Chapter 2

Probabilistic Methods and Technologies of Risk Prediction and Rationale of Preventive Measures by Using "Smart Systems": Applications to Coal Branch for Increasing Industrial Safety of Enterprises

Vladimir Artemyev, Jury Rudenko and George Nistratov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75109

Abstract

Abilities of "smart systems" for processing information, adaptation to conditions of uncertainty, and performance of scientifically proven preventive actions in real time are analyzed. Basic probabilistic models and technologies for the analysis of complex systems, using "smart systems," ways of generation of probabilistic models for prognostic researches of the new systems projected, modernized, or transformed, are proposed. The proposed methods are described to predict risks to lose integrity for complex structures on the given prognostic time and rationale of preventive measures considering admissible risk, estimate "smart system" operation quality, and predict in real time the mean residual time before the next parameter abnormalities. The methods and technologies are implemented on the level of the remote monitoring systems. The application is illustrated on the examples of the joint-stock company "Siberian Coal Energy Company."

Keywords: analysis, method, model, prediction, probability, quality, risk, safety, smart system, technology

1. Introduction

All next years and decades form an epoch of using smart systems. What about the usefulness of smart systems for prediction and rationale of preventive measures against possible threats? To answer this question, we address to some definitions.

According to ISO Guide 73, in general, case risk is defined as the effect of uncertainty on objectives. An effect is a deviation from the expected—positive and/or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can be applied at different levels (such as strategic, organization-wide, project, product, and process). Risk is often characterized by reference to potential events and consequences or a combination of these. Risk may be estimated by a probability of potential events, leading to effects considering consequences. The chapter, including examples, is focused on events leading to losses of system integrity (often with negative consequences). But it does not limit a generality of proposed approaches.

According to ISO/IEC/IEEE 15288 "Systems and software engineering—System life cycle processes," a system is a combination of interacting elements organized to achieve one or more stated purposes. An enabling system is a system that supports a system of interest during its life cycle stages but does not necessarily contribute directly to its function during operation. A system of systems (SoS) is a system of interest whose elements are themselves systems. A SoS brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals. The research covers systems defined in itself as "smart" system or using "smart" systems (see **Figure 1**).

For modern or perspective system or for a system of systems from the point of view of prediction and rationale of preventive measures against possible threats, the "smart" systems are and will be used as the systems in itself or as system elements or enabling systems. In a

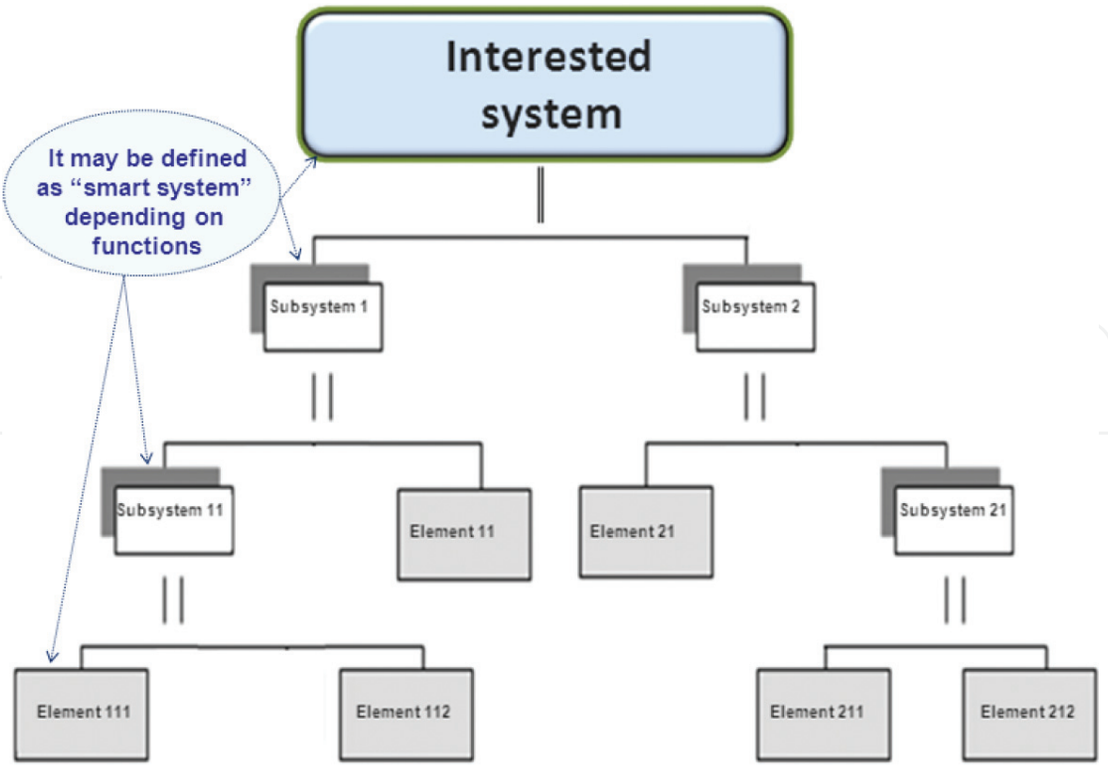

Figure 1. To the definition of "smart system" in a system.

http://dx.doi.org/10.5772/intechopen.75109

general case, "smart" is a mnemonic acronym, giving criteria to guide in the setting of objectives, and "smart systems" are defined as miniaturized devices that incorporate functions of sensing, actuation, and control (www.wikipedia.org, www.thefullwiki.org).

Developing existing researches [1–17], this manuscript includes correct probabilistic interpretation of risk prediction effectively using "smart" systems, some original basic probabilistic models for risk prediction, the improvement of existing risk control concept, and approaches for solving some problems of industrial safety for coal branch.

2. Probabilistic interpretation of risk prediction for effective using "smart" systems

Because "smart" possibilities allow to forecast a future, we should view probabilistic vision of event prediction, its scientific interpretation, and, unfortunately, some existing illusory vision. Here, from the scientific point of view for anticipating dangerous development of events, it is difficult to construct an adequate probability distribution function (PDF) [1–4] of time between losses of system integrity. Damage may be to some extent estimated on practice (we will consider that the deviations in estimations can reach 100%). Therefore, leaving an estimation of a possible damage out of the work, we will stop on researches of a probabilistic component of risk. What deviations in risk predictions are possible here? To answer this question, it is necessary to understand typical metrics and engineering methods of risk predictions, in definition and concept to use "admissible risk," and then to compare various variants.

In practice probabilistic estimations of system integrity losses are quite often carried out by the frequency of emergencies or any adverse events. For example, with reference to safety, it can be frequencies of different danger threats influences, leading to a damage. That is, frequency replaces estimations of probability (risk to lose integrity of system during prognostic period). It is correct? From probability theory it is known that for defined PDF one of its characteristics is the mathematical expectation ($T_{exp.}$). In turn, for PDF of time between losses of system integrity, the mathematical expectation is the mean time between neighboring losses of system integrity $T_{exp.}$, and moreover the frequency $\boldsymbol{\lambda}$ of system integrity losses is equal to $1/T_{exp.}$ If to be guided only by frequency λ (with ignoring PDF) in practice, a large deviation may take place. Indeed, a probability that event has occurred till moment $T_{exp.}$ can be equal to 0.00 for approximation by deterministic (discrete) PDF and 0.36 for exponential approximation (see **Figure 2**). That is, as a result of erroneous choice of PDF, characterized by identical λ, the enormous difference may take place! On the one hand, it means ambiguity of a probabilistic estimation of events, being guided only on frequency λ, and on the other hand, a necessity of search (or creations) of more adequate PDF of time between losses of system integrity is very high.

Often today, engineers prefer exponential PDF: $R(t, \lambda) = 1 - \exp.(-\lambda \cdot t)$. If, for example, for 1 year of prognostic period to put λ about 10^{-3} times in a year or less, then under Taylor's expansion $R(t, \lambda) \approx \lambda \cdot t$ with accuracy $o(\lambda^2 \cdot t^2)$. And, if $t = 1$ year, the absolute value of frequency practically coincides with the value of probability. But if value $\lambda \cdot t$ increases, it is capable to exceed 1 and by definition generally cannot be perceived as probability. Resume: focusing on

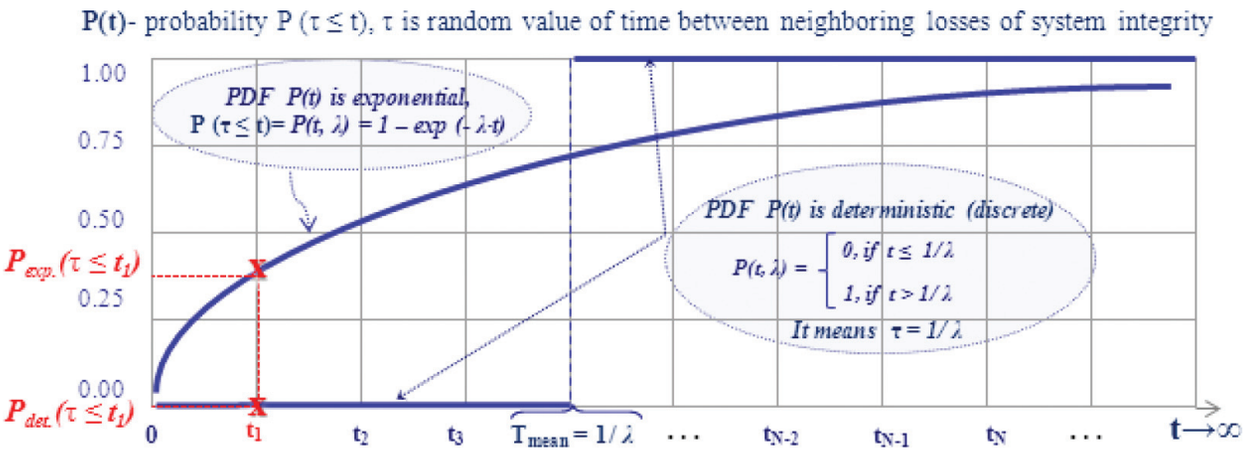

Figure 2. For the same λ, a probability that event has occurred can be equal to 0.00 for approximation by deterministic PDF and 0.36 for exponential PDF approximation.

probability is correct from the point of view of universal risk metric. And, focusing on frequency may be incorrect if $\lambda \cdot t$ is approximately more than 10^{-3}.

The special importance has the concept of "admissible risk." The matter is that there should be a result of the consent of all parties involved in unsafe business on condition that it does not ruin business; by all it is unequivocally estimated and interpreted (not excluding emergencies) and is scientifically proven. In practice frequently the "admissible risk" is interpreted as "border strip," i.e., it is supposed that if it does not cross this "border strip," the system integrity cannot be lost. But in reality it is not so! The residual risk always remains. In operation research the similar restrictions are considered as a starting point for the decision of synthesis problems, connected with searching effective preventive measures of system integrity in life cycle. The complex use of these measures promotes in retaining the risk on the admissible level. It is the typical approach which should work correctly. And how does it work in practice?

