics the probability of SES operation correctness during the given time is equal to:

$$P_{after(2)} = \{P_{after(1)}(V_{part(2)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, \tau_{part(2)})\}^L, \quad (2)$$

where $L=V/(\nu T_{cont.})$, $V_{part(2)}=V/L$, $\tau_{part(2)} = T_{req.}/L$.

Variant 3. The given time for items content analysis is less than the real analysis time ($T_{real}>T_{req.}$) and the content of analyzed items is such small that it is required only one continuous operator's work period ($T_{real} \le T_{cont.}$).

Statement 3. Under the condition of independence for considered characteristics the probability of SES operation correctness during the given time is equal to:

$$P_{after(3)} = (V_{part(3)}/V) \cdot P_{after(1)}\,(V_{part(3)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, T_{req.}) + +[(V-V_{part(3)})/V] \cdot P_{without}, \quad (3)$$

where $V_{part(3)} = \nu T_{req.}$. , $P_{without} = e^{-\mu (V-V\,part(3))}$.

Variant 4. A given time for items content analysis is no less than the real analysis time (i.e. $T_{real}>T_{req.}$). But the content of analyzed items is comparatively large, i.e. $T_{real}>T_{cont.}$.

Statement 4. Under the condition of independence for considered characteristics the probability of SES operation correctness during the given time is equal to:

$$P_{after} = \begin{cases} [V_{part(4)}/V] \cdot after(1)\,(V_{part(4)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, T_{req.}) + \\ + [(V-V_{part(4)})/V] \cdot e^{-\mu (V-V\,part(4))}, \text{ if } T_{req.} \le T_{cont.}; \\ [V_{part(4)}/V] \cdot \{P_{after(1)}\,(V_{part(4.2)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, \tau_{part(4.2)})\}^N + \\ +[(V-V_{part(4)})/V] \cdot e^{-\mu (V-V\,part(4))}, \text{ if } T_{req.} > T_{cont.}, \end{cases} \quad (4)$$

where $V_{part(4)} = \nu T_{req.}$, $V_{part(4.2)}=V_{part(4)}/L$, $\tau_{part(4.2)}=\tau/L$, $L= V_{part(4)}/(\nu T_{cont.})$.

The fraction of no used essential items after analysis equals to $\mu_{after(1)}= \mu \cdot (1-P_{after(1)})$.

The final clear analytical formulas for modeling are received by integration (1) and using (2)-(4). The proofs of Statements are similar to the proofs for the probabilistic modeling [1, 3, 5].

II. The Improved Model for Operation Reliability Prediction

Nowadays in development and utilization an essential part of funds is spent on providing SES operation reliability. Various dangerous impacts on system integrity (these may be failures, defects events, "human factors" events etc.) deteriorate SES operation reliability. The improved model for operation reliability prediction especially uses the elementary events "correct operation" and alternatively "a loss of integrity" to link this model with the previous model and with the following consecutive algorithm for prediction the risks of critical SES operation quality deterioration.

There are examined two general technologies of providing SES operation reliability: periodical diagnostics of system integrity (technology 1, without monitoring between diagnostics) and additionally monitoring between diagnostics (technology 2).

Both Technologies 1 and 2 are focused on devices and systems, for which the SES functions are performed, including monitoring of conditions, actuation and control. Let a set of operating SES and these devices and systems, for which the SES functions are performed, is named a system and described by "black box".

Technology 1 is based on periodical diagnostics of such system integrity. Technology 1 is carried out to detect penetrated sources of potential unreliability or consequences of negative impacts (see Figure 2). The lost system integrity can be detected only as a result of diagnostics, after which recovery of system reliability is started. Dangerous impact on system is acted step-by step: at first a danger source penetrates and then after its activation begins to impact on reliability. System integrity can't be lost before a penetrated danger source is activated. A danger is considered to be realized only after a source of potential unreliability has impacted on a system.

