THE JOURNAL IS INCLUDED IN THE LIST OF THE LEADING JOURNALS AND EDITIONS OF THE HIGHER ATTESTATION COMMISSION (VAK)

Dependability,
DOI:10.21683
ISSN 1729-2646
e-ISSN 2500-3909

THE JOURNAL PROMOTER:
"Journal "Reliability" Ltd

It is registered in the Russian Ministry of Press, Broadcasting and Mass Communications. Registration certificate ПИ 77-9782, September, 11, 2001.

Official organ of the Russian Academy of Reliability

Publisher of the journal
LLC Journal "Dependability"
Director
Dubrovskaya A.Z.
The address: 109029, Moscow, Str. Nizhegorodskaya, 27, Building 1, office 209
Ltd Journal "Dependability"
www.dependability.ru
Printed by JSC "Regional printing house, Printing place" 432049, Ulyanovsk, Pushkarev str., 27. Circulation: 500 copies.
Printing order
Papers are reviewed. Signed print , Volume , Format 60x90/8, Paper gloss

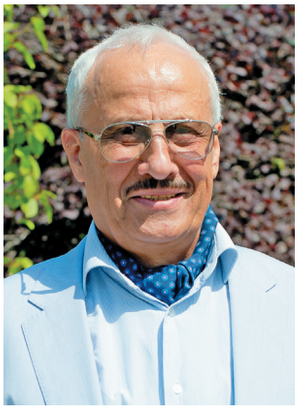
The Journal is published quarterly since 2001.
The price of a single copy is 1045 Rubles, an annual subscription costs 4180 Rubles.
Phone: +7 (495) 967 77 05.
E-mail: dependability@bk.ru.

Papers are reviewed.
Papers are published in author's edition.

THE JOURNAL IS PUBLISHED WITH THE PARTICIPATION AND SUPPORT OF THE JOINT-STOCK COMPANY «RESEARCH AND DESIGN INSTITUTE OF INFORMATISATION, AUTOMATION AND COMMUNICATION ON RAILWAY TRANSPORT» (JSC «NIIAS») AND LLC PUBLISHING HOUSE «TECHNOLOGY»

CONTENTS

Development of the subject matter of the Dependability Journal in 2020



Dear colleagues,

The year 2020 that marks the 70th anniversary of dependability as a science and practicehas begun. Within a relatively short period of time the discipline of dependability became one of the scientific pillars of the development and operation of technical facilities and systems. The first two decades of the development of dependability were marked by an exceptionally high interest in this science by researchers in many countries. The novelty of the problems, the applicable nature, the pressing practical need for solutions, the opportunity to contribute to the new field of knowledge, all of these enabled the establishment of dependability theory.

Progress in the area of dependability enabled the construction of complex multifunctional technical systems. That, in turn, lead to the necessityof solving much more complicated problems of analysis and synthesis of system dependability. For instance, it was required to integrate various forms of redundancy (structural, time, functional, etc.). A strict assessment of the dependability level of complex redundant technical systems through known methods was complicated. Henceis the wide application of methods based on the following two premises:

1. The method is to take into consideration those items or conditions of operation of a technical system that greatly contribute to its dependability. That means that the system's items or conditions of operation (regardless of their number) can be ignored if their contribution to the system dependability is below the value that is acceptable in engineering terms;

2. The method is to be practically applicable in the work of dependability services of enterprises.

An example of implementation of the first premise is the Pareto chart that – as part of a number of practical problems – helped extract relatively small composite groups of the most significant items. Analysis of complex electronic systems often involved assumptions of no consequences and constant failure and recovery rates, which usually did not contradict practical data and allowed using applied mathematics of Markov processes. That mathematics was also applied in dependability management of complex technical systems in operation after the burn-in period and up to wear and ageing.

As the dependability of systems improved, obtaining the required quantities of current statistical data on failures became a problem. Data became incomplete and insufficiently reliable. In this context, the solution to the problems of dependability required the application of the mathematics of fuzzy sets theory, possibility theory, interval averages. That enabled a mathematical integration of all available information on item dependability: statistical data, expert opinions, technological prerequisites, etc. As the result, a sufficiently extensive image of system dependability was created. However, the solutions adopted as part of dependability management raised significant concerns, as the reliability of the initial information and predictions did not always satisfy the system's users. It became natural to manage the dependability of complex systems based on risk assessment: managing investment to enable dependability, managing the useful life of systems, evaluating the criticality of failures, managing the maintenance operation, etc.

The innovative technologies of artificial intelligence significantly extend the boundaries of dependability theory. It is now possible to reliably predict hazardous events and critical failures, reduce the levels of risk, improve the confidence in the made decisions. The methods and models of Data Science enable proactive dependability and safety management of complex technical systems. Hence, to the subject matter of the classical dependability theory, that was defined by the USSR Academy of Sciences member Aksel Berg, it should be added that "under the current conditions, dependability theory is seeking ways of improving dependability based on risk assessment and artificial intelligence".

The topics of the Dependability Journal go hand in hand with the development of the system dependability science and in 2020 will include structural and functional dependability, functional safety, fault tolerance and survivability of systems, standardization and certification, risk management, as well as innovative technologies in dependability and safety. A the same time, the authors are encouraged to review the publications in the respective areas of research, especially foreign ones. This requirement of the Editorial Board is motivated by the rules generally accepted worldwide.

I wish the readers of the Dependability Journal success in their research and practical endeavors, new original findings.

Best regards, Prof. Igor Shubinsky,
Doctor of Engineering Editor-in-Chief

Original article
Dependability, vol. 20 no. 1, 2020 https://doi.org/10.21683/1729-2646-2020-20-1-4-11

Specificity of the development and characteristics of mixed damage to network structures of pipeline transportation systems

Igor A. Tararychkin, *V. Dahl Lugansk National University, Ukraine, Lugansk*
donbass_8888@mail.ru

Igor A. Tararychkin

Abstract. *Pipeline transportation systems are used in various industries for the purpose of delivering various substances and materials to consumers. If, as the result of an accident development, a certain number of random linear elements (pipelines) consecutively fail, such scenario of events is called progressive damage. If several pipelines converging at a node fail simultaneously, such point element of the system is blocked. Progressive blocking of a certain set of nodes of a pipeline system in random order is called a progressive blocking. Simultaneous development within a system of progressive damage to linear elements and blocking of transportation nodes represents mixed damage. Mixed damage is a hazardous form of emergency, and its development causes fast degradation of a system's transportation capabilities. The* **Aim** *of the paper is to study the characteristic properties and patterns of the progress of mixed damage affecting network structures of pipeline systems, as well as evaluating such systems' capability to resist its development.* **Methods of research.** *The characteristics of network entities' resilience to the development of mixed damage were identified by means of computer simulation. The nature of the effects to which a system is exposed was defined with a cyclogram, whose integer parameters indicate the alternation of the process of sequential damage of linear elements and nodes of a network structure.* **Results.** *It has been established that a correct comparison of the resilience of various network structures to mixed damage is only possible with regard to comparable facilities. For that purpose, the analyzed systems must have identical numbers of nodes, linear elements and end product consumers. Additionally, such systems must be exposed to effects with identical cyclograms. It is shown that the correlation of the resilience of comparable network structures does not depend on the specific type of mixed damage cyclogram, but is defined by the nature of the connections within a particular system.* **Conclusions.** *Mixed damage is a hazardous development scenario of an emergency situation that is associated with rapid degradation of the transportation capacity of pipeline systems. The ability of network structures of pipeline systems to resist mixed damage is evaluated based on indicators that are defined by means of simulation. A correct comparison of the resilience of various structures to mixed damage is only possible in case they are comparable. For that purpose, they must have identical numbers of nodes, linear elements and product consumers. Additionally, such systems must be exposed to damage procedures with identical cyclograms. The correlation of the resilience of network structures that comply with the comparability conditions does not depend on the adopted damage cyclogram, but is defined by the existing set of connections within a particular system.*

Keywords: *system, pipeline, structure, mixed damage, resilience.*

For citation: *Tararychkin I.A. Specificity of the development and characteristics of mixed damage to network structures of pipeline transportation systems. Dependability. 2020;1: 4-11. https://doi.org/10.21683/1729-2646-2020-20-1-4-11*

Received on: *22.10.2019 /* **Revised on:** *20.12.2019 /* **For printing:** *20.03.2020*

Pipeline transportation systems are used in various industries for the purpose of delivering various substances, products and materials to consumers [1-4]. Normally, such engineering facilities have complex network structures, a large number of possible states and functional elements [5]. The transition of some structural elements into the down state is of potential hazard, both for the end product consumer, and for the environment [6-9]. If, as the result of processes occurring in the system or the environment, a certain number of random linear elements (pipelines) consecutively fail, such scenario of events is called progressive damage [10].

In case several pipelines converging at a node fail simultaneously, such point element of the system is blocked. It is obvious that a blocked node becomes unable to handle transport streams, while the blocking process can do significant harm to a system's transportation capabilities. Consecutive blocking of system nodes in random order is called progressive blocking [11, 12].

In real operating conditions adverse effects affecting a system may be associated with the simultaneous development of both progressive damage of linear elements, and blocking of transportation nodes. However, the ability of network structures to resist mixed damage that occurs in accordance with the above mechanism is not understood, while in technical literature there is no organized information regarding the dynamics of this process.

The aim of this paper is to study the characteristic properties and patterns of the process of mixed damage affecting network structures of pipeline systems, as well as to evaluate such systems' capability to resist its development.

Let us assume that the process of mixed damage is stationary, i.e. the rates of failure of various structural elements are known (or specified) and do not change over time.

Then, the network entity damage process can be described with an elementary cycle *T*, that repeats many times over the course of an accident until all connections between the source and end product consumers are disrupted. In these circumstances, for each moment of system time we can easily identify the total number of damaged linear elements and blocked transportation nodes.

Thus, if the process dynamics are characterized by the damage to first α linear elements, then blocking of β transportation nodes, the cyclogram of mixed damage process $T(\alpha.\beta)$ provides a complete picture of the effects the analyzed system is affected by.

Thus, characterizing a stationary random process of mixed damage of a network structure using a cyclogram only requires specifying its integer parameters α and β. For instance, if damage occurs by the mechanism of transportation node blocking, such model of action is characterized by cyclogram $T(0.1)$. If the scenario involves progressive damage of linear elements, the above mechanism of system exposure is characterized by cyclogram $T(1.0)$.

The ability of a pipeline system to resist the development of mixed damage was assessed using computer simulation software, similarly to [13, 14].

For the specified network structure and adopted damage cyclogram the following statistical characteristics were specified:

1. Average share of linear system elements φ_{EL}, whose damage causes the disruption of connections between the source and all end product consumers.

2. Average share of transportation nodes φ_{UZ}, whose damage under conditions of mixed damage causes the disruption of connections between the source and all end product consumers.

Paired values φ_{EL} and φ_{UZ} are projections of vector $\vec{\Phi}^*$ on the coordinate axis. The vector characterizes the ability of the analyzed system to resist the development of mixed damage. High values of module $\vec{\Phi}^*$ correspond with high ability of the system to resist the development of such process.

Computer simulation [15-17] of mixed damage was performed using MathCAD [18] according to the following procedure:

1. The initial network structure of a pipeline system is determined by a square incident matrix, similarly to [19, 20].

2. If at a specific moment of system time a linear element is damaged, in the corresponding binary incident matrix all elements in a randomly selected *i*-th line are set to zero. If at the specified moment of system time a transportation node is blocked, all elements in a randomly selected *i*-th line and *i*-th column of the corresponding incident matrix are set to zero.

3. For each moment of system time corresponding reachability matrices are constructed, that are required for the identification of connection between the source node and each of the end product consumers. The network entity damage process ends after all consumers have lost connection with the source node.

4. As the mixed damage process is specified with a cyclogram with known values of parameters α and β, the identification of the moment of system time, when the connection between the source and all product consumers is disrupted, allows identifying the total number of both damaged linear elements, and blocked transportation nodes.

Their respective shares are random values, that were generated as the result of a single system exposure to mixed damage. In order to identify the statistical characteristics of the damage process, the above exposure process must be repeated numerous times in accordance with the adopted cyclogram.

For the purpose of calculation, samples with the size of 10^4 were assigned average values φ_{EL} and φ_{UZ}, as well as the measure of scatter. The adopted sample size allows evaluating the obtained resilience characteristics as having 2 significant decimal figures, which proves to be sufficient for comparing the properties of the network structures examined in this paper [21].

Let us note that a comparison of the resilience to mixed damage is only possible with regard to comparable facilities.

The requirements for comparability of structures are associated with the fulfillment of the following requirements:

1. The network entities must have identical numbers of nodes, linear elements, as well as end product consumers.

2. The compared entities are to be exposed to mixed damage in the same way, i.e. must have the same damage cyclogram.

In this context, let us examine the characteristic features of a set of comparable network structures.

Thus, Figure 1 shows structure diagrams of pipeline systems SMA, …, SMF with a source of the end product *A* and consumers *B*, …, *I* that differ in terms of resilience to mixed damage.

They all include the same number of nodes *R*, edges *Z* and end product consumers *U*. Correct comparison of the resilience characteristics requires creating identical damage conditions.

The specified values φ_{EL} and φ_{UZ} allow estimating if the analyzed systems are able to resist mixed damage. The resilience characteristics obtained for various damage conditions are shown in Figure 2.

A comparison of structures' resilience to mixed damage is only possible along the directions shown with arrows in the graph, as in this case the parameters of the corresponding cyclograms α and β remain unchanged. We can see that from SMA to SMB and to SMF the resilience of the analyzed structures progressively declines regardless of the used damage cyclogram.

That means that for a random set of comparable network structures the correlation between their resilience does not depend on the specific conditions of mixed damage. Therefore, we can argue that any structural variations aimed at improving systems' resilience to mixed damage have a positive effect on its behaviour in the event of accidents regardless of the specific type of implemented cyclogram. Additionally, the data in Figure 2 allow concluding that the blocking of transportation nodes is the most hazardous scenario of network entity failure.

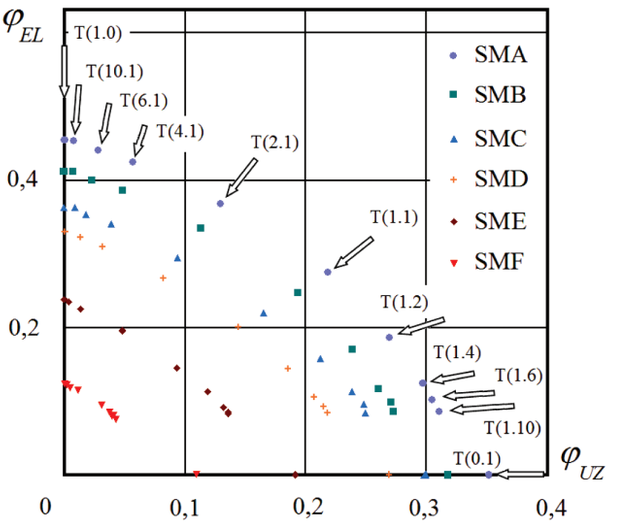


Figure 2 – Values φ_{EL} and φ_{UZ} specified for the sets of structures SMA, …, SMF.

In this context, of interest is the estimation of the variation of values φ_{EL} and φ_{UZ} of the set of comparable network structures with various resilience to mixed damage, for instance, as they change from SMA to SMF.

