BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

**Artificial Intelligence Advances**
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

# Probabilistic Rationale of Actions for Artificial Intelligence Systems Operating in Uncertainty Conditions

**Andrey I. Kostogryzov**[1,2*]

1. Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Vavilova Str. 44, bld.2, Moscow, 119333, Russia
2. Gubkin Russian State University of Oil and Gas (National Research University) Leninsky Av. 65, bld. 1, Moscow, 119991, Russia

ARTICLE INFO

*Article history*
Received: 10 September 2019
Accepted: 15 October 2019
Published Online: 30 October 2019

*Keywords:*
Analysis
Artificial intelligence systems
Model
Operation
Prediction
Probability
Rationale
Risk
System
System engineering

ABSTRACT

The approach for probabilistic rationale of artificial intelligence systems actions is proposed. It is based on an implementation of the proposed interconnected ideas 1-7 about system analysis and optimization focused on prognostic modeling. The ideas may be applied also by using another probabilistic models which supported by software tools and can predict successfulness or risks on a level of probability distribution functions. The approach includes description of the proposed probabilistic models, optimization methods for rationale actions and incremental algorithms for solving the problems of supporting decision-making on the base of monitored data and rationale robot actions in uncertainty conditions. The approach means practically a proactive commitment to excellence in uncertainty conditions. A suitability of the proposed models and methods is demonstrated by examples which cover wide applications of artificial intelligence systems.

## 1. Introduction

Different mathematical models and methods are applied in system analysis. System analysis is required at level of the international standards of system engineering - for example, ISO/IEC/IEEE 15288 "System and software engineering – System life cycle processes", ISO 17359 "Condition monitoring and diagnostics of machines - General guidelines", IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems" etc. It is recommended for using every time across all life-cycle to analyze performance, system behaviour, feasibility, affordability, critical quality characteristics, technical risks, sensitivity for

**Corresponding Author:*
*Andrey I. Kostogryzov,*
*Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Vavilova Str. 44, bld.2, Moscow, 119333, Russia; Gubkin Russian State University of Oil and Gas (National Research University) Leninsky Av. 65, bld. 1, Moscow, 119991, Russia;*
*Email: Akostogr@gmail.com*

 DOI: https://doi.org/10.30564/aia.v1i2.1195

changes of critical parameters values etc. Artificial intelligence systems (AIS) which are understood here as systems, performing functions by logic reasoning on the base of data processing, also needs system analysis because of their complexities and uncertainty conditions.

***Note:*** *System is combination of interacting elements organized to achieve one or more stated purposes (according to ISO/IEC/IEEE 15288).*

Considering AIS specificity there may be some scientific problems devoted to:

(1) system analysis of uncertainty factors, capabilities of operation in real time, information gathering and processing, protection from authorized access and dangerous influences;

(2) analysis of system requirements to acceptable conditions;

(3) system analysis and optimization in architectural design;

(4) comparative and prognostic estimations of quality, safety, interaction "user-system" and conditions, optimization of different processes, rationale of operation in uncertainty, etc.

Now there isn't enough universal effective approach to rationale of actions for AIS operating in uncertainty conditions. In practice for each concrete case it is often used subjective expert estimations, a regression analysis of collected data, a simulation of processes [1-14]. It means, that search of new methods for advanced rationale actions of AIS and by AIS is today very important. The proposed approach is focused on probabilistic rationale of actions to operate in uncertainty conditions against existing approaches for which applied mathematical methods cover mainly information processing in the logician if …, that … and/or tracing situations by a man-operator. An application scope of this paper covers AIS supporting decision-making in intellectual manufacture (for example, in dispatcher intelligence centers) and robotics systems operating in uncertainty conditions and used to provide operation efficiency or/and increase reliability and safety (including aerial, land, underground, underwater, universal and functionally focused AIS).

The main efforts of this paper are not connected with illustrating the capabilities of AIS, but they are focused on demonstrating the applicability of original probabilistic models and methods to improve some of the existing capabilities of AIS [15-45]. For this goal by the use of these probabilistic models the next specific problems are covered:

(1) the problem 1 - to rationale a rational variant for decision-making on the base of monitored data about events and conditions, and

(2) the problem 2 - to rationale a robot actions under limitations on admissible risks of "failures" (according to ISO Guide 73 risk is defined as effect of uncertainty on objectives considering consequences. An effect is a deviation from the expected — positive and/or negative).

***Note:*** *Some relevant problems (such as the problems of robotics orientation, localization and mapping, information gathering, the perception and analysis of commands, movement and tactile, realizations of manipulations for which different probabilistic methods are also applicable) have not been covered by this work.*

The proposed approach for solving AIS problems are based on theoretical and practical researches [15-45] and need to be used either in combination or in addition to existing methods which are used now in AIS. There, where it is required often prognostic system analysis or where the used approaches are not effective, the proposed probabilistic approach can be used as rational basis or alternative. The ideas of this approach may be applied also by using another probabilistic models which supported by software tools and can predict success or risks on a level of probability distribution functions (PDF). The structure of this research is shown by the Figure 1.

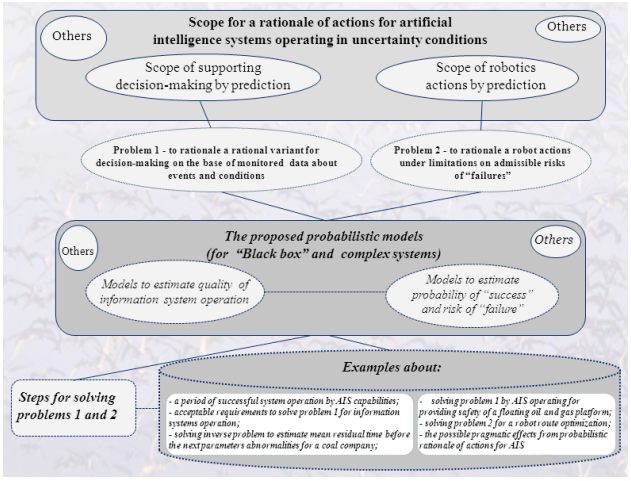


**Figure 1.** The structure of the research

Various fields of the examples applications have been chosen purposely to demonstrate universality and analytical usefulness of the probabilistic approach. The proposed models and methods are an original Russian creation, they have been presented at seminars, symposiums, conferences, ISO/IEC working groups and other forums since 2000 in Russia, Australia, Canada, China, Finland, France, Germany, Italy, Kuwait, Luxembourg, Poland, Serbia, the USA, etc. The supporting software tools were awarded by the Golden Medal of the International Innovation and Investment Salon and the International Exhibition "Intellectual Robots", acknowledged on the World's fair



DOI: https://doi.org/10.30564/aia.v1i2.1195

of information technologies CeBIT in Germany, noted by diplomas of the Hanover Industrial Exhibition and the Russian exhibitions of software.

## 2. The essence of the approach

The AIS behaviour corresponding to the rationale of actions for AIS operating in uncertainty conditions means proactive commitment to excellence. Such behaviour is based on an implementation of the next proposed interconnected ideas 1-7.

***Idea 1*** is concerning the usual concept and properties of probability distribution functions (PDF) [15] for a continuous random variable of time. PDF for a time variable $\tau$ is nondecreasing function P(t) whose value for a given point $t \geq 0$ can be interpreted as a probability that the value of the random variable $\tau$ is less or equal to the time value t, i.e. $P(t)=P(\tau \leq t)$. Additionally $P(t)=0$ for $t<0$, and $P(t) \rightarrow 1$ for $t \rightarrow \infty$. In general case the solutions for the problems 1 and 2 are based on using concept of the probabilities of "success" and/or "unsuccess" (risk of "failure") during the given prognostic time period $t_{req.}$. This probability is a value for a point $t_{req.}$ and is defined by created PDF.

***Idea 2***. The processes, connected with data processing, and used information should provide required AIS operation quality (because AIS is a system, performing functions by logic reasoning on the base of data processing). And corresponding probabilistic methods should appropriate for prognostic estimations.

***Idea 3***. The PDF should be presented as analytical dependence on input parameters. It needs to solve direct and inverse problems to rationale of actions in a real time of AIS operation. For example, for a simple element PDF P(t) of time $\tau$ between losses of element integrity may be presented by analytical exponential approximation, i.e. $P(t) = 1-\exp(-\lambda t)$, where $\lambda$ is frequency of failures (losses of element integrity). At the same time frequency of failures may be represented as a sum of frequencies of failures because of specific reasons for each failure type – for example, failure from "human factor" $\lambda_1$, from hardware $\lambda_2$, from software $\lambda_3$ and so on. For this use case PDF may be presented as $P(t) =1-\exp[-(\lambda_1+\lambda_2+\lambda_3+\ldots)t]$. Then if the adequate function P(t) is built in dependence on different parameters and if admissible level for probability is given than inverse problem may be solved.

***Note.*** *The rationale for exponential approximation choice in practice see, for example, in* [28, 30].

***Idea 4.*** The PDF should be adequate, it means a dependence on several essential parameters which define AIS operation and on which "success" or "failure" of AIS operation is mainly dependent. For example the way for risks prediction based on uses only one parameter - frequency of failures $\lambda$ - is popular today. This implies the use of corresponding exponential PDF – see Figure 2. Only one connection of the frequency of failures $\lambda$ with random time variable $\tau$ between losses of system integrity may be interpreted as the requirement: "to provide no failures during required time with probability no less than the given admissible probability $P_{adm.}$ this required time should be no more than $t_{req.} = 1/\lambda_{adm.}$, here $\lambda_{adm.}=-\ln(1-R_{adm.})$". But for AIS element it is rough and unpromising engineering estimations because capabilities of monitoring conditions and recovery of the lost element integrity are ignored. Such disregard deforms very essentially probabilistic estimations of probabilistic risk values and can't be useful for scientific search of effective counteraction measures against different threats. Deviations from more adequate PDF estimations are very high [33,44,45]. On Figure 3 the limitations to admissible risks, fragment of exponential and an adequate PDF of time between losses of system integrity with identical frequency of system integrity losses are illustrated (in conditional units). It means more adequate PDF allows more right understanding of probabilistic AIS vision of events prediction with scientific interpretation considering situations in time line.