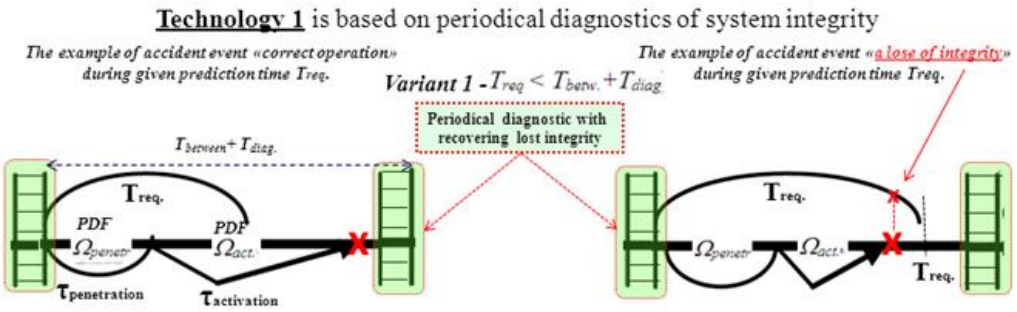

Figure 2: *Some explanation for probabilistic modeling Technology 1*

Technology 2, unlike the previous one, implies that an operator performs the functions of monitoring system integrity between diagnostics (operator may be a SES-device or a SES, combined by a man, or their combination). In case of detecting a danger source of potential unreliability an operator recovers system integrity. The ways of integrity recovering are analogous to the ways of technology 1. Correct operator's actions provide a neutralization of a source of potential unreliability. A penetration of a danger source of potential unreliability is possible only if an operator makes an error but an impact on reliability (with the lost integrity) occurs if the source is activated before the next diagnostic. Otherwise the source will be detected and neutralized during the next diagnostic (see Figure 3).

It is supposed for technologies 1 and 2 that the used SES diagnostic possibilities allow to provide required system integrity recovery after revealing penetrated sources or consequences of impacts. Assumption: for all time input characteristic the 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.

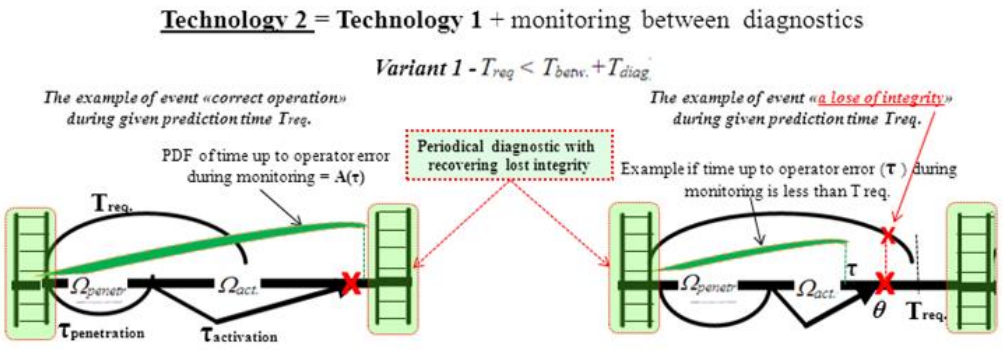

Figure 3: *Some explanation for probabilistic modeling Technology 2*

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 5-8 are used [1, 3, 5, 11].

Statement 5 (for technology 1). Under the condition of independence of considered characteristics the probability of reliable system operation for variant 1 is equal to

$$P_{(1)}(T_{req}) = 1 - \Omega_{penetr} * \Omega_{activ}(T_{req}), \quad (5)$$

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring impacts for penetrating a danger source; $\Omega_{activ}(t)$ – is the PDF of activation time of a source of potential unreliability.

Statement 6 (for technology 1). Under the condition of independence for considered characteristics the probability of reliable system operation for variant 2 may be equal to:

measure a)

$$P_{(2)}(T_{req})=N((T_{betw}+T_{diag})/T_{req})P_{(1)}^{N}(T_{betw}+T_{diag})+(T_{rmn}/T_{req})\ P_{(1)}(T_{rmn}), \quad (6)$$

where $N=[\ T_{req.}/(T_{betw.}+\ T_{diag.})]$ – is the integer part,
$T_{rmn} = T_{req} - N(T_{betw}+T_{diag})$;

measure b)

$$P_{(2)}(T_{req})=P_{(1)}^{N}(T_{betw}+T_{diag})P_{(1)}(T_{rmn}). \quad (7)$$

The probability of success within the given time $P_{(1)}(T_{given})$ is defined by (5).

Statement 7 (for Technology 2). Under the condition of independence for considered characteristics the probability of reliable system operation for variant 1 is equal to

(8)

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

Here A(t) is the PDF of time from the last finish of diagnostic time up to the first operator error (is similar to PDF A(t) from subsection 3.1). T_{MTBF} is the mean time between errors.

Statement 8 (for Technology 2). Under the condition of independence of considered characteristics the probability of reliable system operation for variant 2 may be equal to:

measure a)

$$P_{(2)}\ (T_{req}) = N((T_{betw}+T_{diag})/T_{req})\ P_{(1)}^{N}(T_{betw}+T_{diag}) +(T_{rmn}/T_{req})\ P_{(1)}(T_{rmn}), \quad (9)$$

measure b)

$$P_{(2)}\ (T_{req}) = P_{(1)}^{N}(T_{betw}+T_{diag})\ P_{(1)}(T_{rmn}),\ \text{(see (7))},$$

where the probability of success within the given time $P_{(1)}(T_{req})$ is defined by (8).

The final clear analytical formulas for modelling are received by Lebesque-integration of expression (8) with due regard to Statements 5-8. The models are supported by software tools [1-2, 5, 11].

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.