Here, it is to quite pertinently address the developed form of the quantitative requirements, connected with the level of admissible risks. The elementary forms of requirements are:

- "A frequency λ of system integrity losses should not exceed admissible level $\lambda_{adm.}$."
- "Probability to lose integrity of system during time T_{req} should not exceed admissible level $R_{adm.}(T_{req})$."
- Their combination.

What engineering explanations occur in practice? They are as follows:

- If the limitation on the admissible level of probability $R_{adm.}(T_{req})$ is set, it means that crossing "border strip" should not occur on an interval of time from 0 to T_{req}. For exponential approximations there is an unequivocal functional dependence: $\lambda_{adm.} = -\ln(1 - R_{adm.}(T_{req}))$. That is, this dependence means that a given value of admissible probability $R_{adm.}(T_{req})$ corresponds unequivocally with a value of the maximum frequency of system integrity losses.

http://dx.doi.org/10.5772/intechopen.75109

- If the limitation on the admissible level of maximum frequency of system integrity losses $\lambda_{adm.}$ is set, it means that for exponential approximations the function of probability from time t is considered: $R(t, \lambda_{adm.}) = 1 - \exp.(-\lambda_{adm.} \cdot t)$. That is, this is the same "border strip" but in the form of the function from t and without an obvious binding to value T_{req}. This level of limitation by function $R_{adm.}(T_{req})$ is logically to interpret also as "admissible" for the period of time from 0 to t. Admissible risk in the point of probability $P_{adm.}(t_{req.})$ for time $t_{req.}$ May be prolonged on the level of PDF by exponential distribution and the admissible frequency of system integrity losses $\lambda = -\ln(1 - P_{adm.}(t_{req.}))$. It is convenient, but is it adequate? In reality a vision about exponential PDF for behavior of "smart" system may be roughly erroneous (see **Figure 3**).

Despite obvious incompleteness of the elementary forms of requirements to "admissible risks" (in reality, only the limitations in one or several points) and the absence of interrelations with a kind of real PDF of time between losses of system integrity (depending from many parameters: structure of system, heterogeneity of threats, different measures of counteraction to threats, etc.), these forms have got accepted by engineering community. In the further statement of the work, we will be guided by these elementary forms of requirements to "admissible risks." They also allow to extract latent knowledge from the results of adequate probabilistic modeling.

Today, specifications of safety in different fields characterize a frequency $\boldsymbol{\lambda}$ of system integrity losses at the level 10^{-3}–10^{-7} times a year. As a matter of fact, it is one danger event for 1000 years, i.e., cannot be tested in system life! In practice it can be estimated by means of mathematical and/or physical modeling. And, from statistics we know only that at the Russian systems of oil and gas industry, thousand emergencies are annually. But, the number of incidents with a comprehensible result (with prevented emergencies) is usually a hundred times more!

Accordingly, there is an important question: what frequencies of system integrity losses should be used for risk predictions and where does it take? If these are only the frequencies of emergencies, the predicted risks will be essentially underestimated! These final frequencies are output

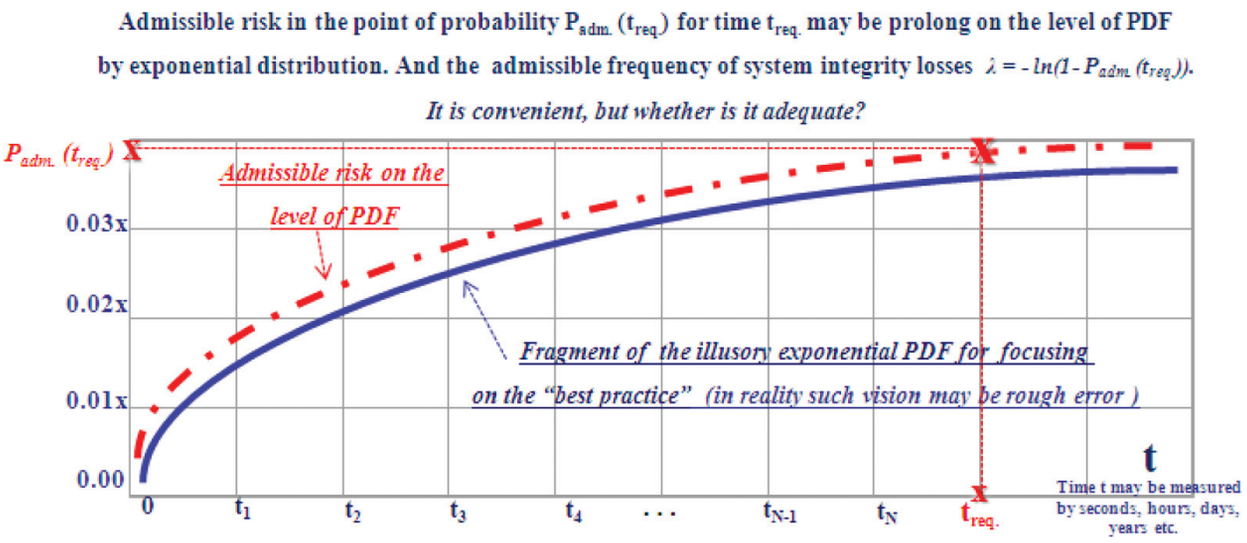

Figure 3. About erroneous vision of exponential PDF approximation instead of more adequate approximation.

instead of input data for modeling. Estimate, please: if to be guided by these frequencies and to consider that 50–70% of failures are the result of "human factor," it should mean that the frequency of critical errors from "human factor" on systems is about one time in thousand years! However, that is not so in real life! Errors are committed much more often. But they are under control, and the majority of them is in due time corrected. As consequence of these counteraction measures, required system integrity (including safety) is reached. The answer arises obviously: the frequency λ of system integrity losses used at risk predictions itself should pay off by the results of probabilistic modeling. Indeed, for adequate risk prediction, there is an important frequency of all the primary incidents (including neutralized incidents at the expense of control measures, maintenance, and timely reaction on initial signs of threat development).

Consideration of "smart" system possibilities for proactive diagnostics of system integrity, monitoring of conditions, and recovering the lost integrity allows to create more adequate

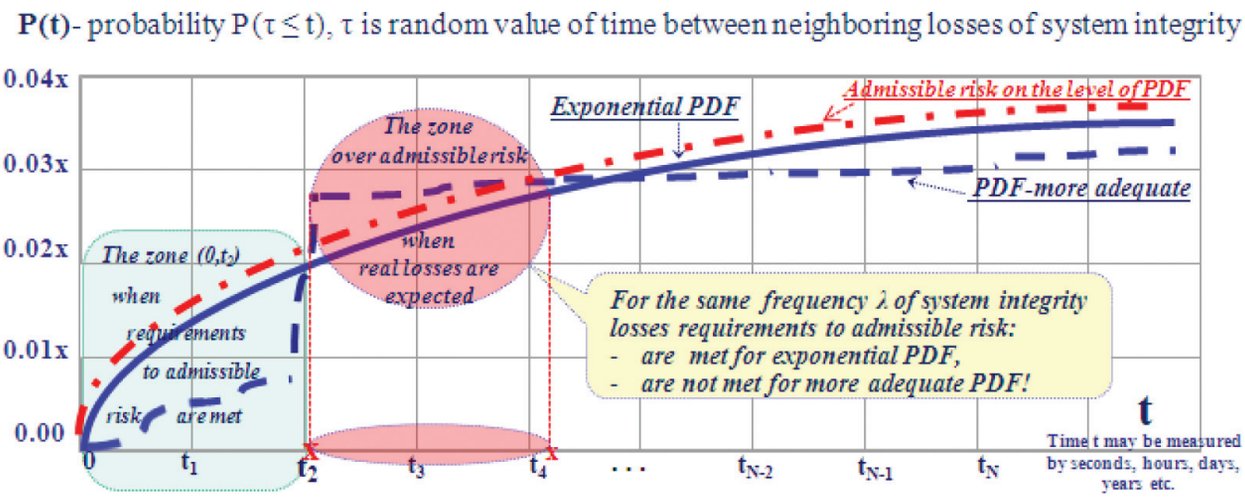

Figure 4. The possible variants of correlations of the limitations to admissible risks, exponential, and an adequate PDF of time between losses of system integrity with identical frequency of system integrity losses λ.

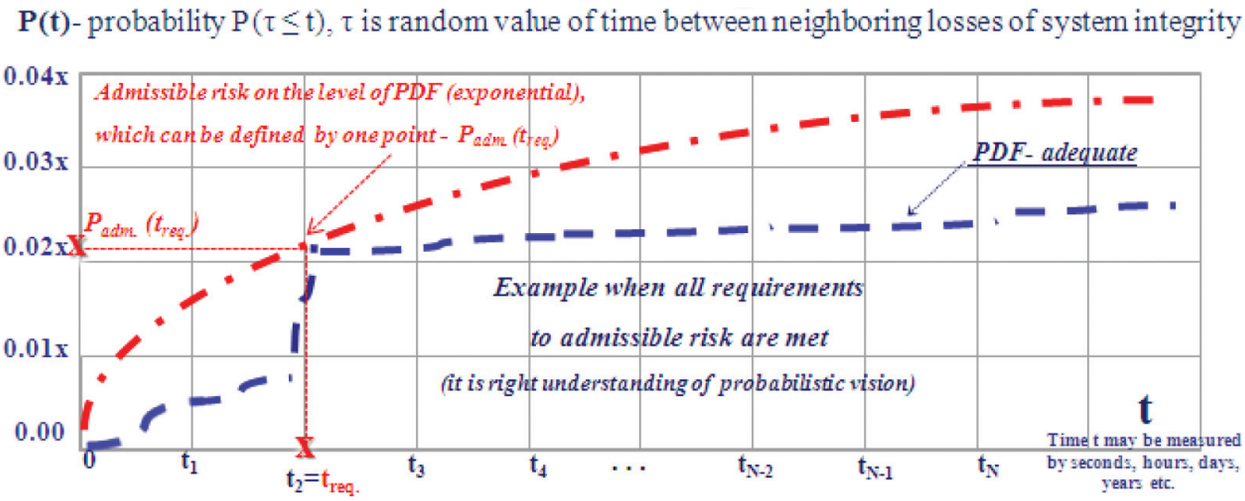

Figure 5. All requirements to admissible risk are met for an adequate PDF of time between losses of system integrity.

PDF for risk predictions. In **Figure 4** 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 demonstrated. The errors in comparison with vision in **Figure 3** are noted.

An example when all requirements to admissible risk are met is presented on **Figure 5**. It is the right understanding of probabilistic vision of event prediction with scientific interpretation considering situations in **Figure 4**.

3. Some basic probabilistic models for risk prediction

Considering possibilities of "smart" systems, two general technologies of providing protection in different spheres are described: proactive periodical diagnostics of system integrity (technology 1) and additionally monitoring between diagnostics (technology 2) including recovery of integrity [2–3, 6–10]. These models allow to create more adequate PDF of time before the next event of the lost integrity.

3.1. The models for the systems that are presented as one element ("black box")

Technology 1 is based on proactive diagnostics of system integrity that are carried out periodically to detect danger occurrences into a system or consequences of negative influences. The lost system integrity can be detected only as a result of diagnostics, after which the recovery of integrity is started. Dangerous influence on system is acted step by step: at first a danger occurrence into a system and then after its activation begins to influence. System integrity cannot be lost before an occurred danger is activated. A danger is considered to be realized only after a danger has activated and influenced on a system. Otherwise, the danger will be detected and neutralized during the next diagnostic.

