Kostogryzov Andrey

Nistratov Andrey

Zubarev Igor
Research Institute of Applied Mathematics and Certification, Moscow, Russia

Stepanov Pavel
Institute of Informatics Problems of the Russian Academy of Sciences, Moscow, Russia

Grigoriev Leonid
The Gubkin Russian State University of Oil and Gas, Moscow, Russia

About accuracy of risks prediction and importance of increasing adequacy of used probabilistic models

Keywords

model, optimization, probability, quality, resources, risk, system, technology

Abstract

The work purpose is the quantitative proof of importance and necessity of increasing adequacy of probabilistic models, described by probability distribution functions (PDF) of time between losses of system integrity. For purpose achievement the analysis of probabilistic metrics of risks and the elementary forms to establish an admissible risks is carried out, some ways of increasing an adequacy of probabilistic models for complex structures are described. Possibilities of extracting the latent knowledge from an adequate PDF are shown. Practical value of the researches are the revealed possibilities for a substantiation of more effective system decisions at the expense of increasing accuracy of risks prediction. Effects are demonstrated by examples.

1. Introduction

Today creation of technologies of effective risks management, based on modern methods of prediction, essentially lags behind requirements of practice. In many respects it may be explained not only by high complexity and a cost of development and maintenance of these technologies, but also incomplete understanding of what and how latent knowledge can be extracted from results of adequate probabilistic modelling. The first methods of risks prediction in interests of system reliability and safety have been developed dozens years ago. And scientific researches in these directions proceed [1]-[10], etc. However, this creative activity requires the confirming estimations convincing of efficiency. How many percent the results of modelling are differed for usual and more detailed models? Whether it is necessary to spend efforts for detailed researches and creation of new probabilistic models? Questions sound is banal, but there is an impression, that a search of answers is not in focus of due attention. The work purpose is the quantitative proof of importance and necessity of increasing adequacy of probabilistic models, described by probability distribution functions (PDF) of time between losses of system integrity. PDF of time between failures is an analogue from reliability theory. System integrity is defined as such system state when system purposes are achieved with the required quality (for example, the losses of integrity as results of different threats influences can lead to losses of system safety or operation quality, to system effectiveness decrease, to emergencies and, as consequence, to real either possible damages or the missed benefit).

For purpose achievement the analysis of probabilistic metrics of risks and the elementary forms to establish an admissible risks is carried out, some ways of increasing an adequacy of probabilistic models for complex structures are described. Possibilities of extracting the latent knowledge from an adequate

PDF are shown. Practical value of the researches are the revealed possibilities for a substantiation of more effective system decisions at the expense of increasing accuracy of risks prediction. Effects are demonstrated by examples.

2. The analysis of probabilistic metrics of risks and the elementary forms to establish an admissible risks

In general case the risk may be estimated by multiplication of a probability of danger threats influences, leading to a damage, on a damage. Here the most difficulties from the scientific point of view for anticipating dangerous development of events is to construct an adequate PDF 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 hundreds percent). 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 risks predictions, in definition and concept of use «admissible risk», and then to compare various variants.

In practice probabilistic estimations of system integrity losses quite often carry out by the frequency of emergencies or any adverse events. For example, with reference to safety it can be frequencies of different danger threats influences, leading to a damage. I.e. frequency replaces estimations of probability (risk to lose integrity of system during prognostic period). Whether it is correct? From probability theory it is known, that for defined PDF one of its characteristics is the mathematical expectation ($T_{exp.}$). 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 rhe frequency **λ** 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 0.00 for approximation by deterministic (discrete) PDF and 0.36 for exponential approximation. I.e. as a result of erroneous choice of PDF, characterized by identical λ, the enormous difference may take place! On the one hand it means ambiguity of a probabilistic estimation of events, being guided only on frequency λ, and with another one – a necessity of search (or creations) more adequate PDF of time between losses of system integrity is very high.

Often today engineers prefer exponential PDF: R(t, λ) = 1 – exp (-λ·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, λ) ≈ λ·t with accuracy o($\lambda^2 \cdot t^2$). And, if t=1 year the absolute value of frequency practically coincides with value of probability. But if value λ·t increases, it is capable to exceed 1 and by definition generally cannot be perceived as probability. Resume: focusing on probability is correct from point of view of universal risk metric. And focusing on frequency may be incorrect if λ·t is approximately more than 10^{-3}.