***Note:*** *System integrity is defined as such system state when system purposes are achieved with the required quality.*

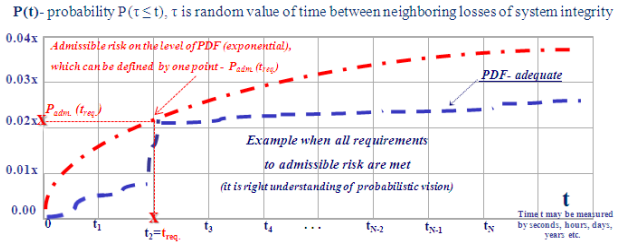


**Figure 2.** The possible variants of correlations for admissible risks, exponential and an adequate PDF of time between losses of system integrity with identical frequency of losses

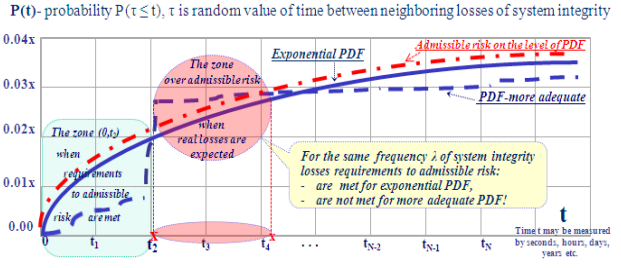


**Figure 3.** All requirements to admissible risk are met for an adequate PDF of time between losses of system integrity

***Idea 5.*** Because an AIS is a complex system and this

AIS may be subsystem or element of comprehensive complex system, the proposed approach should allow a generation of probabilistic models for prediction of "success" or "failure" of AIS actions in uncertainty conditions. In general case an input for generated models used in real time should consider system complexity, periodical diagnostics, monitoring between diagnostics, recovery of the lost integrity for every system element and also processes, connected with data processing, and used information. As an output of such generated models adequate PDF of time τ between losses of system (subsystem, element) integrity should be produced in analytical form.

***Idea 6***. Input for probabilistic modeling should be formed mainly from gathered data and established specific order of AIS actions.

***Idea 7***. To probabilistic rationale of actions for AIS operating in uncertainty conditions the problems of optimization should be solved. Optimization should be performed in real time by defined beforehand optimization problem statement. Every time the used optimization problem statement should be appropriated for solving specific problem 1or 2. For probabilistic rationale of actions the prognostic period should be defined so to be in time to do the given action or complex of actions on acceptable level according to optimization criterion or to perform preventive action (with which the initiation of performing an action or solving a problem is connected) or/and to recover operation capabilities (which can be lost).

For the approach implementation the next probabilistic models are proposed.

## 3. The Description of the Proposed Models

In general case a probabilistic space ($\Omega$, $B$, $P$) for probabilistic modeling is created [15], where: $\Omega$ - is a limited space of elementary events; $B$ – a class of all subspace of $\Omega$-space, satisfied to the properties of σ-algebra; $P$ – is a probability measure on a space of elementary events $\Omega$. Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \rightarrow p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$.

In order not to overload the reader with mathematical details, the final formulas for calculations are presented in the Appendixes A and B.

### 3.1 About AIS operation quality

The proposed models help to implement ideas 1 and 2.

In general case AIS operation quality is connected with requirements for reliable and timely producing complete, valid and/or, if needed, confidential information. The gathered information is used for proper AIS specificity. The abstract view on a quality of used information is presented on Figure 4.

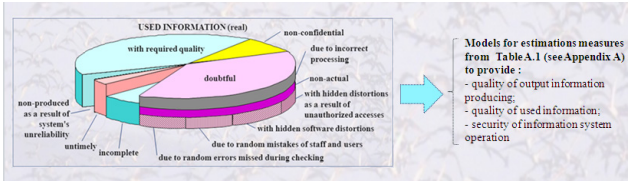


**Figure 4.** Abstract explanation for a quality of used (real) information against required one

The proposed models for the estimation of information systems operation quality are described in Table A.1 of Appendix.

The main analytical models and calculated measures are the next:

(1) "The model of functions performance by a complex system in conditions of unreliability of its components";

(2) "The models complex of calls processing";

(3) "The model of entering into IS current data concerning new objects of application domain";

(4) "The model of information gathering";

(5) "The model of information analysis";

(6) "The models complex of dangerous influences on a protected system";

(7) "The models complex of an authorized access to system resources".

Risk to lose integrity (R) is an addition to 1 for probability of "success" (P), i.e. R=1-P considering consequences.

These models, supported by different versions of software Complex for Evaluation of Information Systems Operation Quality, registered by Rospatent №2000610272 [46], may be applied and improved for solving problems 1 and 2.

### 3.2 About Risks Prediction for System Formalized as "Black box"

The proposed models helps to implement ideas 1, 3, 4.

In general case successful system operation (not only AIS) is connected with system counteraction against various dangerous influences on system integrity - these may be counteractions against failures, defects events, "human factors" events, etc. There are proposed the formalization for two general technologies of providing counteraction against threats: periodical diagnostics of system integrity (technology 1, without monitoring between diagnostics) and additionally monitoring between diagnostics (technology 2). As a rule these technologies are implemented by AIS.



DOI: https://doi.org/10.30564/aia.v1i2.1195

***Technology 1*** is based on periodical diagnostics of system integrity, that is carried out to detect danger sources penetration into a system or consequences of negative influences (see Figure 5). 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.

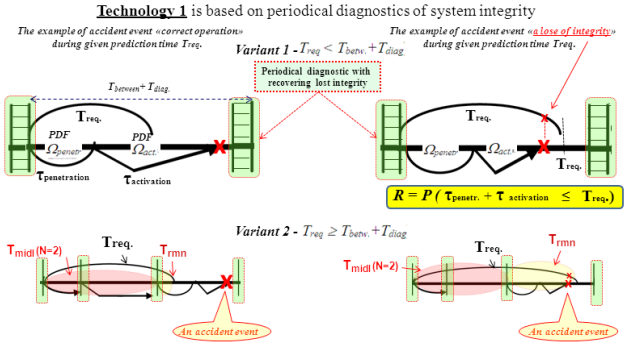


**Figure 5.** Some accident events for technology 1 (left – correct operation, right – a lose of integrity during prognostic period $T_{req.}$)

***Technology 2***, unlike the previous one, implies that system integrity is traced between diagnostics by operator (operator functions may be performed by a man or special AIS component 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 – see Figure 6.

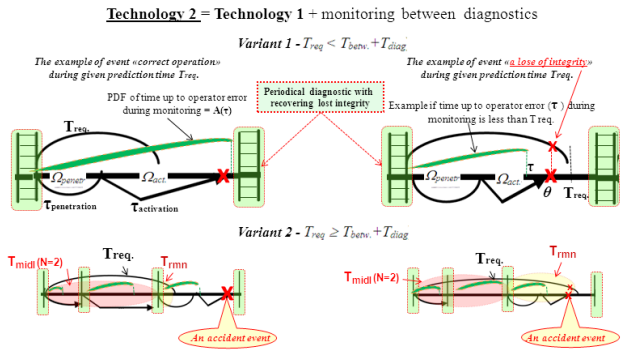


**Figure 6.** Some accident events for technology 2 (left – correct operation, right – a lose of integrity during prognostic period $T_{req.}$)

Faultless operator's actions provide a neutralization of a danger source trying to penetrate into a system. 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.

The probability of correct system operation within the given prognostic period (i.e. probability of "success" - P) may be estimated as a result of use the models presented in Appendix B. Risk to lose integrity (R) is an addition to 1 for probability of correct system operation (P), i.e. R=1-P considering consequences.

## 3.3 About a Generation of Probabilistic Models for Complex System

The proposed method for a generation of probabilistic models helps to implement ideas 1 and 5.

The basic ideas of correct integration of probability metrics are based on a combination and development of models. For a complex systems with parallel or serial structure described there are proposed the next method to generate adequate probabilistic models [25,26,28-30]. This method uses the usual way of probability theory for independent random variables. However, given the importance to rationale the generation of new probabilistic models for complex system, the approach is described below.

Let's consider the elementary structure from two independent parallel or series elements. Let's PDF of time between losses of i-th element integrity is $B_i(t) = P(\tau_i \leq t)$, then:

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

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

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

 DOI: https://doi.org/10.30564/aia.v1i2.1195

$$B(t)=P[\max(\tau_1,\tau_2)\leq t]=P(\tau_1\leq t)P(\tau_2\leq t)=B_1(t)B_2(t) \quad (2)$$

Applying recurrently expressions (1) – (2), it is possible to build PDF of time between losses of integrity for any complex system with parallel and/or series structure and theirs combinations.

An example of complex system integrating two serial complex subsystems (abstraction) is presented by Figure 7. For this integration the next interpretation of elementary events is used: complex system integrating compound components "Intellectual tructure 1 and 2" is in condition "correct operation" ("success") during given period $T_{req.}$ if during this period "AND" component "Intellectual tructure 1" "AND" component "Intellectual tructure 2" (both are special complex subsystems including AIS subsystems and elements) are in condition "correct operation" ("success").

All ideas for analytical modeling complex systems are supported by the software tools "Mathematical modeling of system life cycle processes" – "know how" (registered by Rospatent №2004610858), "Complex for evaluating quality of production processes" (registered by Rospatent №2010614145) and others [46-51].