Note: it is supposed that used diagnostic tools allow to provide system integrity recovery after revealing of danger occurrences into a system or consequences of influences.

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics. In case of detecting a danger, an operator recovers system integrity (ways of dangers removing and system recovery are the same as for technology 1). Faultless operator's actions provide a neutralization of a danger. When a complex diagnostic is periodically performed, this time operators are alternated. An occurrence of a danger is possible only if an operator makes an error, but a dangerous influence occurs if the danger is activated before the next diagnostic.

The probability of system operation with required safety and quality within the given prognostic period (i.e., probability of success) may be estimated as a result of using the next models for technologies 1 and 2. Assumption: for all time input characteristic, the probability distribution functions exist. Risk $R(T_{req})$ to lose integrity (safety, quality, or separate property,

e.g., reliability), i.e., to be though one time in "red" range during period T_{req}, is addition to 1 for probability $P(T_{req})$ of providing system integrity ("probability of success," i.e., to be in "green" or "yellow" ranges all period T_{req}). $R(T_{req}) = 1\text{-}P(T_{req})$ considering consequences.

The next variants for technologies 1 and 2 are possible: 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 prognostic 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, and T_{diag} is the diagnostic time.

The next formulas for PDF of time between the losses of system integrity are proposed [2–3].

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

$$P_{(1)}(T_{req}) = 1 - \Omega_{occur}{}^{*}\, \Omega_{activ}(T_{req}), \tag{1}$$

where $\Omega_{occur}(t)$ is the PDF of time between neighboring occurrences of danger (from the "green" to the "yellow" range), mathematical expectation $T_{occur} = \sigma^{-1}$; $\Omega_{activ}(t)$ is the PDF of activation time of occurred danger (threat: from the first input at the "yellow" range to the first input in the "red" range), and mathematical expectation is β. The PDF $\Omega_{occur}(t)$ and $\Omega_{activ}(t)$ may be exponential (see rationale in [6]). For different threats a frequency of dangers for these PDF is the sum of frequencies of every kind of threats.

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

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

where $N = [T_{req.}/(T_{betw.} + T_{diag.})]$ may be real (for PDF) or the integer part (for estimation of deviations).

$$T_{rmn} = T_{req} - N(T_{betw} + T_{diag}).$$

The probability of providing system integrity within the given time $P_{(1)}(T_{given})$ is defined by Eq. (1).

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

$$P_{(1)}(T_{req}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{\tau}^{T_{req.}} d\,\Omega_{penetr}{}^{*}\,\Omega_{act.}(\theta) \tag{3}$$

Here, $A(\tau)$ is the PDF of time between operator's errors. $A(\tau)$ may be exponential PDF (see rationale in [6]).

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

http://dx.doi.org/10.5772/intechopen.75109

$$P_{(2)}(T_{req}) = N((T_{betw} + T_{diag})/T_{req})\, P_{(1)}{}^{N}(T_{betw} + T_{diag}) + (T_{rmn}/T_{req})\, P_{(1)}(T_{rmn}), \quad (4)$$

where the probability of providing system integrity within the given time $P_{(1)}(T_{req.})$ is defined by Eq. (3).

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

The models are applicable to the system presented as one element. The main result of such system modeling is a probability of providing system integrity or of losses of system integrity during the given period of time. If a probability for all points $T_{req.}$ from 0 to ∞ will be calculated, a trajectory of the PDF for each combined element depending on threats, periodic control, monitoring, and recovery time is automatically synthesized.

3.2. Probabilistic approach to estimate "smart" system operation quality

In general case "smart" system operation always aims to provide reliable and timely producing the complete, valid and, if needed, confidential information for its proper further pragmatic use, including incorporate functions of sensing, actuation, and control. And, potential threats to "smart" system operation are influencing the used information (**Figure 6**).

In general case a probabilistic space (Ω, B, P) for an evaluation of system operation processes is proposed, where Ω is the limited space of elementary events; B is the class of all subspace of Ω space, satisfied to the properties of σ-algebra; and P is the probability measure on a space of elementary events Ω. 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 $\sum_k p_k = 1$. Such space (Ω, B, P) is built [6] and proposed for use because "smart" system may be considered as specially focused information system, incorporating functions of sensing, actuation, and control. The proposed analytical models and calculated measures are as follows [6]:

"The model of function performance by a complex system in conditions of unreliability of its components" (the measures: T_{MTBF} is the mean time between failures; $P_{rel.}(T_{given})$ is the probability of reliable operation of IS, composed by subsystems and system elements, during the

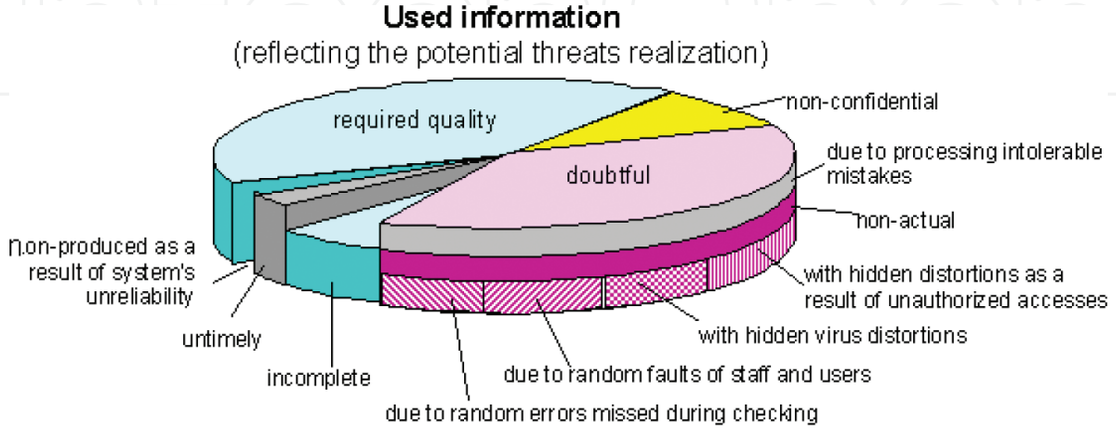

Figure 6. Potential threat realization to "smart" system operation on the level of used information.

given period T_{given}; and $P_{man}(T_{given})$ is the probability of providing faultless man's actions during the given period T_{given}).

"The model complex of call processing" (the measures for the different dispatcher technologies (for unpriority call processing in a consecutive order for single-tasking processing mode, in a time-sharing order for multitasking processing mode; for priority technologies of consecutive call processing with relative and absolute priorities; for batch call processing; for combination of technologies above): the mean wait time in a queue; the mean full processing time, including the wait time; P_{tim} is the probability of well-timed processing during the given time; the relative portion of all well-timed processed calls; the relative portion of well-timed processed calls of those types for which the customer requirements are met C_{tim}).

"The model of entering into IS current data concerning new objects of application domain" (the measure: P_{compl} is the probability that IS contains complete current information about the states of all objects and events).

"The model of information gathering" (the measure: $P_{actual.}$ is the probability of IS information actuality on the moment of its use).

"The model of information analysis" (the measures: P_{check} is the probability of error absence after checking; the fraction of errors in information after checking; $P_{process}$ is the probability of correct analysis results obtained; the fraction of unaccounted essential information).

"The model complex of dangerous influences on a protected system" (the measures: $P_{inf.l.}(T_{given})$ is the probability of required counteraction to dangerous influences from threats during the given period T_{given}).

"The model complex of an authorized access to system resources" (the measures: P_{prot} is the probability of providing system protection from an unauthorized access by means of barriers; $P_{conf.}(T_{given})$ is the probability of providing information confidentiality by means of all barriers during the given period T_{given}).

These models, supported by different versions of software Complex for Evaluation of Information Systems Operation Quality, patented by Rospatent №2,000,610,272 (CEISOQ+), may be applied and improved for solving such system problems in "smart" system life cycle as rationale of quantitative system requirements to hardware, software, users, staff, and technologies; requirement analysis; estimation of project engineering decisions and possible danger; detection of bottlenecks; investigation of problems concerning potential threats to system operation and information security; testing, verification, and validation of "smart" system operation quality; rational optimization of "smart" system technological parameters; and rationale of projects and directions for effective system improvement and development.

3.3. The generation of new models for complex systems

The basic ideas of correct integration of probabilistic metrics are based on a combination and development of the offered models [2–3, 6–10]. For a complex system estimation with parallel or serial structure, new models can be generated by methods of probability theory. For this

http://dx.doi.org/10.5772/intechopen.75109

purpose in analogy with reliability, it is necessary to know a mean time between losses of integrity for each element. Let's consider the elementary structure from two independent parallel elements that means logic connection "OR" or series elements that means logic connection "AND" (see **Figure 7**).

The PDF of time between neighboring losses of ith element integrity is $B_i(t) = P(\tau_i \le t)$; then:

(1) Time between losses of integrity for system combined from series connected independent elements is equal to a minimum from two times τ_i: failure of the first or second elements (i.e., the system goes into a state of lost integrity when either the first or second element integrity will be lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\min(\tau_1,\tau_2)\le t)=1- P(\min(\tau_1,\tau_2)>t)=1-P(\tau_1>t)P(\tau_2 > t)= 1 - [1-B_1(t)]\,[1- B_2(t)], \quad (5)$$

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

$$B(t)=P(\max(\tau_1,\tau_2)\le t)=P(\tau_1 \le t)P(\tau_2 \le t)=B_1(t)B_2(t). \quad (6)$$

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

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

The known kind of the more adequate PDF allows to define accordingly mean time between neighboring losses of system integrity $T_{exp.}$ (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, e.g., 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 [2–3, 6].

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"

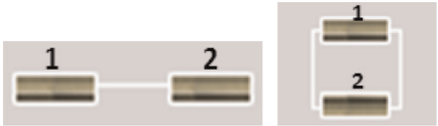

Figure 7. Illustration of system, combined from series (left) or parallel (right) elements.

(registered by Rospatent №2,004,610,858), and "complex for evaluating quality of production processes" (patented by Rospatent №2,010,614,145) [8–9].

4. The improvement of existing risk control concept

The purposed approach to improve existing risk control concept includes (see **Figure 8**) [11–17]:

- Creation and perfection of probabilistic models for problem decision
- Automatic combination and generation of new probabilistic models
- Forming the storehouse of risk prediction knowledge
- For storehouse, dozens of variants of the decision of typical industrial problems for risk control

For example, *system*, combined from complex interested system and "smart" system (also it may be SoS), can be analyzed by the formula (5) and probabilistic models described above (see **Figure 9**). The correct operation of this *system of system* during the given period means during the given period of prediction both the first and the second complex systems should operate correctly according their destinations. That is, integrated system is in the state "Integrity (correct operation)" if "AND" the interested system left and "AND" the "smart" system right are in the state "Integrity (correct operation)."