The special importance has the concept of "admissible risk». The matter is 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 proved. In practice frequently the «admissible risk» is interpreted as "border strip", i.e. it is supposed, that if do not cross this "border strip", the system integrity cannot be lost. But in reality it 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. Complex use of these measures promotes to retaining the risk on admissible level. It is the typical approach which should work correctly. And how it work in practice?

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

«A frequency λ of system integrity losses should not exceed admissible level $\lambda_{adm.}$»;

and-or «probability to lose integrity of system during time T_{req} should not exceed admissible level $R_{adm.}$ (T_{req})»;

and-or their combination.

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

if the limitation on an 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})). I.e. this dependence means: a given value of admissible probability $R_{adm.}$ (T_{req}) corresponds unequivocally with a value of the maximum frequency of system integrity losses;

if the limitation on an admissible level of maximum frequency of system integrity losses $\lambda_{adm.}$ is set, it means, that for exponential approximations function of probability from time t is considered: R(t, $\lambda_{adm.}$) = 1 – exp (-$\lambda_{adm.}$·t) . I.e. this is the same "border strip", but in the form of 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.

Despite obvious incompleteness of the elementary forms of requirements to «admissible risks» (in reality – only the limitations in one or several points) and absence of interrelations with a kind of real PDF of time between losses of system integrity (depending from many parameters: structure of system, heterogeneity of threats, different measures of counteraction to threats etc.), these forms 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 results of adequate probabilistic modelling.

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

Accordingly, there is an important question: what frequencies of system integrity losses should be used for risk predictions and where it to take? – If these are only the frequencies of emergencies the predicted risks will be essentially underestimated! These final frequencies are output instead of input data for modelling. 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, the frequency of critical errors from "human factor» on dangerous enterprises is about 1 times 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 obvious - the frequency **λ** of system integrity losses used at risk predictions, itself should pay off by results of probabilistic modelling. Indeed, for adequate risks prediction there is important a frequency of the all primary incidents (including neutralized incidents at the expense of control measures, maintenance and timely reaction on initial signs of threats development).

3. Some ways of increasing adequacy of probabilistic models

We present some ways of increasing adequacy of probabilistic models by the examples of different consideration of real protection processes against dangerous influences and the creation algorithm of integration PDF for complex systems [1]-[4], [6]-[10]. Nowadays at system development and utilization an essential part of funds is spent on providing system protection from various dangerous influences able to violate system integrity (these may be failures, incidents events, capable to lead to failures, "human factors", information security events, terrorists attacks, etc). There are described two general technologies of providing protection in different spheres: proactive periodical diagnostics of system integrity (technology 1) and additionally monitoring between diagnostics (technology 2), researches are in [2]-[9]. These models allow to create more adequate PDF of time between losses of system integrity.

3.1. The models for the systems that are presented as one element

Technology 1 is based on proactive diagnostics of system integrity, that are carried out periodically to detect danger sources penetration into a system or consequences of negative influences. The lost system integrity can be detect only as a result of diagnostics, after which 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.

Note. It is supposed that used diagnostic tools allow to provide necessary system integrity recovery after revealing of danger sources penetration into a system or consequences of influences.

Technology 2, unlike the previous one, implies that operators alternating each other trace system integrity between diagnostics. In case of detecting a danger source an operator recovers system integrity (ways of danger sources removing 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.

The probability of correct system operation within the given prognostic period (i.e. probability of

success) may be estimated as a result of use the next models (assumption: for all time input characteristic the probability distribution functions (PDF) exist). Risk to lose integrity (safety, quality or separate property, for example – reliability) is an addition to 1 for probability of providing system integrity (correct system operation or "probability of success") R=1-P.
There are possible the next variants for technology 1 and 2: variant 1 – the given prognostic period T_{req} is less than established period between neighboring diagnostics ($T_{req} < T_{betw.}+T_{diag}$); variant 2 – the assigned period T_{req} is more than or equals to established period between neighboring diagnostics ($T_{req} \geq T_{betw.}+T_{diag}$). Here $T_{betw.}$ – is the time between the end of diagnostic and the beginning of the next diagnostic, T_{diag} – is the diagnostic time.
The next formulas for PDF of time between the losses of system integrity are proposed (Author – A. Kostogryzov [2]-[9]).

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

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

where $\Omega_{penetr}(t)$ – is the PDF of time between neighboring influences for penetrating a danger source; $\Omega_{activ}(t)$ – is the PDF of activation time of a penetrated danger source. These PDF $\Omega_{penetr}(t)$ and $\Omega_{activ}(t)$ may be exponential PDF. For different danger threats a frequency **λ** for these PDF is the sum of frequencies of every kind of threats.