In order to trace such dynamics, it is required to choose for structure SMA that has the high resilience, such damage cyclogram that complies with condition $\varphi_{EL} = \varphi_{UZ}$. In this

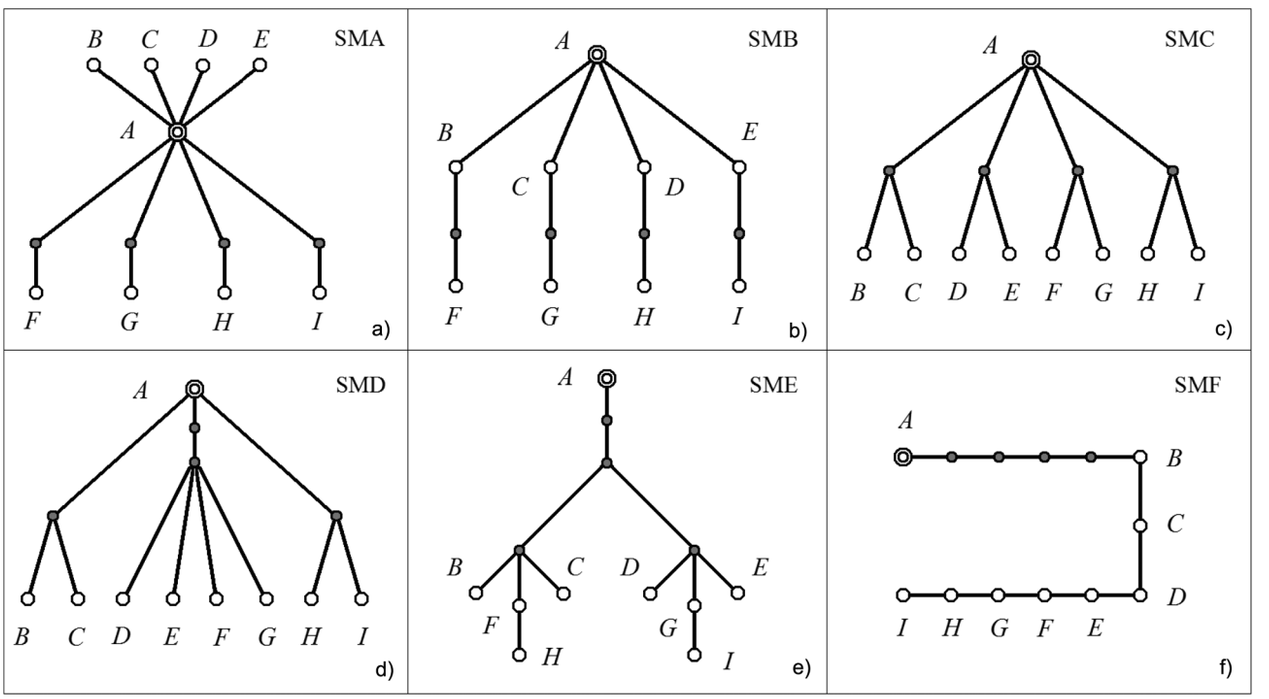


Figure 1 – Structure diagrams of SMA (a), … SMF (f) pipeline transportation systems.

case the deterioration of the systems' resilience characteristics from SMA to SMF will occur from the same starting positions. If that condition is fulfilled, we can clearly see how structural variations reflect on the variation of the contribution of individual components to the final resilience of network structures to mixed damage.

A series of simulation experiments on the SMA structure allowed concluding that near equality $\varphi_{EL} \approx \varphi_{UZ}$ is achieved in case cyclogram $T(3.8)$ is used. The variation of the position of vector $\vec{\Phi}^*$ on a plane under the mixed damage process $T(3.8)$ as regards the set of comparable network structures SMA, …, SMF is shown in Figure 3. The value of the module of vector $\vec{\Phi}^*$ is defined as:

$$\left| \vec{\Phi}^* \right| = \sqrt{\varphi_{EL}^2 + \varphi_{UZ}^2}.$$

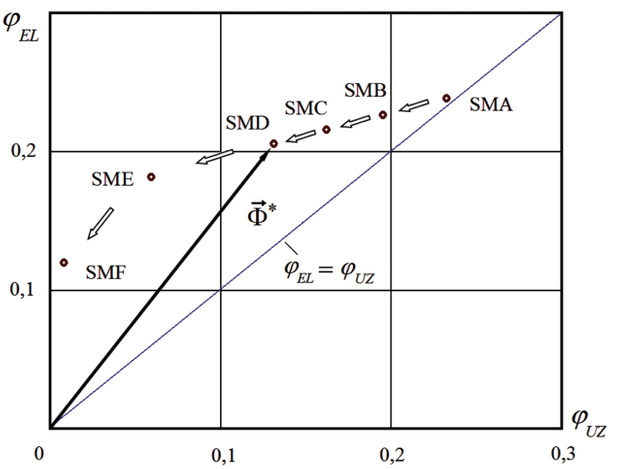


Figure 3 – Mixed damage resilience characteristic of network structures through vector $\vec{\Phi}^*$

The reduction of the values of individual components (axial projections of vector $\vec{\Phi}^*$) φ_{EL} and φ_{UZ} from SMA to less resilient network structures is shown in Figure 4. As for structure SMA, condition $\varphi_{EL} \approx \varphi_{UZ}$ is met, the height of the corresponding columns in the diagram is about the same.

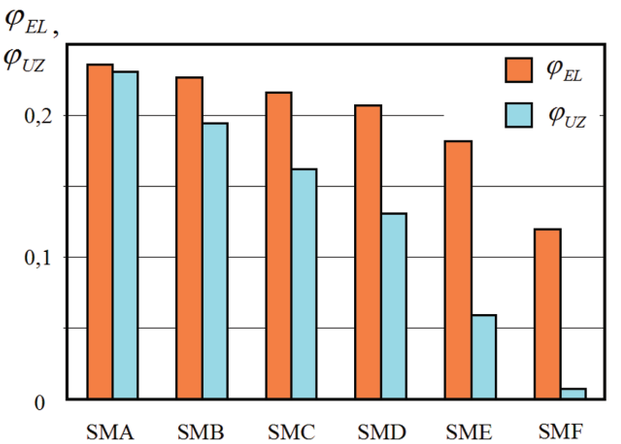


Figure 4 – Diagrams of values φ_{EL} and φ_{UZ} variation from SMA to SMF.

Additionally, it can be seen that in case of progressive transition from SMA to less resilient network structures, a relatively slow decline of value φ_{EL} can be observed. At the same time, the decline of values φ_{UZ} happens rapidly, which largely defines the observed effect of resilience deterioration.

Thus, the obtained result allows concluding that ensuring system resilience to mixed damage should be primarily based on measures aimed at improving their resilience to progressive blocking of transportation nodes.

Let us also note the following detail that was identified based on the analysis of data of Figure 2. If the mixed damage of a set of network structures proves to be similar to the process of progressive blocking of transportation nodes ($\beta >> \alpha$) or the process of linear elements failure ($\alpha >> \beta$), the respective points of the graph are placed too close to each other, which complicates the assessment of the obtained result.

For that reason, the identification of a system's ability to resist mixed damage is to be done using a test load with a cyclogram of type $T(1.1)$. Such exposure is a sequence of random damage to linear and point elements of a system and, in this sense, is balanced. Then, the resilience of comparable network structures should be compared subject to damage conditions according to cyclogram $T(1.1)$.

Let us assume that it is required to estimate the ability to resist the development of mixed damage of pipeline systems, whose structure diagrams are shown in Fig. 5. The above systems are defined by the presence of source A, identical number of transportation nodes, linear elements, as well as end product consumers (B, …, G). Let us evaluate their resilience for various conditions of mixed damage.

The results of conducted calculations are shown in Figure 6 and allow concluding that resilience to damage progressively declines in the course of transition from the system designated SUA to the system SUB and further from SUC to SUD.

Additionally, on plane we can define conventional boundaries of areas with different mechanisms of network structure damage. Thus, for range of Ω_E values φ_{EL} and φ_{UZ}, damage primarily occurs due to the failure of linear elements, while in area Ω_U mostly transportation nodes get blocked.

If for cyclogram $T(\alpha.\beta)$ condition $\alpha >> \beta$ is fulfilled, such nature of exposure of a network entity is associated with primarily linear element damage. Then, the comparability requirements can be somewhat reduced and we can consider as such systems with matching total numbers of linear elements and end product consumers only. If the above systems are exposed to damage with identical cyclogram, the expected values φ_{EL} should be used as criteria that allow estimating their resilience to mixed damage.

If the cyclogram features the parameter correlation $\beta >> \alpha$, such exposure is associated with the damage to primarily transportation nodes.

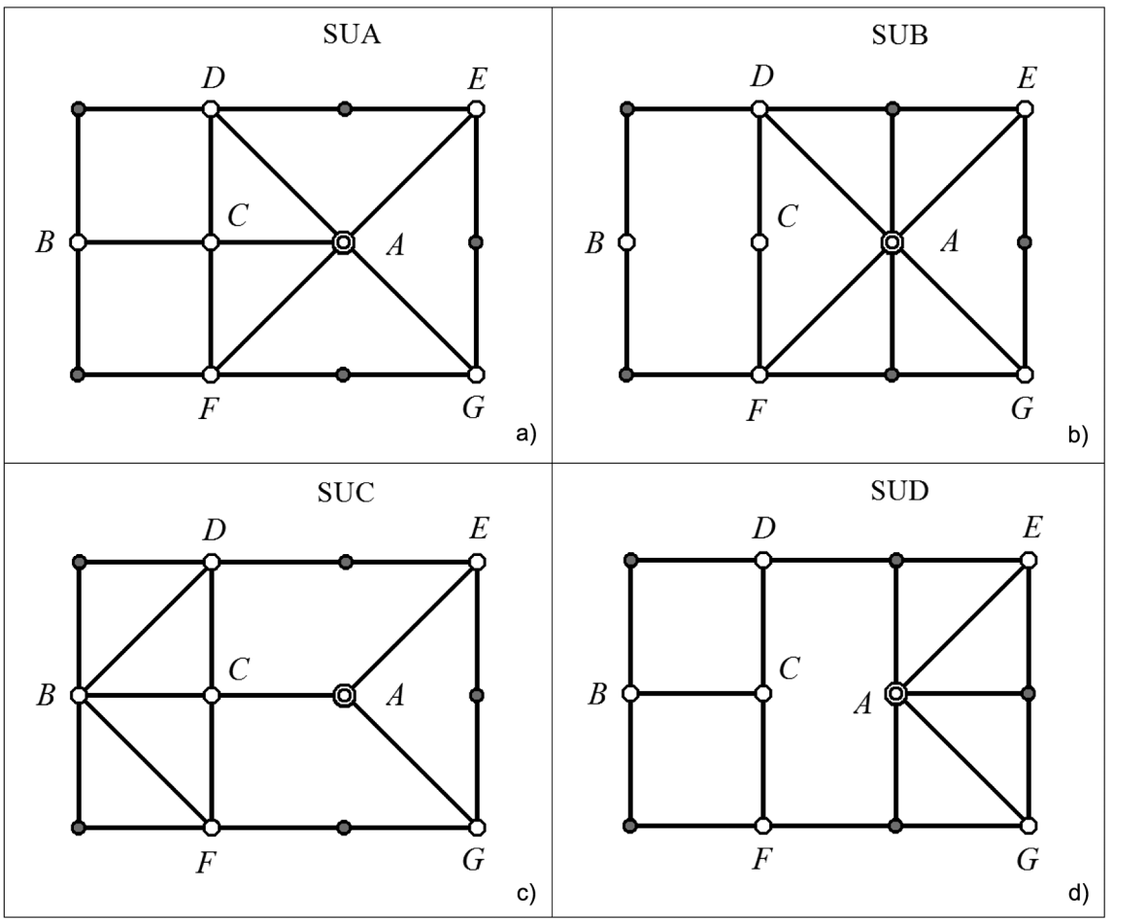


Figure 5 – Structure diagrams of SUA (a), … SUD (d) pipeline transportation systems.

Under such conditions systems with identical numbers of nodes and end product consumers will be comparable.

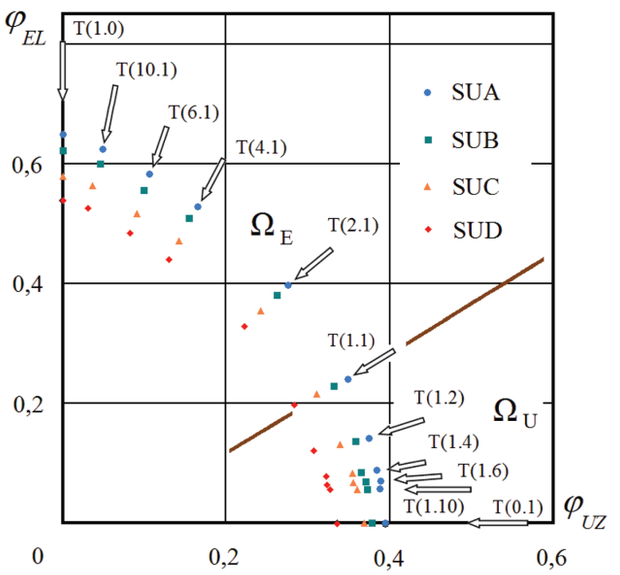


Figure 6 – Resilience characteristics specified for network structures SUA, …, SUD.

If such items are exposed to damage with identical cyclogram, the expected values φ_{UZ} are criteria that characterize their resilience to mixed damage.

Thus, the elimination of some limitations with regard to the identification of comparability of network entities for specific conditions of mixed damage enables analysis and solution of a wider range of applied problems.

Let us assume that it is required to evaluate the resilience and adopt a design solution regarding the practical application of one of the alternative network structures shown in Figure 7 subject to the threat of mixed damage.

All those facilities have identical numbers of nodes, linear elements and end product consumers (B, …, G). In case of mixed damage to the above structures with cyclogram $T(1.1)$ the comparison of values $|\vec{\Phi}^*|$ allows comparing the correlation of their resilience. This feature should be used for substantiation and adoption of design solutions.

Thus, Table 1 shows corresponding expected values that allow concluding that in case of mixed damage (regardless of the specific exposure conditions) the most resilient is the structure designated SFB that is to be regarded as the solution to the original problem.

The SFA and SFC network structures have about the same resilience, as their values of vector module $\vec{\Phi}^*$ are almost identical.

Let us now assume that the chosen SFB network structure is potentially exposed to external effects causing damage to primarily transportation nodes. Let us evaluate the feasibility of improving its resilience through structural modifications

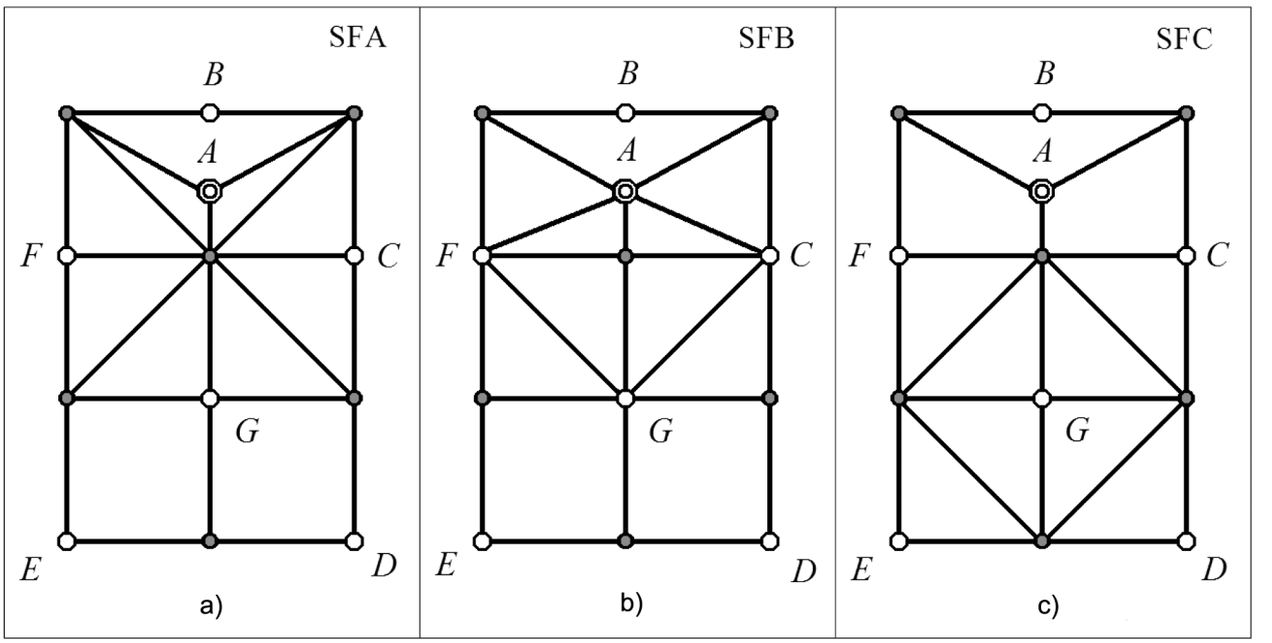


Figure 7 – Structure diagrams of SFA (a), … SFC (c) pipeline transportation systems.

Table 1. Resilience characteristics of comparable network structures for the adopted conditions of mixed damage

Designation of structure	Designation of mixed damage cyclogram	Estimated characteristics of resilience		
		φ_{EL}	φ_{UZ}	$\left\vert \vec{\Phi}^{*} \right\vert$
SFA	T(1.1)	0.168	0.288	0.333
SFB		0.187	0.323	0.373
SFC		0.167	0.286	0.331

and use of additional linear elements. Such derived structure designated SFW is shown in Fig. 8 (a).