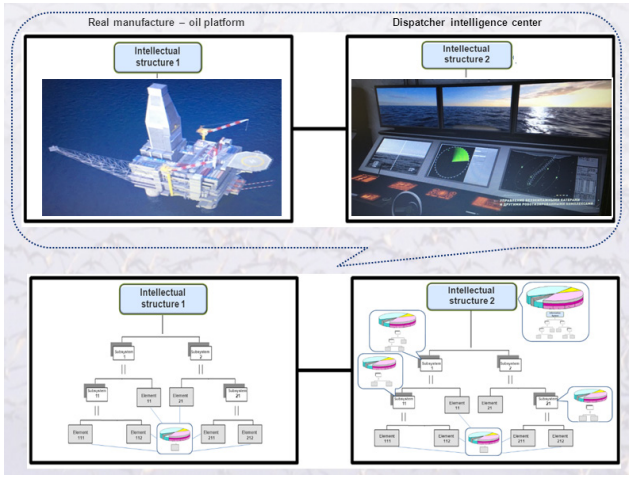


**Figure 7.** An example of complex system integrating two serial complex intellectual structures which also are complex subsystems (abstraction)

### 3.4 About Data Forming for Probabilistic Modeling

The proposed practical way to data forming helps to implement idea 6.

For each critical parameter (for which prognostic estimations are needed to do actions) the ranges of acceptable conditions can be established. The traced conditions of monitored parameters are data about a condition before and on the current moment of time. For example, the ranges of possible values of conditions may be established: "Working range inside of norm", "Out of working range, but inside of norm", "Abnormality" for each separate critical parameter. If the parameter ranges of acceptable conditions are not established in explicit form than for modeling purpose the may be implead and can be expressed in the form of average time value. These time values are used as input for probabilistic modeling. For example, for coal mine some of many dozens heterogeneous parameters are: for ventilation equipment - temperature of rotor and engine bearings, a current on phases and voltage of stator; for modular decontamination equipment - vacuum in the pipeline, the expense and temperature of a metano-air mix in the pipeline before equipment, pressure in system of compressed air, etc. It may be interpreted similarly by light signals – "green", "yellow", "red" - see Figure 8 and following Example 6.3.

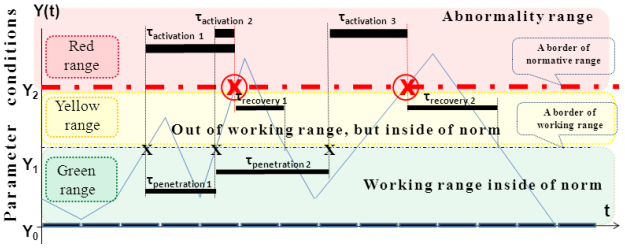


**Figure 8.** An example of universal elementary ranges for monitoring data about events and conditions

## 4. Optimization Problem Statements for Rationale Actions

The proposed optimization problem statements for rationale actions helps to implement idea 7. For example the proposed ideas 2-6 may be supported by the next typical optimization problem statements for AIS [25,28,30]:

(1) on the stages of system concept, development, production and support: system parameters, software, technical and control measures (Q) are the most rational for the given prognostic period if on them the minimum of expenses ($Z_{dev.}$) for creation is reached

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

(1A) 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 development, operation or maintenance conditions; or

(1B) at limitations on admissible risk to lose system integrity $R \leq R_{adm.}$ and expenses for operation $C_{oper.}(Q) \leq C_{adm.}$ and under other development, operation or mainte-



DOI: https://doi.org/10.30564/aia.v1i2.1195

nance conditions; or

(1C) at limitations presented as combination 1A) and 1B);

(2) on utilization stage:

(A) system parameters, software, technical and control measures (Q) are the most rational for the given period of AIS operation if on them the maximum of probability of correct system operation is reached

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

(2A.a) 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; or

(2A.b). at limitations on admissible risk to lose system integrity $R \leq R_{adm.}$ and expenses for operation $C_{oper.}(Q) \leq C_{adm.}$ and under other operation or maintenance conditions; or

(2A.c). at limitations presented as combination 2A.a) and 2A.b);

(B) system parameters, software, technical and control measures (Q) are the most rational for the given period of system operation if on them the minimum of risk to lose system integrity is reached

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

(2B.a) 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; or

(2B.b) at limitations on admissible risk to lose system integrity $R \leq R_{adm.}$ and expenses for operation $C_{oper.}(Q) \leq C_{adm.}$ and under other operation or maintenance conditions; or

(2B.c). at limitations presented as combination 2A.a) and 2A.b);

These statements may be transformed into the problems of expenses minimization in different limitations. There may be combination of these formal statements in system life cycle.

Note. Another variants of optimization problem statements are possible.

## 5. The incremental algorithms for solving the problems 1 and 2

The proposed algorithms for solving the problems 1 and 2 are based on using the models and methods above.

### 5.1 The Algorithm for Solving Problem to Rationale a Rational Variant for Decision-making on the Base of Monitored Data About Events and Conditions (problem 1)

It is supposed that the terms "success" and accordingly "unsuccess" ("failure") are defined in terms of admissible condition of interested system to operate for the purpose according to required quality.

***Note:*** *For example for each parameter of equipment the ranges of possible values of conditions may be estimated as "Working range inside of norm" and "Out of working range, but inside of norm" ("success") or "Abnormality" ("failure"), interpreted similarly light signals – "green", "yellow", "red". For this definition a "ailure" of equipment operation characterizes a threat to lose system norm integrity after danger influence (on the logic level this range "Abnormality" may be interpreted analytically as failure, fault, losses of quality or safety etc.).*

The proposed steps for solving problem 1 to rationale a rational variant for decision-making on the base of monitored data about events and conditions may be carried out by the next 4 steps – see Figure 9.

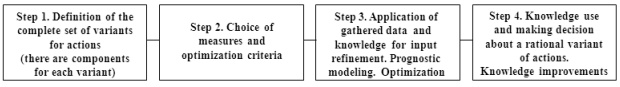


**Figure 9.** Steps for solving problem 1

***Step 1***. The complete set of variants for actions is defined, including for each variant – a definition of compound components is being. Each use case may be characterized by an expected benefit in comparable conventional units. If the objective value of a benefit can't be defined, expert value of a level of "success" may be established, for example, on a dimensionless scale from 0 to 100 (0 – «no benefit», i.e. "failure", 100 – «the maximal benefit », i.e. complete "success").

***Step 2.*** The measures and optimization criteria are chosen (see sections 3 and 4). As criteria there can be accepted:

(1) maximum of benefit as a result of system operation under the given conditions and limitations on the acceptable risk of "failure" and/or other limitations;

(2) maximum probability of "success" or minimum risk of "failure" under limitations.

***Step 3***. The knowledge is used to refine the input for modeling. Using the probabilistic models and methods for each variant, the "success" measures are calculated for the given prognostic period. From a set of possible variants the optimal one is chosen according to the step 2 criterion.

 DOI: https://doi.org/10.30564/aia.v1i2.1195

***Note:*** *Formal statements of optimization may be connected with maximization of benefit at limitations on admissible levels of quality and/or risks measures or with minimization of risks at limitations on admissible levels of benefit and/or quality and/or risks measures and/or under other operation or maintenance conditions (see section 4).*

***Step 4.*** A decision for the optimal variant of actions (defined in step 3) is made. In support of the efficiency of the functions, the achievable benefit calculated at step 3 is recorded. New knowledge is improved and systematized by comparing it with reality (including comparisons of probabilistic estimations and real events).

***Note:*** *A solution that meets all conditions may be not existing. In this case, there is no optimal variant of system operation on the base of monitored data about events and conditions.*

### 5.2 The Algorithm for Solving Problem to Rationale a Robot Actions under Limitations on Admissible Risks of "Failures" (problem 2)

The approach for solving problem 2 to rationale a robot actions under limitations on admissible risks of "failures" is demonstrated in application to robot route optimization in conditions of uncertainties.

For a robot, the concept of "failure" under uncertainty is defined as the failure to achieve the goal within a given time. It is assumed that there are several possible routes to achieve the goal, and uncertainties may include both the conditions for robot operation (including random events in orientation, localization and mapping). The minimum risk of "failure" under the existing conditions and limitations is set as a criterion of optimization.

The proposed steps for solving problem 2 of robot route optimization under limitations on admissible risks of "failure" under conditions of uncertainties may be carried out by the next 4 steps – see Figure 10.

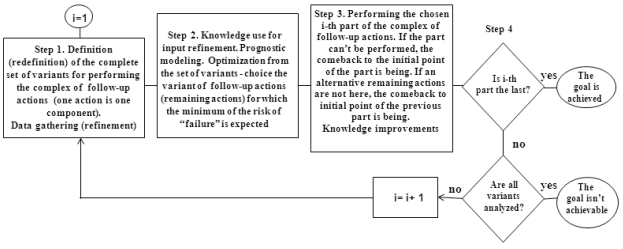


**Figure 10.** Steps for cognitive solving problem 2

***Step 1***. The complete set of route variants to achieve the goal within the given time, and for each variant – a set of components, is defined (redefined). Data characterizing every part of route for each of the variants are gathered (refined) for modeling. To do this, a specific robot can use data from various sources (for example, from air drones, intelligent buoys on the water or sensors under water, etc.). If necessary, possible damages are taken into account. For example, each use case may be characterized by an expected damages in comparable conventional units. If the objective value of a damage can't be defined, expert value of expected level of "failure" for each variant may be set, for example, on a dimensionless scale from 0 to 100 (0 – «no damages», i.e. "success", 100 – «the maximal damage»).

The index i of the first part of the selected route is set to the initial value i=1.

***Step 2***. The knowledge is used to refine the input for prognostic modeling. Using probabilistic model, a calculation of the probability of "failure" (risk of "failure") is carried out for each variant. From the set of variants (remaining route) the optimal one is chosen, for its the minimum probability of "failure" (risk of "failure") is achieved.

***Step 3***. The robot overcomes the i-th part of the selected route. If the part can't be overcome, the comeback to the initial point of the part is being. If an alternative route isn't here, the comeback to initial point of the previous part is being. The input for modeling every part of possible route for each of the variants are updated. New knowledge is improved and systematized by comparing it with reality (including comparisons of prognostic risks and real events).