Thus, the proposed improved that risk control concept can be useful to perform effectively functions: risk prediction; rationale of quantitative system requirements to hardware, software, users, staff, and technologies; requirement analysis; estimation of project engineering decisions and possible danger; detection of bottlenecks; investigation of problems concerning potential threats to operation of complex systems; validation of system operation quality; rational optimization of system parameters; and rationale of plans, projects, and directions for effective system utilization, improvement, and development. The expected pragmatic effect is as follows: it is possible to provide essential system quality and safety rise and/or avoid wasted expenses in system life cycle bases on the rational application of improved concept.

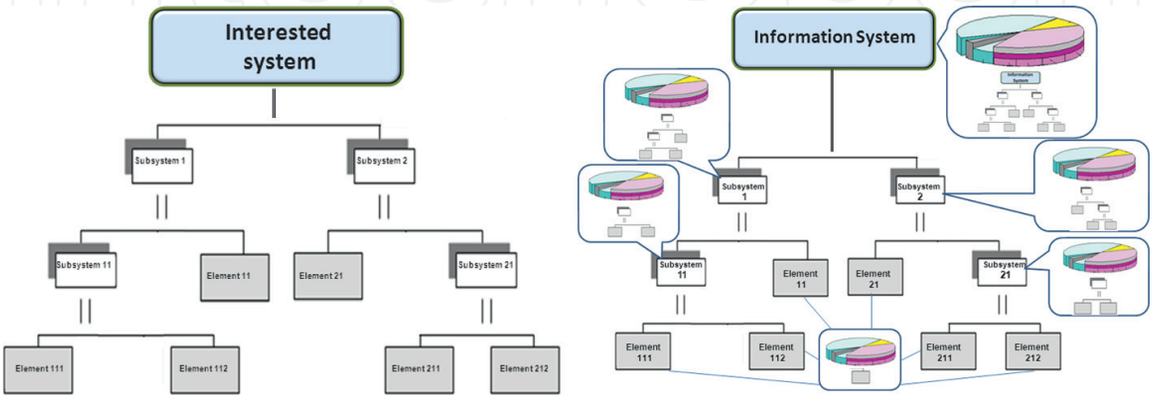

Figure 8. The purposed approach to improve existing risk control concept.

http://dx.doi.org/10.5772/intechopen.75109

Figure 9. *System* of two different complex systems (serial combination) for modeling integrated system.

5. About some problems of industrial safety for coal branch

As an example of effectively solving the problems of industrial safety, we consider an experience of the joint-stock company "Siberian Coal Energy Company (SUEK)" (see www.suek.com). SUEK is one of the world's largest coal companies with production assets in Russia and a global trading network. SUEK delivers long-term value to shareholders at every stage of the value chain—mining, processing, transportation, and shipment—through port facilities, sales, and distribution (**Figure 10**). This value chain includes different SoS. In practice many SoS of SUEK use "smart" systems [11, 14].

Below are the aspects researched:

- Probabilistic analysis of the remote monitoring system (RMS) possibilities for increasing industrial safety of critical infrastructure safety (CIS).
- Estimating in real time the mean residual time before the next parameter abnormalities considering the results of the control of equipment and technological process conformity to the set normative in real time.

5.1. Probabilistic analysis of the remote monitoring system possibilities

For coal branch the developments of mine, buildings, and constructions should be equipped by a complex of systems and means that provide the organization and implementation of coal

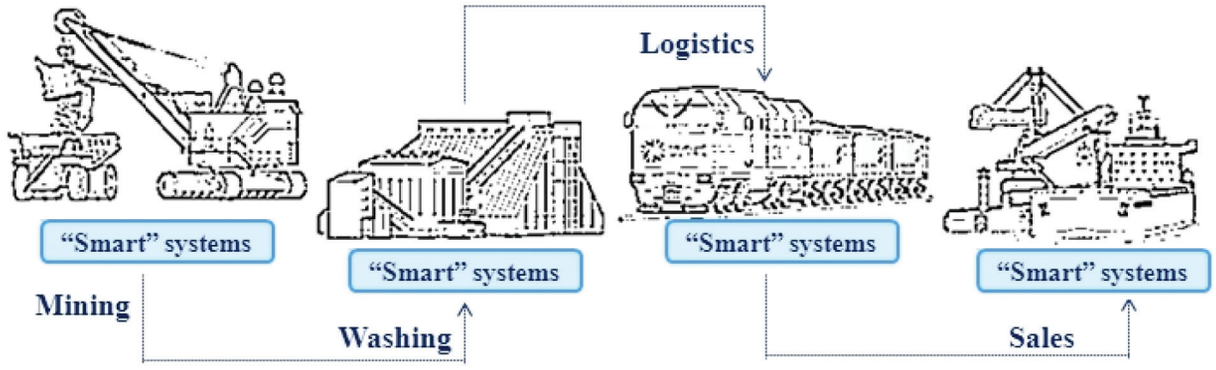

Figure 10. The SUEK value chain includes "smart" systems everywhere.

work safety and technological and productions control in normal and emergency conditions. This complex of systems and means should be integrated into multifunctional safety system (MFSS) with the following main functions:

- Monitoring and prevention of conditions of occurrence of geodynamic, aerologic, and technogenic danger.
- The control of technological process conformity to the set normative in real time.
- Application of counteremergency protection systems.

The usual approaches to critical infrastructure safety (CIS) which have been developed in last dozen years, based on many respects on subjective safety estimations "on places", have reached a high but not sufficient level of efficiency. For the account of interests of all interested parties and the further business development today, rethinking system possibilities of applied information technologies for increasing safety and extracting the innovative effects are not used fully till now.

Search of cardinal directions of improving CIS, favorable to business and the state, has led to comprehension of sharp necessity and expediency of creation and implementation of remote monitoring system (RMS) that is an important part of MFSS. RMS transforms an internal information support of separate CIS in a mode of a needed transparency and wide availability of CIS state in real time for all interested and responsible parties. Along with it on the basis of rational RMS implementation, the transition from the existing subjective expert approach to the risk-based approach for critical infrastructure safety receives necessary information filling.

The proposed probabilistic analysis of RMS operation in their influence on integral risks to lose system integrity is based on researching real remote monitoring systems implemented in Russia for oil and gas CIS. In application to composed and integrated CIS with RMS and without RMS, the earlier models, developed by authors, are used [1–10]. The received results are applicable for an analytical rationale of system requirements to RMS, system definition of the balanced preventive measures of systems, and subsystem and element integrity support at limitations on resources and admissible risks.

Requirements to monitoring and prognosis for critical systems are established at the level of many international standards, for example, ISO 17359, ISO 13381–1, ISO 13379, IEC 61508–1 [18–21], etc. Today, a monitoring of parameter conditions is carried out to increase reliability and industrial safety of critical systems, improve their health management, and provide predictive maintenance and operation efficiency. Here, critical systems are understood as objects of dangerous manufacture and the equipment, energy objects, power and transport systems, and others. Different data about current conditions of parameters become accessible in real time. So, for coal mine some of many dozens of heterogeneous parameters are for ventilation equipment (VE) (temperature of rotor and engine bearings, a current on phases, and voltage of stator) and for modular decontamination equipment (MDE) (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.). Effects from RMS may be reached on the basis of gathering and analytical processing in real time the information on controllable parameters of objects monitored (see **Figure 11**). RMS is intended for a possibility of prediction, the prevention of possible

http://dx.doi.org/10.5772/intechopen.75109

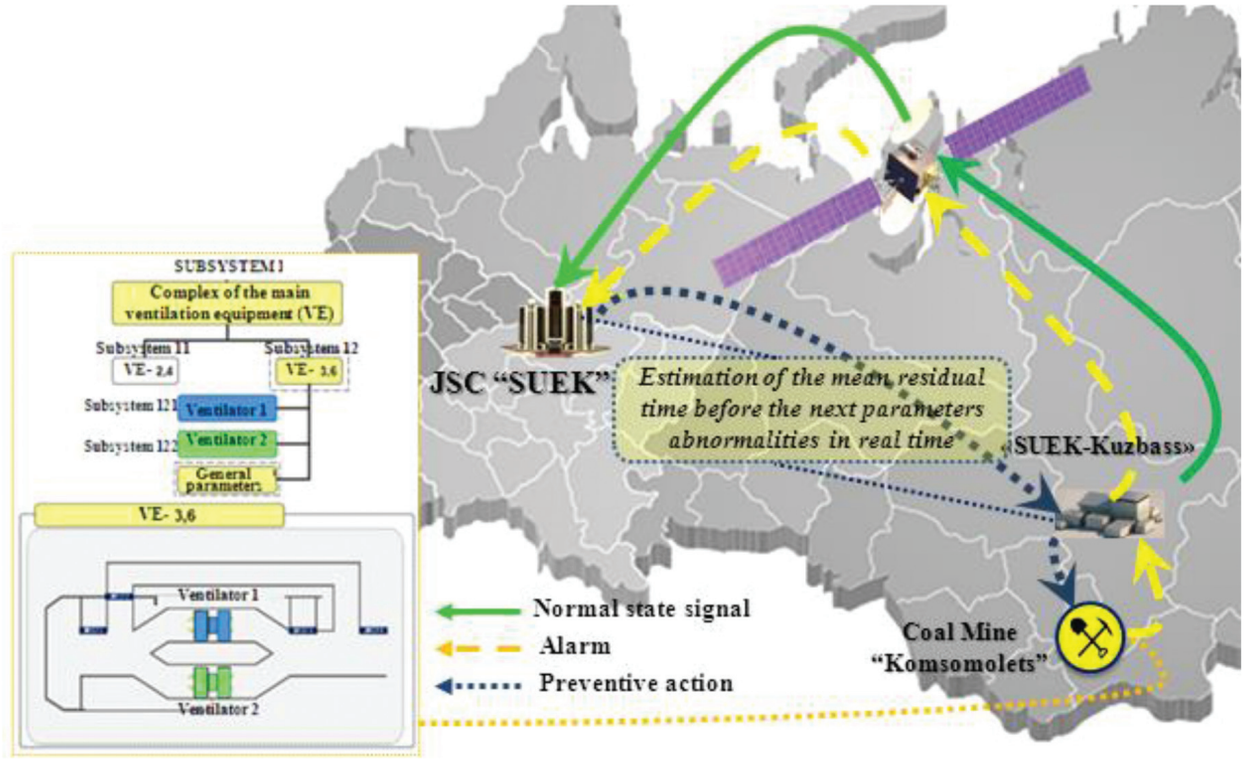

Figure 11. Example of reaction in real time.

emergencies, minimization of a role of human factor regarding control, and supervising functions. The role of RMS is defined by their functions, to the basic of which concern:

- Remote continuous monitoring of CIS condition in real time (gathering data about key parameters of technological processes; gathering and processing data of industrial inspection, the information of technical condition and equipment diagnostics, and the information on the presence of failures and incidents; and results of system recovery, etc.)
- Analytical data processing
- Prediction of risks to lose object integrity
- Display of parameter conditions and predictions with the necessary level of details

In this subsection analytical decomposition and the subsequent integration of complex systems are used according to propositions above in Sections 1–4. Admissible conditions (ranges) of traced parameters for each element, the reservation possibilities, implemented technologies of the control, and recovery of integrity are considered.