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

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

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

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

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

Here $A(t)$ is the PDF of time between operator's error.

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

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

where the probability of success within the given time $P_{(1)}(T_{given})$ is defined by (3).
The final clear analytical formulas for modelling are received by Lebesque-integration of (3) expression.
Many models are applicable to the system presented as one element. The main result of such system modelling is probability of providing system integrity (correct system operation) 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. The creations of more adequate models for complex system

The basic ideas of correct integration of probability metrics are based on a combination and development of the offered *models* [2]-[9]. For a complex system estimation with parallel or serial structure existing models can be developed by usual methods of probability theory. For this purpose in analogy with reliability it is necessary to know a mean time between losses of integrity for each element. Let's consider the elementary structure from two independent parallel elements that means logic connection "OR" or series elements that means logic connection "AND".

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 τ_i: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when either 1st, or 2nd element integrity will be lost). For this case the PDF

of time between losses of system integrity is defined by expression

$$B(t) = P(\min(\tau_1,\tau_2)\leq t) = 1 - P(\min(\tau_1,\tau_2)>t)$$

$$= 1 - P(\tau_1>t)P(\tau_2 > t)$$

$$= 1 - [1-B_1(t)]\,[1- B_2(t)]. \qquad (5)$$

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 1st or 2nd elements (i.e. the system goes into a state of lost integrity when both 1st and 2nd element integrity will be lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\max(\tau_1,\tau_2)\leq t) = P(\tau_1 \leq t)P(\tau_2 \leq t)$$

$$= B_1(t)B_2(t). \qquad (6)$$

Note. The same approach is developed also by Prof. E.Ventcel in 80th, Prof**.** K.Kolowrocki [1], Prof. E.Zio [10] and others researchers.

Thus an adequacy of probabilistic models is reached by the consideration of real processes of control, monitoring, element recovery for complex structure. Applying recurrently expressions (5) – (6), it is possible to receive 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 by traditional methods of mathematical statistics), and a frequency $\boldsymbol{\lambda}$ of system integrity losses $\boldsymbol{\lambda}$=1/ $T_{exp.}$. This can allow to compare the accuracy against the elementary exponential model (P(t, λ) = 1 – exp (- λ·t)).

All these ideas are implemented in the software technologies of risk prediction for complex systems, for example, the “Complex for evaluating quality of production processes” (patented by Rospatent №2010614145) [2], [7], [9].

4. What latent knowledge can be extracted from adequate PDF?

In *Figure 1* 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.

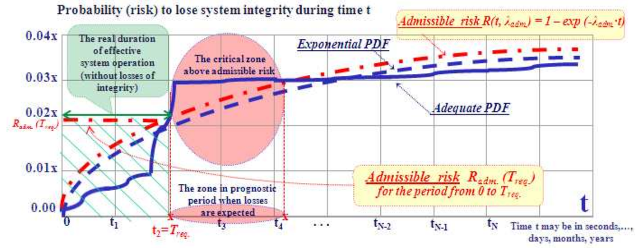

Figure 1. Fragment demonstrating the possible variants of correlations of the limitations to admissible risks, exponential and an adequate PDF of time between losses of system integrity with identical frequency of system integrity losses λ

Being guided by exponential approximation of PDF, it is possible to ascertain easily: are the requirements to level of admissible risks met? If it is below of "border strip" - the requirement is met, if it is above of "border strip" - the requirement isn’t met! Also this is all extracted knowledge… From "pluses" - only convenience of comparison. And all!

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

- to calculate more accurate the dependencies of the probability to lose system and subsystem integrity during time t from characteristics of occurrence and development of different danger threats, real protection processes against dangerous influences and also from a structure of system;
- to estimate accuracy of risk prediction in comparison with exponential approximation of PDF of time between losses of system integrity;
- to define a real duration of effective system operation (i.e. without losses of integrity) considering real protection measures for making decision about predictive counteraction measures against threats in time;
- to define critical zone above admissible risk when losses of system integrity are expected in prognostic period for making decision about predictive counteraction measures or justifying a revision of admissible risks for these zones (considering risk avoiding and mitigation);
- to compare a real duration of effective system operation (i.e. without losses of integrity) considering real protection measures with the same period for exponential approximation of PDF of time between losses of system integrity.