***Step 4.*** If, after overcoming the i-th part, the robot arrived at the intended point of route (i.e., the last part of the route is overcome and the goal is achieved), then the solution for optimizing the route is complete. If the robot hasn't yet arrived at the intended point (i.e. the last part of the route isn't overcome), then the complete set of different route variants for achieving the goal is redefined (similar to step 1). The input for modeling every part of possible route for each of the variants are updated, i= i+1. Then steps 2-4 are repeated until the last part of the route is overcome on the set of possible variants (i.e. it means the goal is achieved and problem 2 is solved).

If the set of possible options is exhausted and the goal is not achieved, it is concluded that the goal is unattainable with the risk of "failure" less than the acceptable risk (i.e., it means an impossibility of solving problem 2 in the defined conditions).

Thus, to rationale a robot actions under limitations on admissible risks of "failures" (i.e. to a "successful" solution of problem 2) in real time, information gathering, probabilistic predictions for possible route variants, their comparison, the choice of the best variant, the implementation of further actions, the improvement, systematization



DOI: https://doi.org/10.30564/aia.v1i2.1195

and use of knowledge are being.

## 6. Examples

### 6.1 About a Period of Successful System Operation by AIS Capabilities

The example is related partly to solving the problem 1 and concerning an estimation of successful system operation during a long time by AIS capabilities in comparison against an usual system without or with usual sensors (without artificial intelligence capabilities to logic reasoning).

How long time may be a period of successful system operation by AIS capabilities? And what about conditions for this long period?

Those threats to system operation which are known, traced at diagnostics and do not cause irreversible consequences at the first influence, are considered only. Besides, it is supposed, that an integrity can be operatively recovered after AIS recovering reaction at the earliest stages of detection of dangerous or guarding symptoms. Moreover, at modeling the time of full integrity recovering is artificially reduced till diagnostic time. Thus, the elementary condition "acceptable integrity" means such system state when system purposes are achieved with the required quality, i.e. absence of danger source or neutralization of a penetrated source at the earliest stage prior to the its danger influence after activation. It (as supposed by the model) enough for successful AIS operation.

***Note:*** *The above assumptions are supposed for modeling. In a reality it may be not always so. These conditions are considered for interpretation of modeling results.*

To compare system operation with AIS capabilities against an usual system (without artificial intelligence capabilities) for the same conditions we consider AIS possibilities to provide "acceptable integrity" by continuous monitoring with artificial intelligence logic reasoning. Let's the threats to system integrity are being about 1 time a day because of natural or technogenic threats and "human factor". Let's also after occurrence of a danger source an average activation time is equal to 6 hours, during which else it is possible to prevent or neutralize negative influence.

Two variants of reaction caring of AIS integrity are compared. 1st variant (an usual system) considers the address to a recovering center about 1 time a month and reception of necessary recovering procedures within 4 hours after diagnostics. 2nd variant means AIS performing functions of diagnostics every 4 hours and recovering acceptable integrity within one hour. For all variants mean time between operator's error during continuous monitoring of system integrity is estimated not less than 1 year (for general technology 2). Initial input data for probabilistic modeling are reflected by the Table 1, the used model is described in subsection 3.2 of this paper.

**Table 1.** Input for estimation

| Input for modeling | Variants for comparisons | |
|---|---|---|
| | 1-st (an usual system) | 2-nd (an AIS) |
| The given prognostic period ("in future") | 3 years | 5 years |
| The frequency of influences for penetrating into system | 1 day$^{-1}$ | 1 day$^{-1}$ |
| The mean activation time | 6 hours | 6 hours |
| The time between the end of diagnostic and the beginning of the next diagnostic | 1 month | 4 hours (by AIS capabilities) |
| The diagnostic time | 4 hours | 1 hour (by AIS capabilities) |
| The mean time between operator's error during continuous monitoring of system integrity | 1 year | 1 year |

Some probabilities of providing system integrity in dependence on input, changing in diapason -50%+100% from Table 1 data, are presented on Figures 11-139. They cover dependences on the given prognostic period, the time between the end of diagnostic and the beginning of the next diagnostic, the mean time between operator's error during continuous monitoring of integrity. Deviations for other dependences are insignificant.

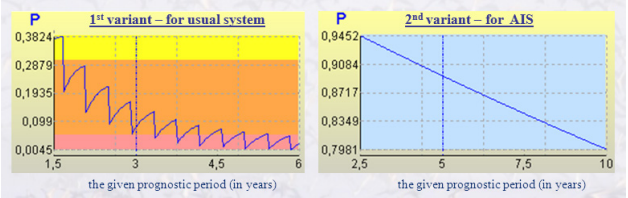


**Figure 11.** The probability of providing system integrity in dependence on the given prognostic period

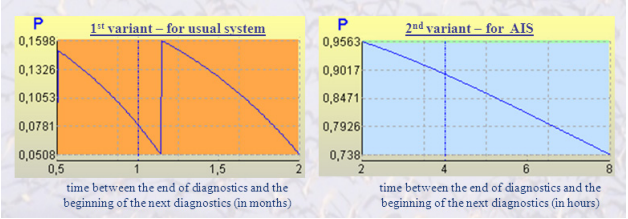


**Figure 12.** The probability of providing system integrity in dependence on the time between the end of diagnostics and the beginning of the next diagnostics

 DOI: https://doi.org/10.30564/aia.v1i2.1195

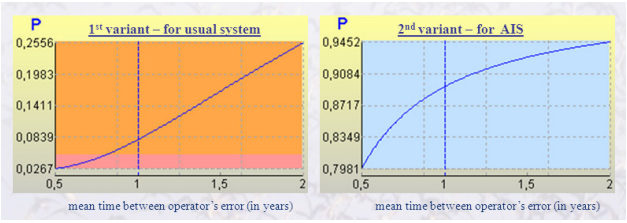


**Figure 13.** The probability of providing system integrity in dependence on the mean time between operator's errors during continuous monitoring of system integrity

Results of modeling show, that for 1st variant (for an usual system) the probability to provide "acceptable integrity" during 1 year is equal to 0.39, during 2 years – not less than 0.16, during 3 years – only 0.07. It means practically the inevitability of a failure during 2-3 years. 2nd variant (for AIS) with operative recovering is more effective. Really, it is possible to provide "acceptable integrity" for system operation with AIS capabilities within 3-5 years with probability about 0.90-0.93 – it may be interpreted as successful operation 9 times from 10 possible five-year periods. These results of modelling should serve a rationale for development counteractions against threats. Conditions for five-year period of successful system operation with AIS capabilities are presented in Table 1 for 2nd variant.

Note. Serrated and nonmonotonic character of dependence on Figures 11, 12 (left) is explained by the periodic diagnostics, monitoring presence or absence and their quantitative values, and also because of parameter "N" is integer part – see Appendix B. Detais see in [30].

Of course the concepts "acceptable integrity" and "failure" of special system should be defined in details (which produced input for modeling). However the expected modeling results against typical plausible input for this this simple example has also demonstrated for readers a suitability of the proposed probabilistic "Black box" models (from section 3).

## 6.2 Example 2 of Acceptable Requirements to Solve Problem 1 for Information Systems Operation

The example is connected with rationale a rational requirements to information system (IS) operation for providing high information quality for using in an AIS. Information systems are systems for which input is information and output (as result of IS operation) also is information for following use according to purpose. This example summarizes the numerous results of researches performed for IS operating in government agencies, manufacturing structures (including power generation, coal enterprises, oil-and-gas systems), emergency services etc. [20,25,28,30-33,35-45]. The results are based on described modeling to provide quality of output information producing, quality of used information IS and security of IS operation (see Table A.1 from Appendix A).

According to this generalization for the best practice of IS operation the acceptable requirements are the next (see the measures from Table 1):

(1) to provide quality of output information producing:

A. Probability of providing reliable function performance during given time should be no less than 0.99;

B. System availability should be no less than 0.9995;

C. Probability of well-timed calls processing during the required term should be no less than 0.95;

D. Relative portion of well-timed processed calls of those types for which the customer requirements are met should be no less than 95%;

(2) to provide quality of used information:

A. Probability that system contains information about states of all real object and coincides should be no less than 0.9;

B. Probability of information actuality on the moment of its use should be no less than 0.9;

C. Probability of errors absence after checking should be no less than 0.97;

D. Probability of correct analysis results obtaining should be no less than 0.95;

E. Probability of providing information confidentiality during objective period should be no less than 0.999;

(3) to provide security of IS operation:

A. Probability of faultless (correct) operation under dangerous influence on IS during given time should be no less than 0.95;

B. Probability of system protection against unauthorized access should be no less than 0.99.

These values characterizes some admissible limitations for probabilities of "success" (P) and risks of "unsuccess" (R=1-P) for information systems operation quality.

The fulfillment of these requirements is a certain scientifically proved guarantee of the quality of information used by AIS.

## 6.3 Example of Solving Inverse Problem to Estimate the Mean Residual Time before the Next Parameters Abnormalities for a Coal Company

The example demonstrates an AIS possibility on the base of solving inverse problem by model described in subsection 3.2 and Appendix B to a rationale of actions in a real time for a coal company

Conditions of parameters, traced by dispatcher intelligence center, are data about a condition before and on the



DOI: https://doi.org/10.30564/aia.v1i2.1195

current moment of time, but always the future is more important for all. With use of current data responsible staff (mechanics, technologists, engineers, etc.) should know about admissible time for work performance to maintain system operation. Otherwise because of ignorance of a residual time resource before abnormality the necessary works are not carried out. I.e. because of ignorance of this residual time it is not undertaken measures for prevention of negative events after parameters abnormalities (failures, accidents, damages and-or the missed benefit because of equipment time out). And on the contrary, knowing residual time before abnormality these events may be avoided, or system may be maintained accordingly. For monitored critical system the probabilistic approach to estimate the mean residual time before the next parameters abnormalities for each element and whole system is proposed.

For every valuable subsystem (element) monitored parameters are chosen, and for each parameter the ranges of possible values of conditions are established: "In working limits", "Out of working range, but inside of norm"), "Abnormality" (interpreted similarly light signals – "green", "yellow", "red") – see Figures 8 and 14. The condition "Abnormality" characterizes a threat to lose system integrity.