The resilience characteristics of the SFB and SFW systems for the adopted damage conditions can be compared, as they have the same total number of nodes and end product consumers. Let us apply a mixed damage procedure – for instance, with cyclogram T(1.3) – to the above systems. Values specified subject to the results of simulation are shown in Table 2.

As we can see, the inclusion into the SFB system of additional pipelines enables higher resilience, when damage affects predominantly point elements.

If, in the process of operation, the SFB system is exposed to damage to predominantly linear elements, we would be interested in finding a solution that would have a positive effect on its resilience to the above effects.

Let us reduce the number of nodes in the SFB system to $R = 11$, while preserving the total number of linear elements ($Z = 23$) and product consumers ($U = 6$). The structure of such pipeline system designated SFX is shown in Fig. 8 (b). The resilience of the SFB and SFX systems can be compared after the definition of the corresponding values for the specified damage conditions of predominantly linear elements. Thus, the values for each of the analyzed network structures damaged in accordance with the adopted cyclogram T(3.1) obtained as the result of simulation, are shown in Table 2. It can be seen that the structural changes implemented in the SFX diagram have a positive effect on the system's resilience and are recommended for practical application.

Thus, when estimating the mixed damage resilience of a set of comparable network structures one must specify corresponding values $\left\vert \vec{\Phi}^{*} \right\vert$ in the test input conditions structure with characteristics $\alpha = \beta = 1$. Then the adjustment of the systems under consideration in terms of their resilience to mixed damage is to take into consideration the fact that more resilient systems have higher values of $\left\vert \vec{\Phi}^{*} \right\vert$. This criterion must be used as part of design solutions.

However, in some cases the specificity of the damaging effects allows slightly reducing the specified requirements

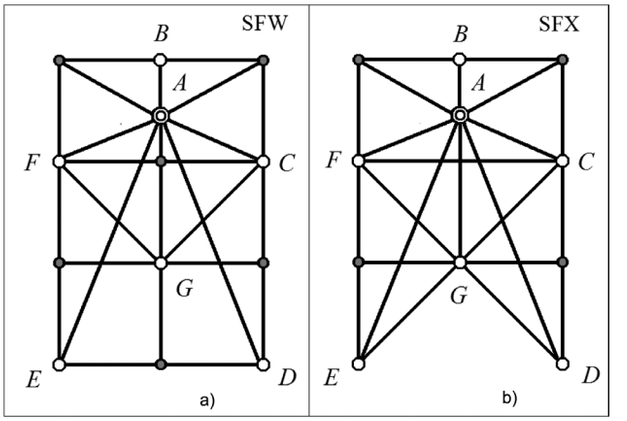


Figure 8 – Structure diagrams of systems resulting from the inclusion into SFB of additional linear elements (a) and exclusion of nodes (b).

Table 2. Estimated characteristics of network structures resilience

Designation of structure	Composition of structural elements	Designation of damage cyclogram	Resilience characteristics	
			φ_{UZ}	φ_{EL}
SFB	*R*=13, *Z*=23, *U*=6	*T*(1.3)	0.349	-
		T(3.1)	-	0.413
SFW	*R*=13, *Z*=26, *U*=6	*T*(1.3)	0.391	-
SFX	*R*=11, *Z*=23, *U*=6	*T*(3.1)	-	0.454

Table 3. Conditions of comparability and evaluation criteria network structures resilience

Specificity of damage	Cyclogram parameter	Conditions of comparability of network structures	Evaluation criteria of system resilience
Balanced damage to structural elements	$\alpha = \beta = 1$	Identical numbers of linear elements, nodes and product consumers	$\left\vert \vec{\Phi}^{*} \right\vert = \sqrt{\varphi_{EL}^2 + \varphi_{UZ}^2}$
Predominant damage to linear elements	$\alpha >> \beta$	Identical numbers of linear elements and product consumers	$0 < \varphi_{EL} < 1$
Predominant blocking of transportation nodes	$\beta >> \alpha$	Identical numbers of nodes and product consumers	$0 < \varphi_{UZ} < 1$

and thus extending the options of comparative estimation of the properties of the analyzed systems.

Thus, Table 3 shows recommendations regarding the conditions of comparability and selection of criteria of systems resilience evaluation for various procedures of mixed damage. Their practical value is associated with the feasibility of a wider use of the identified patterns and theoretical findings.

Conclusions

1. Mixed damage is a hazardous development scenario of an emergency situation that is associated with rapid degradation of the transportation capacity of pipeline systems.

2. The ability of network structures of pipeline systems to resist mixed damage is evaluated based on φ_{EL}, φ_{UZ} and $\left\vert \vec{\Phi}^{*} \right\vert$, that are defined by means of simulation.

3. A correct comparison of the resilience of various structures to mixed damage is only possible in case they are comparable. For that purpose, they must have identical numbers of nodes, linear elements and product consumers. Additionally, such systems must be exposed to damage procedures with identical cyclograms.

4. The correlation of the resilience of network structures that comply with the comparability conditions, does not depend on the adopted damage cyclogram, but is defined by the existing set of connections within a particular system.

References

[1] Barker G. The Engineer's Guide to Plant Layout and Piping Design for the Oil and Gas Industries. Gulf Professional Publishing; 2018.

[2] Bahadori A. Hazardous Area Classification in Petroleum and Chemical Plants. A Guide to Mitigating Risk. CRC Press; 2017.

[3] Toghraei M. Piping and Instrumentation Diagram Development. John Wiley & Sons, Inc; 2019.

[4] Wilson B. Detail Engineering and Layout of Piping Systems. Titles on Demand; 2015.

[5] Bochkov A.V., Ponomarenko D.V. [Methodological foundations of monitoring and prediction of process safety in PAO Gazprom]. *Gas Industry Magazine*. 2017;3(749):20-30. (in Russ.)

[6] Flammini F., editor. Critical Infrastructure Security. Assessment, Prevention, Detection, Response. WIT Press, UK; 2012.

[7] Riabinin I.A. [Dependability and safety of structurally complex systems]. Saint Petersburg: Politekhnika; 2000. (in Russ.)

[8] Ivantsov O.M., Mazur I.I. [Safety of pipeline systems]. Moscow: Yelima; 2004. (in Russ.)

[9] Bochkov A.V. [Problems of hazard estimation and risk management of critical infrastructure facilities of the Gazprom Group: an analytical review]. *Vesti gazovoy Nauki*. 2018;2(34):51-87. (in Russ.)

[10] Tararychkin I.A. Ensuring resilience of pipeline transportation systems to damage to network structure elements. *Dependability.* 2018;18(1):26-31.

[11] Tararychkin I.A. [Strategies to protect pipeline transportation facilities to structural damage in emergency situations]. *Bezopasnost truda v promyshlennosti*. 2018;2:52-57. (in Russ).

[12] Tararychkin I.A. [Description and comparative analysis of the strategies of protection of pipeline systems from damage to transportation nodes]. *Gas Industry Magazine*. 2019;2:72-77. (in Russ)

[13] Tararychkin I.A. Computer simulation of development of accidents and damage to the structural elements of pipeline transport systems. *Oil and Gas Technologies*. 2019;2: 53-59. (in Russ.)

[14] Tararychkin I.A., Blinov S.P. [Simulation of the process of damage to pipeline network structures]. *World of Transport and Transportation*. 2017;15(2):6-19. (in Russ.)

[15] Zarubin V.S., Krishchenko A.P., editors. [Mathematic simulation in engineering]. Textbook for higher education. 2nd edition. Moscow: Bauman MSTU Publishing; 2003. (in Russ)

[16] Kupriashkin A.G. [Introduction into system simulation: Textbook]. Norilsk: Norilsk Industrial Institute Publishing; 2015. (in Russ.)

[17] Strogaliov V.P., Tolkachiova I.O. [Simulation]. Textbook. Moscow: Bauman MSTU Publishing; 2008. (in Russ.)

[18] Okhorzin V.A. [Computer simulation in Mathcad]. Moscow: Finansy i statistica; 2006. (in Russ.)

[19] Tararychkin I.A., Blinov S.P. [Simulation of the process of progressive damage to pipeline transportation systems with protected linear elements]. *Problemy sbora, podgotovki i transporta nefti i nefteproduktov*. 2018;1(111):75-85. (in Russ.)

[20] Tararychkin I.A., Blinov S.P. [The distinctive features of damage to network structures and development of accidents in pipeline transportation facilities]. *Bezopasnost truda v promyshlennosti*. 2018;3:35-39 [in Russian].

[21] Hudson D. [Statistics for physicists. Lectures on elementary statistics and probability]. Moscow: Mir; 1970. (in Russ.)

About the author

Igor A. Tararychkin, Doctor of Engineering, Professor, V. Dahl Lugansk National University, Ukraine, Lugansk, e-mail: donbass_8888@mail.ru.

The author's contribution

The author has analyzed the resilience of pipeline transportation systems affected by developing process of mixed damage to structural elements. The statistical characteristics of the process and conditions of comparability of systems in case of accidental damage to linear and point elements were defined.

Computer simulation of the process of mixed damage was conducted. The characteristics that enable the assessment of individual systems to resist the development of this process were identified. A method was proposed of comparative estimation of the resilience of comparable network structures affected by possible accident development by the mechanism of mixed damage.

Original article
Dependability, vol. 20 no. 1, 2020 https://doi.org/10.21683/1729-2646-2020-20-1-12-19

Plan of tests with addition. Efficient estimate of dependability indicators

Viktor S. Mikhailov, *D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow*
Mvs1956@list.ru

Viktor S. Mikhailov

Abstract. *The* **Aim** *of the paper consists in improving the efficiency of dependability indicator estimation for the plan of tests with addition, i.e. probability of no-failure and mean time to failure. Due to economic considerations, determinative dependability tests of highly dependable and costly products involve minimal numbers of products, expecting failure-free testing or testing with one failure, thus minimizing the number of tested products. The latter case is most interesting. By selecting specific values of the acceptance number Q and number of tested products, the tester performs a preliminary estimation of the dependability indicator, while selecting Q = 1 the tester minimizes the risks caused by an unlikely random failure. However, as the value Q grows, the number of tested products does so as well, which makes the testing costly. Therefore, the reduction of the number of products tested for dependability is the first-priory problem and, in this context, economic planning of testing with addition is becoming increasingly important. We will consider binomial tests (original sample) with addition of one product (oversampling) to testing in case of failure of any of the initially submitted products. Testing ends when all submitted products have been tested with any outcome (original sampling and oversampling). Hereinafter it is understood that the testing time is identical for all products. Testing with the acceptance number of failures greater than zero (Q > 0) conducted with addition allows reducing the number of tested products through successful testing of the original sample.* **Methods.** *Efficient estimation is based on the integral approach formulated in many papers. The integral approach is based on the formulation of the rule of efficient estimate selection* $\hat{\theta}_0(\tau;n;k,m)$ *specified on the vertical sum of absolute (or relative) biases of estimates* $\hat{\theta}(n;k,m)$ *selected out of a certain set based on the distribution law parameter, where n is the number of products initially submitted to testing. The criterion of selection of an efficient estimate of the probability of failure (or PNF) at a set of estimates* $\hat{\theta}(\tau;n;k,m)$ *is based on the total square of absolute (or relative) biases of the mathematical expectation of estimates* $E\hat{\theta}(\tau;n;k,m)$ *from probability of failure p for all possible values of p, n.* **Conclusions.** *The paper examines the probability of no-failure estimates for the plan of tests with addition. For the case of n > 3, the estimates* $\hat{P}=1-\hat{p}=1-\frac{r}{n+k}$ *and composite estimate* $1-\overline{p}(\tilde{v}(\beta=0,5))$ *are more efficient in comparison with estimate* $1-\tilde{v}(\beta=0,5)$*. The composite estimate of the probability of no-failure* $1-\overline{p}(\tilde{v}(\beta=0,5))$ *should be used in failure-free tests. For the case of n > 3, testing with the acceptance number of failures greater than zero (Q > 0) conducted with addition allows reducing the number of tested products through successful testing of the original sample. The composite estimate of the mean time to failure* $\hat{T}_1=\frac{\tau}{-\ln(1-\overline{p}(k,m,n,\beta=0,6))}$ *is bias-efficient among the proposed mean time to failure estimates. The obtained composite estimates* $\overline{p}$ *and* $\hat{T}_1$ *are of practical significance in the context of failure-free testing with addition***.**

Keywords*: Bernoulli scheme, test plan, point estimate, probability of no-failure, efficient estimate, mean time to failure.*

For citation: *Mikhailov V.S. Plan of tests with addition. Efficient estimate of dependability indicators. Dependability. 2020;1: 12-19. https://doi.org/10.21683/1729-2646-2020-20-1-12-19*

Received on: *09.09.2019 /* **Revised on:** *14.12.2020 /* **For printing:** *20.03.2020*

Introduction

Due to economic reasons, determinative dependability tests of highly dependable, costly products involve minimal numbers of products, expecting failure-free testing (acceptance number $Q = 0$) or testing with one failure ($Q = 1$), thus minimizing the number of tested products. The latter case is most interesting. By selecting specific values of the acceptance number Q and number of tested products, the tester performs a preliminary estimation of the dependability indicator, while selecting $Q = 1$ the tester minimizes the risks caused by an unlikely random failure. However, as the value Q grows, the number of tested products does so as well, which makes the testing costly. Therefore, the reduction of the number of products tested for dependability is the first-priory problem and, in this context, economic planning of testing with addition is becoming increasingly important [1].

Preparation of the plan of tests with addition

We will consider binomial tests (original sample) [1, 2] with addition of one product (oversampling) to testing in case of failure of any of the initially submitted products. Testing ends when all submitted products have been tested with any outcome (original sampling and oversampling). Hereinafter it is understood that the testing time is identical for all products.

Testing with the acceptance number of failures greater than zero ($Q > 0$) conducted with addition allows reducing the number of tested products through successful testing of the original sample.

The Aim of the paper

The aim of the paper consists in improving the efficiency of dependability indicator estimation for the plan of tests with addition, i.e. probability of no-failure (PNF) and mean time to failure (MTF).

Properties of probability of no-failure estimates for a plan of tests with addition

Let n be the number of tested same-type products initially submitted to testing, while $R=r$ is the number of failed products, including k failures out of n initially submitted products and m failures out of k subsequently submitted products, i.e. $r=k+m$. Then, the number of tested products will be $N=n+k$. For the sake of convenient formula writing, in some cases (where possible), the designations of random values will be identical to their representations. Let failures be independent events, then the probability of occurrence is equal to r failures over the testing period (hereinafter referred to as $P_n(R=r)$) will be expressed with the formula that results from the following procedure ($n \geq k \geq m; r = k + m \leq 2n$):

$$P_k(m) := C_k^m p^m q^{k-m};$$

$$P_n(k) := C_n^k p^k q^{n-k} \sum_{m=0}^{k} P_k(m) = C_n^k p^k q^{n-k},$$

where $q=1-p$, p is the probability of failure, C_n^k is the number of combinations k out of n elements.

$$P_n(k,m) := P_n(k) P_k(m) = C_n^k C_k^m p^{k+m} q^{n-m},$$

$$P_n(R=r) = \sum_{k=0}^{n} \sum_{m:m+k=r,\, m \leq k} P_n(k,m),$$

$$r = k + m = 0,1,2,\ldots,2n;\ k = 0,1,2,\ldots,n;$$
$$m : m + k = r, m \leq k.$$

Out of the definition of probability $P_n(k = x, m = y) = P_n(k = x) P_n(m = y)$, where $x, y = 0,1,2,\ldots,n$ and $P_n(R=r)$ we can easily obtain the probabilistic function of the plan of tests with addition:

$$P_{n\sum}(k \leq x, m \leq y) = \sum_{k=0}^{x} \sum_{m:m+k \leq x+y,\, m \leq k,\, m \leq y} P_n(k,m). \quad (1)$$

The average number of tested products over the period of testing with addition comprises the number of initially submitted products and the average number of those initially submitted products that failed, i.e. $N=n+np$. Then, the average number over the period of testing with addition will be $E(R,n)=Np=E(k,n)+E(m,n)=np+np*p=(n+np)p=n(p+p^2)$.

The PNF estimate $\hat{p} = \frac{r}{n+k}$ is efficient for a plan of tests with addition [1]. Let us examine the properties of the obtained estimate $\hat{p} = \frac{r}{n+k}$ and, as a consequence, PNF estimate $\hat{P} = 1 - \hat{p} = 1 - \frac{r}{n+k} = \frac{n-m}{n+k}$ [1].