III. The Algorithm of Prediction the Risks of Critical SES Operation Quality Deterioration

The critical deterioration of SES operation quality means such deterioration of operation reliability or correctness when the performance of destined functions (of data sensing, information processing or transfer, monitoring of conditions, actuation or control of devices or other systems) doesn't meet

the defined requirements during given time.

Considering uncertainties the requirements to operation quality in SES life cycle (on stages of consept, development, production, utilization or support) may be defined in terms of admissible risks, for example: "the quality of SES operation is estimated as "acceptable" if the risk of operation reliability or correctness deterioration during given time of expected hard scenarios is less than established admissible risk".

The proposed consecutive algorithm for prediction the risks of SES operation quality deterioration is the next.

1. The acceptable level for the probability of reliable system operation during given time is defined. It should be achievable level considering system goals, possible conditions and dangers of uncertainties, resources, time and possible damages from unreliability. For estimations the improved model for operation reliability prediction may be used (from subsection 3.2). The used value T_{MTBF} is related with mean time between failures for SES.

Note. Here a set of operating SES and devices and systems, for which the SES functions are performed, is named a system.

2. The acceptable level for the probability of SES operation correctness during the given time is defined. It should be the level, possible near to acceptable level for the reliability, achievable considering SES goals, possible conditions of uncertainties, resources, time and possible damages from incorrectness. For estimations the improved model of items content analysis may be used (from subsection 3.1).

3. The maximal mean time between errors of the 1st type for which the calculated probability of SES operation correctness during the given time is equal to acceptable level, is defined for the given another input characteristics. For calculations the improved model of items content analysis may be used (from subsection 3.1).

4. The maximal mean time between errors of the 2nd type for which the calculated probability of SES operation correctness during the given time is equal to acceptable level, is defined for the given another input characteristics. For calculations the improved model of items content analysis may be used (from subsection 3.1).

5. Among the values of the mean time between errors of the 1st type and the mean time between errors of the 2nd type the minimum (min) and maximum (max) are defined.

6. Considering the specificity of SES, mean time between errors is defined (it is the weighed value inside of diapason of (min, max), considering frequency of errors of the 1st and 2nd types). Also in special case this may be or the mean time between errors of the 1st type or the mean time between errors of the 2nd type. This value (which characterizes SES operation correctness) is used instead of T_{MTBF} in modeling by using the improved model for operation reliability prediction may be used (from subsection 3.2). But now there are calculations in terms of risks. And results of modeling characterize the predicted risks of critical operation quality deterioration considering reliability and correctness for SES that are described by "black box".

IV. The Integrated Model to Predict Risks for SES, Composed as Complex Structures

For a complex system 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 neighboring 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 lost integrity when either 1st, or 2nd element integrity will be lost). For this case the

PDF of time between the losses of system integrity is defined by expression

$$B(t) = P(\min(\tau_1,\tau_2)\le t)=1-P(\min(\tau_1,\tau_2)>t) = 1-P(\tau_1>t)P(\tau_2> t)= 1 - [1-B_1(t)]\,[1- B_2(t)], \quad (10)$$

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

$$B(t)=P(\max(\tau_1,\tau_2)\le t)=P(\tau_1 \le t)P(\tau_2 \le t)=B_1(t)B_2(t). \quad (11)$$

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 (10) – (11), it is possible to create PDF of time between the 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 $T_{exp.}$ (may be calculated from this PDF as mathematical expectation), and a frequency λ of system integrity losses, $\lambda=1/T_{exp.}$.

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. The formulas for probabilistic modeling technologies 1 and 2 and the proofs of them are proposed in [1-2, 5]

All these ideas are implemented by the software technologies of risk prediction for complex systems, for example, the "Mathematical modeling of system life cycle processes" – "know how" (registered by Rospatent №2004610858), "Complex for evaluating quality of production processes" (registered by Rospatent №2010614145) [1-2, 5 - 11].

V. Some Statements for System Optimization

Here a set of operating SES and devices and systems, for which the SES functions are performed, is named also a system.

The results of modeling processes can and should be used for optimization of systems operation on the base of risk prediction. For example, there are applicable the next general formal statements of problems for system optimization [1-2, 10-11]:

1) on the stages of system concept, development, production and support:

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

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

at limitations on probability of an admissible level of risks $R(Q) \le R_{adm.}$ and/or 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 on them the minimum of risks is reached:

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

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

Of course these statements may be transformed into problems of minimization of expenses or mathematical expectation of damages in different limitations. System parameters, software, technical and management measures (Q) is a rule a vector of input – see sections 2 and 3. There may be combination of these formal statements in system life cycle**.**

VI. Examples

The examples cover:

- comparison of possibilities of SES, acting as operators of medium-level (Examples 1 and 2) and skilled operators (Example 3);
- estimation of SES operation reliability without considering correctness of information processing (Example 4) and SES operation considering correctness and reliability (Example 5);
- rationale requirements to admissible level for the errors of analysis (of 1st and 2nd types) during SES information processing and predictions of the risks of critical SES operation quality deterioration during 1 month and 1 year (Examples 6 and 7);
- sensitivity estimation of predicted risks in dependence on changing initial data of probabilistic modeling of SES operation in diapason -50%+100% (Examples 1-7);
- reference on the efficiency in practice applications (Examples 8 and 9).