Besides, after creating more adequate PDF, it is possible to extract additional knowledge by usual methods of probability theory (see, for example,

[10]) - to calculate from known PDF the mean time between neighboring losses of system and subsystem integrity T_{mean} , and the frequency **λ** of system and subsystem integrity losses (**λ** = 1/ T_{mean}) considering real protection processes and conditions of dangerous influences.

Some examples help to fill quantitatively an importance of increasing adequacy of used probabilistic models.

5. About accuracy of risk prediction

For dangerous industrial object we studied the questions of predicting risks to lose object safety (integrity) by PDF, created by methods of part 3, on the examples connected with "human factor».

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

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

Example 2. We will concentrate on the analysis of errors of skilled workers from the point of object safety. Raising adequacy of modelling, in addition to initial data of the *Example 1* we will consider, that mean recovery time of the lost integrity of object equals to 1 days instead of 10 minutes [9]. What knowledge can be extracted from risk prediction?

The extracted knowledge from the results of modelling (see *Figure 2*). Calculated PDF fragment shows: risk to lose object safety increases from 0.0006 (for a year) to 0.0119 (for 20 years). Thus the calculated from PDF mean time between neighboring losses of object safety T_{mean} equals to 493 years. I.e. the frequency λ=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 threats development. To the point: the frequency λ of system safety losses is extracted latent knowledge from PDF, built in calculated form. And it demonstrate the answer for the question from the end of part 2 (what frequencies of system integrity losses should be used for risk predictions and where it to take?).

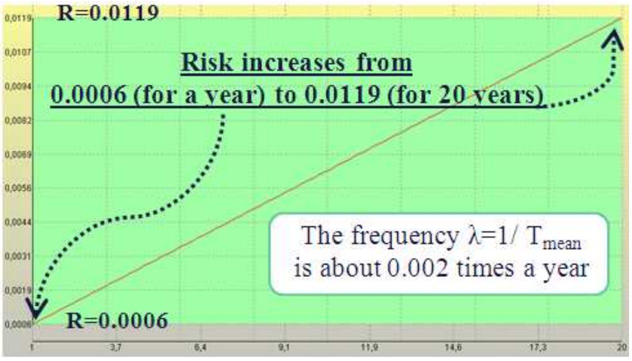

Figure 2. Calculated PDF fragment for *Example 2*

If to compare with exponential approximation of PDF with the same frequency λ, the risk to lose object safety will grow from level 0.002 (for a year) to 0.04 (for 20 years). These are also extracted latent knowledge considering Taylor's expansion R(t, λ) ≈ λ·t (see part 2). Difference is in 3.3 – 3.4 times more against adequate PDF. To feel, how much 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. I.e. the real duration of effective object operation (i.e. without losses of safety) is 3 times more!

Example 3. *Example 2* 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 (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 modelling. Let's estimate risk to lose object safety for this variant (all input data for each from 2 parallel elements are the same, that in the *Example 2*).

The extracted knowledge from the results of modelling (see *Figure 3*). Calculated PDF fragment shows: 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. I.e. the frequency λ of system safety losses is about 0.0015 times a year. It is 8000 times less (!) in comparison with a primary frequency of occurrence of the latent or obvious threats (once a month). And at the expense of reservation estimated T_{mean} is 34.5% longer in comparison with T_{mean} from the *Example 2*.

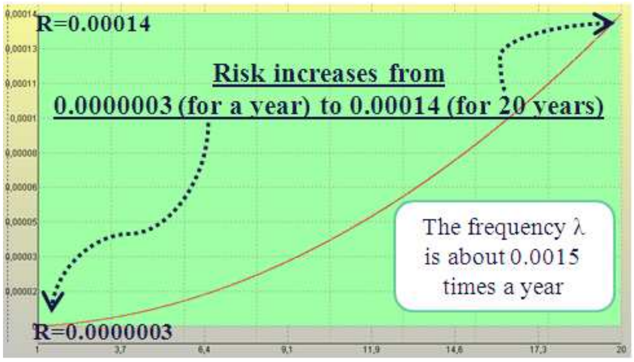

Figure 3. Calculated PDF fragment for *Example 3*

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

Example 4. Dangerous manufacture is a complex of diverse processes, in each of which «the human factor» is the bottleneck. The larger enterprise the risks higher. Let’s analyze a system of complex gas preparation at an enterprise of a gas craft. The typical processes are:
1) processes, connected with operation of entrance threads;
2) processes of low temperature gas separations;
3) process of gas measuring;
4) processes of gas heating and reduction, candle and torch separation;
5) processes, connected with methanol storage and using, storage, giving and drainage dumps of condensate and diesel fuel;
6) processes of management in a service of Chief engineer;
7) processes of management in a service of the Chief of production;
8) processes of shop divisions;
9) processes of control & information system operation.