Let $k+m=r>1$, $\hat{p} = \frac{r}{n+k} = \frac{r}{n+r-m}$, then for various $m_1 > m_2$ the following inequality is fulfilled

$$\hat{p}(k_1 + m_1 = r; k_1, m_1) = \frac{r}{n+r-m_1} >$$

$$> \hat{p}(k_2 + m_2 = r; k_2, m_2) = \frac{r}{n+r-m_2}. \quad (2)$$

I.e. the dependability of the controlled batch of products subject to the results of testing of a sample, in which the number of failed products out of the initially submitted is higher, than in the sample of the compared batch of products under the same number of failures, will always be higher, than that of the compared batch of products. In other words, while comparing the results of two finalized samples (under the assumption of identical numbers of failures), the priority in terms of dependability is given to those products, whose failures primarily occurred within the initial sample, rather

than the additional one. And in this regard oversampling enables remedial action in case of unsuccessful initial testing. That constitutes the advantage of the test plan with addition.

Unbiassed estimates

The mathematical expectation of the estimate $\hat{p}(n;k,m)=\frac{r}{n+k}$ will be expressed with formula [1]:

$$E\left(\hat{p}\left(n;k,m\right)\right)=\sum_{r=0}^{2*n}\frac{r}{n+k}P_n(r).$$

Estimate $\hat{p}(n;k,m)=\frac{r}{n+k}$, is generally biased $E\left(\hat{p}\left(n;k,m\right)\right)\neq p$ [1].

By equating mathematical expectation of the estimate $\hat{p}(n=1)$ to parameter p we can easily obtain the unbiassed estimate of the probability of failure $\hat{p}_1$ for the case of n=1 [1]:

$$\hat{p}_1=\begin{cases}0, r=0\\ 1, r>0\end{cases}=\begin{cases}0,\ r=0,k=0,m=0;\\ 1,\ r=1,k=1,m=0;\\ 1,\ r=2,k=1,m=1.\end{cases}$$

An unbiassed estimate is an indicator function, i.e. in case of failures estimate $\hat{p}_1$ becomes equal to one, otherwise to zero. The case of $n = 1$ is practically uninteresting as it is the same as the binomial plan and thus is not further considered in this paper.

The mathematical expectation of the estimate $\hat{p}(n=2)=\frac{r}{2+k}$:

$$n=2:E\left(\hat{p}\right)=\sum_{r=0}^{4}\hat{p}(r)P\left(n=2,R=r\right).$$

The unbiassed estimate for parameter p in case $n = 2$ will be expressed with formula [1]:

$$\hat{p}_2(k,m)\equiv\begin{cases}p_{00}=0, r=0,k=0,m=0;\\ p_{10}=1/2, r=1,k=1,m=0;\\ p_{11}=5/8, r=2,k=1,m=1;\\ p_{20}=6/8, r=2,k=2,m=0;\\ p_{21}=7/8, r=3,k=2,m=1;\\ p_{22}=1, r=4,k=2,m=2.\end{cases}$$

This estimate is not the only one. The second variant of parameter p estimation for the case of $n = 2$ [1]:

$$\hat{w}_2\left(r\right):\hat{w}_2\left(0\right)=0;\ \hat{w}_2(1)=\frac{1}{2};$$

$$\hat{w}_2(2)=\frac{2}{3};\ \hat{w}_2(3)=\frac{5}{6};\ \hat{w}_2(4)=1.$$

The unbiassed estimate of the probability of failure for the case of n=3 ($\hat{w}_3(r)$) [1]:

$$\hat{w}_3\left(r\right):\hat{w}_3\left(0\right)=0;\ \hat{w}_3\left(1\right)=\frac{1}{3};\ \hat{w}_3\left(2\right)=\frac{1}{2};\ \hat{w}_3\left(3\right)=\frac{9}{14};$$

$$\hat{w}_3\left(4\right)=\frac{65}{84};\ \hat{w}_3\left(5\right)=\frac{75}{84};\ \hat{w}_3\left(6\right)=1.$$

Estimates $\hat{p}$, $\hat{p}_2$, $\hat{w}_2\left(r\right)$, $\hat{w}_3\left(r\right)$ become useless, when it is required to estimate the unknown parameter p not equal to zero and one.

Let us introduce the concept of centered estimate [1, 7] (not to be confused with the central estimate [4]), namely: let the probability of failure estimate (hereinafter referred to as $\hat{v}$) center the probability function (in our case that is $P_{n\sum}(x,y)$ relative to the limit boundaries of its value range). That means that the ranges $[0;\hat{v}]$ and $[\hat{v};1]$ of the values of such estimates with the probability of 0.5 cover the estimated parameter p. Such estimates we will call centered. Let us note that centered estimates for some test plans are close to efficient estimates [7]. In our case the centered estimate $\hat{v}(\beta=0,5)$ is found using formula $P_{n\sum}\left(x,y\right)=\beta=0,5$, where β does not possess confidence probability any more. Let us also note that the distribution law of statistic $\hat{v}$ is defined by the distribution law of random value R, which allows identifying the confidence boundaries.

Out of the definition of centered estimate follows that it defines the lower (upper) confidence limits (hereinafter referred to as LCL (UCL) of the range of unknown parameter p with confidence probability γ = 0.5 or significance level α = 0.5. On the other hand, any estimate of the LCL (UCL) of an unknown parameter range p can be interpreted as a point estimate of parameter p with a strong downward (upward) bias. The LCL (hereinafter referred to as $\hat{p}_L$) (UCL (hereinafter referred to as $\hat{p}_U$) of the range of unknown parameter p with confidence probability γ = 1 – α is calculated according to formula (the case of monotonous decrease [1]):

$$P_{n\sum}\left(x,y,\hat{p}_L\right)=\gamma,\ P_{n\sum}\left(x,y,\hat{p}_U\right)=\alpha. \qquad (3)$$

Let us note that centered estimates are – in terms of their efficiency – close to the best estimates [7-9], and despite the optimistic definition of the centered estimate $\hat{v}(\beta=0,5)$ this estimate is biased with respect to the estimated parameter $L\left(\hat{v}(n;r;\beta=0,5)\right)>0$. However, this bias can be reduced, thus improving the efficiency [9]. For that purpose, it will suffice to minimize functional $L\left(\tilde{v}(n;r)\right)$ by varying the probability value β=0,5+x in formula $P_{n\sum}=0,5+x$, where x>0 is a positive real number. Thus obtained estimate (hereinafter referred to as $\tilde{v}(\beta=0,5+x)$) is already not centered, but its bias is smaller compared to that of the centered estimate $\hat{v}(\beta=0,5)$, and therefore estimate $\tilde{v}(\beta=0,5+x)$ can be expected to have higher efficiency.

Let us note that function $P_{n\sum}$ monotonously decreases as p grows (proven for cases of n<3) [1], therefore equation

$$P_{n\sum} = \beta = 0,5 + x$$

has a unique solution. Let us once again note that probability β does not imply confidence probability and cannot organize a two-sided confidence interval, as its boundaries "overlap" in opposing directions. Probability β is an indicator parameter that discriminates an estimate out of a set of similar ones in terms of the method of construction β≥0,5.

Additionally, the confidence boundary (β≤0,5) represents a point estimate with a strong bias in relation to the estimated parameter. As the confidence probability β>0 grows, the two-sided confidence interval degenerates first into a point, then stops existing. The one-sided confidence interval stops being such as confidence probability β>0,5 grows, as, with high probability β>0,5, will not cover the estimated parameter. The set of estimates with indicator parameter $\tilde{v}(\beta = 0,5 + x)$ becomes a potential carrier of the efficient estimate.

Let us formulate the selection criterion of the efficient estimate of probability of failure (or PNF), construct – on the basis of the formulated criterion – an improved (but biased) failure probability estimation (and therefore, PNF estimation) for a plan of testing with addition for the case of $n > 3$ and choose the efficient estimate out of those available.

Methods of research of dependability indicator estimates

Efficient estimation is based on the integral approach formulated in [6-11]. The integral approach is based on the formulation of the rule of efficient estimate selection $\hat{\theta}_0(n;k,m)$ specified on the vertical sum of absolute (or relative) biases of estimates $\hat{\theta}_0(n;k,m)$ selected out of a certain set based on the distribution law parameter, where n is the number of products initially submitted to testing.

Criterion of selection of efficient estimation for PNF

The criterion of selection of an efficient estimate of the probability of failure (or PNF) at a set of estimates $\hat{\theta}_0(n;k,m)$ is based on the total square of absolute (or relative) biases of the mathematical expectation of estimates $E\hat{\theta}(n;k,m)$ from probability of failure p for all possible values of p, n.

Let τ be the test time of one product, then the selection of the efficient estimate of the probability of failure (or PNF) will only require the notion of bias-efficient estimate and variation of parameter p within $0 \le p \le 1$. Therefore, for the sake of simplicity, as the criterion for obtaining an efficient estimate $\hat{\theta}_0(n;k,m)$ functional (hereinafter referred to as $L(\hat{\theta}(n;k,m))$) is constructed over limited set $1 \le n \le I$ [7-9]:

$$L\left(\hat{\theta}(n;k,m)\right) = \frac{1}{I}\sum_{n=1}^{I}\int_0^1 \left\{E\hat{\theta}(n;k,m) - p\right\}^2 \partial p. \qquad (4)$$

Estimate $\hat{\theta}_0(n;k,m)$, that minimizes functional $L(\hat{\theta}(n;k,m))$ over the given set of estimates, is called the bias-efficient estimate over the given set of biased estimates. Among the estimates, that afford about the same minimum to functional $L(\hat{\theta}(n;k,m))$, we should choose the estimate that has the minimal mean-square deviation (classical definition of the efficient unbiassed estimate [2]). We will call this estimate more efficient in comparison with the selected ones.

For the purpose of selecting the estimates with minimal deviation, a functional is constructed (hereinafter referred to as $D(\hat{\theta}_0(n;k,m))$ based on the accumulation of mathematical expectations of the squares of relative deviations of estimates $\hat{\theta}_0(n;k,m)$ from parameter p for all possible values p, n [7-9]:

$$D\left(\hat{\theta}(n;k,m)\right) = \frac{1}{I}\sum_{n=1}^{I}\int_0^1 E\left\{\hat{\theta}(n;k,m) - p\right\}^2 \partial p. \qquad (5)$$

We will call estimate that affords zero to functional $L(\hat{\theta}_0(n;k,m))=0$ (unbiassed estimate) and minimum to functional $D(\hat{\theta}_0(n;k,m))$ absolutely bias-efficient.

Let us limit the scope of tests $4 \le n \le 10$, which, for highly dependable and complex products is the cost limit. Then formula (4) will be written as:

$$L\left(\hat{\theta}(n;k,m)\right) = \frac{1}{7}\sum_{n=4}^{10}\int_0^1 \left\{E\hat{\theta}(n;k,m) - p\right\}^2 \partial p.$$

While formula (5) will be written as:

$$D\left(\hat{\theta}(n;k,m)\right) = \frac{1}{7}\sum_{n=4}^{10}\int_0^1 E\left\{\hat{\theta}(n;k,m) - p\right\}^2 \partial p.$$

The performed calculations showed that estimate $\hat{v}(\beta = 0,5 + x)$, that minimizes functionals $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$, corresponds with β=0,5+x=0,5, i.e. $x = 0$ and subsequently $\hat{v}(\beta = 0,5) = \tilde{v}(\beta = 0,5 + x)$.

Table 1 shows the results of substitution into functionals $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$, in accordance with formulas (1) and (2), of the following probability of failure estimates $\hat{\theta}$: $\tilde{v}, \hat{p}, \overline{p}$ [1], where

$$\overline{p} = \begin{cases} \tilde{v}\left(0, n, \beta = 0,5\right), r = 0; \\ \dfrac{r}{n+k},\ r > 0. \end{cases}$$

Functionals $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$ were calculated with the step of $\partial p = 10^{-3}$. Implicit estimates $\tilde{v}$ and $\overline{p}$ were calculated with the accuracy of 10^{-4}. The scope of tests was limited with the range of $4 \le n \le 10$.

Out of Table 1 follows that under the scope of tests $4 \le n \le 10$ estimate $\hat{p}$ and composite estimates dominate and acquire minimal biases.

Out of Table 1 also follows that estimate $\hat{p}$ and composite estimates $\overline{p}$ are almost equal in terms of deviations of their values from parameter p and insignificantly exceed as such estimate $\tilde{v}$. Therefore estimate $\hat{p}$ can be adopted as the desired bias-efficient estimate among the available ones, when the scope of tests is n>3. However, when it is required to

Table 1. Results of the substitution of available probability of failure estimates into functionals $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$

Type of functional	$\tilde{v}(\beta=0,5)$ $4\le n\le 10$	$\hat{p}=\frac{r}{n+k}$ $4\le n\le 10$	$\overline{p}(\tilde{v}(\beta=0,5))$ $4\le n\le 10$
$L(\hat{\theta}(n;k,m))$	0,00229	0,000219	0,000805
$D(\hat{\theta}(n;k,m))$	0,0205	0,0186	0,0164

estimate unknown parameter p with a value other than zero and one, estimate $\overline{p}$ should be used.

Let us note that, when calculating, variation of the step of summation ($\partial p=10^{-3}$) modifies the results of the functional, but does not bring essential changes. The result of comparison does not affect the estimates.

Example 1. Products are part of a redundant unit. It is required to perform a point estimation of the products' PNF subject to the results of binomial tests of such products' dependability. While planning determinative dependability tests the tester calculated sample size (N=n+k=5) assuming a single failure (Q=k=1), thus minimizing the risks caused by the occurrence of such unlikely random failure.

The predicted value of PNF was calculated using a bias-efficient composite estimate [9]:

$$\dot{P}=\begin{cases}1-\tilde{b}\left(0,N,\beta=0,86\right), R=0;\\ 1-\frac{R}{N},\ R>0,\end{cases}$$

where $\tilde{b}\left(0,N,\beta=0,86\right)$ is the implicit estimate of the binomial test plan [9]. The predicted value of PNF was $\dot{P}(r=1)=1-\frac{r}{N}=\frac{4}{5}=0,8$, which complies with the product's performance specification (PNF is to be not less than 0.8). Given that, during the test time, product failure is unlikely, it was decided to conduct dependability testing using addition in order to save costs. The testing can have two outcomes, i.e. failure-free and one failure (planned). In case of failure-free testing, there is no need for testing with oversampling. The calculations of possible PNF values are given in Tables 2 and 3.

Let us note that in case of binomial testing with curtailed sample N=n=4, Q=0 and when one failure r=1 occurs, the rules require retesting according to the same rules, as $\dot{P}=1-\frac{r}{N}=\frac{3}{4}=0,75<0,8$ [3]. Repeated binomial testing does not allow failures. Performing failure-free binomial tests with the acceptance number of failures of Q=1 will require a sample of size N=5, that is larger than the initial sample used in testing with addition N=4.

That is the advantage of testing with addition that allows making conclusions regarding the compliance with specifications based on the results of a single test with different outcomes, i.e. N=n+k=4, r=0 and N=n+k=5, r=1 (without same-scope (N=n+k=4, r=0) testing as in the case of binomial testing, where one failure is allowed Q=0).

Example 2. Per example 1, the tester, while calculating the size of the sample (N=4), made an allowance for one failure (Q=k=1). The predicted value of PNF was $\dot{P}=1-\frac{r}{N}=\frac{3}{4}=0,75$, which complies with the product's performance specification (PNF is to be not less than 0.75). Given that, during the test time, product failure is unlikely, it was decided to conduct dependability testing using addition in order to save costs. The calculations of possible PNF values are given in Tables 4 and 5.