**Figure 14.** Example of a prognozed residual time before the next parameter abnormality

For avoiding the possible crossing a border of "Abnormality" a prediction of residual time, which is available for preventive measures, according to gathered data about parameter condition fluctuations considering ranges is carried out. The approach allow to estimate residual time before the next parameter abnormality (i.e. time before first next coming into "red" range) [35]. The estimated residual time $T_{resid}$ is the solution $t_0$ of equation:

$$R(T_{penetr}, t, T_{betw}, T_{diag}, T_{req.}) = R_{adm.}(T_{req}) \quad (3)$$

concerning of unknown parameter t, i.e. $T_{resid} = t_0$.

Here $R(T_{penetr}, t, T_{betw}, T_{diag}, T_{req.})$ is risk to lose integrity, it is addition to 1 for probability $P(T_{req.})$ of providing system integrity ("probability of success"), for calculations the formulas (B.1)–(B.3). $T_{penetr}$ is the mathematical expectation of PDF $\Omega_{penetr}(\tau)$, it is defined by parameter statistics of transition from "green" into "yellow" range (see Figure 8). The others parameters $T_{betw}$, $T_{diag}$ in (3) are known – see Appendix B. The main practical questions are: what about $T_{req.}$ and what about a given admissible risk $R_{adm.}(T_{req})$? For answering we can use the properties of function $R(T_{penetr}, t, T_{betw}, T_{diag}, T_{req.})$:

(1) if parameter t increases from 0 to ∞ for the same another parameters, the function R(…, t, …) is monotonously decreasing from 1 to 0 (for N – real, i.e. no integer part), if the mean activation time of occurred danger (threat - from the 1-st input at the "yellow" range to the 1-st input in the "red" range) is bigger to lose integrity is less;

(2) if parameter $T_{req}$ increases from 0 to ∞ for the same another parameters, the function $R(\ldots,T_{req})$ is monotonously increasing from 0 to 1, i.e. for large $T_{req}$ risk approaches to 1.

It means the such maximal x exists when t=x and $T_{req.}$=x and $0<R(T_{penetr}, x, T_{betw}, T_{diag}, x)<1$. I.e. the residual time before the next parameter abnormality (i.e. time before first next coming into "red" range) is equal to defined x with confidence level of admissible risk $R(T_{penetr}, x, T_{betw}, T_{diag}, x)$. So, if $T_{penetr}$ =100 days, for $R_{adm.}$= 0.01 residual time x≈2.96 weeks (considering decisions of recovery problems of integrity every 8 hours). Adequate reaction of responsible staff in real time is transparent for all interested parties. Details see [35].

## 6.4 Example of Solving Problem 1 by AIS Operating for Providing Safety of a Floating Oil and Gas Platform

For estimation and rationale the possibilities of a floating oil and gas platform operation (considered as a system) the probabilistic modeling is being to answer the next question: "What risks to lose system integrity may be for a year, 10 and 20 years if some subsystems are supported by special AIS on the levels which are proper to skilled workers (optimistic view) and to medium-level workers (realistic view)?"

Let for studying efficiency a system is decomposed on 9 subsystems, for example - see Figure 15. System components are: 1st - a construction of platform; 2nd - an AIS on platform for robotics monitoring and control; 3rd - an underwater communication modem; 4th - a remote controlled unmanned underwater robotic vehicle; 5th - a sonar beacon; 6th - an autonomous unmanned underwater robotic vehicle; 7th - non-boarding robotic boat - a spray of

 DOI: https://doi.org/10.30564/aia.v1i2.1195

the sorbent; 8th - non-boarding robotic boat – a pollution collector; 9th - an unmanned aerial vehicle. Data is monitored from different sources and processed by the models described above in section 3.

***Note:*** *Of course every subsystem also may be considered as a special complex system.*

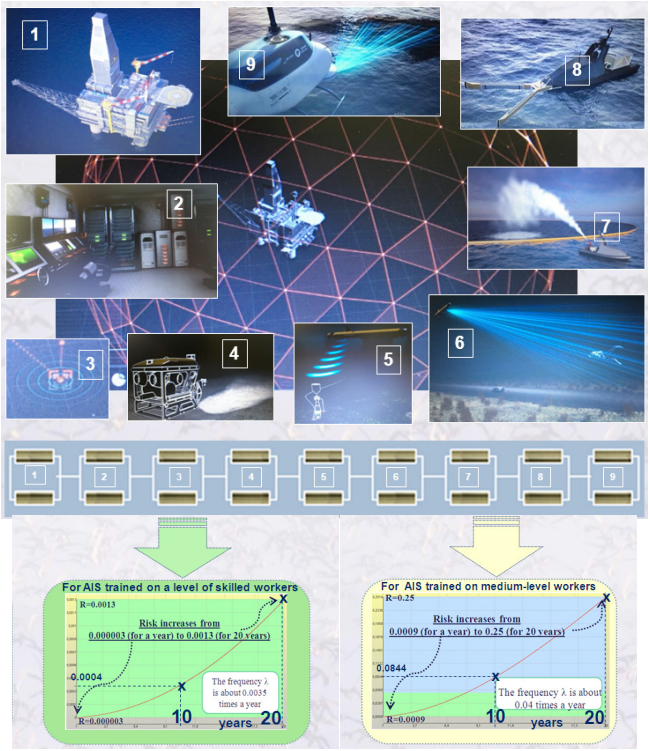


**Figure 15.** Subsystems operating for providing safety of a floating oil and gas platform

The information from monitored data and a time data of enterprises procedures are used as input for using models from Table A.2 and performing steps 1-4 (from Figure 9) in real time. Here risks to lose system integrity during given period $T_{given}$ means risks to be at least once in state "Abnormality" within $T_{req.}$. The functions of modeling may be performed on special servers (centralized or mapped). If virtual risks are computed for all points $T_{req.}$ from 0 to ∞, the calculated values form a trajectory of the PDF. The mathematical expectation of this PDF means the mean residual time to the next state "Abnormality". It defines mean time before failures (MTBF) from this PDF. Requirements to IS operation quality should meet admissible levels recommended in Example 2.

To answer the question of the example let the next input are formed from data monitored and the time data of enterprises procedures.

Let for every system component a frequency of occurrence of the latent or obvious threats is equal to once a month, mean activation time of threats is about 1 day. The system diagnostics are used once for work shift 8 hours, a mean duration of the system control is about 10 minutes, mean recovery time of the lost integrity of object equals to 1 day. The workers (they may be robotics, skilled mechanics, technologists, engineers etc.) are supported by capabilities of an intellectual system allowing estimations in real time the mean residual time before the next parameters abnormalities. Formally they operate as parallel elements with hot reservation. Workers are capable to revealing signs of a critical situation after their occurrence owing to the support of intellectual systems. If all subsystems are supported by intellectual systems on the level which is proper to skilled workers (optimistic view), workers can commit errors on the average not more often once a year. If all subsystems are supported by intellectual system on the level which is proper to medium-level workers (realistic view) only one difference is – medium-level workers can commit errors more often in comparison with skilled workers, for one element it is equal to 1 time a month instead of once a year.

Further we do the steps 1-4 from Figure 9. Computed risks to lose system integrity on Figure 15 means the risks of "failure" for every subsystem which can be detailed to the level of every separate critical parameter of equipment.

The fragments of built PDFs on Figure 15 show:

(1) if all subsystems are supported by intellectual system on the level which is proper to skilled workers (optimistic view) the risk of "failure" increases from 0.000003 for a year to 0.0004 for 10 years and to 0.0013 for 20 years. The MTBF equals to 283 years;

(2) if all subsystems are supported by intellectual system on the level which is proper to medium-level workers (realistic view) the risk of "failure" increases from 0.0009 for a year to 0.0844 for 10 years and 0.25 for 20 years. The MTBF equals to 24 years. It is 11.4 times less against the results for optimistic view.

Such effects (MTBF = 283 years for optimistic view and MTBF = 24 years for realistic view) are owing to implemented technology of counteractions to threats. These are some estimations for example assumptions. Please, compare the effects against primary frequency of occurrence of the latent or obvious threats is equal to once a month, mean activation time of threats is about 1 day + workers errors.

### 6.5 Example of Solving Problem 2 for a Robot Route Optimization

Applicability of the proposed probabilistic methods and models to solving problem 2 (of robot actions optimization under limitations on admissible risks of "failure") is



DOI: https://doi.org/10.30564/aia.v1i2.1195

demonstrated to improve some of the existing capabilities of a rescue robot, interconnected with accessory drone, for route optimization in conditions of uncertainties. Similar problems of specific rescue robot route optimization from point A (Start) to point E (End) can arise in burning wood, in mountains, in the conditions of a city, and in other situations in conditions of uncertainties. Specific cases of uncertainties can be connected additionally with complex conditions of environment and necessity of robotics orientation, localization and mapping that influences on input for the proposed probabilistic models.

On this simplified hypothetical example of moving some rented values by means of the pilotless car from point A to the final point E of a route (from where the SOS signals are following) we will demonstrate the proposed approach to route optimization with acceptable risk of "failure" less than 0.1 (i.e. a probability of success should be more than 0.9) under conditions of uncertainties during the route – see Figure 16.


**Figure 16.** Possible robot route from point A (Start) to point E (End)

The next steps from Figure 10 are performed.

***Step 1***. The complete set of route variants to achieve the goal within given 2 hours, and for each variant – a set of components, is defined: ABCDE, ABGKLDE, ABGHLDE. Let data characterizing every part of route for each of the variants are gathered from drone-informant, processed and prepared for modeling - frequencies of the occurrences of potential threats are: for ABCDEF = 1 time at 10 hours, ABGKLDEF = 1.5 times at 10 hours, ABGHLDE = 2 times at 10 hours (since 08.00 a.m. to 18.00 a.m. what is connected with drone capabilities); mean activation time of threats = 30 minutes; time between the end of diagnostics and the beginning of the next diagnostics = 2 minutes; diagnostics time = 30 seconds; recovery time = 10 minutes; given prognostic period =2 hours.

i=1.