RMS is intended for a possibility of prediction, the prevention of possible emergencies, minimization of a role of human factor regarding control, and supervising functions. It may be reached on the basis of gathering and analytical processing in real time the information on controllable parameters of objects monitored. For example, objects monitored for oil and gas CIS are the technological equipment and processes of extraction, transportation, refining, the personnel, systems, and means of safety support.

The role of RMS is defined by their functions, to the basic of which concern:

- Remote continuous monitoring of CIS condition in real time (gathering data about key parameters of technological processes; gathering and processing data of industrial inspection, the information of technical condition and equipment diagnostics, and the information on the presence of failures and incidents; and results of system recovery, etc.)
- Analytical data processing
- Prediction of risks to lose CIS integrity
- Display of CIS conditions and predictions with the necessary level of details

Unlike the usual control which is carried out at enterprises (when the state supervising body in the field of industrial safety and frequently also the enterprise/holding bodies of the industrial safety control receive the information only upon incident or failure, not possessing the actual information about deviations at an initial stage when still it is possible to prevent failure), RMS translates the control, a transparency of CIS conditions, the important real-time information (about the facts and predictions), and also necessity of proper response to critical deviations for absolutely new time scale characterized as the scale of real time, measured by seconds-minutes.

Effects from the remote control can be reached only when quality of RMS operation is provided. It means that it is reliable and timely producing the complete, valid, and, if needed, confidential information by RMS.

Generally, system analysis of RMS operation consists in evaluation of reliability, timeliness, completeness, validity, and confidentiality of the used information. In special cases for compound subsystems and system elements, not all measures may be used. For example, for a subsystem of information security enough to use the measures to evaluate protection from an unauthorized access and information confidentiality during the given time period. Dependence of the purposes of researching RMS can be decomposed to the level of compound subsystems and separate elements (see **Figure 6**).

In this case according to the system engineering principles, the operation quality of every component should be evaluated.

For evaluating integral RMS operation quality, the next measure is proposed: the probability of providing reliable and timely representation of the complete, valid, and confidential information during the given time ($P_{RMS}(T_{given})$).

In general case

$$P_{RMS}(T_{given}) = P_{rel.RMS}(T_{given}) \bullet C_{tim\ RMS} \bullet P_{compl..RMS} \bullet P_{actual..RMS} \bullet P_{check\ RMS} \bullet P_{process.RMS} \bullet P_{inf.l.\ RMS}\ (T_{given}) \bullet P_{man\ RMS}(T_{given}) \bullet P_{prot.RMS} \bullet P_{conf.RMS}\ (T_{given}),$$

where all measures are calculated by the models proposed in Section 2.

For complex structures the ideas of combination of the models is proposed in [15]. It allows in an automatic mode to generate new models at the expense that there is possible evaluation of the measures above.

http://dx.doi.org/10.5772/intechopen.75109

When not all system elements and subsystems are captured by RMS capabilities, two subsystems, operated in different time scales, are cooperated in the CIS. A part of CIS, captured RMS, is served in real time, and the other part is in a usual time scale (with information gathering by a principle "as it is possible to receive"). In many critical situations, this usual time scale cannot be characterized as adequate to a reality. With the use of the offered approach, the system with usual control (UC), used for CIS, i.e., without RMS application, can be estimated. Generally, the analyzed critical infrastructure is presented as a combination "System+RMS" and usual "System without RMS." And, "System+RMS" is a combination of "Structure for RMS" and "RMS" (see **Figure 12**). For these systems some measures of the information delivery may not answer requirements of real time—"System+RMS" because RMS operation quality is inadequate and "System without RMS" without RMS.

All the great number of the factors characterizing threats to analyzed critical infrastructure is considered as 100%, and total frequency of dangerous deviations is designated through λ_{Σ}. Frequency of potentially dangerous deviations traced by "System + RMS" is designated (λ_{RMS}). Frequency of occurrence of other potentially dangerous deviations which are not traced by RMS (i.e., for "System without RMS") is designated ($\lambda_{\Sigma} - \lambda_{RMS}$).

For "System + RMS" the RMS operation quality during the time of prediction T_{given} is evaluated by probability $P_{RMS}(T_{given})$. And, the risk of critical deviation for safety during the time of prediction T_{given}, designated as $R_{RMS}(T_{given})$, can be evaluated by the earlier methods [2–3, 5–17]. For the usual "System without RMS," the same measures $P_{UC}(T_{given})$ and $R_{UC}(T_{given})$ can be used with specified value of input for probabilistic modeling.

Then, in general form, the risk $R(T_{given})$ to lose integrity for analyzed critical infrastructure during the time of prediction T_{given} can be evaluated by the formula:

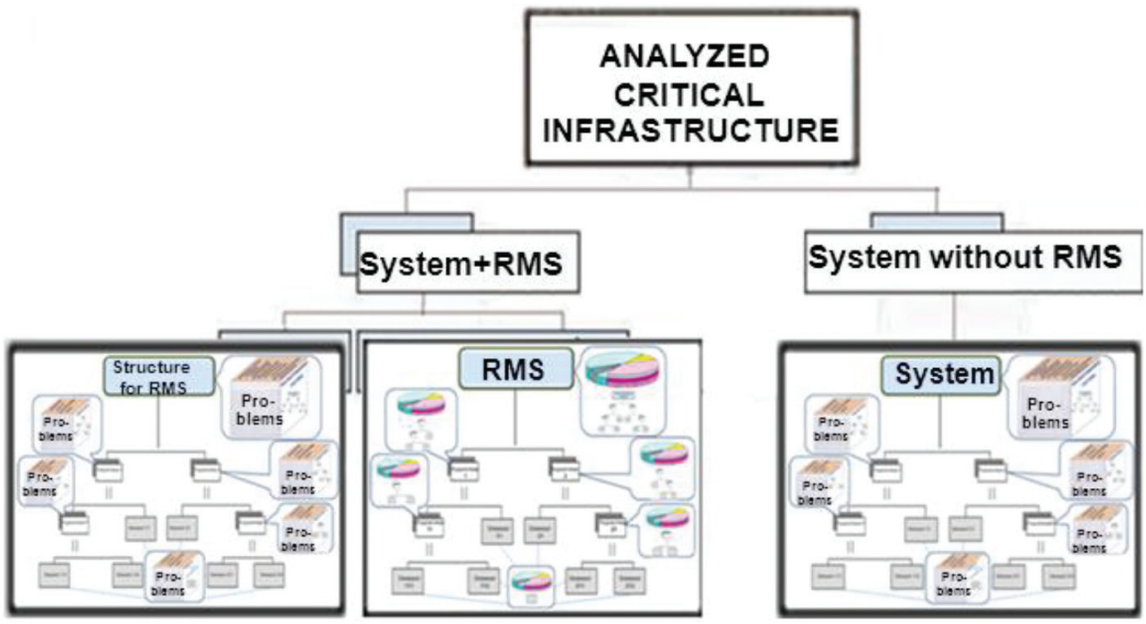

Figure 12. Decomposition of analyzed critical infrastructure to fill influence of RMS.

$$R(T) = 1 - [(\lambda_{RMS} / \lambda_{\Sigma}) P_{RMS} (T_{given}) (1 - R_{RMS} (T_{given})) + ((\lambda_{\Sigma} - \lambda_{RMS}) / \lambda_{\Sigma}) P_{UC} (T_{given}) (1 - R_{UC} (T_{given}))],$$

where expression in square brackets is a probability of successful operation of analyzed critical infrastructure. Depending on the made risk definition in special cases, it can be interpreted as probability of safe or reliable operation or probability of norm observance for critical parameters of the equipment or others in the conditions of associated potential threats. The case $\lambda_{\Sigma} = \lambda_{RMS}$ means full capture of critical infrastructure by RMS capabilities.

5.2. Estimating the mean residual time before the next parameter abnormalities

Unfortunately, in the world the universal approach to adequate prognosis of the future parameter conditions on the basis of current data is not created yet. The uncertainty level is too high. Nevertheless, in practice for each concrete case, subjective expert estimations, regression analysis of collected data, and simulation are often used. And, probabilistic models applied in some cases contain many simplifications, and they frequently do not consider an infrastructure of complex systems, heterogeneity of threats, distinctions in technologies of the control, and recovery of integrity for various elements of these systems [2–3]. The same aspects and also rarity of many random events (with some exceptions) do an ineffective statistical estimation of residual time before the next parameter abnormalities. At the same time, scientifically proven prognosis of a residual time resources is necessary for acceptance of preventive measures on timely elimination of the abnormality reasons. The above-stated characterizes an actuality of this and similar researches for different industrial areas [11–17].

Traced conditions of parameters are data about a condition before and on the current moment of time, but always the future is more important for all. With the 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. That is, because of ignorance of this residual time, measures for prevention of negative events after parameter abnormalities (failures, accidents, damages, and/or the missed benefit because of equipment time out) are not undertaken. And, on the contrary, knowing residual time before abnormality, these events may be avoided, or the system may be maintained accordingly. For monitored critical system, the probabilistic method to estimate the mean residual time before the next parameter abnormalities for each element and whole system is proposed.

By principles of system engineering (e.g., according to ISO/IEC/IEEE 15288), the complex system is decomposed to compound subsystems and elements with formal definition of states (see **Figure 13**).

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,” and “Abnormality” (interpreted similarly light signals (“green,” “yellow,” “red”) (see **Figure 14**). The condition “Abnormality” characterizes a threat to lose system integrity (on the logic level, this range “Abnormality” may be interpreted analytically as failure, fault, unacceptable risk or quality, etc.).

http://dx.doi.org/10.5772/intechopen.75109

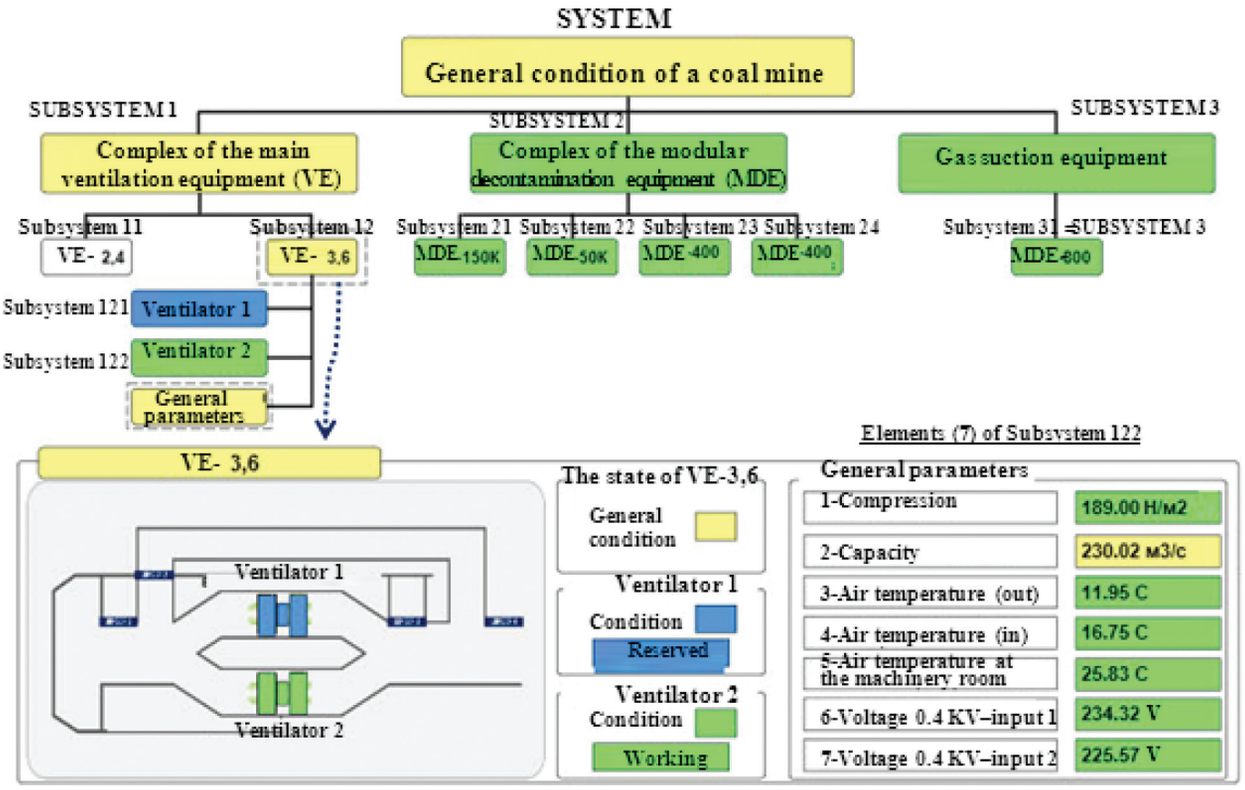

Figure 13. Example of system decomposition.