Let's put, the workers, interacted (including reservation and supports of another), are involved in each of processes. Their activity is modelled by the models of part 3 – see *Example 3*. The high adequacy is reached by decomposition of system structure of workers set (a set of “human factor”) to 9 logical subsystems of workers, each of which implements corresponding typical processes 1)-9). Safety of system is provided, if "AND" the 1st subsystem, “AND" the 2nd, … “AND" the 9th subsystem safety is provided – see *Figure 4*. Those input data for every element are the same as in *Example 3*.

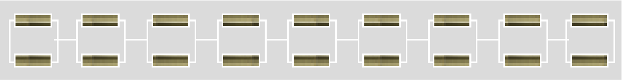

Figure 4. Illustration of system, combined
from parallel and series subsystems

Question: what risks are possible because of «human factor» during term from one to 20 years of operation of the enterprise?

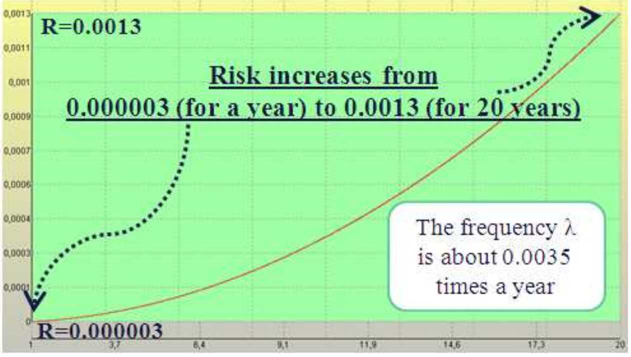

Figure 5. Calculated PDF fragment for *Example 4*

The extracted knowledge from the results of modelling (see *Figure 5*). Calculated PDF fragment shows: risk to lose object safety increases from 0.000003 (for a year) to 0.0013 (for 20 years). Thus the mean time between neighboring losses of object safety T_{mean} equals to 283 years. I.e. the frequency λ of system safety losses is about 0.0035 times a year. It is 2.3 times more often against the results of *Example 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 object safety will grow from level 0.0035 (for a year) to 0.07 (for 20 years).

Difference is in 54 – 1167 times more against adequate PDF.

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

Example 5. How much risks will increase, if in a system of the *Example 4* only medium-level workers are used?

The extracted knowledge from the results of modelling (see *Figure 6*). Calculated PDF fragment shows: risk to lose object safety increases from 0.0009 (for a year) to 0.25 (for 20 years). Thus the mean time between neighboring losses of object safety T_{mean} equals to 24 years. I.e. the frequency λ of system safety losses is about 0.04 times a year. It is 11.4 times less often against the results of *Example 4* for skilled workers. In comparison with a primary frequency of occurrence of the latent or obvious threats (once a month) the frequency λ is 21 times lower!

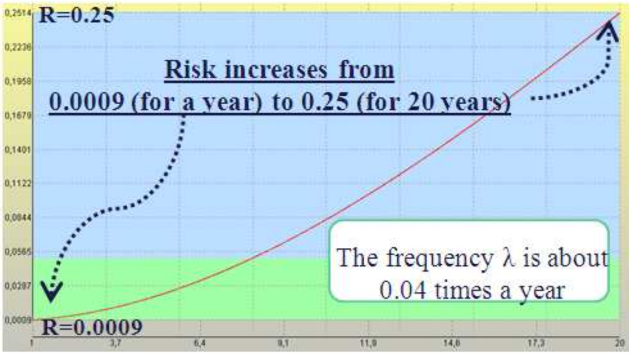

Figure 6. Calculated PDF fragment for *Example 5*

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

6. How to use extracted knowledge?

The extracted knowledge should be used for system analysis and optimization. The formal statements of problems for system optimization are generally maximization of a prize (profit, a degree of quality or safety, etc.) at limitations on expenses, some risks etc. or minimization of expenses at limitations on an admissible levels of risks etc.