Example 1 (estimation of items analysis correctness when functions of SES are performed by a man-operator).

Let's consider at first a situation when the items are analyzed by a man-operator of medium-level qualification. Similar systems are peculiar to many operating systems. Thus owing to purely human restricted possibilities operator covers only that volume of the items content which is capable to process for the given time. Let this analyzed content includes 20 items (in conditional units). Speed of the analysis is 20 items in a minute. Frequency of the 1st type errors (when unessential item is wrongly considered as essential) is equal to 1 error in a day. Mean time between errors of the 2nd type (when essential item is missed) is equal to 1 month. Operators replace each other through 2 hours for keeping attention concentration (it is a time of continuous operator's work). The given time for items content analysis is equal to 1 minute. It is required to estimate a correctness of items content analysis.

Solution. The analysis of modeling results by the improved model of items content analysis (see subsection 3.1) has shown the following. The probability of a man operation correctness will make 0.9993, that means absolutely correct processing with reference to small content volume 20 items. At increase items content volume twice the probability of operation correctness decreases to 0.5 – see Figure 4a). It is connected by that at the defined speed of analysis (20 items in a minute) for 1 minute half from 40 items will be analyzed only. The same effect is observed at researches of dependence of probability of operation correctness on speed of the analysis – see Figure 4b).

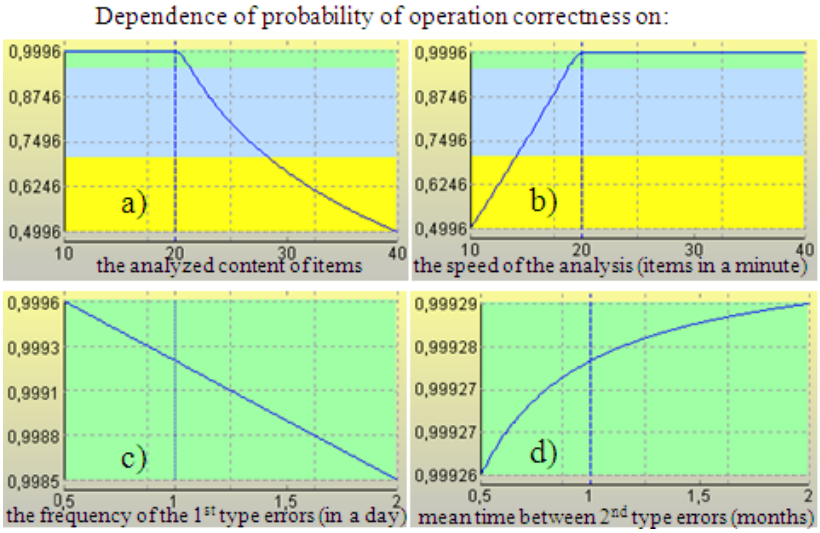

Figure 4. Dependence of probability of operation correctness on:
a) the frequency of the 1st type errors (errors in a day); b) the speed of the analysis (items in a minute); c) the frequency of the 1st type errors (errors in a day); d) the mean time between errors of the 2nd type (months)

At the same time, change in a diapason -50 % + 100 % of frequency of the 1st type errors (Figure 4c)) and mean time between errors of the 2nd type (Figure 4d)) insignificantly impact probability of operation correctness.

The analysis of Example 1 has shown, that without SES use for a man-operator of medium-level qualification the content volume and speed of the analysis are critical only. The small volume analyzed items content on a man in practice is caused by the limited human possibilities. Thus big volumes of data which are expedient for considering at decision-making, are missed from consideration.

Example 2 (estimation of SES operation correctness).

For real SES the volume of the analyzed items content increases in hundred times. Let SES under the characteristics of a correctness of actions is similar to a man-operator of medium-level qualification (for example, it is neurosystem, trained on level of the specialist of medium-level qualification). Unlike conditions of the Example 1 the content in volume of 2000 items is analyzed at speed of the analysis about 2000 items in a minute (i.e. SES is 100 times more productivity). Unlike man-operator SES does not requires to keep attention concentration (it performs automatically). Therefore for SES the period of continuous work is defined at 2000 hours, that are equivalent approximately to 3 months and is comparable with the period between technical maintenance regulations at the enterprises. The given time for items content analysis is equal to 1 minute still. It is required to estimate operation correctness of items content analysis for such SES.