For avoiding the possible crossing of 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, should be carried out. For prediction the following are proposed: (1) a choice of probabilistic models for construction (PDF of time before the next abnormality for one element ("black box")), (2) development of the algorithm of generation (PDF of time before the next abnormality for complex system), and 3) formalization of calculative methods of estimating the mean residual time before the next parameter abnormalities for monitored critical system.

The method allows to estimate residual time before the next parameter abnormality (i.e., time before the first next coming into "red" range) [14].

The method allows to estimate residual time before the next parameter abnormality $T_{resid(1)}$ for a given admissible risk $R_{adm.}(T_{req})$ to lose integrity. The estimated $T_{resid(1)}$ is the solution t_0 of equation:

$$R(T_{occur}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.}) = R_{adm.}(T_{req}) \quad (7)$$

concerning of unknown parameter t, i.e., $T_{resid(1)} = t_0$.

Here, $R(T_{occur}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.})$ is the risk to lose integrity; it is addition to 1 for probability $P(T_{req})$ of providing system integrity ("probability of success"), and for calculations formulas (1)–(7) are used (see SubSection 3.1 of this article). So, for exponential PDF, formula (1) transforms into formula.

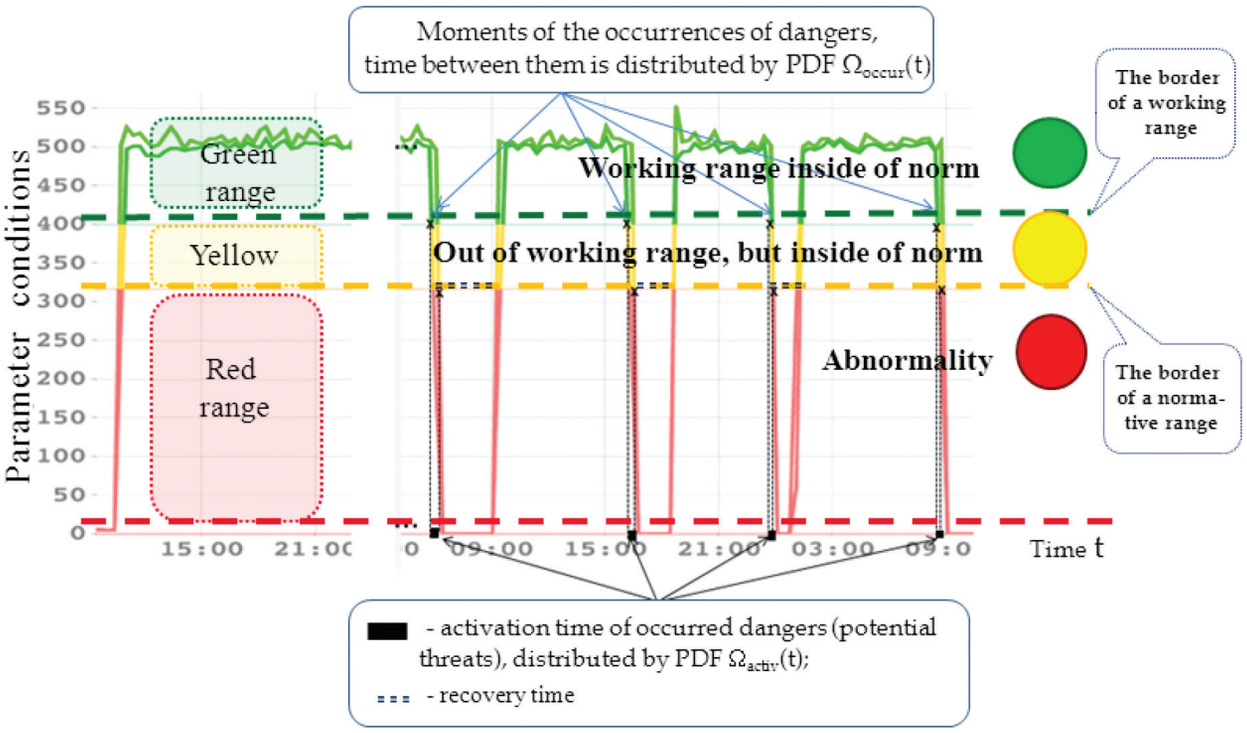

Figure 14. Elementary ranges for parameter conditions.

This formula is used for Eq. (7).

T_{occur} is the mathematical expectation of PDF Ω_{occur} (τ); it is defined by parameter statistics of transition from "green" into "yellow" range (see **Figure 3**). The other parameters T_{betw} and T_{diag} in formula (7) are known. The main practical questions are as follows: what about $T_{req.}$ and what about the given admissible risk $R_{adm.}(T_{req})$? For answering we can use the properties of function $R(T_{occur}, t, T_{betw}, T_{diag}, T_{err.}, T_{req.})$:

- If parameter t increases from 0 to ∞ for the same another parameters, the function R(…, t, …) is monotonously decreasing from 1 to 0, i.e., if the mean activation time of occurred danger (threat: from the first input at the "yellow" range to the first input in the "red" range) is bigger, to lose integrity is less.
- If parameter T_{req} increases from 0 to ∞ for the same other parameters, the function $R(…,T_{req})$ is monotonously increasing from 0 to 1, i.e., for large T_{req} risk approaches to 1.

It means that the such maximal x exists when t = x and $T_{req.}$ = x and $0 < R(T_{occur}, x, T_{betw}, T_{diag}, T_{err.}, x) < 1$. That is, the residual time before the next parameter abnormality (i.e., time before the first next coming into "red" range) is equal to the defined x with the confidence level of admissible risk $R(T_{occur}, x, T_{betw}, T_{diag}, T_{err.}, x)$.

For example, if T_{occur} = 100, T_{betw} = 8 hours, T_{diag} = 1 hour, $T_{err.}$ = 0, and $R_{adm.}$ = 0.05, unknown x is defined from equation, considering (1), (7):

So, if T_{occur} = 100 days, for $R_{adm.}$ = 0.01 residual time x ≈ 2.96 weeks (considering decisions of recovery problems of integrity every 8 hours).

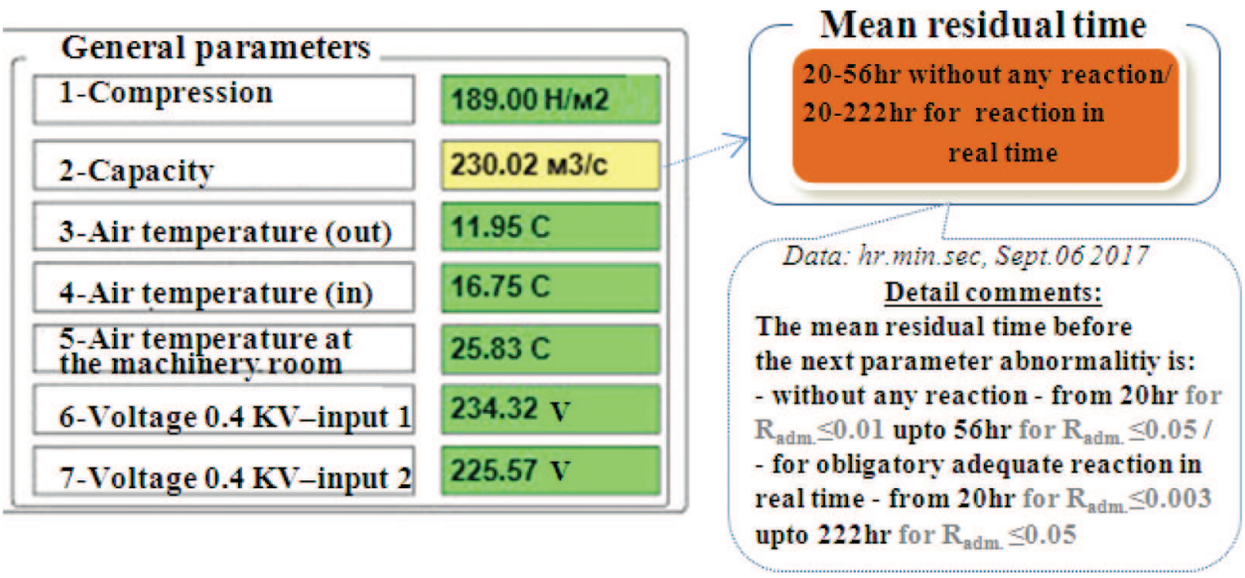

Figure 15. Example of residual time and comments.

The method is implemented by RMS. At once after crossing "yellow" border from "green," the automatic prediction of the mean residual time before the next parameter abnormalities (from the first input at the "yellow" range to the first input in the "red" range) is displayed (see **Figure 15**).

Adequate reaction of responsible staff in real time is transparent for all interested parties.

5.3. About some effects from adequate probabilistic methods and technology applications

Some effects from the proposed adequate probabilistic methods and technologies of RMS are estimated on the level of predicting risks to lose object safety (integrity) by PDF [16].

Example 5.3.1. According to statistics from multifunctional safety system (MFSS), a frequency of occurrence of the latent or obvious threats is equal to once a month, and an average time of development of threats (from occurrence of the first signs of a critical situation up to failure) is about 1 day. A work shift is equal to 8 hours. The system control is used once for work shift, and a mean duration of the system control is about 10 minutes (it is supposed that recovery of object integrity is expected also for 10 minutes). The workers (they may be mechanics, technologists, engineers, etc.) of medium-level and skilled workers are capable to revealing signs of a critical situation after their occurrence, and workers of the initial level of proficiency are incapable. Medium-level workers can commit errors on the average not more often once a month, and skilled workers are not more often once a year. How consideration of the qualification level influences on predicted risks to lose object safety for a year and for 10 years?