***Step 2 (i=1).*** Using probabilistic model, a calculation of the probability of "failure" is carried out for each variant. From the set of variants ABCDE, ABGKLDE, ABGHLDE the shorter variant ABCDE for which risk is equal to 0.034 is chosen (for the route ABGKLDEF risk=0.051, for route ABGHLDEF risk=0.067). The relevant data from the drone about the local fire conditions and the weather on the part BCDE to 8.00 a.m. are taken into account.

***Step 3 (i=1)***. The robot overcomes the part AB of route. For the new initial point B the input for modeling every part of possible route are updated in real time for routes BCDE, BGKLDE, BGHLDE.

***Step 4 (i=1)***. The robot hasn't yet arrived at the intended point E (i.e. the last part of the route isn't overcome).

i= i+1=2.

***Step 2 (i=2 for variants BCDE, BGKLDE, BGHLDE).*** Input for modeling isn't changed. Risks are the same. From the route variants BCDE, BGKLDE, BGHLDE the shorter one BCDEF (with minimal risk) is chosen.

***Step 3 (i=2 for variant BCDE)***. The robot overcomes the part BC. For the new initial point C the input for modeling every part of possible route are updated in real time: dense fog in forest thicket on the CD part does not allow further movement. And additional information for robot is: the local weather improvements in the next 2 hours are not expected. Part CD is impassable. The comeback to the initial point B of the part is being.

***Step 2 (i=2 for two remaining variants)***. From variants BGKLDE, BGHLDE the shorter one BGKLDE (with minimal risk 0.051) is chosen.

***Step 3 (i=2 for variant BGKLDE)***. The robot overcomes the part BG. For the new initial point G the input for modeling every part of possible route are updated in real time: according drone from 9.00 a.m. on parts GK and KL the imminent fire is detected. The gathered information and knowledge are used to clarify the input for modeling, namely: the frequency threats in the part GKL increases from 1.5 to 2.5 times at 10 hours. Using a probabilistic model for each variant, a recalculation of the risk of failure is carried out. Of the variants GKLDE, GHLDE the variant GHLDE is chosen (risk is equal to 0.067, for the route GKLDE risk equals 0.083).

***Step 4***. After overcoming the part GHLDE the robot arrived at the intended point E of route in given time.

Thus the way ABCBGHLDE is the result of optimization before and on the route. The robot purpose was achieved owing to preventive measures which were de-

 DOI: https://doi.org/10.30564/aia.v1i2.1195

fined by using risk control on the way (with controlled probability of "success" more than 0.9).

### 6.6 What about the Possible Pragmatic Effects from Probabilistic Rationale of Actions for AIS?

Author of this article took part in creation of the Complex of supporting technogenic safety on the systems of oil&gas transportation and distribution and have been awarded for it by the Award of the Government of the Russian Federation in the field of a science and technics. The AIS is a part of 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 17.

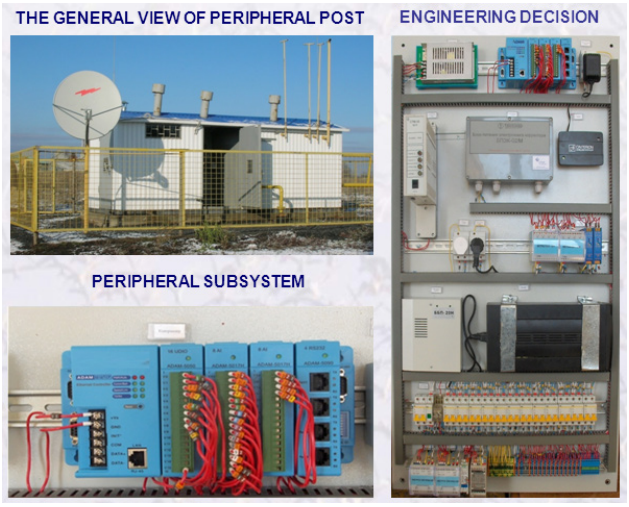


**Figure 17.** The AIS as a hard-software part to support technogenic safety on the objects of oil&gas distribution

The applications of this 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 [32].

## 7. Conclusion

The proposed approach for probabilistic rationale of AIS actions includes description of the proposed models, optimization methods for rationale actions, incremental algorithms for solving:

(1) the problem 1 - to rationale a rational variant for decision-making on the base of monitored data about events and conditions, and

(2) the problem 2 - to rationale a robot actions under limitations on admissible risks of "failures".

The proposed models include models to estimate AIS operation quality and risks prediction for system formalized as "Black box", algorithm to build new probabilistic models for complex system. The practical way to data forming for probabilistic modeling is described.

A suitability of the approach is demonstrated by examples about:

(1) a period of successful system operation by AIS capabilities;

(2) acceptable requirements to solve problem 1 for information systems operation;

(3) solving inverse problem to estimate the mean residual time before the next parameters abnormalities for a coal company;

(4) solving problem 1 by AIS operating for providing safety of a floating oil and gas platform;

(5) solving problem 2 for a robot route optimization;

(6) the possible pragmatic effects from probabilistic rationale of actions for AIS.

The proposed approach means practically a proactive commitment to excellence in uncertainty conditions.

## Appendix A. The Models to Estimate AIS Operation Quality

The probabilistic models for the estimation of information systems operation quality are presented by the formulas (A.1) – (A.14) in Table A.1.

**Table A.1** The probabilistic models for the estimation of information systems operation quality (the proof and details - see [20-22,24,25,28])

| Models. Input | Evaluated measures |
|---|---|
| The model of functions performance by a complex system in conditions of unreliability of its components.<br>Input:<br>N(t) - is the probability distribution function (PDF) of time between neighboring failures ($T_{MTBFnk}$ is the mean time); W(t) – is the PDF of repair time ($T_{rep.}$ is the mean time); V(t) – is the PDF of given time if this time is random value ($T_{req.}$ is the mean time).<br>Note. The next variants are used by the software tools [35-37].<br>N(t), W(t) are exponentially distributed (i.e. enough mean times - $T_{MTBFnk}$, $T_{rep.}$), V(t) is determined (i.e. $T_{req.}$ is const). | Probability $P_{rel}$ of providing reliable function performance during given time.<br>$P_{rel} = \int_0^\infty \left\{ \int_t^\infty V(\tau - t) dN(\tau) \right\} dt \Big/ \int_0^\infty td[N * W(t)]$, (A.1)<br>* - is the convolution sign. |



DOI: https://doi.org/10.30564/aia.v1i2.1195

| Models. Input | Evaluated measures |
|---|---|
| The models complex of calls processing for the different dispatcher technologies.<br>Input for M/G/1/∞:<br>$\lambda_i$ – frequency of the i–th type calls for processing;<br>$\beta_i$ – mean processing time of the i–th type calls (without queue).<br>Note. The software tools [35-37] allow to estimate and to compare effectiveness of the next dispatcher technologies for modeling by M/G/1/∞:<br>- technology 1 for apriority calls processing: in a consecutive order for single-tasking processing mode; in a time-sharing order for multitasking processing mode;<br>- priority technologies of consecutive calls processing 2-5: technology 2 for calls processing with relative priorities in the order "first in - first out" (FIFO); technology 3 for calls processing with absolute priorities in the order FIFO; technology 4 for batch calls processing (with relative priorities and in the order FIFO inside a batch) [7]; technology 5 is a combination of technologies 2, 3, 4 [8]. | Probability $P_{tim.i}$ false of well-timed processing of i-type calls during the required term<br>$P_{tim.i} = P\left(t_{full.i} \le T_{req.i}\right) = \frac{\int_0^{\gamma_i^2 T_{req.i}/T_{full.i}} t^{\gamma_i - 1} e^{-t} dt}{\int_0^{\infty} t^{\gamma_i - 1} e^{-t} dt}$, (A.2)<br>$\gamma_i = \frac{T_{full.i}}{\sqrt{T_{full.i2} - T_{full.i}^2}}$,<br>Relative portion of all well-timed processed calls – S and relative portion of well-timed processed calls of those types for which the customer requirements are met – C:<br>$S = \frac{\sum_{i=1}^{I} \lambda_i P_{tim.i}}{\sum_{i=1}^{I} \lambda_i}$,<br>$C = \frac{\sum_{i=1}^{I} \lambda_i P_{tim.i} \left[ Ind(\alpha_1) + Ind(\alpha_2) \right]}{\sum_{i=1}^{I} \lambda_i}$,<br>$Ind(\alpha) = \begin{cases} 0, & \text{if } \alpha = true \\ 1, & \text{if } \alpha = false \end{cases}$,<br>a1=(there is used criterion 1 and $T_{full\ i} \le T_{req.i}$);<br>a2=(there is used criterion 2 and $P_{tim\ i} \ge P_{req.i}$).<br>Criterion 1 is if there is required $T_{full\ i} \le T_{req.i}$ to be i-type calls processed in time, criterion 2 is if there is required $P_{tim\ i}=P(T_{full\ i} \le T_{req.i}) \ge P_{adm.i}$ to be i-type calls processed in time, $P_{adm.i}$ - is admissible level for well-timed processing of i-type calls during the required term $P_{req.i}$<br>The formulas for mean response time $T_{full}$ of i-type calls and for 2nd moment $T_{full.i2}$ - see [20-22,24,25,28] . |
| The model of entering into system current data concerning new objects of application domain.<br>Input:<br>$q_m$ - the probability that m new objects appear in random moment, intervals between these moments are exponentially distributed with parameter λ.<br>$\Phi(z) = \sum_{m>0} q_m z^m$ -is productive (generating) function;<br>$B(t)$ – is the PDF of time for new information revealing and preparing, transfer and entering into data base.<br>Note. The next variants are used by the software tools [35-37]: Φ(z)=z; B(t) is exponentially distributed. | Probability $P_{comp.}$ that system contains information about states of all real object and coincides<br>$P_{comp.} = exp\left\{-\lambda \int_0^{\infty} \left[1 - \Phi(B(t))\right] dt\right\}$, (A.3) |