Solution**.** The probability of correct SES operation will make the same 0.9993. At increase items content volume twice the probability of operation correctness decreases to 0.5 also, as well as in the Example 1 (Figure 5a)). The results of the calculated dependence of operation correctness probability on the speed of the analysis are similar also (Figure 5b)).

At the same time, change in a diapason -50 % + 100 % of frequency of the 1st type errors (Figure 5c)) and mean time between errors of the 2nd type (Figure 5d)) also insignificantly impacts probability of operation correctness.

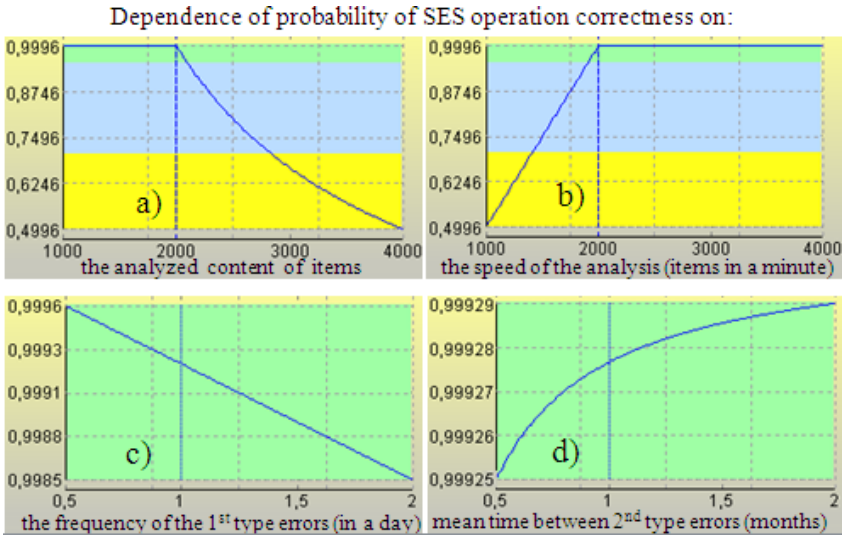

Figure 5. Dependence of probability of SES operation correctness on:
a) the analyzed content of items; b) the speed of the analysis (items in a minute);
c) the frequency of the 1st type errors (errors in a day); d) the mean time between errors of the 2nd type (months)

However, at all similarity of dependences on Figures 4 and 5 conclusions by the Example 2 are essentially others. Preliminary explanatories are the following – multiplying the volume 2000 items on probability of correct SES operation 0.9993, we receive, that in average there are correctly analyzed 1998.6 items. It means, that for 1.4 analyzed items (in average) a correctness is not provided! For example, incorrect interpretation in real time of one-two factors of threats in dangerous manufacture can lead for few minutes to occurrence of an explosive situation. If to provide quality and efficiency of SES application on a scientific basis, it is necessary to raise the correctness of SES operation for volume 2000 items to the level about 0.9998 so that the average quantity of items for which the correctness is not provided, was less than 0.5 (2000·0.9998=1999.6, i.e. only 0.4 items will be analyzed incorrectly).

Example 3 (estimation of operation correctness for SES with the improved characteristics).

Let SES is similar to the specialist of a high skill level (for example, well trained neurosystem). It is expressed that unlike conditions of the Example 2 the frequency of 1st type errors decreases twice, i.e. makes 0.5 errors a day. And mean time before error of 2nd type let will make 6 months (i.e. in 6 times more). Creation of such SES will demand increase in expenses essentially. Other conditions are the same, that in the Example 2. It is required to estimate changes in estimations concerning results of the Example 2 and to optimize requirements to such SES characteristics for admissible level of operation correctness.

Solution**.** For solving the proposed methods are applied (see section 5).The probability of correct SES operation will make the same 0.9993. At changes volume of the analyzed items and speed of analysis the dependencies of the probabilities of correct SES operation are similar resulted on Figure 5 a) and 5b).

Input changes in diapason -50 % + 100% led to following effects - see Figure 6a), b):

decrease in frequency of 1st type errors on the average more often 1 errors for three days provide probability of correct SES operation more low 0.9998;

keeping mean time between errors of the 2nd type up to 12 months can't increase the probability of correct SES operation more than 0.9997.

Researches have shown, that any efforts for increasing mean time between errors of the 2nd type in 2 times, demanding in practice essential expenses, will not lead to a desirable SES operation

correctness (more 0.9998). Therefore optimization by criterion «quality - cost» the choice of requirements "mean time between errors of the 2nd type should not be less than 6 months" is made, reaching the effects at the expense of decrease in frequency of 1st type errors.