Criterion of selection of efficient estimate for mean time to failure

Let us assume that the products' time to failure follows the exponential distribution law of probabilities (hereinafter referred to as d.l.) with parameter T_0, where the latter is

Table 2. Results of failure-free testing per example 1

PNF (failure-free tests with addition) r=0, n=4, N=n+k=4+0=4, Q=1			PNF (binomial tests) r=0, N=n=4, Q = 0 $\dot{P}=1-\tilde{b}(0,N,\beta=0,86)$
$1-\tilde{v}$ β=0,5 [1]	$1-\hat{p}=1-\frac{r}{n+k}$	$1-\overline{p}\left(\tilde{v}\right)$ β=0,5	
0,871	1	0,871	0,963

Table 3. Results of tests with one failure per example 1

PNF (failure-free tests with addition) r=1, n=4, N=n+k=5, Q = 1			PNF (binomial tests) r=1, N=n=5, Q = 1 $\dot{P}=1-\frac{r}{N}$
$1-\tilde{v}$ β=0,5	$1-\hat{p}$	$1-\overline{p}\left(\tilde{v}\right)$ β=0,5	
0,687	0,8	0,8	0,8

Table 4. Results of failure-free testing per example 2

PNF (failure-free tests with addition) r=0, k=0, n=3, N=n+k=3+0=3, Q=1				PNF (binomial tests) r=0, N=n=3, Q = 0 $\dot{P} = 1 - \tilde{b}(0, N, \beta = 0{,}86)$
$1 - \tilde{v}$, β=0,5	$1 - \hat{p} = 1 - \frac{r}{n+k}$	$1 - \hat{w}_3(0)$	$1 - \overline{p}(\tilde{v})$, β=0,5	
0,841	1	1	0,841	0,951

Table 5. Results of tests with one failure per example 2

PNF (failure-free tests with addition) r=1, k=1, n=3, N=n+k=4, Q=1				PNF (binomial tests) r=1, N=n=4, Q = 1 $\dot{P} = 1 - \frac{r}{N}$
$1 - \tilde{v}$, β=0,5	$1 - \hat{p}$	$1 - \hat{w}_3(1)$	$1 - \overline{p}(\tilde{v})$, β=0,5	
0,616	0,75	0,642	0,75	0,75

identical to the mean time to failure (hereinafter referred to as MTF). Then the expected value of PNF of one product within the given time τ will be defined by the equation:

$$P_0(\tau) = e^{\left(-\frac{\tau}{T_0}\right)}.$$

As the quality criterion of the obtained efficient estimate of MTF a functional is constructed (hereinafter referred to as $V(\hat{\theta})$), that is based on the sum of the squares of relative biases of mathematical expectations of estimates $\hat{\theta}(k, m, n, \tau)$ relative to parameter t of the exponential d.l. (MTF) for all possible values of t, n [6]:

$$V\left(\hat{\theta}(k,m,n,\tau)\right) = \\ = \frac{1}{3}\sum_{i=3}^{5}\frac{1}{10}\sum_{n=1}^{10}\int_0^{\infty}\left(\frac{1}{t}\right)^2 \{E\hat{\theta}(k,m,n,\tau = 10^i) - t\}^2 \partial t. \quad (3)$$

Integration is performed using all possible values of parameter (MTF) $t \in [0;\infty]$.

Let us examine the functional (hereinafter referred to as $H(\hat{\theta})$) based on the sum of mathematical expectations of the squares of relative deviations of estimates $\hat{\theta}(k, m, n)$ relative to parameter t of the exponential d.l. (MTF) for all possible values of t, n [6]:

$$H\left(\hat{\theta}(k,m,n,\tau)\right) = \\ = \frac{1}{3}\sum_{i=3}^{5}\frac{1}{10}\sum_{n=1}^{10}\int_0^{\infty}\left(\frac{1}{t}\right)^2 E\{\hat{\theta}(k,m,n,\tau = 10^i) - t\}^2 \partial t. \quad (4)$$

The purpose of functionals $H\left(\hat{\theta}(k,m,n,\tau)\right)$ is to identify the scatter of the values of the available estimates.

Estimate that minimizes the available functionals is efficient among the available estimates of MTF.

Selection of the efficient estimate of MTF

Let us define the estimate of MTF ($\hat{T}_2$) for the plan of tests with addition as:

$$\hat{T}_2 = \frac{S(k,m,\tau,s_i,n)}{R},$$

where s_i are the instants of failure, i=1,2,…, R>0, S – is the total operation time. Let us complete estimate $\hat{T}_2$ for the case of R = 0 with value $\hat{T}_2$=$S(k,m,\tau,n)$.

Another case. In order to avoid dividing by zero while estimating the MTF $\hat{T}_2$, let us represent it as follows:

$$\hat{T}_3 = \frac{S(k,m,\tau,s_i,n)}{R+1}.$$

Let us consider a simple case and reduce the number of variables for estimates $\hat{T}_3$ and $\hat{T}_2$. For that purpose, let us assume that scatter s_i is symmetrical in relation to τ/2. That can be fulfilled for highly dependable products $\frac{\tau}{T_0} < 0{,}1$ [3]. Therefore $S(k,m,\tau,n)$= $(n–k)$*τ+$(k+m)$*τ/2.

Let us define the following estimates of MTF for the plan of tests with addition as:

$$\hat{T}_0 = \frac{\tau}{-\ln(1-\tilde{v}(k,m,n,\beta = 0{,}5))},$$

$$\hat{T}_1 = \frac{\tau}{-\ln(1-\overline{p}(k,m,n,\beta = 0{,}6))}.$$

Functionals $V(\hat{\theta}(\tau;n;k,m))$ and $H(\hat{\theta}(\tau;n;k,m))$ were calculated with the step of $\partial p = 10^{-3}$. Implicit estimates $\tilde{v}$ and $\overline{p}$ were calculated with the accuracy of 10^{-4}.

Table 6. Results of substitution into functionals $V(\hat{\theta}(\tau;n;k,m))$ and $H(\hat{\theta}(\tau;n;k,m))$ of MTF estimates: $\hat{T}_0$, $\hat{T}_1$, $\hat{T}_2$, $\hat{T}_3$

Type of functional	$\hat{T}_0(\tilde{v})$ β=0,5	$\hat{T}_1(\overline{p})$ β=0,6	$\hat{T}_2 = \frac{S}{R}$	$\hat{T}_3 = \frac{S}{R+1}$
$V(\hat{\theta}(\tau;n;k,m))$	10,89	10,80	2363	1836
$H(\hat{\theta}(\tau;n;k,m))$	27,47	25,54	2373	1845

Table 7. Results of failure-free testing per example 3

PNF (failure-free tests with addition) r=0, k=0, n=4, N=n+k=4+0=4, Q=1 $\hat{T}_1 = \frac{\tau}{-\ln(1-\overline{p}(k=0,m=0,n,\beta=0,5))}$	PNF (binomial tests) r=0, N=n=4, Q = 0 $\hat{T}_{БИ} = \begin{cases} \frac{\tau}{-\ln(1-\frac{r>0}{n})} \\ \frac{\tau}{-\ln\left(1-\tilde{b}\left(r=0,n,\beta=0,6\right)\right)} \end{cases}$
$\frac{10000}{-\ln(1-\tilde{v}(k=0,m=0,n=4,\beta=0,5))} = 72411$	$\frac{10000}{-\ln\left(1-\tilde{b}\left(r=0,n=4,\beta=0,6\right)\right)} = 78304$

Table 8. Results of tests with one failure per example 3

PNF (failure-free tests with addition) r=1, k=1, n=4, N=n+k=4+1=5, Q=1 $\hat{T}_1 = \frac{\tau}{-\ln(1-\overline{p}(k,m,n,\beta=0,5))}$	PNF (binomial tests) r=1, N=n=5, Q = 1 $\hat{T}_{БИ} = \begin{cases} \frac{\tau}{-\ln(1-\frac{r>0}{n})} \\ \frac{\tau}{-\ln\left(1-\tilde{b}\left(r=0,n,\beta=0,6\right)\right)} \end{cases}$
$\frac{10000}{-\ln(1-\frac{k+m}{n+k})} = 44814$	$\frac{10000}{-\ln(1-\frac{1}{5})} = 44814$

Table 6 shows the results of substitution into functionals $V(\hat{\theta}(\tau;n;k,m))$ and $H(\hat{\theta}(\tau;n;k,m))$, in accordance with formulas (3) and (4), of the following MTF estimates $\hat{\theta}$: $\hat{T}_0$, $\hat{T}_3$, $\hat{T}_1$, $\hat{T}_2$.

Out of Table 6 follows that estimate

$$\hat{T}_1 = \frac{\tau}{-\ln(1-\overline{p}k,m,n,\beta=0,6))}$$

is efficient out of the available estimates.

Example 3. Per example 1, products were tested during 10 000 hours. Let us use the classical efficient estimate of MTF $\hat{T} = \frac{\tau}{-\ln(1-\hat{b}\left(r,n\right))}, \hat{b}\left(r,n\right) = \frac{r}{n}$ for binomial plan [7] and efficient estimate of MTF $\hat{T}_b = \frac{\tau}{-\ln(1-\tilde{b}(R=0,N,\gamma=0,6))}$ [9], and construct on their basis the following composite estimate of MTF for binomial testing:

$$\hat{T}_{BT} = \begin{cases} \frac{\tau}{-\ln(1-\hat{b})}, R>0; \\ \frac{\tau}{-\ln\left(1-\tilde{b}\left(R,n,\beta=0,6\right)\right)}, R=0, \end{cases}$$

where $\tilde{b}(r,n,\beta=0,6)$ is the implicit estimate of the probability of failure of the binomial test plan [9].

$$\hat{T}_{BT}\left(r=1,n=5\right) = \frac{\tau}{-\ln(1-\tilde{b}(r,n))} =$$

$$= \frac{10000}{-\ln(1-\frac{r}{n})} = \frac{10000}{-\ln(1-\frac{1}{5})} = 44814 \text{ hours},$$

which is in compliance with the performance specification ($T_0 \geq 40000$) for the products. Given that during the test time product failure is unlikely, it was decided to conduct dependability testing using addition in order to save costs.

Conclusions

PNF estimates for the plan of tests with addition were examined. For the case of $n > 3$, estimates $\hat{P} = 1-\hat{p} = 1-\frac{r}{n+k}$ and $1-\overline{p}(\tilde{v}(\beta=0,5))$ (composite estimate) are more efficient in comparison with estimate $1-\tilde{v}(\beta=0,5)$. The composite estimate of PNF $1-\overline{p}(\tilde{v}(\beta=0,5))$ should be used in failure-free tests.

For the case of $n > 3$, testing with the acceptance number of failures greater than zero ($Q > 0$) conducted with addition allows reducing the number of tested products through successful testing of the original sample.

The composite estimate of MTF $\hat{T}_1 = \frac{\tau}{-\ln(1-\overline{p}(k,m,n,\beta=0,6))}$ is bias-efficient among the proposed MTF estimates.

The obtained composite estimates $\overline{p}$ and $\hat{T}_1$ are of practical significance in the context of failure-free testing with addition.

References

[1] Mikhailov V.S. Plan of tests with addition. Dependability. 2019;3:12-20.

[2] Borovkov A.A. [Mathematical statistics]. Novosibirsk: Nauka; Institute of Mathematics Publishing; 1997. (in Russ.)

[3] Barzilovich E.Yu., Beliaev Yu.K., Kashtanov V.A. et al. Gnedenko B.V., editor. [Matters of mathematical dependability theory]. Moscow: Radio i sviaz; 1983. (in Russ.)

[4] Shulepin V.P. [Mathematical statistics. Part 1. Parametric statistics]. Tomsk: Izdatelstvo NTL; 2012. (in Russ.)

[5] Dwight H.R. Tables of integrals and other mathematical data. Moscow: Hauka; 1966.

[6] Mikhaylov V.S. [Investigation of integral estimates]. Reliability & Quality of Complex Systems. 2018;2(22):3-10. (in Russ.)

[7] Mikhaylov V.S. Implicit estimates for the NBτ test plan. Reliability and quality of complex systems. 2018;1(21):64-71. (in Russ.)

[8] Mikhailov V.S., Yurkov N.K. Estimates of reliability indicators for fault-free tests conducted according to the binomial plan. Reliability and quality of complex systems. 2018;4(24):29-39. (in Russ.)

[9] Mikhaylov V.S., Yurkov N.K. A special case of finding effective estimates. Reliability and quality of complex systems. 2019;2:103-113. (in Russ.)

[10] Mikhailov V.S. Efficient estimation of mean time to failure. Dependability 2016;4:40-42.

[11] Mikhailov V.S. Estimation of the gamma-percentile life for the binomial test plan. Dependability 2019; 2:18-21.

About the author

Viktor S. Mikhailov, Lead Engineer, D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow, e-mail: Mvs1956@list.ru

The authors' contribution

Mikhailov V.S. constructed efficient estimates for a plan of tests with addition, such as probability of no-failure $\overline{p}$ и and mean time to failure $\hat{T}_1$. The obtained estimates of $\overline{p}$ and $\hat{T}_1$ are practically applicable in tests that produce no failures and are conducted according to a plan of testing with addition

On the consideration of progressive failure at the stage of design

Andrey I. Dolganov, *SEVERIN DEVELOPMENT Ltd., Russian Federation, Moscow*
dolganov-58@mail.ru

Andrey I. Dolganov

Abstract. *The stress that affects structures and their mechanical and geometrical parameters are random values. For that reason, the dependability of a construction facility (technical system) is generally evaluated in terms of the probability of no-failure over the estimated period of operation. The paper shows the feasibility of dependability analysis of building systems in the course of their design using logical and probabilistic methods, presents algorithms for regulating their dependability. It examines the feasibility of assuring the dependability of a construction project using the example of a double-span whole hinged beam. The paper also establishes the requirement of accounting for all possible destruction models of a building system. The dependability of a double-span whole hinged beam is estimated based on the probability of non-occurrence of all possible destruction models or one of a set of possible kinematic mechanisms. A kinematic mechanism forms a chain of plastic hinges or a chain of progressive failures of effective sections. In other words, the task of preventing progressive collapse comes down to ensuring the required dependability of both the building as a whole, and its individual members (effective sections) by adjusting qualitative and quantitative indicators of the dependability structure. The dependability of a member is understood as its ability to maintain internal force within the effective section at least as high as the external force. It is shown that correct design solutions, rational choice of materials and load non-exceedance probabilities enables specified dependability of a building system. In some cases that allows saving materials, in others enables lower probabilities of failure. Constructing the dependability structure of a technical system enables a quantitative estimation of the most hazardous design models of destruction, rational management of the choice of safety factors of load bearing members, redistribution of such safety factors, thus preventing progressive collapse. The introduced differential characteristics of the members' "weight", "significance", "contribution" and "specific contribution" allows demonstrating the distribution of the roles of each member within the specified structure in terms of specific problems, including accounting for the possibility of progressive collapse. The study has shown that the removal of undependable vertical load bearing structures does not solve the problem of dependability of a construction project, including protection against progressive collapse. It has been established that the design of structures, including in terms of considerations of progressive failure, must involve constructing a system dependability structure using kinematic analysis, identifying the most important and significant members of such structure and – using special adjustment techniques – obtaining the required structure dependability. That will enable significant resource saving and reduction of costs associated with the development of construction operations.*

Keywords: *probability, kinematic mechanism, dependability, plastic hinge, progressive collapse, destruction scheme, technical system.*

For citation: *Dolganov A.I. On the consideration of progressive failure at the stage of design. Dependability. 2020;1: 20-24. https://doi.org/10.21683/1729-2646-2020-20-1-20-24*

Received on: *28.08.2019 /* **Revised on:** *15.02.2020 /* **For printing:** *20.03.2020*

Initial observations

The paper examines the problem of accounting for progressive failure at the design stage. The requirement of progressive collapse calculation is set forth in Item 5.2.6 of GOST 27751-2014 Reliability for constructions and foundations. The calculations aim at preventing progressive (avalanche-type) destruction of buildings and structures.

According to the Guidelines for protection of tall building against progressive collapse and Guidelines for protection of monolithic residential buildings against progressive collapse developed by the Moscow City Architecture Committee in 2006 and 2005 respectively, as well as STO 008-02495342-2009 Prevention of progressive collapse of in-situ reinforced concrete building structures. Design and calculation, design should take into consideration the possible destruction (removal) of vertical structures of one (any) floor of a building:

1) two intersecting walls within the sections between the intersection (for instance, the building's corner) and the nearest aperture in each wall or vertical joint with a differently oriented wall (but with total length of the wall not more than 7 m);

2) freestanding column (pylon);

3) column (pylon) with sections of adjacent walls with the total length of 7 m.

At the same time, it is allowed to multiply standard characteristics of strength of materials by the extra factor of operating conditions of accidental limit state that is assumed to be from 1.1 to 1.25.

This approach to design allows doubling the span of flexible members and reducing the probability of non-exceedance of design strength.

Thus, by multiplying the standard strength (500 MPA) of A500 reinforcement steel by 1.15 we obtain 575 MPA, which is above the average value of 550 MPA. In other words, the resulting probability of non-exceedance of reinforcement steel strength is below 0.5.

According to the above recommendations, it is allowed to multiply the standard strength of concrete by 1.25. For instance, for B40 cement the estimated strength will be: $29 \times 1.25 = 36.25$ MPA. A the same time, the average value under the variation coefficient is 0.1 is 34.69 MPA. In other words, the resulting probability of non-exceedance of estimated strength is 0.326.

Thus, a structure designed per the above recommendations has inherently unacceptably low dependability along with unjustifiable overspending of materials, e.g. reinforcement steel (this can be compared to a situation where an airliner loses a wing or its size is reduced mid-flight).