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

workers, risk equals to 0.0006 for a year and 0.0058 for 10 years because of effective monitoring using RMS possibilities.

Example 5.3.2. We will concentrate on the analysis of errors of skilled workers from the point of object safety. Raising adequacy of modeling, in addition to initial data of Example 5.3.1, we will consider that mean recovery time of the lost integrity of object equals to 1 day instead of 10 minutes [10]. What effect may be from risk prediction?

Calculated PDF fragment shows (see **Figure 16**) that risk to lose object safety increases from 0.0006 (for a year) to 0.0119 (for 20 years). Thus, the calculation from PDF mean time between neighboring losses of object safety T_{mean} equals to 493 years. That is, the frequency $\lambda = 1/T_{mean}$ of system safety losses is about 0.002 times a year. It is 6000 times less (!) in comparison with a primary frequency of occurrence of the latent or obvious threats (once a month). And, estimated T_{mean} is almost 500 times more in comparison with a primary mean time between errors of skilled workers (once a year). And, such effect can be reached at the expense of undertaken control measures, monitoring, and system recovering in case of revealing in time the signs of threat development. To the point, the frequency λ of system safety losses is extracted latent knowledge from PDF, built in a calculated form.

If to compare with exponential approximation of PDF with the same frequency λ, the risk to lose object safety will grow from level 0.002 (for a year) to 0.04 (for 20 years). These are also extracted latent knowledge considering Taylor's expansion $R(t, \lambda) \approx \lambda \cdot t$ (see Section 2). Difference is in 3.3–3.4 times more against adequate PDF. To feel, it is enough to ascertain that for created PDF the border of admissible risk 0.002 will be reached for 3 years, not for 1 year as for exponential PDF. That is, the real duration of effective object operation (i.e., without losses of safety) is three times more!

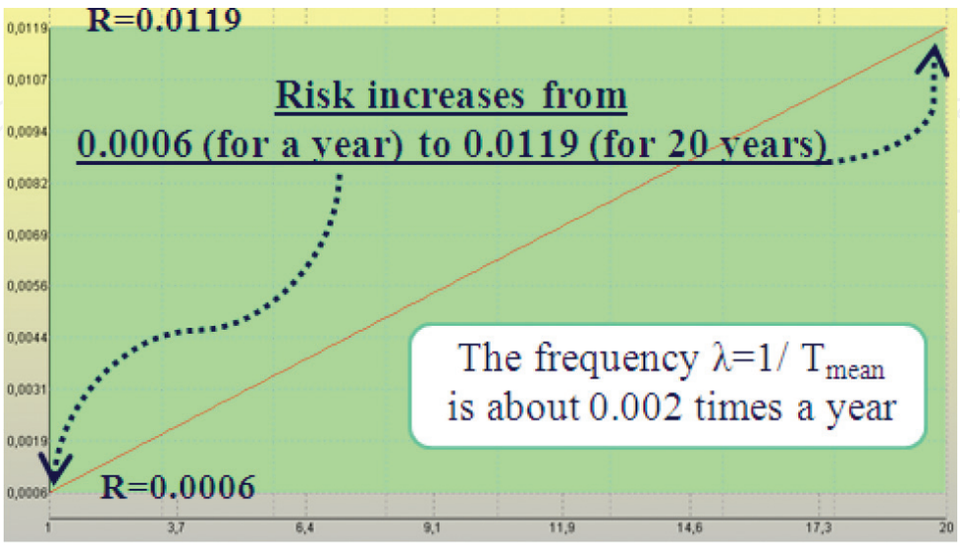

Figure 16. Calculated PDF fragment for Example 5.3.2.

http://dx.doi.org/10.5772/intechopen.75109

Example 5.3.3. This allowed to estimate operation of object as "black box," described by characteristics of skilled workers. On dangerous manufacture critical operations are carried out by skilled workers in interaction with RMS (including reservation and supports of another). Formally, they operate as parallel elements with hot reservation. Thereby, the consideration of such interaction allows to increase adequacy of modeling. Let's estimate risk to lose object safety for this variant (all input data for each from two parallel elements are the same that in Example 5.3.2).

Calculated PDF fragment shows (see **Figure 17**) that risk to lose object safety increases from 0.0000003 (for a year) to 0.00014 (for 20 years). Thus, the mean time between neighboring losses of object safety T_{mean}, calculated from known PDF, equals to 663 years. That is, the frequency λ of system safety losses is about 0.0015 times a year. It is 8000 times less (!) in comparison with a primary frequency of occurrence of the latent or obvious threats (once a month). And, at the expense of reservation estimated, T_{mean} is 34.5% longer in comparison with T_{mean} from Example 5.3.2.

If to compare with exponential approximation of PDF with the same frequency λ, the risk to lose object safety will grow from level 0.0015 (for a year) to 0.03 (for 20 years). Difference is in 200–5000 times more against adequate PDF. The border of admissible risk 0.0015 will be reached for 195 years, not for 1.3 year as for exponential PDF. That is, the real duration of effective object operation (i.e., without losses of safety) is 150 times more! Such effect can be reached at the expense of mutual aid (reservation and supports) of skilled workers using RMS.

Example 5.3.4. Come back to the SUEK value chain (see **Figure 10**). According to system engineering principles (see ISO/IEC/IEEE 15288 and **Figure 1**), we decompose logically this chain into nine serial components. Components from 1 to 6 are united by MFSS of mine, component 7 is associated with washing factory, component 8 is associated with transport, component 9 is associated with port (see **Figure 18**). For every element of this chain, a specific

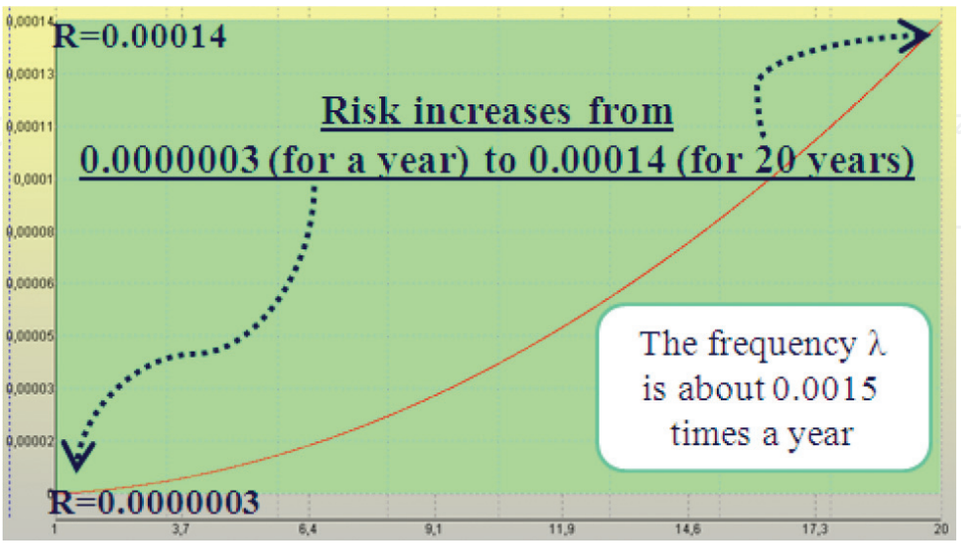

Figure 17. Calculated PDF fragment for Example 5.3.3.

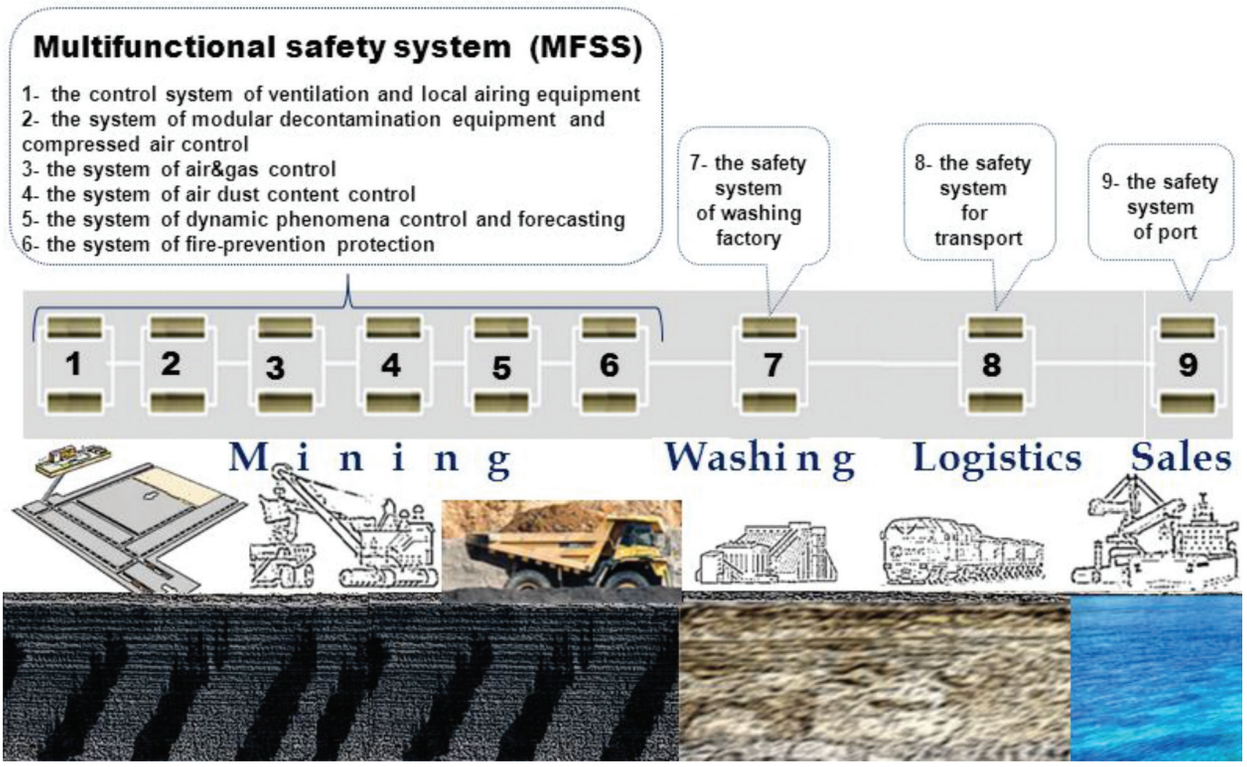

Figure 18. Illustration of system, combined from parallel and series subsystems.

set of threats exists. Let us analyze a system of such value chain. The typical systems of this value chain, including MFSS, are:

1. The control system of ventilation and local airing equipment.
2. The system of modular decontamination equipment and compressed air control.
3. The system of air and gas control.
4. The system of air dust content control.
5. The system of dynamic phenomena control and forecasting.
6. The system of fire prevention protection.
7. The safety system of washing factory.
8. The safety system for transport.
9. The safety system of port.

What about the safety for analyzed value chain for existing threats considering possibilities of remote monitoring systems (RMS), covering all components of chain?