| Models. Input | Evaluated measures |
|---|---|
| The model of information gathering.<br>Input:<br>C(t) is the PDF of time between essential changes of object states, $\xi_i$ – is the mean time;<br>B(t) is the PDF of time for information gathering and preparing, transfer and entering into system;<br>Q(t) is the PDF of time interval between information updating, q is the mean time (only for mode $D_2$);<br>the mode $D_1$ of gathering: information is gathered in order "immediately after an essential object state change;<br>the mode $D_2$ of gathering: information is gathered without any dependencies on changes of objects current states (including regulated information gathering).<br>Note. The next variants are used by the software tools [35-37]: B(t), C(t) are exponentially distributed, Q(t) is V(t) is determined or exponentially distributed. | Probability $P_{act}$ of information actuality on the moment of its use:<br>(1) for the mode $D_1$ when information is gathered in order "immediately after an essential object state change:<br>$P_{act} = \frac{1}{\xi_i} \int_0^{\infty} B(t)[1 - C(t)]dt$, (A.4)<br>(2) for the mode $D_2$ when information is gathered without any dependencies on changes of objects current states (including regulated information gathering)<br>$P_{act} = \frac{1}{q_1} \int_0^{\infty} \left\{ [1 - Q(t)][1 - \int_0^{\infty} C(t+\tau) dB(\tau)] \right\} dt$, (A.5) |
| The model of information analysis.<br>Input:<br>$T_{req.}$ - assigned term for analysis;<br>N(t) is the PDF of time between type I analysis errors, $\eta^{-1}$ is the mean time;<br>M(t) is the PDF of time between the neighboring errors in checked information; $A$(t) is the PDF of analyzed type II errors, $T_{MTBF}$ is the mean time;<br>μ is the relative fraction of errors in information content (destined for problems of checking) or the relative fraction of information essential for analysis (destined for problems of analysis);<br>$T_{real}$= V/ν - is the real time for complete information analysis;<br>V – is a content of analyzed information;<br>ν - is an analyzed speed;<br>$T_{cont.}$ - is time of continuous analyst's work.<br>Note. The next variants are used by the software tools [35-37].<br>$T_{req.}$ - is an assigned term (deadline) for analysis; V, ν, $T_{cont.}$ and $T_{req.}$ are assigned as deterministic values;<br>N(t)=1–exp(-t×η);<br>M(t) =1 –exp(-t×μ×ν);<br>$A$(t)= 1–exp(-t/ $T_{MTBF}$). | Probability $P_{after}$ of errors absence after checking (probability $P_{after}$ of correct analysis results obtaining):<br>Variant 1. An assigned term for analysis is no less than the real analysis time ($T_{real} \le T_{req.}$) and the content of analyzed information is such small that it is required only one continuous analyst's work period ($T_{real} \le T_{cont.}$).<br>$P_{after(1)}(V, \mu, \nu, n, T_{MTBF}, T_{cont.}, T_{req.}) = \left[1 - \hat{N}(V/\nu)\right] \cdot \left\{ \int_0^{V/\nu} dA(\tau)[1 - M(V/\nu - \tau)] + \int_{V/\nu}^{\infty} dA(t) \right\}$ (A.6)<br>Variant 2. An assigned term for analysis is no less than the real analysis time (i.e. $T_{real} \le T_{req.}$). But the content of analyzed information is comparatively large, i.e. $T_{real} > T_{cont.}$.<br>$P_{after(2)} = \{P_{after(1)}(V_{part(2)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, \tau_{part(2)})\}^N$, (A.7)<br>N=V/(ν $T_{cont.}$), $V_{part(2)}$=V/N, $\tau_{part(2)} = T_{req.}$/N.<br>Variant 3. An assigned term for analysis is less than the real analysis time ($T_{real} > T_{req.}$) and the content of analyzed information is such small that it is required only one continuous analyst's work period ($T_{real} \le T_{cont.}$).<br>$P_{after(3)} = (V_{part(3)}/V) \times P_{after(1)}(V_{part(3)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, T_{req.}) + [(V - V_{part(3)})/V] \times P_{without}$, (A.8)<br>where $V_{part(3)} = \nu T_{req.}$, $P_{without} = e^{-\mu (V - V_{part(3)})}$.<br>Variant 4. An assigned term for analysis is no less than the real analysis time (i.e. $T_{real} > T_{req.}$), but the content of analyzed information is comparatively large, i.e. $T_{real} > T_{cont.}$.<br>$P_{after} = \begin{cases} [V_{part(4)}/V] \times P_{after(1)}(V_{part(4)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, T_{req.}) + [(V - V_{part(4)})/V] \times e^{-\mu (V - V_{part(4)})}, \text{if } T_{req.} \le T_{cont.}; \\ [V_{part(4)}/V] \times \{P_{after(1)}(V_{part(4.2)}, \mu, \nu, \eta, T_{MTBF}, T_{cont.}, t_{part(4.2)})\}^N + [(V - V_{part(4)})/V] \times e^{-\mu (V - V_{part(4)})}, \text{if } T_{req.} > T_{cont.}, \end{cases}$ (A.9) |

 DOI: https://doi.org/10.30564/aia.v1i2.1195

| Models. Input | Evaluated measures |
|---|---|
| The models complex of an authorized access to system resources during objective period.<br>Input (for estimation of confidentiality):<br>M is the conditional number of a barriers against an unauthorized access;<br>$F_m(t)$ is the PDF of time between changes of the m-th barrier parameters;<br>$U_m(t)$ is the PDF of parameters decoding time of the m-th security system barrier, $u_m$ – the mean time of a barrier overcoming;<br>H(t) – is the PDF of objective period, when resources value is high.<br>Note. The next variants are used by the software tools [35-37]:<br>$U_m(t)$is exponentially distributed;<br>$F_m(t)$ and H(t) are determined or exponentially distributed. | Probability $P_{value}$ of system protection against unauthorized access during objective period<br>$P_{value} = 1 - \prod_{m=1}^{M} P_{over.m}$, (A.10)<br>where $P_{over\ m}$ – is the risk of overcoming the m-th barrier by violator during objective period when resources value is high,<br>$P_{over.} = \frac{1}{f_m}\int_0^{\infty} dt \int_t^{\infty} dF_m(\tau) \int_0^t dU_m(\theta)[1 - H(\theta)]$, |
| The models complex of dangerous influences on a protected system.<br>Input:<br>$\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source, for $\Omega_{penetr.}(t)=1-e^{-\sigma t}$, σ - is the frequency of influences for penetrating;<br>$\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source, for $\Omega_{activ}(t)=1-e^{-t/\beta}$, β – is the mean activation time;<br>$T_{req}$ – is the required period of permanent secure system operation;<br>$T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, $T_{diag}$ – is the diagnostic time.<br>Note. The next variants are used by the software tools [35-37]:<br>$\Omega_{penetr}(t)$ and $U_m(t)$ are exponentially distributed. | Probability $P_{infl}$ of faultless (correct) operation during given time:<br>variant 1 – the assigned period $T_{req}$ is less than established period between neighboring diagnostics ($T_{req} < T_{betw.}+T_{diag}$)<br>$P_{infl.(1)}(T_{req}) = 1 - \Omega_{penetr} * \Omega_{activ}(T_{req})$, (A.11)<br>variant 2 – the assigned period $T_{req}$ is more than or equals to established period between neighboring diagnostics ($T_{req} \geq T_{betw.}+T_{diag}$):<br>$P_{inf1.(2)} = \frac{N(T_{betw.}+T_{diag.})}{T_{req.}} \cdot P_{inf1.(1)}{}^{N}(T_{betw.}+T_{diag.}) + \frac{T_{req.} - N(T_{betw.}+T_{diag.})}{T_{req.}} P_{inf1.}(T_{betw.}+T_{diag.})$, (A.12)<br>where $N=\lfloor T_{req.}/(T_{betw.}+T_{diag.})\rfloor$ – is the integer part. |
| The models complex of an authorized access to system resources.<br>Input (for estimation of confidentiality):<br>M is the conditional number of a barriers against an unauthorized access;<br>$F_m(t)$ is the PDF of time between changes of the m-th barrier parameters;<br>$U_m(t)$ is the PDF of parameters decoding time of the m-th security system barrier, $u_m$ – the mean time of a barrier overcoming.<br>Note. The next variants are used by the software tools [35-37]:<br>$U_m(t)$is exponentially distributed;<br>$F_m(t)$ is determined or exponentially distributed. | Probability $P_{prot}$ of system protection against unauthorized access:<br>$P_{prot} = 1 - \prod_{m=1}^{M} P_{over\ m}$, (A.13)<br>where $P_{over\ m}$ – is the probability of overcoming the m-th barrier by violator,<br>$P_{over\ m} = \frac{1}{f_m}\int_0^{\infty}[1 - F_m(t)]U_m(t)dt.$ (A.14) |

***Note:*** The final clear analytical formulas are received by Lebesque-integration of (A.1). (A.3) – (A.6), (A.10), (A.14).

## Appendix B. The Models to Predict Risks for "Black box"

The proposed models allow to estimate preventive risks for being control in real time. The approach for modeling is based on algorithmic building new probabilistic models – see Table B.1.

The probabilistic models for the estimation of preventive risks for being control in real time is presented by the formulas (B.1) – (B.6) in Table B.1.