The subject matter

A considerable contribution to dependability estimation of complex technical systems and research of structural redundancy was made in [1–3]. In [4], the problem of dependability estimation and construction of its structure was solved using the recurrent logical and probabilistic method.

The point of the below method of estimation of the possibility of progressive failure consists in the rational management of the dependability of individual components of technical systems. A simple example of double-span whole beam (Fig. 1.) is considered. The logical and probabilistic method of orthogonalization is used for its clarity [1, 5].

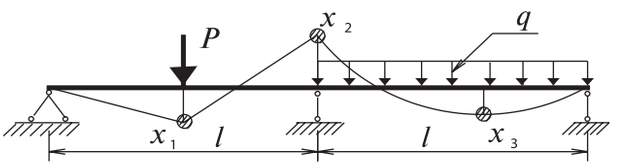


Figure 1 – The simplest technical system.

As kinematic analysis shows, the system (Fig. 1.) will fail in case of simultaneous failure of sections x_1 and x_2 or x_1 and x_3, or x_2 and x_3, i.e. in case of occurrence of one of the possible models of the kinematic mechanism. The above combinations of x_i ($i = 1, 2, 3$) are in fact the dependability structure of a technical system. Values x_i can be associated both with the probabilities of no-failure of system R_i, and probabilities of failure Q_i.

The matters of assignment of dependability levels for element x_i and methods of identifying the probabilities of no-failure of systems R_c are examined in [6, 7]. In other words, quantitatively system dependability is estimated using one of its indicators, i.e. probability non-occurrence of any possible models of destruction of a technical system or probability of development of one of a set of kinematic mechanisms.

As a kinematic mechanism forms a chain of plastic hinges (failures of members, effective sections), the task of prevention of a progressive collapse comes down to the assurance of the required dependability of its individual members (effective sections).

For cases when it must be decided with which section (member) dependability adjustment is to start in order to obtain the most rational technical system structure, special quantitative characteristics are used, i.e. "weight", "significance" and "contribution" of such member within the system's dependability structure. The above characteristics can allow identifying the "trouble spots" in a technical system, choosing optimal redundancy and rationally adjusting its dependability.

It is known that the initial dependability level of a technical system is defined by internal and external factors. For example, a structure's internal factors include the random nature of the geometrical parameters, mechanical characteristics of materials, etc. The external factors include the random nature of gravity, temperature loads, uneven settlement of undersoil, etc. For that reason dependability adjustment takes into consideration the independence of the external and internal factors. For instance, changes in the gravity loads do not modify the probability of non-exceedance of the mechanical characteristics of materials.

Below is the algorithm of dependability adjustment of a technical system. Formulas are given without derivations. The theoretical justification of formulas can be found in [1].

1. A structure diagram is constructed for dependability calculation of building systems

1.1. We identify all system components (effective sections), in which plastic hinges are allowed: x_i, i = 1, 2, 3 (Fig. 1).

1.2. Using kinematic analysis, all possible destruction models are specified for a technical system and written as conjunctions K_i:

$$y(x_1, x_2, x_3) = \begin{vmatrix} x_1x_2 \\ x_1x_3 \\ x_2x_3 \end{vmatrix} = \begin{vmatrix} K_1 \\ K_2 \\ K_3 \end{vmatrix}. \quad (1)$$

1.3. Using standard methods, expression (1) is transformed into orthogonal sum-of-products form (2):

$$y(x_1, x_2, x_3) = \begin{vmatrix} K_1 \\ K_1^{/}K_2 \\ K_1^{/}K_2^{/}K_3 \end{vmatrix} = \begin{vmatrix} x_1x_2 \\ x_1x_2^{/}x_3 \\ x_1^{/}x_2x_3 \end{vmatrix}, \quad (2)$$

where $K_1^{/}K_2 = \begin{vmatrix} x_1^{/} \\ x_1x_2^{/} \end{vmatrix} x_1x_3 \Big| = \left|x_1x_2^{/}x_3\right|$,

$$K_1^{/}K_2^{/}K_3 = \begin{vmatrix} x_1^{/} & x_1^{/} \\ x_1x_2^{/} & x_1x_3^{/} \end{vmatrix} x_2x_3 \Big| = \left|x_1^{/}x_2x_3\right|.$$

1.4. The final formula of dependability structure for the considered technical system is written:

$$R_c = R_1R_2 + R_1Q_2R_3 + Q_1R_2R_3. \quad (3)$$

The matters of assignment of dependability levels for element x_i and methods of identifying the probabilities of no-failure of technical systems R_c are examined in [6, 7]. In the examined example, we will assign identical dependabilities of sections (probabilities of no-failure): $R_1 = R_2 = R_3 = 0.9$. Then, system dependability will be:

$$R_c = R^2 \times (1 + 2 \times Q) = 0.9^2 \times \\ \times [1 + 2 \times (1 - 0.9)] = 0.972.$$

2. Parameters of the structure diagram are defined: "weight", "significance" and "contribution"

2.1. The "weight" of elements

$$g_{x_i} = \frac{G\{\Delta_{x_i} y(x_1, \ldots, x_n)\}}{2^n} = \sum_{j=1}^{l} 2^{-(r_j-1)} - \sum_{f=1}^{k} 2^{-(r_f-1)}, \quad (4)$$

where r_j is the rank of conjunction with x_i; r_f is the rank of conjunction with $x_i^{/}$.

For the considered example, the standard "weight" of element x_i, i = 1, 2, 3 is:

$$g_{x_1} = \frac{G\{\Delta_{x_1} y(x_1, x_2, x_3)\}}{2^3} = \frac{4}{8} = 0,5,$$

$$g_{x_2} = \frac{G\{\Delta_{x_2} y(x_1, x_2, x_3)\}}{2^3} = \frac{4}{8} = 0,5,$$

$$g_{x_3} = \frac{G\{\Delta_{x_3} y(x_1, x_2, x_3)\}}{2^3} = \frac{4}{8} = 0,5.$$

The example shows that the "weights" of elements x_i, i = 1, 2, 3 are identical. Therefore, the "weight" of elements in the dependability structure of the system is identical. The "weight" of an element characterizes the relative number of such critical up states of a system, in which the failure of such element causes the failure of the system (and vice versa, its recovery causes the recovery of the system).

2.2. The "significance" of elements

The "significance" shows the effect of the element on the system's dependability.

$$\zeta_{x_i} = \frac{\partial P\{y(x_1, \ldots, x_n) = 1\}}{\partial P\{x_i = 1\}} = \frac{\partial R_c}{\partial R_i}. \quad (5)$$

For element 1, "significance" is:

$$\zeta_{x_1} = \frac{\partial y_c}{\partial x_1} = x_2 + x_2^{/}x_3 - x_2x_3 = 0,1 + 0,9 \cdot 0,1 - 0,1^2 = 0,180.$$

2.3. "Contribution" of the elements

The "contribution" of element x_i in system $y(x_1, \ldots, x_n)$ is the product of the probability of no-failure of element R_i and its "significance", i.e.:

$$B_{x_i} = R_i \frac{\partial R_c}{\partial R_i}. \quad (6)$$

For element 1 the "contribution" is:

$$B_{x_i} = x_i^{/} \frac{\partial y_c}{\partial x_i} = 0,9 \cdot 0,18 = 0,162.$$

The criterion of "contribution" characterizes the increment of system dependability after the recovery of element x_i from down or conditionally down state into up state with actual probability of no-failure of R_i.

2.4. "Specific contribution" of elements

The "specific contribution" of element x_i in system $y(x_1, \ldots, x_n)$ is the standardized "contribution" of such element, i.e.

$$b_{x_i} = B_{x_i} / \sum_{i=1}^{n} B_{x_i} = 0,162 / (3 \times 0,162) = 0,333. \quad (7)$$

The criterion of "contribution" enables rational definition of the priority of elements' recovery in the system.

3. The structural components of system dependability are defined

3.1. The "qualitative" components of dependability

The "qualitative" $\Delta R_c,q$ structural components of a technical system's dependability include the quality of materials, state of technology, probability of non-exceedance of design strengths of materials, loads, etc.

$$\Delta R_{c,q} = \sum_{i\in M_1} \frac{\partial R_c}{\partial R_i}\Delta R_i + \sum_{i,j\in M_2} \frac{\partial^2 R_c}{\partial R_i \partial R_j}\Delta R_i \Delta R_j + \ldots$$
$$\ldots + \rightarrow + \sum_{i,j,\ldots,k\in M_l} \frac{\partial^l R_c}{\partial R_i \partial R_j \ldots \partial R_k}\Delta R_i \Delta R_j \ldots \Delta R_k + \ldots$$
$$\ldots + \Delta R_1 \Delta R_2 \ldots \Delta R_n \qquad (8)$$

or in case of equal increments of dependability in effective sections ΔR_i

$$\Delta R_{c,q} = \sum_{j=1}^{n} C_n^j \frac{\partial^j R_c}{\partial R_i \ldots \partial R_k}(\Delta R_j)^j. \qquad (9)$$

Let us perform a qualitative progressive increment of the dependability of sections, e.g. up to 0.99. That can be achieved, for instance, by reducing the design loads. The difference between the specified, new (0.99) and initial (0.9) levels of dependability of sections ΔR_i, i = 1, 2, 3 will be: $\Delta R_1 = \Delta R_2 = \Delta R_3 = 0.99 - 0.9 = 0.09$.

According to formula (8) or (9), let us identify the qualitative increment of dependability:

$\Delta R_c,q = \Delta R \times [2R(1+2Q–R)] + \Delta R^2 \times [(1–2R) + 2\times(Q–R)] + \Delta R^3 \times (–2) =$

$= 0.09 \times [2 \times 0.9 \times (1 + 2 \times 0.1 – 0.9)] + 0.09^2 \times [1 – 2 \times 0.9) + 2 \times (0.1–0.9)] + 0.09^3 \times (–2) = 0.0277.$

System dependability subject to the qualitative increment became: 0.972 + 0.0277 = 0.9997.

We will get the same result if we substitute the required dependabilities of sections (0.99) into formula (3):

$R_c = 0.99^2 \times [1 + 2 \times (1 – 0.99)] = 0.9997.$

If we follow the Guidelines for protection of tall buildings against progressive collapse and Guidelines for protection of monolithic residential buildings against progressive collapse developed by the Moscow City Architecture Committee in 2006 and 2005 respectively, as well as STO 008-02495342-2009 Prevention of progressive collapse of in-situ reinforced concrete building structures. Design and calculation, we reduce the probabilities of non-exceedance of materials strength when we multiply them by the extra factor of conditions of operation for the accidental limit state. For that reason, the qualitative increment of dependability in this case is negative: – 0.0277. In other words, the dependability of sections will become: 0.9 – 0.0277 = 0.8723. System dependability will become $R_c = 0.8723^2 \times [1 + 2 \times (1–0.8723)] = 0.9552$.

3.2. The "quantitative" components of dependability

The "quantitative" components $\Delta R_c,v$ of the dependability structure of a technical system are materials reservation, reinforcing laps, additional pylons, connections, etc.

In case of quantitative variation of dependability, e.g. in case of duplication of the i-th element with same-type element x_i, the dependability of such group increases by ΔR_z [1]:

$$\Delta R_z = (2R_i - R_i^2) - R_i, \qquad (10)$$

the dependability of the whole system increases by R_c,v:

$$\Delta R_{c,v} = \frac{\partial R_c}{\partial R_i}\Delta R_z = \frac{\partial R_c}{\partial R_i} R_i Q_i, \qquad (11)$$

where $Q_i = 1 – R_i$ is the probability of failure of the i-th section.

It is evident from (11) that a quantitative increment of system dependability depends on the "significance" and dependability of the duplicating element.

In the general case, in case of duplication of several elements up to the maximum possible number n, we will obtain

$$\Delta R_{c,v} = \sum_{i\in M_1} R_i Q_i \frac{\partial R_c}{\partial R_i} + \sum_{i,j\in M_2} R_i R_j Q_i Q_j \frac{\partial^2 R_c}{\partial R_i \partial R_j} + \ldots$$
$$\ldots + \sum_{i,j,\ldots,k\in M_l} R_i R_j \ldots R_k Q_i Q_j \ldots \rightarrow$$
$$\rightarrow \ldots Q_k \frac{\partial^l R_c}{\partial R_i \partial R_j \ldots \partial R_k} + \ldots + R_1 R_2 \ldots R_n Q_1 Q_2 \ldots Q_n. \qquad (12)$$

A quantitative variation of dependability can be achieved, for instance, by means of adjusting structural redundancy. For instance, as it was mentioned above, that may include reinforcing laps, addition of pylons or ties.

In the joint of section 2 (Fig. 1), let us make a provision for additional cover plates on beams or reinforcing lap (for reinforced concrete beams) able to withstand the ultimate moment. Thus, we duplicate element 2. We will calculate the quantitative increment of system dependability using formula (11):

$$\Delta R_{c,v} = \frac{\partial R_c}{\partial R_i}\Delta R_z = \frac{\partial R_c}{\partial R_i} R_i Q_i = 0,9997 \times$$
$$\times (1 + 0,0003 - 0,9997) \times 0,9997 \times 0,0003 = 1,8 \times 10^{-7}.$$

As calculations show, the addition of pylons, reinforcing lap or other ties does not result in a significant increment of dependability for the considered system.

Additionally, extra reinforcement of concrete structures (the case of concrete failure) may cause the inverse effect, i.e. reduced dependability. That is caused by the fact that in case of extra reinforcement the element's operation involves only one material, i.e. concrete. The variation coefficient of the strength of concrete is much higher than that of reinforcement steel.

System dependability subject to the qualitative and quantitative increment will be: R_c = 0.972 + 0.0277 + 0.00 000018 = 0.9997. That is about 3.43 of the standard value,

which complies with current expectations regarding the implications of dependability for building systems. Currently, dependability of sections of engineering structures of normal criticality projects is about 0.99865 [6].

Conclusion

According to current regulatory documents on the calculation of progressive collapse, the removal of vertical load-bearing members and associated reservation of additional materials, e.g. reinforcement steel, does not solve the problem of assuring required dependability of technical systems. Subsequently, such actions are useless, while this method of dependability adjustment is self-deceitful.

Progressive collapse can be prevented by rationally adjusting the selected safety factors of the load-bearing members and their redistribution through the construction of the dependability structure of a technical system as an obligatory part of its design. Additionally, the construction of the dependability structure of a technical system enables a quantitative estimation of the most hazardous design models of destruction, demonstration of the distribution of the role of all members within the specified structure as part of progressive collapse problem solution.

It is also shown that, as the dependability of a member deteriorates, its significance and contribution to the dependability structure of the considered technical system grow, and vice versa. System dependability does not change proportionally to the changes in the dependability of member (sections).

Thus, the design of structures, including in terms of consideration of progressive failure, must involve (along with the calculations per two groups of limit states) constructing a technical system dependability structure, identifying the most important and significant members of such structure and – using special adjustment techniques – obtaining the required structure dependability. That will enable significant resource saving and reduction of costs.

References

[1] Riabinin I.A., Cherkesov G.N. [Logical and probabilistic methods of dependability study of structurally complex systems]. Moscow: Radio i sviaz; 1981. (in Russ.)

[2] Schäbe H., Shubinsky I.B. Limit reliability of structural redundancy. Dependability. 2016;16(1):9-13. DOI: 10.21683/1729-2646-2016-16-1-3-13.

[3] Shubinsky I.B. [Structural dependability of information systems. Methods of analysis]. Ulianovsk: pechatny dvor; 2012. (in Russ.)

[4] Dolganov A.I. [Dependability assessment of site-cast multi-floor buildings]. Industrial and civil engineering. 2010;8:50-51. (in Russ.)

[5] Dolganov A.I. [Dependability of framed concrete structures]. Magadan: MAOBTI; 2001. (in Russ.)

[6] Dolganov A.I. Sakharov A.V. On the assignment of dependability level. Dependability. 2018;3:18-21.

[7] Dolganov A.I. [On the dependability of mass-built structures]. Industrial and civil engineering. 2010;11:66-68. (in Russ.)

About the author

Andrey I. Dolganov, Doctor of Engineering, Technical Director, SEVERIN DEVELOPMENT, Russian Federation, Moscow, e-mail: dolganov-58@mail.ru

The author's contribution

Dolganov A.I. analyzed the construction accidents that occurred in Russia between 2001 and 2018, developed a method that is based on a probabilistic model and allows adjusting the dependability of technical systems, thus preventing progressive collapse with the probability adopted in industrial and civil engineering. The paper shows the applicability of the method to any building system. It also proposes developing the indicator of probability of no-failure for the purpose of technical system design using such parameters as significance, importance and contribution of each member (structure) within the dependability structure of a building.