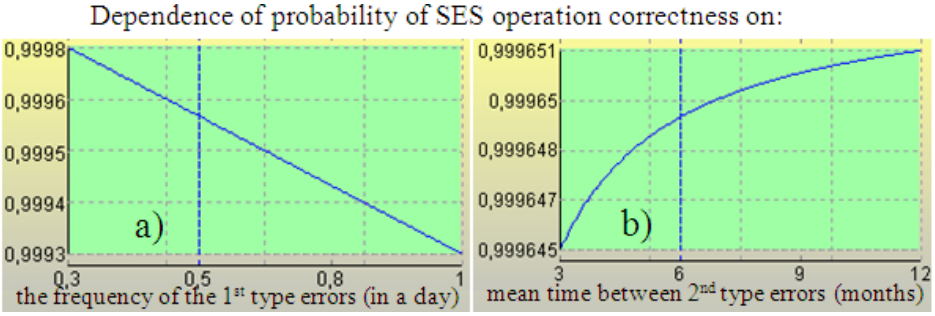

Figure 6. Dependence of probability of SES operation correctness on:
a) the frequency of the 1st type errors (errors in a day); b) the mean time between errors of the 2nd type (months)

Scientifically proved requirements by results of example 3 look as follows. For providing admissible high level of operation correctness (0.9998 and more) frequency of 1st type of errors should not exceed 1 error for three days, and mean time between errors of the 2nd type should not be less than 6 months. Let's remember this result.

Further we pass to application of the improved model for operation reliability prediction and the consecutive algorithm for prediction the risks of critical SES operation quality deterioration (subsections 3.2 and 3.3).

Example 4 (estimation of SES operation reliability without considering operation correctness).

Let's frequency of occurrence of the impacts for penetrating a danger source is equal to 300 times a year, and the mean activation time of a source of potential unreliability = 24 hours. The time between diagnostics of integrity traced by SES is equal to 1 hour. Duration of diagnostics and, if needs, a restoration of the lost integrity is equal in average to 20 minutes. The mean time before failures for SES is estimated about 2 years. It is required to predict SES reliability within prognostic period from 1 till 2 years.

Solution**.** The modeling results have shown - at change of input in a diapason -50 % + 100% the probability of reliable SES operation within 1 year is from 0.9993 to 0.9999. And even at increase prognostic period till 2th years the required probability for initial input data does not fall less 0.9995. Such usual estimation picture without considering correctness essentially varies if to consider not only reliability, but also SES operation correctness.

Example 5 (consideration of items analysis correctness and operation reliability when functions of SES are performed by a man-operator).

We take for a basis from the Example 4 initial given frequency of occurrence of the impacts for penetrating a danger source (300 times a year) and duration of diagnostics (20 minutes), and from the Example 1 - time between integrity diagnostics (8 hours instead of 1 hour from the Example 4), and the mean time before operator errors at monitoring is equal to 1 days (instead of 2th years from the Example 4). It is required to predict for 1 month and 1 year risks of critical operation quality deterioration taking into account impact of uncertainties on correctness and reliability (consequences in practice may be expressed in occurrence of emergencies, harm to health, damages) and estimate sensitivity of predicted risks.

Solution**.** The risks of critical operation quality deterioration during 1 month will make about 0.33 (considered consequences in practice may be expressed in occurrence of emergencies, harm to health, damages). The modeling has shown - at change of input in a diapason -50 % + 100% the risk

during 1 month is from 0.11 to 0.70 (see Figure 7, demonstrating also sensitivity of predicted risks). A virtual interpretation of these figures may be the following: if to compare a lot of months of a similar mode of operation (for example, 100 months) in 17 % to 70 % of these months emergencies because of operator critical errors in the analyzed information will take place.

It is expected the risk to lose integrity increases in depending on increasing time between integrity diagnostics, duration of diagnostics, prognostic period (the logic explanation see [2,5].

Results for prognostic period 1 year (the risk is near 0.99) confirm inevitability of emergencies for this long period.