Extracted knowledge from adequate PDF allows to use predicted risks, that are more accurate in hundred-thousand times (!). From *Examples 4-5* the use of existing approaches, based on exponential approximation of PDF to estimate risk to lose object safety, the enterprise should consider expected duration of continuous effective (safe) object operation about one month for medium-level workers and 7 months for skilled workers. These expectations are connected with high expenses and influences on enterprise business. But more accurate risk prediction from *Example 4* confirms that for skilled workers the enterprise may be sure in safety during 24 years (not for 7 months as for exponential PDF), and *Example 5* confirms that for medium-level workers the enterprise may be sure in safety during 2 years (not for one month). Both more accurate predictions allow to do business with assurance, having scientific justification.

The important note: in all examples the verisimilar input, peculiar to the various enterprises of dangerous manufacture, are used for modelling (for example: frequency of occurrence of the latent or obvious threats from "human factor" is equal to once a month). They "were not adjusted" in any way to standard admissible risks for dangerous industrial object (no rare than 10^{-3} – 10^{-7} dangerous events a year). But as a result of application of more adequate models the output estimations of risks are near to the standard limitations. The difference is only in the creation of functional dependence of risk from input (on a level of PDF), with which possibilities of analytical decisions of problems for system analysis and optimization are appeared.

Thus on the base of very different results of risk prediction (for existing and proposed approaches) the decisions for business are scientifically justified and correct for adequate modelling.

5. Conclusion

1. For adequate risks prediction there is important a frequency of the all primary incidents (including neutralized incidents at the expense of control measures, maintenance and timely reaction on initial signs of threats development) and also different protection processes.

2. The presented ways of increasing adequacy of the PDF of time between losses of system integrity consider frequency of occurrence and development of different danger threats, real protection processes against dangerous influences (proactive periodical diagnostics, monitoring between diagnostics, recovery of the lost system integrity) and the complex structure of system. The known kind of the more adequate PDF allows to define accordingly a frequency of system integrity losses for comparing

the accuracy of risk prediction against the elementary exponential approximation.

3. The researches quantitatively proved, that the popular today the mode for risks prediction based on uses of frequencies of emergencies (and corresponding exponential PDF) is a rough and unpromising engineering way. Its application deforms very essentially probabilistic estimations of risks and can't be useful for scientific search of effective counteraction measures against different threats (deviations from more adequate estimations of risks are very high: more than thousand percent (!)).

At the expense of application of more adequate models to the analysis of "human factor» the real possibility of decreasing frequency of system integrity losses in thousand times to level 10^{-3} – 10^{-7} times a year (!) in comparison with primary frequency of incidents once a month is proved. Comparison at identical frequency of system integrity losses has shown, that for more adequate PDF the level of risk is less in hundred-thousand times (!) and the real period of effective system operation (without losses of integrity) is more in tens-hundreds times against the exponential approximation.

4. More accurate predictions, made by adequate probabilistic models, allow to do business with assurance, having scientific justification.

References

[1] Kolowrocki, K. & Soszynska-Budny, J. (2011). *Reliability and Safety of Complex Technical Systems and Processes*. DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited, 405.

[2] Kostogryzov, A., Grigoriev, L., Nistratov, G., Nistratov, A. & Krylov, V. (2013). Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes. *American Journal of Operations Research*, Special Issue, 3, 1A, 217-244. Available from: http://www.scirp.org/journal/ajor/

[3] Kostogryzov, A., Nistratov, A. & Nistratov, G. (2012). Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems. *Proceedings of the 6st International Summer Safety and Reliability Seminar*, Poland, 3, 1, 1-14.

[4] Kostogryzov, A. & Nistratov, G. (2004). Standardization, mathematical modelling, rational management and certification in the field of system and software engineering. Moscow, *Armament. Policy. Conversion*, 395 (*in Russian*)

[5] Kostogryzov, A. I. & Nistratov, G. A. (2005). 100 Mathematical Models of System Processes According International Standards Requirements. *Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models*. Maiority, Italy, University of Solerno, 196-201.

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

[7] Kostogryzov, A., Nistratov, G. & Nistratov, A. (2013). The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. *International Journal of Engineering and Innovative Technology (IJEIT)*, 3, 3, 146-155. www.ijeit.com/archive.php

[8] Kostogryzov, A.I. & Stepanov, P.V. (2008). Innovative management of quality and risks in systems life cycle, Moscow, *Armament. Policy. Conversion*, 404 (*in Russian*)

[9] Nistratov, A. (2013). *The technique of prediction of technogenic risks and its implementation by the use of Internet technology*. The dissertation on a scientific degree PhD. Scientific supervisor – Stepanov P. V., Institute of Informatics Problems of the Russian Academy of Sciences, Moscow, Russia.

[10] Zio, E. (2006). *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific, 222.