Dependability, vol. 20 no. 1, 2020 Original article
https://doi.org/10.21683/1729-2646-2020-20-1-25-31

On the organization of the dependability service in a machine-building company

Maria V. Belousova[1], Vitaly V. Bulatov[2]*
[1] *Saint Petersburg State University, Russian Federation, Saint Petersburg*
[2] *Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia*
* *bulatov-vitaly@yandex.ru*

Maria V. Belousova

Vitaly V. Bulatov

Abstract. *Historically, dependability services originated within design units of companies. A design engineer had his/her own ideas about the quality control of released products. As the initial application field of the dependability theory was the aerospace industry, he/she understood that the presence of errors and omissions within a product could cause catastrophic consequences [1]. Along with the dependability unit the quality and technical supervision service was developing, and that was primarily tasked with organizing and conducting acceptance testing, receiving inspection and prevention of a product's non-compliance with technical documentation. At one point, a conflict arouse between the two branches, which lead to a general misunderstanding of responsibilities and disorganization of the product dependability control. As a result, in some companies the dependability service is integrated with the quality service, in others it is subordinated to the design bureau. Additionally, operational dependability evaluation requires an uninterruptible source of reliable information on the reliability and maintainability of the equipment. The quality of this information depends on the interaction between the dependability service and the maintenance service. The latter is to compare the repair reports that specify the recovery time and operation time of the product and promptly submit that data for dependability calculation. Thus, the following questions arise: which activities are to be performed by the dependability service, who is to be subordinated to whom, who is the owner of the processes associated with the estimation of dependability parameters? It is important to understand the purpose of establishing a dependability unit in a company, what authority its employees possess, what results the management expects to obtain. The formalization of the research findings presents a problem. As of today, there is no single approach to formalized calculations, preparation of dependability analysis reports. The research findings are to be sent to all the involved business units, therefore a convenient form of information representation must be developed. A special attention must be given to personnel training in terms of technical system dependability. Industrial products become more and more complex, new technologies are developed, and old approaches to dependability calculation and analysis do not always ensure acceptable results. That is not surprising, as the significance of the use of reliable and substantiated methods of dependability estimation is very understated. That is due to the fact, that many believe that the dependability theory is based on the research of the physical, design-specific causes of failure, physicochemical processes, etc., meaning that a dependability engineer is first and foremost a design or process engineer. However, it should not be forgotten that the general dependability theory is subdivided into the mathematical (mathematical methods of the probability theory), statistical (method of mathematical statistics) and physical (research of materials properties variations). Subsequently, a dependability service is to conduct analysis based on competent application of mathematics alongside activities associated with products design research. Proposals regarding future developments in this area, including the education system, will be welcome.* **Aim.** *To propose an approach to the organization of the dependability service in a modern machine-building company taking into account advanced methods and concepts of dependability analysis at all lifecycle stages of a product.* **Conclusions.** *The paper suggests an organizational structure of a dependability unit for a transport machine building company. The interactions between the dependability service and other business units is examined. A number of factors affecting the efficient operation of the dependability service are identified.*

Keyword: *dependability theory, dependability service, engineering, organizational structure, operational efficiency, human resources management.*

For citation: *Belousova M.V., Bulatov V.V. On the organization of the dependability service in a machine-building company. Dependability. 2020;1: 25-31. https://doi.org/10.21683/1729-2646-2020-20-1-25-31*

Received on: *04.11.2019* / **Revised on:** *18.02.2020* / **For printing:** *20.03.2020*

Introduction

As of late, the problem of dependability estimation of output products has been growing in importance. The organization of a company's dependability service is necessary and relevant in such areas as transport machine-building, automobile production, aircraft industry. However, this subject matter is not extensively covered in foreign and Russian literature. For instance, [2] examines the dependability service functionality only in terms of product development. In [3], the matters and approaches to product operation data processing are examined, yet no algorithm for controlling this process algorithm is proposed.

In [4], the following concept of dependability bureau functionality is set forth: "The dependability bureau performs guidance over the key business units and coordinates the measures aimed at improving the dependability of the output products. The functions of the dependability service are an obligatory part of the general technical policy of a company."

In the meantime, as the scope and range of products grow, the requirements for the competence of the employees involved in the calculation and compliance verification of dependability indicators are increasing as well. A dependability team that consists of capable people, but that is part of another unit and does not have sufficient authority, is an unnecessary luxury [5].

A company's management must be interested in correct operation of the dependability service, vest it with required authorities and involve the unit's employees in the solution of relevant issues in the course of design and operation.

A company that has a qualified dependability service can manage its economic efficiency in the following ways:

• reducing the scope of costly tests or even replacing some items of the respective methods with dependability indicator calculation data obtained in operation that are equivalent in terms of efficiency and correctness;

• recording accurate information on failures of automated data collection systems, which subsequently enables speedy repairs (STPA, unfailing source of supply, etc. are predefined depending on the place of operation) and modify a product's design;

• predicting dependability indicators at various lifecycle stages in order to enable production schedule adjustment and selection of optimal service and repair strategy;

• reducing costs associated with disruption of supplies based on the prediction of dependability-oriented demand for various types of components of the output products.

Dependability service functionality

One of the possible problems at the early stages of dependability service operations is the lack of clear responsibility delimitation. That is due to the fact that the matters of dependability pertain to the interests of the maintenance service, design unit, process engineering bureau and unit responsible for testing to name just a few.

It is not uncommon when the difference between the estimation of dependability and quality is misunderstood. They are often considered to be the same thing, as they have common analytical tools. For instance, FMEA (Failure Mode and Effects Analysis) can be performed by both quality and dependability engineers, however the results will differ. The role of the quality service consists in assessing (the process) of product manufacture, component supplier control. A dependability engineer examines the failure mechanisms that affect the product's operability; identifies the failure frequency patterns using statistical methods; analyses dependent failures of the elements that affect other parts of the system. For that reason, while everyone uses the same FMEA tool, it is used for different purposes: a quality engineer assesses an industrial process, while a dependability engineer assesses a product's design.

Maximizing the efficiency of dependability supervision organization requires identifying the primary functions of the dependability service of a machine-building company:

• product dependability calculation;

• development of structure diagrams of dependability;

• development of programs and methods of operational dependability testing;

• introduction of dependability estimation in the development plan of any product;

• substantiation of the limit values of mean time to failure and recovery time;

• analysis of the common database of dependability longevity tests;

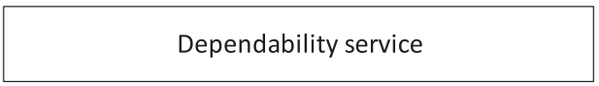
• supervision of completion and optimization of claim register structure;

• informing the company's employees on failures and development of recommendations for various units, whose activities affect the final dependability characteristics of a product.

A certain procedure must be established to regulate the delivery of information materials to the dependability unit. It is recommended to adopt obligatory review by the dependability service employees of such documents as the technical conditions, operator's manuals, program and method of testing, etc. [1].

Organizational structure

If a company views itself as an organization involved in dependability analysis, the responsibility for the design, system engineering, life cycle calculation and responsibility for product quality and dependability assessment should be distinguished. From the project management point of view, it is very important not to miss the stage of development, at which the dependability analysis is conducted. If otherwise, the project itself (prototype manufacture/commencement of batch manufacture, etc.) may become irrelevant, as dependability calculation at the design stage is essentially risk analysis, and incorrectly calculated risks can undermine any project. A common problem is when dependability engineers



Education	Higher	Higher	Higher	Vocational secondary
Working day	Secondary/Full employment	Secondary/Full employment	Full/Contract/Partial	Full employment
Duties	• Calculation of products' dependability indicators in operation • Development of method of estimations of dependability indicators in operation • Development of dependability standards and guidelines • Dependability estimation at the stage of design • Development of recommendations for increased products dependability • Calculation of dependability indicators required for LCC		• Development of programs and applications for automated dependability calculation (according to dependability engineer's specifications) • S&R database administration	• Preparation of documents • Collection of specific information • Logging

Figure 1 – Organizational structure of dependability service.

are tasked with functions they have nothing to do with. An example is life cycle cost (LCC) calculation, of which the process is often assigned to the dependability engineer, while the dependability unit is only responsible for two types of parameter (out of over 10 involved in the calculation), i.e. the failure flow and mean time to restoration of the structure's units and components.

In [6], it is stressed that a company's management is to be responsible for all dependability-related performance indicators; a list of primary requirements for successful organization of dependability management processes is given.

In [7], three models for organization of dependability engineer operations within a company are considered, i.e. functional (linear), project-oriented and matrix models. The linear model implies direct subordination of the dependability engineer to the head of the unit that he/she is assigned to. That may be the quality service or the design bureau. This approach implies the presence of one or two dependability engineers and a dependability coordination manager. An obvious shortcoming of this approach consists in the fact that manufacturing and field data need to be obtained, which requires assistance from other units of the company. In a project-oriented

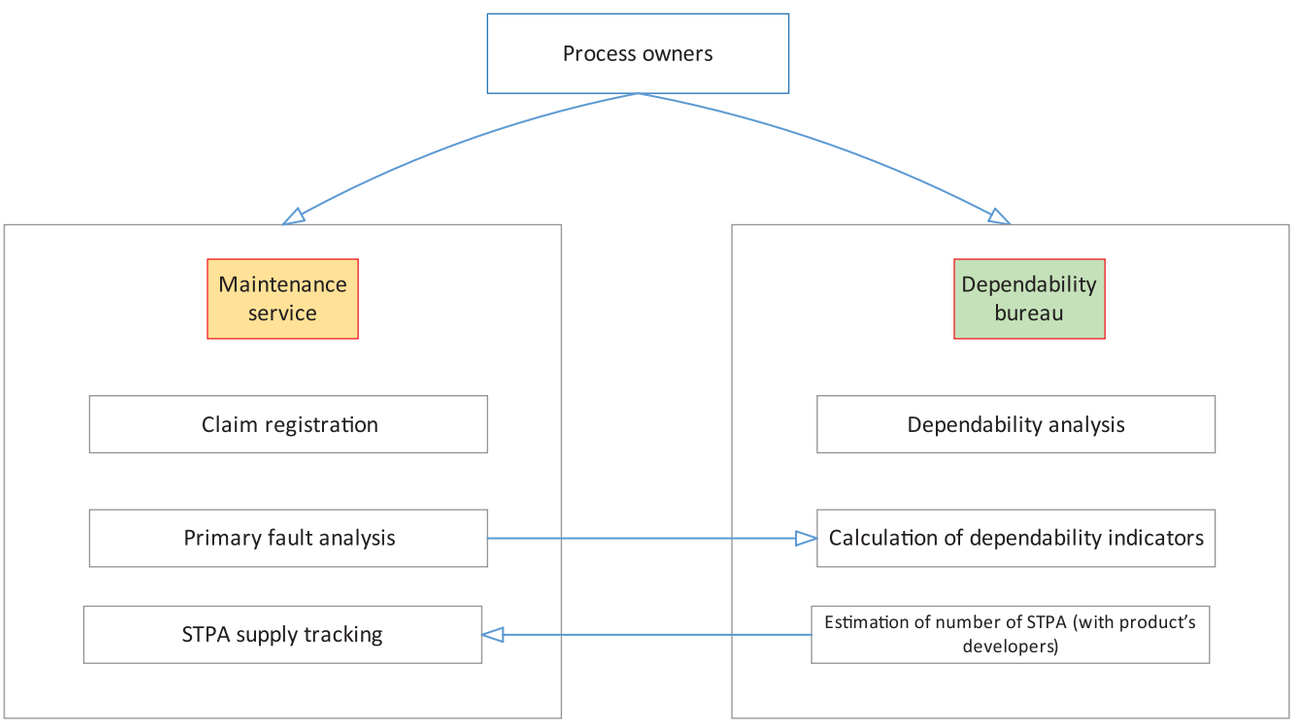


Figure 2 – Interaction between the maintenance service and the dependability service.

structure, the dependability engineer is appointed as part of a specific project and supports a single product. Thus, a dependability service is decentralized, which causes increased support of a product with unique problems that require special attention. On the other hand, decentralization causes duplication of functions and processes per each type of product. A single approach to dependability analysis, e.g. FMEA, may be not in place either. In case of matrix organization the employees of the dependability service belong to a single structure, e.g. the design bureau, but, if required, are temporarily assigned to specific products or projects. Thus, this approach is a combination of the above structures. The matrix organization implies the presence of a coordination manager for dependability and standardization of dependability analysis processes. The structure is flexible, but at the same time subordination-related conflicts may arise. The employees may receive orders from the manager, rather than their direct superior.

An organizational structure of the dependability service is examined in [8]. It implies a three-level system with the lead engineer at the top, design, logistics and system engineering managers at the second level. The bottom level consist of a design engineer with the knowledge of design dependability, a service engineer with knowledge of maintainability assessment and reliability-centered maintenance (RCM) and a system engineer with the knowledge of system dependability.

However, such a structure is difficult to implement in a Russia company: the design engineer is busy developing models and releasing drawings, the service engineer does repairs and is involved with warranty-related financial matters, and to find a system engineer is difficult as well. Additionally, it must be taken into consideration that collection and analysis of data must be done continuously, which requires the development and administration of databases.

In [9], the matters related to the role of the dependability unit of a company are raised as well. The unit's close association with the quality service is noted. However, in the presented diagram [9, p. 45] the dependability unit is independent and is subordinated to the Warranty Director. It should be noted that the structure does not show lines of interaction between the dependability unit, the design bureau and the quality service.

Thus, the following organizational structure of the dependability bureau is proposed (Fig. 1). This structure implies the independence of the dependability unit from

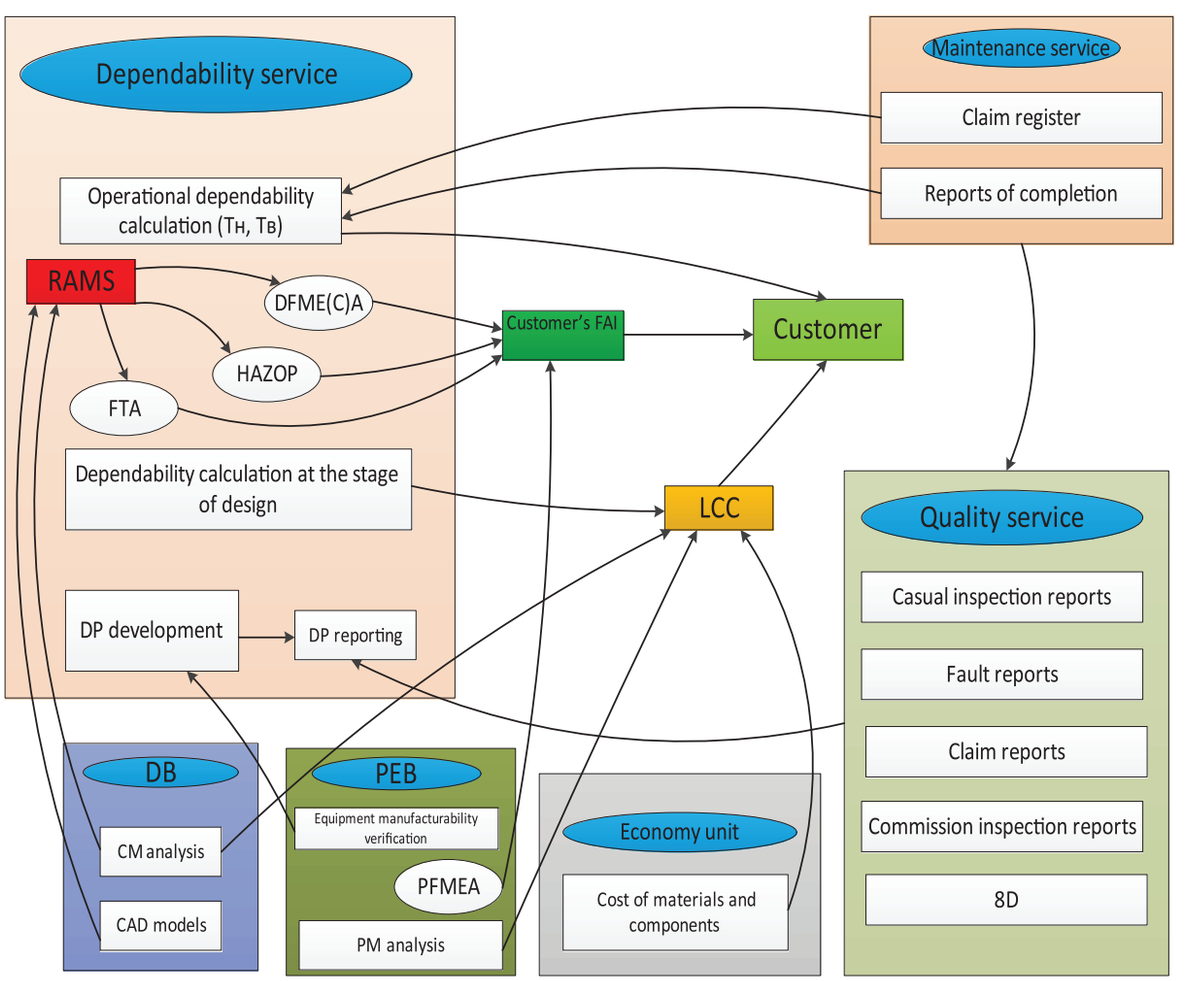


Figure 3 – Interactions between the dependability service and other business units of a company.