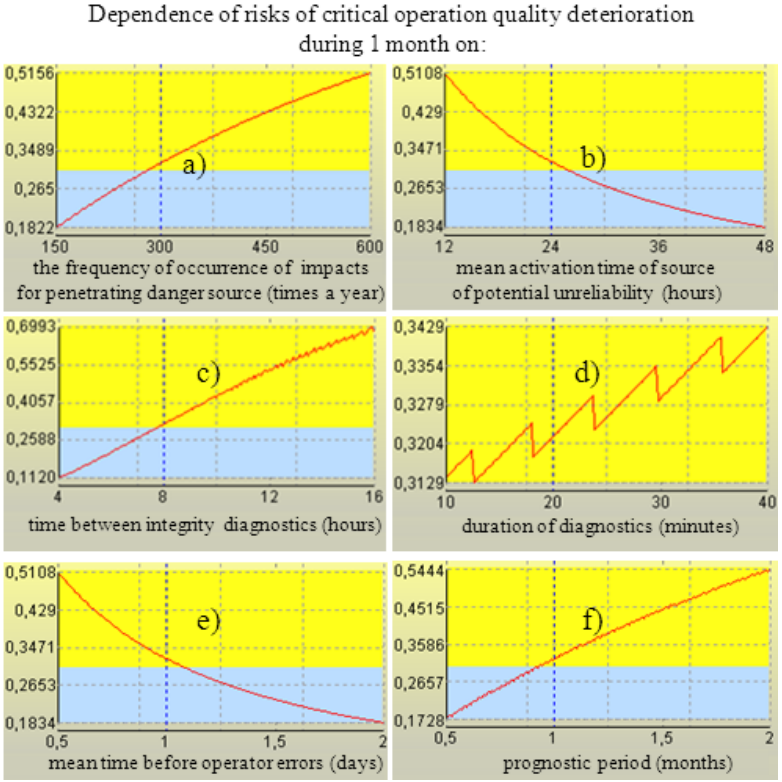

Figure 7 Dependence of risks of critical operation quality deterioration during 1 month on: a) the frequency of occurrence of impacts for penetrating danger source (times a year); b) mean activation time of source of potential unreliability (hours); c) time between integrity diagnostics (hours); d) duration of diagnostics (minutes); e) mean time before operator errors (days); f) prognostic period (months)

Example 6 (the primary consideration of 1st type of errors during SES operation, when unessential item is wrongly considered as essential).

The applications area for such SES is characterized by a weak degree of scrutiny, for example, there may be prospecting works on shelves of Arctic regions or space research, innovative researches. Critical deterioration of SES operation in practice can be expressed in wrong primary conclusions, wasted expenses, unforeseen emergencies and damages etc. For similar SES the errors of 1st type are much more often, rather than errors of 2nd type. To form input we use the results of researches of example 3 (for providing SES operation correctness - a frequency errors of 1st type should not exceed one error for three days) are used. Other input - from the Example 5. The differences are only: time between integrity diagnostics = 1 hour, and the mean time before operator errors at monitoring = 3 days. It is required to predict for 1 month and 1 year risks of critical operation quality deterioration taking into account impact of uncertainties on correctness and reliability.

Solution**.** The risks of SES critical operation quality deterioration during 1 month will make about 0.004 and during 1 year - about 0.05 (considering consequences).

The modeling results have shown - at change of input in a diapason -50 % + 100% the risk during 1 month is in diapason from 0.0016 to 0.0124 and during 1 year - from 0.002 to 0.139 (see Fig. 8, demonstrating also sensitivity of predicted risks).

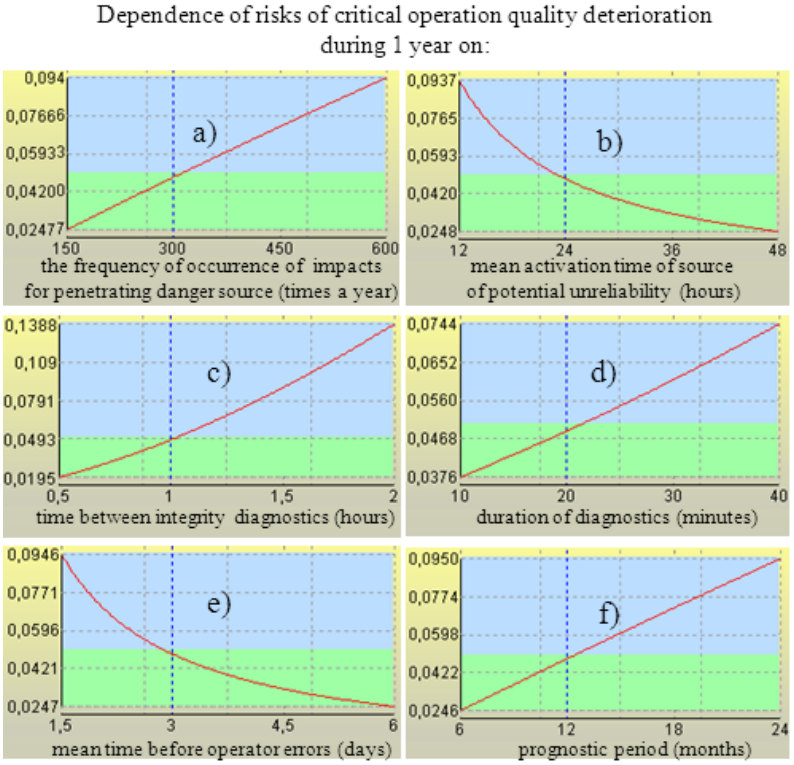

Figure 8 Dependence of risks of critical operation quality deterioration during 1 year on: a) frequency of occurrence of impacts for penetrating danger source (times a year); b) mean activation time of source of potential unreliability (hours); c) time between integrity diagnostics (hours); d) duration of diagnostics (minutes); e) mean time before operator errors (days); f) prognostic period (months)

Example 7 (the primary consideration of 2nd type of errors during SES operation, when essential item is missed).