**Table B.1** – The models to predict risks for "Black box" (the proof and details - see [24, 25, 28, 30, 44-45])

| Models, methods | Evaluated measures | Formulas |
|---|---|---|
| The model for technology 1 ("Black box").<br>Note. Technology 1 (without monitoring between diagnostics) 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. 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.<br>Input:<br>$\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source;<br>$\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source;<br>$T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, $T_{diag}$ – is the diagnostic time. | Risk to lose system integrity (R). Probability of providing system integrity (P) | R=1-P considering consequences.<br>Variant 1 – the given prognostic period $T_{req}$ is less than established period between neighboring diagnostics<br>($T_{req} < T_{betw.}+T_{diag}$):<br>$P_{(1)}(T_{req}) = 1 - \Omega_{penetr} * \Omega_{activ}(T_{req})$. (B.1)<br>Variant 2 – the assigned period $T_{req}$ is more than or equals to established period between neighboring diagnostics<br>($T_{req} \geq T_{betw.}+T_{diag}$):<br>measure a)<br>$P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\ P_{(1)}{}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\ P_{(1)}(T_{rmn})$, (B.2)<br>where $N=[T_{given}/(T_{betw.}+T_{diag.})]$ is the integer part, $T_{rmn} = T_{given} - N(T_{betw}+T_{diag})$;<br>measure b)<br>$P_{(2)}(T_{req}) = P_{(1)}{}^{N}(T_{betw}+T_{diag})\ P_{(1)}(T_{rmn})$, (B.3),<br>where the probability of success within the given time $P_{(1)}(T_{req})$ is defined by (B.1). |



DOI: https://doi.org/10.30564/aia.v1i2.1195

| Models, methods | Evaluated measures | Formulas |
|---|---|---|
| The model for technology 2 ("Black box"). Note. 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. Input: Additionally to Input for technology 1: A(t) - is the PDF of time from the last finish of diagnostic time up to the first operator error | Risk to lose system integrity (R). Probability of providing system integrity (P) | R=1-P considering consequences. Variant 1 - ($T_{req} < T_{betw.}+T_{diag}$): $P_{(1)}(T_{req}) = 1 - \int_0^{T_{req}} dA(\tau) \int_\tau^{T_{req}} d\Omega_{penetr} * \Omega_{act}(\theta).$ (B.4) Variant 2 – ($T_{req} \geq T_{betw.}+T_{diag}$): measure a) $P_{(2)}(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\, P_{(1)}{}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn})$, (B.5) measure b) $P_{(2)}(T_{req}) = P_{(1)}{}^{N}(T_{betw}+T_{diag})\, P_{(1)}(T_{rmn})$,(B.6), where N is the same and the probability of success within the given time $P_{(1)}(T_{req})$ is defined by (B.4) |

***Note:*** The final clear analytical formula (B.4) is received by its Lebesque-integration

## References


[1] Alan Turing, Computing Machinery and Intelligence, Mind, vol. LIX, 1950, 236: 433—460.

[2] Experimental Robotics. Springer, 2016: 913.

[3] A. Ajoudani, Transferring Human Impedance Regulation Skills to Robots, Springer, 2016: 180.

[4] Geometric and Numerical Foundations of Movements. Springer, 2017: 417.

[5] Robotics Research. Springer, 2017: 646.

[6] Cybernetics Approaches in Intelligent Systems. Computational Methods in Systems and Software, vol. 1, Springer, 2017: 405.

[7] Applied Computational Intelligence and Mathematical Methods. Computational Methods in Systems and Software, 2017, 2: 393.

[8] R. Valencia, J. Andrade-Cetto, Mapping, Planning and Exploration with Pose SLAM, Springer, 2018: 124.

[9] The DARPA Robotics Challenge Finals: Humanoid Robots To The Rescue, Springer, 2018: 692.

[10] G. Antonelli, Underwater Robots, Springer, 2018: 374.

[11] Cognitive Reasoning for Compliant Robot Manipulation, Springer, 2019: 190.

[12] G. Venture, J.-P. Laumond, B. Watier Biomechanics of Anthropomorphic Systems, Springer, 2019: 304.

[13] A. Santamaria-Navarro, J. Solà, J. Andrade-Cetto, Visual Guidance of Unmanned Aerial Manipulators, Springer, 2019: 144.

[14] S. Tadokoro, Disaster Robotics, Springer, 2019: 532.

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

[16] Martin J. System Analysis for Data Transmission. V. II, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1972.

[17] Gnedenko B.V. et al. Priority queueing systems, MSU, Moscow, 1973: 448.

[18] Kleinrock L. Queueing systems, V.2: Computer applications, John Wiley & Sons, New York, 1976.

[19] Matweev V.F. & Ushakov V.G. Queuing systems. MSU, Moscow, 1984: 242.

[20] Kostogryzov A.I. Conditions for Efficient Batch Job Processing of Customers in Priority-Driven Computing Systems Where the Queueing Time Is Constrauned, «Avtomatika i telemehanika». 1987, 12: P.158-164.

[21] Kostogryzov A.I. Study of the Efficiency of Combinations of Different Disciplines of the Priority Service of Calls in the Computer Systems, «Kibernetika i sistemny analiz». 1992, 1: 128-137.

[22] Kostogryzov, A.I., Petuhov, A.V. & Scherbina, A.M.. Foundations of evaluation, providing and increasing output information quality for automatized system. Moscow: "Armament. Policy. Conversion", 1994.

[23] Gnedenko B.V., Korolev V. Yu., Random Summation: Limit Theorems and Applications. – Boca Raton: CRC Press, 1996.

[24] 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: 63-70.

[25] Kostogryzov A., Nistratov G.: Standardization, mathematical modelling, rational management and certification in the field of system and software engineer-


 DOI: https://doi.org/10.30564/aia.v1i2.1195

ing. Armament.Policy.Conversion, Moscow, 2004.

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

[27] Korolev V.Yu., Sokolov I.A., Mathematical Models of Non-Homogeneous Flows of Extremal Events. -- Moscow: TORUS-PRESS, 2008.

[28] Kostogryzov A.I., Stepanov P.V.: Innovative management of quality and risks in systems life cycle (modern standards and ideas of system engineering, mathematical models, methods, techniques and software tools complexes for system analysis, including modelling through Internet, 100 examples with an explanation of logic of the reached results, useful practical recommendations). Moscow, Armament. Policy.Conversion, Moscow, 2008.

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

[30] 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.

[31] Grigoriev L., Guseinov Ch., Kershenbaum V., Kostogryzov A. The methodological approach, based on the risks analysis and optimization, to research variants for developing hydrocarbon deposits of Arctic regions. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, 2014, 5(1-2): 71-78.

[32] Akimov V., Kostogryzov A., Mahutov N. at al. Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of Mahutov N.A. Znanie, Moscow, 2015.

[33] Kostogryzov A., Nistratov A., Zubarev I., Stepanov P., Grigoriev L. About accuracy of risks prediction and importance of increasing adequacy of used adequacy of used probabilistic models. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, 2015, 6(2): 71-80.

[34] Eid, M. and Rosato, V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, 2016: 43-62.

[35] Artemyev V., Kostogryzov A., Rudenko Ju., Kurpatov O., Nistratov G., Nistratov A.: Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. In: Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 2017: 368-373.

[36] Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Klimov S., Grigoriev L.: The method of rational dispatching a sequence of heterogeneous repair works. Energetica, 2017, 63(4): 154-162.

[37] Kostogryzov A., Stepanov P., Nistratov A., Atakishchev O.: About Probabilistic Risks Analysis During Longtime Grain Storage. In: Proceedings of the 2nd Internationale Conference on the Social Science and Teaching Research (ACSS-SSTR), Volume 18 of Advances in Social and Behavioral Science. Edited by Harry Zhang. Singapore Management and Sports Science Institute, PTE.Ltd., 2017: 3-8 .

[38] Kostogryzov A., Stepanov P., Grigoriev L., Atakishchev O., Nistratov A., Nistratov G.: Improvement of Existing Risks Control Concept for Complex Systems by the Automatic Combination and Generation of Probabilistic Models and Forming the Storehouse of Risks Predictions Knowledge. In: Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM), Phuket, Thailand. DEStech Publications, Inc., 2017: 279-283.

[39] Kostogryzov A., Atakishchev O., Stepanov P., Nistratov A., Nistratov G., Grigoriev L.: Probabilistic modelling processes of mutual monitoring operators actions for transport systems. In: Proceedings of the 4th International Conference on Transportation Information and Safety (ICTIS), Canada, Banff, 2017: 865-871.

[40] Kostogryzov A., Panov V., Stepanov P., Grigoriev L., Nistratov A., Nistratov G.: Optimization of sequence of performing heterogeneous repair work for transport systems by criteria of timeliness. In: Proceedings of the 4th International Conference on Transportation Information and Safety (ICTIS), Canada, Banff, 2017: 872-876.

[41] Kostogryzov A., Nistratov A., Nistratov G., Atakishchev O., Golovin S., Grigoriev L.: The probabilistic analysis of the possibilities to keep "organism integrity" by continuous monitoring. In: Proceedings of the International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA), Chengdu, China. Atlantis Press, Advances in Intelligent Systems Research, 2018, 159: 432-435.

[42] Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S.: Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. In: Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 2018: 298-303.

[43] Kostogryzov A., Grigoriev L., Kanygin P., Golovin



DOI: https://doi.org/10.30564/aia.v1i2.1195

S., Nistratov A., Nistratov G.: The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization. International Conference on Physics, Computing and Mathematical Modeling (PCMM), Shanghai, DEStech Publications, Inc., 2018: 93-97.

[44] 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. Edited by Andrey Kostogryzov, IntechOpen, 2018: 23-51.

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

[46] Kostogryzov A.I., Bezkorovainy M.M., Lvov V.M., Nistratova E.N., Bezkorovainaya I.V. Complex for Evaluation of Information Systems Operation Quality – "know-how" (CEISOQ), registered by Rospatent №2000610272.

[47] Kostogryzov A.I., Nistratov G.A., Nistratova E.N., Nistratov A.A. Mathematical modeling of system life cycle processes – "know-how", registered by Rospatent №2004610858.

[48] Kostogryzov A.I., Nistratov G.A., Nistratova E.N., Nistratov A.A. Complex for evaluating quality of production processes, registered by Rospatent №2010614145.

[49] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote analytical support of informing about the probabilistic and time measures of operating system and its elements for risk-based approach, registered by Rospatent №2018617949.

[50] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote rationale of requirements to means and conditions for providing "smart" systems operation quality, registered by Rospatent №2018618572.

[51] Kostogryzov A.I., Nistratov G.A., Nistratov A.A. Remote probabilistic prediction of informatized systems operation quality, registered by Rospatent №2018618686.

 DOI: https://doi.org/10.30564/aia.v1i2.1195