Let's put that the workers, interacted with RMS, participate in each chain process. Their activity is modeled by the models of Section 3, considering examples above. The high adequacy is reached by decomposition of chain system to nine logical subsystems, each of which

http://dx.doi.org/10.5772/intechopen.75109

implements corresponding typical functions of Systems 1–9. Safety of whole value chain system is provided, if "AND" the first subsystem, "AND" the second, …, and "AND" the ninth subsystem safety are provided (see **Figure 18**). Reservation of elements for every subsystem is explained by RMS possibilities. Those input data for every element are the same as in Example 5.3.3.

Calculated PDF fragment shows (see **Figure 19**) that risk to lose safety increases from 0.000003 (for a year) to 0.0013 (for 20 years). Thus, the mean time between neighboring losses of safety T_{mean} equals to 283 years. That is, the frequency λ of system safety losses is about 0.0035 times a year. It is 2.3 times more often against the results of Example 5.3.3. In comparison with a primary frequency of occurrence of the latent or obvious threats (once a month), the frequency λ is 3430 times lower!

For exponential approximation of PDF with the same frequency λ, the risk to lose safety will grow from level 0.0035 (for a year) to 0.07 (for 20 years). Difference is in 54–1167 times more against adequate PDF.

The border of admissible risk 0.002 will be reached for 24 years, not for 7 months as for exponential PDF (see Section 2). That is, the real duration of effective operation (i.e., without losses of safety) is 41 times more!

Example 5.3.5. How much risks will increase, if in a system of value chain from Example 5.3.4 only medium-level workers are used?

Calculated PDF fragment shows (see **Figure 20**) that risk to lose safety increases from 0.0009 (for a year) to 0.25 (for 20 years). Thus, the mean time between neighboring losses of safety T_{mean} equals to 24 years. That is, the frequency λ of system safety losses is about 0.04 times a year. It is 11.4 times less often against the results of Example 4 for skilled workers. In

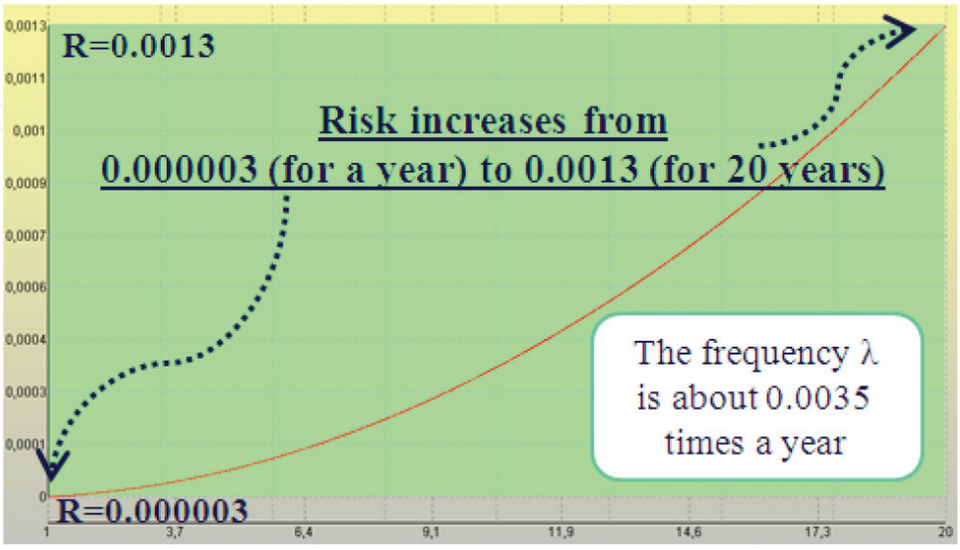

Figure 19. Calculated PDF fragment for Example 5.3.4.

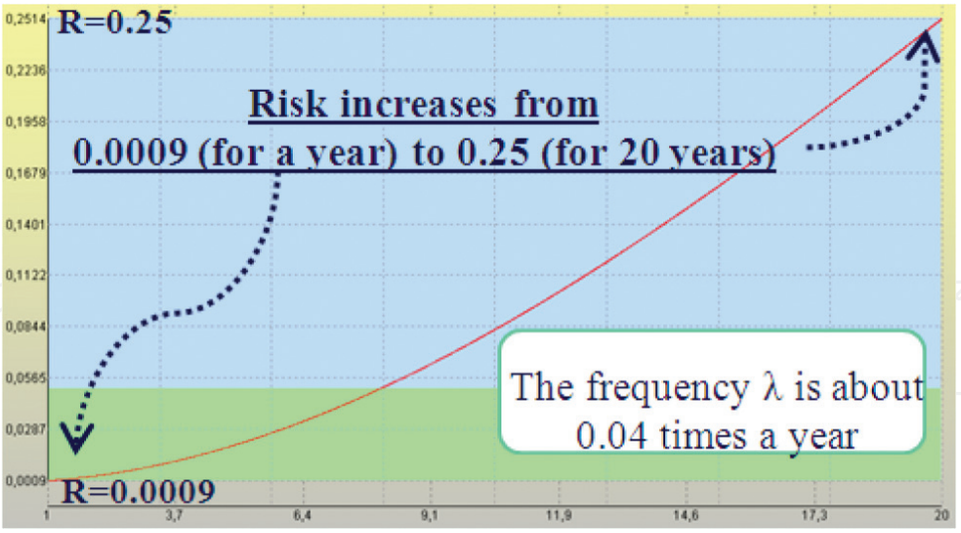

Figure 20. Calculated PDF fragment for Example 5.3.5.

comparison with a primary frequency of occurrence of the latent or obvious threats (once a month), the frequency λ is 21 times lower!

For exponential approximation of PDF with the same frequency λ, the risk to lose safety will grow from level 0.04 (for a year) to 0.55 (for 20 years). Difference is 2.2–44.4 times more against adequate PDF. The border of admissible risk 0.002 will be reached for 2 years, not for one month as for exponential PDF. That is, the real duration of effective operation (i.e., without losses of safety) is 24 times more!

6. Instead of conclusion

The proposed probabilistic methods help the system using "smart systems":

- To predict risks to lose integrity for complex structures on the given prognostic time
- To rationale of preventive measures considering admissible risk
- To estimate "smart system" operation quality
- To predict in real time the mean residual time before the next parameter abnormalities

The algorithm of creating more adequate PDF of time between losses of system integrity, considering for every element different threats, possibilities of control, monitoring, and recovery, allows to improve accuracy of probability predictions in hundred-thousand times (!) in comparison with exponential approximation.

The purposed approach allows to improve existing risk control concept, including creation and perfection of probabilistic models for problem decision, automatic combination, and generation of new probabilistic models, forming the storehouse of risk prediction knowledge; for storehouse, dozens of variants of the decision of typical industrial problems for risk control.

The application of the methods and technologies by the joint-stock company "Siberian Coal Energy Company," implemented on the level of the remote monitoring systems, allowed to rethink system possibilities for increasing reliability and industrial safety, improve multifunctional safety systems, decrease risks, and provide predictive maintenance and operation efficiency in company value chain.

Author details

Vladimir Artemyev[1], Jury Rudenko[1] and George Nistratov[2]*

*Address all correspondence to: george.icie@gmail.com

1 JSC "SUEK", Moscow, Russia

2 Scientific Research Institute of Applied Mathematics and Certification, Moscow, Russia

References

[1] Feller W. An Introduction to Probability Theory and its Applications. Vol. II. Willy; 1971

[2] Kostogryzov A, Nistratov G. Standardization, mathematical modeling, rational management and certification in the field of system and software engineering, Moscow. Armament Policy Conversion. 2004. 395 p

[3] Kostogryzov AI, Stepanov PV. Innovative management of quality and risks in systems life cycle, Moscow. Armament Policy Conversion. 2008. 404p. (in Russian)

[4] Zio E. An introduction to the basics of reliability and risk analysis. World Scientific. 2006. 222 p

[5] Kostogryzov A, Nistratov A, Nistratov G. Applicable technologies to forecast, analyze and optimize reliability and risks for complex systems. Proceedings of the 6st International Summer Safety and Reliability Seminar, Poland. September 2012;**3**(1):1-14

[6] Kostogryzov A, Nistratov G, Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma: InTech. 2012. pp. 127-196. Available from: http://www.intechopen.com/books/total-quality--management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[7] Kostogryzov A, Grigoriev L, Nistratov G, Nistratov A, Krylov V. Prediction and optimization of system quality and risks on the base of modeling processes. American Journal of Operations Research, Special Issue;**3**(1A):217-244

[8] January 2013, Available from: http://www.scirp.org/journal/ajor/

[9] Kostogryzov A, Nistratov G, Nistratov A. The innovative probability models and software Technologies of Risks Prediction for systems operating in various fields. International Journal of Engineering and Innovative Technology (IJEIT). September 2013;**3**(3):146-155. http://www.ijeit.com/archive.php

[10] Kostogryzov AI et al. Security of Russia. Legal, Social&Economic and Scientific & Engineering Aspects. The Scientific Foundations of Technogenic Safety. Machutov N, editor. Moscow, Znanie. 2015. 936 p

[11] Kostogryzov AI, Kosterenko VN, Timchenko AN, Artemyev VB. Osnovy protivoavariynoy ustoychivosty ugolnych predprijatiy (The Foundations of Counteremergency Stability for Coal Enterprises). V. 6 "Industrial safety". Book 11. - Moscow: "Gornoje delo" Kimmerijsky Center Ltd. – 336 p

[12] Kostogryzov AI, Stepanov PV, Nistratov GA, Nistratov AA, Grigoriev LI, Atakishchev OI. Innovative management based on risks prediction. In: Zheng, editor. Information Engineering and Education Science. London: Taylor & Francis Group; 2015. pp. 159-166. ISBN 978-1-138-02655-1

[13] Kostogryzov A, Stepanov P, Nistratov A, Nistratov G, Zubarev I, Grigoriev L. Analytical modeling operation processes of composed and integrated information systems on the principles of system engineering. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars. 2016;**7**(1):157-166. Available from: http://jpsra.am.gdynia.pl/archives/jpsra-2016-contents/

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

[15] Svetlana J, Tatiana K, Andrey K, Oleg K, Andrey N, George N. The probabilistic analysis of the remote monitoring systems of critical infrastructure safety. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars. 2017;**8**(1):183-188. http://jpsra.am.gdynia.pl/archives/jpsra-2017-contents/

[16] Andrey K, Oleg A, Pavel S, George N, Andrey N, Leonid G. Probabilistic modelling processes of mutual monitoring operators actions for transport systems. Proceedings of the 4th International Conference on Transportation Information and Safety, ICTIS 2017. pp. 865-871

[17] 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. Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM 2017), August 6–7, Phuket, Thailand. DEStech Publications, Inc. pp. 279-283

[18] ISO 17359. Condition monitoring and diagnostics of machines - General guidelines

http://dx.doi.org/10.5772/intechopen.75109

[19] ISO 13381–1. Condition monitoring and diagnostics of machines - Prognostics - Part 1: General guidelines

[20] ISO 13379. Condition monitoring and diagnostics of machines - General guidelines on data interpretation and diagnostics techniques

[21] IEC 61508–1. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

IntechOpen

IntechOpen