The applications area for such SES is characterized by a high degree of scrutiny, for example, there may be monitoring of a current condition of the equipment and comparisons with admissible norms (for example, temperatures, pressure and so on – see requirements of standards ISO 13379, ISO 13381, ISO 17359, IEC 61508, etc.). Traced conditions of parameters are data about a condition before and on the current moment of time. Critical deterioration of SES operation in practice can be expressed in negative events after parameters abnormalities - failures, accidents, damages and-or the missed benefit because of equipment time out, etc. For similar SES the errors of 2nd type are much more often, rather than errors of 1st type. To form input we use the results of researches of example 3 (for providing SES operation correctness - "mean time between errors of the 2nd type should not be less than 6 months" instead of 3 days from Example 6) are used. Other input - from the Example 6. It is required to predict for 1 month and 1 year risks of critical operation quality deterioration taking into account impact of uncertainties on correctness and reliability.

Solution**.** The risks of SES critical operation quality deterioration during 1 month will make about 0.00007 and during 1 year - about 0.00086 (considering consequences). The modeling results have shown - at change of input in a diapason -50 % + 100% the risk during 1 month is in diapason from 0.00003 to 0.00021 and during 1 year - from 0.00032 to 0.00247 (see Fig. 9, demonstrating also sensitivity of predicted risks).

A virtual interpretation of these figures for 1 year SES operation may be the following: if to compare a lot of years of a similar mode of SES operation (for example, 1000 years) at worst within one or two years from 1000 years emergencies may be happen because of possible errors of 2nd type during items analysis by SES.

Example 8 (about pragmatic effects). Many examples demonstrating applications of the integrated model to predict the risks of critical operation quality deterioration for SES, composed as complex structures and optimization solutions cover oil&gas systems, systems of coal branch, robotic and automated systems [1-2, 5-11]. So, the Complex 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 SES of Complex to feel vibration, a fire, the flooding, unauthorized access, hurricane, and also intellectual SES of the reaction, capable to recognize, identify and predict a development of extreme situations. For 200 objects in several regions of Russia the applications of Complex 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 [6].

Conclusion

The methodology for risks of critical operation quality deterioration for SES is proposed. Complexity and uncertainties, impacting on SES operation correctness and reliability, are considered. Methodology covers improved models to estimate information correctness and operation reliability, consecutive algorithm to predict risks (for "black box»), integrated model to predict the risks for SES, composed as complex structures. Statements for optimization problems in SES life cycle are formulated. Researches have shown comparable impacts on SES operation quality from failures (reliability) and errors (correctness). The levels about 0.999-0.9997 and more for probability of SES operation correctness and reliability and about 0.01 – 0.001 and less for risks of critical SES operation quality deterioration during 1 year (against consequences) are achievable. The benefit from SES implementations in a system life cycle may be commensurable with expenses for a creation of this system.

References

[1] Kostogryzov, A. and Nistratov, G. Standardization, mathematical modelling, rational management and certification in the field of system and software engineering. Armament.Policy.Conversion, Moscow, 2004.

[2] Zio, En. An Introduction to the Basics of Reliability and Risk Analysis, World Scientific Publishing Co.Pte.Ltd., 2006.

[3] Kostogryzov, A.I. and Stepanov, P.V. Innovative management of quality and risks in systems life cycle. Moscow, Armament.Policy.Conversion, Moscow, 2008.

[4] Kolowrocki, K. and Soszynska-Budny, J. Reliability and Safety of Complex Technical Systems and Processes, Springer-Verlag London Ltd., 2011.

[5] 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: 127-196.

[6] Abrosimov, N., at al. Security of Russia. Legal, Manufacturing&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of Mahutov N.A. Znanie, Moscow, 2015.

[7] Artemyev, V., Rudenko, Ju., Nistratov, G. Probabilistic modeling in system engineering. Probabilistic methods and technologies of risks prediction and rationale of preventive measures

by using "smart systems". Applications to coal branch for increasing Industrial safety of enterprises, IntechOpen, 2018: 23-51.

[8] Kershenbaum, V., Grigoriev, L., P. Kanygin, Nistratov, A. Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems, IntechOpen, 2018: 55-79.

[9] Abrosimov, N., at al. Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic, Technologic and Technospheric Safety / Edited by N.Machutov – Moscow, «Znanie», 2018

[10] Lepikhin, A., Moskvichev, V., Machutov, N. Probabilistic Modelling in Solving Analytical Problems of System Engineering, Probabilistic modeling in system engineering. InTech, 2018, 3-22

[11] Kostogryzov, A., Korolev, V. Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems, IntechOpen, 2019. Doi: http://dx.doi.org/10.5772/intechopen.89168

[12] Kostogryzov, A., Kanygin, P., Nistratov, A. Probabilistic comparisons of systems operation quality for uncertainty conditions. RTA&A No1(56), 2020, 15:63-73.

Received: May 30, 2020
Accepted: August 20, 2020