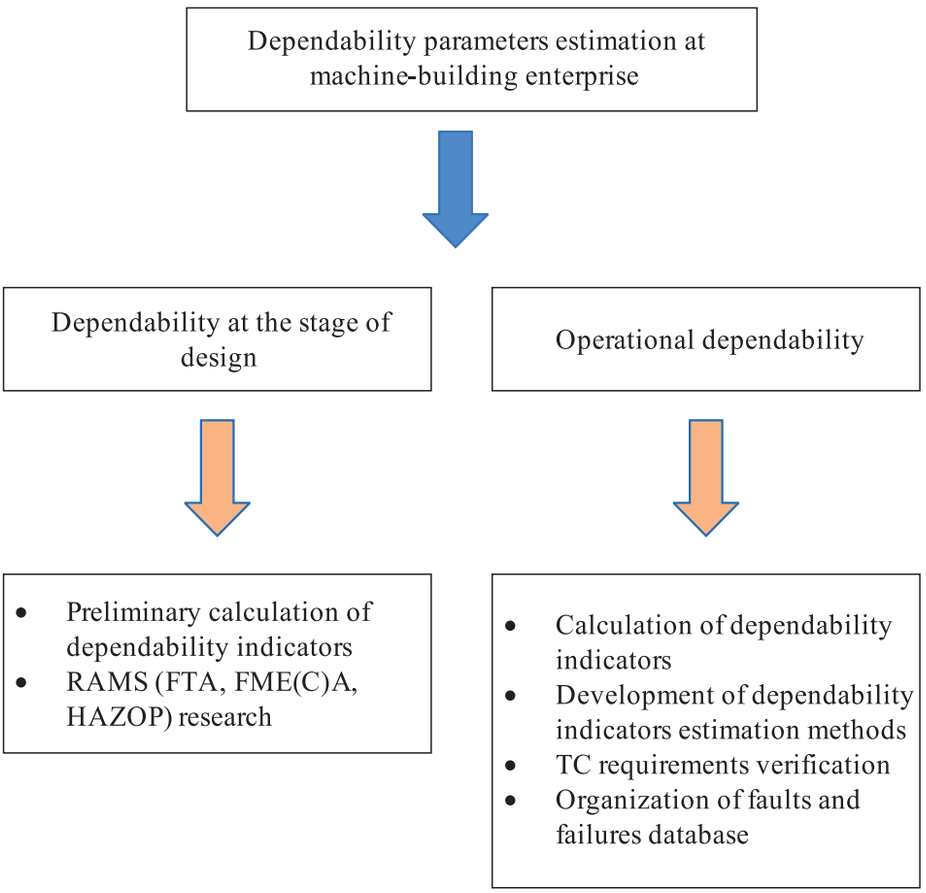


Figure 4 – Estimation of dependability parameters in a machine-building company.

the key technical units of the company and direct subordination to its Technical Director. The dependability service is involved with a wide range of matters, therefore at least two engineers are required, which would enable multitasking. A situation when one of the engineers has a degree in general engineering and another is a mathematician is optimal. Aside from engineers, the operation of the dependability service must also involve an IT specialist tasked with developing programs and applications for automated dependability calculation, as well as support of updating of databases.

Another important aspect is the relations between the maintenance service and the dependability unit. It is very important to clearly define the process owners at each level of failure information processing, otherwise the analysis of the causes of failures parameter evaluation may be complicated or undoable. The key element is the specialists who are responsible for the input of information per in and out of warranty repair reports, perform detailed analysis and evaluate every claim. The following model of interaction between the maintenance service and the dependability service is proposed (Fig. 2). In this structure the maintenance service is responsible for the following processes: claim register keeping, filling in completion reports and delivery of data to the dependability service, control of STPA stock status based on estimated data.

The dependability data collection system is to efficiently affect all the company's business processes and improve the dependability of the released products. This system is to provide the developer with comprehensive and clear data on past failures of units and elements, display the causes and measures taken to eliminate the failures [1].

The process of collection and processing of initial information on faults is to be automated to the fullest possible extent. This process is examined in detail in [10] using the example of the claim register form with a multilevel structure of the output product catalog of a transport machine-building company.

The interaction between the dependability service and a company's units is shown in Fig. 3. At the center of the diagram is the LCC block. Thus, we stress that the life cycle cost calculation is a company's primary goal that is addressed by the above units together, but the owner of the process is the Director General.

Formalization of the types of dependability service activities

The dependability bureau plays a crucial role in many of a company's processes, and subsequently releases a large amount of documentation: Fault Tree Analysis

(FTA), FME(C)A and HAZOP (Hazard and Operability) protocols, dependability indicator calculations, programs and methods of operational dependability testing. Dependability calculation can be subdivided into design and operational (Figure 4). Either one has its own specificity, yet they must be interrelated: the dependability indicators defined based on the information on similar products or calculated using specialized software at the stage of design must be verified at the stage of operation and fed back to design calculation. Feedback enables targeted identification of weak design elements, analysis of the causes of failures and timely design and engineering measures aimed at preventing the causes of recurrent failures [11].

Both the calculations and dependability analysis are to be formally documented at the stage of design and operational dependability calculations.

As of today, there are neither sound methods of such research, nor strict rules of documentation preparation. If dependability calculation at the stage of design can be represented as an RR (calculations) design document according to GOST 2.102-68, the fault tree analysis (FTA) does not have a common form of presentation and follows the recommendations of some translated foreign standards.

Matters related to human resources

Given the above, among the existing problems one should mention the lack of qualified personnel in the dependability estimation department. In the Federal State Educational Standard for Higher education there is no degree or program associated with technical system dependability, while in the Unified Skills Guide for Positions of Managers, Specialists and Non-manual Workers there is no such a position as “dependability engineer” (except from the aerospace industry). For that reason it is proposed to develop a corresponding Master’s program. The applicants must have a Bachelor’s degree in engineering or mathematics. The Master students must be offered an extended course of mathematical subjects, complex system dependability, as well as disciplines in the area of technical diagnostics.

Conclusion

The paper presents an organizational structure of the dependability unit of a transport machine-building company and examines the interactions between the dependability service and other units of a company.

This approach was proposed by the authors based on their own experience of operations in the dependability service of a company that produces rolling stock components, and the experience of interaction with the dependability units of customer companies.

An undeniable advantage of dependability engineering consists in the potential development of new methods in the process of dependability estimation of released products, implementation of plans for optimization of calculations and failure data classification. However, this potential may be thwarted due to the above factors, i.e.:

- absence of significant authority and competences in decision-making;
- poorly established interaction between the dependability unit and other business units (Fig. 3), which makes it impossible to coordinate dependability improvement measures;
- insufficiency of the interdisciplinary approach to the company-wide process organization in terms of dependability. In other words, a dependability engineer is assigned the role of primarily a design engineer, maintenance service engineer, IT specialist, etc., rather than functions associated with the calculation and analysis of technical system dependability.

The outlined approach to the organization of the dependability service is to clarify the role of dependability at all lifecycle stages to the top and project managers of machine-building companies. It must be understood that mistakes at early stages of dependability unit establishment, misunderstanding of the purpose and interaction between business units may cause financial losses. On the other hand, correct understanding of the functionality of the dependability service enables an efficient use of a company’s resources.

References

[1] Berdichevsky B.E., editor. [Dependability handbook in 3 volumes. Volume 3]. Moscow: Mir; 1970. (in Russ.)

[2] Shishmariov V.Yu. [Dependability of technical systems]. Moscow: Academia; 2010. (in Russ.)

[3] Kogge Yu.K., Maysky R.A. [Foundations of dependability of aviation equipment]. Moscow: Mashinostroyenie; 1993. (in Russ.)

[4] Pronikov A.S. [Dependability of machines]. Moscow: Mashinostroyenie; 1978. (in Russ.)

[5] lloyd D., Lipov M. Reliability: management, methods and mathematics. Moscow: Sovetskoye radio; 1964.

[6] GOST R 51901.3-2007 Risk management. Guidelines for dependability management. Moscow: Standartinform; 2008. (in Russ.)

[7] Ebeling C. An introduction to reliability and maintainability engineering. McGraw-Hill; 1997.

[8] Wessels W., Sillivant D. Affordable reliability engineering. Life-Circle Cost analysis for sustainability and logistical support. CRC Press; 2015.

[9] Van Valkenburg M. Reference Data for Engineers: Radio, Electronics, Computers and Communications. Newnes; 2002.

[10] Belousova M.V., Bulatov V.V. [Automation of claim data processing in machine-building companies]. Proceedings of the XIV International Conference on electromechanics and Robotics “Zavalishin’s Readings ER(ZR)-2020”. SUAI; 2019. (in Russ.)

[11] [Dependability of engineering products. A practical guide for standardization, validation and assurance. Moscow: Izdatelstvo standartov; 1990. (in Russ.)

About the authors

Maria V. Belousova, post-graduate student, Department of Modeling of Economic Systems, Saint Petersburg State University, Russian Federation, Saint Petersburg, e-mail: 27bmw1993@mail.ru.

Vitaly V. Bulatov, Candidate of Engineering, Senior Lecturer in Electromechanics and Robotics, Saint Petersburg State University of Aerospace Instrumentation, Russian Federation, Saint Petersburg, e-mail: bulatov-vitaly@yandex.ru.

The authors' contribution

Belousova M.V. Developed the structure of the dependability service, analyzed the process of interaction between the dependability service and the maintenance service and examined the personnel-related matters; reviewed the Russian experience of organization of dependability services in companies, summed up the primary dependability functions in a company and potential for future development.

Bulatov V.V. Analyzed the state of the art of the problem under consideration, reviewed the foreign experience of organization of dependability services in companies, proposed an organizational structure of the dependability service, described the interaction between the dependability service and other business units of a company.

Calculation of an SPTA set using the Dialog computer simulation system (Part 1. General provisions for the calculation of an SPTA set)

Boris A. Dolgopolov[1]*, Yuri G. Zayko[1], Viktor A. Mikhailov, Alexander V. Trakhtomirov
[1]RC Module, Russian Federation, Moscow, [2]NPP AVT, Ukraine, Kharkov
** dolgopolov@module.ru*

Boris A. Dolgopolov

Yuri G. Zayko

Viktor A. Mikhailov

Alexander V. Trakhtomirov

Abstract. *The paper describes the design concept of the DIALOG simulation software suite (SSS) intended for calculating the dependability indicators of electronic systems (ES) of random configuration, as well as solving problems associated with assuring the functional dependability of such systems. The DIALOG SSS employs a specially designed DIALOG-SINTEZ technology that enables automatic synthesis of event simulation models in the form of programs in the selected programming language. In DIALOG SSS, the input data include: system composition in the form of a combination of conventional blocks; criteria of failure event occurrence and repairs; random value parameters (failures of system components in various modes of operation, SPTA requests, etc.); stages of system operation and types of repairs; list of calculated indicators. For the purpose of ensuring the required indicators, the simulation models undergo statistical testing under modified indicators of random values in each new test. Based on the accumulated results of all the performed tests the required indicators are calculated. The DIALOG SSS consists of four components: DIALOG-NRS is intended for the calculation of dependability indicators of non-repairable redundant systems; DIALOG-RRS is intended for the calculation of dependability indicators of repairable redundant systems, as well as the number of and cost of warranty repairs; DIALOG-ZIP-NS is intended for SPTA sets calculation for simple non-redundant systems; DIALOG-ZIP-RS is intended for SPTA sets calculation for any redundant systems. SPTA set calculation is normally done using standard procedures described in regulatory documents. In solving the direct problem of optimal SPTA set calculation, the input data includes the required value of one of the two SPTA sufficiency indicators (SI) and type of costs that are to be optimized (minimized) in order to achieve the target values of SI. In solving the inverse problem of optimal SPTA set calculation, it is required to ensure the specified costs of the initial SPTA supply. As the SPTA supply SI, the mean spare parts (SP) supply delay time out of SPTA $t_{d.SPTA}$ and SPTA availability coefficient $C_{a.SPTA}$ are used. SPTA optimization using the DIALOG-ZIP SSS allows improving user options through the following additional characteristics: SPTA SP failure logging; optimization of SP count and accounting for the their characteristic features for the purpose of SP emergency delivery (ED); capability to use products with any type of redundancy; when using SPTA-G group set, capability to include differently-structured products into ESs. The paper sets forth the structure diagram of the DIALOG SSS programs interaction, that implies three modes of operation of the simulation model: SI calculation for specific SPTA contents; calculation of preliminary SPTA supply before the beginning of optimization; calculation of optimal SPTA set. The authors examine the matters related to the selection of the required number and duration of simulation model testing.*

Keywords: *simulation, SPTA set, SPTA sufficiency indicators, methods of calculating and estimating SPTA indicators.*

For citation: *Dolgopolov B.A., Zayko Yu.G., Mikhailov V.A., Trakhtomirov A.V. Calculation of an SPTA set using the Dialog computer simulation system (Part 1. General provisions for the calculation of an SPTA set). Dependability. 2020;1: 32-38. https://doi.org/10.21683/1729-2646-2020-20-1-32-38*

Received on: *06.12.2019* / **Revised on:** *17.02.2020* / **For printing:** *20.03.2020.*

DIALOG simulation software suite (SSS)

As of late, simulation has become a widely used tool for researching the behaviour and identifying various characteristics of ESs [1], [2].

The DIALOG SSS is intended for calculating the dependability indicators of ESs of any configuration, as well as solving problems associated with assuring their functional dependability. The indicators are calculated using simulation models.

The development of such models has the following distinctive characteristics: the model is to accurately reflect the details of a system's behaviour when affected by failures, in the course of repairs, under control inputs, etc. That can be achieved through universal high-level languages [4] and development of event-oriented models [3]. However, developing such models is associated with significant costs and is time-consuming.

In order to solve this problem, the DIALOG SSS employs a specially designed DIALOG-SINTEZ technology that – based on the description of the simulated system – enables automatic synthesis of event simulation models in the form of program source code in the selected programming language.

The development of simulation models using this process is based on the following properties of the considered systems:

– if a system's behaviour, when affected by failures of its components, is determined only by its composition, connections between components and criteria of failure occurrence, the structure of event models and their fragments for systems with various configurations can be made identical;

– the operating diagram of such a system's dependability can be presented as a combination of conventional blocks, the number of the types of which is limited and sufficient for describing the system.

That will allow creating a common foundation for all models of the selected type, and the input data that defines the configuration and specificity of each system's behaviour can be in the form of modifications or additions to the model foundation.

DIALOG-SINTEZ uses the following tools:

– a template that is a set of model fragments in the selected programming language;

– programs for preparation of input data saved as text files;

– simulation model synthesis program that transforms the text files that describe the system into model fragments and integrates them with the template. The result is an event simulation model in the original programming language. In DIALOG, Fortran and a library of specialized subprograms are used for that purpose.

The event-oriented nature of the synthesized models along with the use of a universal programming language allows reproducing a system's behaviour with any level of accuracy, while automatic synthesis makes model creation several times faster and simpler by doing away with the stage of programming. The time taken to create a model is primarily defined by the time of input data preparation.

Below are the input data used for synthesis in the DIALOG SSS:

– system composition in the form of a combination of conventional blocks;

– criteria of failure and repair occurrence;

– random value parameters, i.e. system component failures in various modes, requests to SPTA, etc.;

– stages of system operation and types of repairs;

– list of calculated indicators.

For the purpose of ensuring the required indicators, the simulation models undergo statistical testing under modified random values in each new test. Based on the accumulated results of all the performed tests, the required indicators are calculated.

The DIALOG SSS consists of four components:

– Part 1. DIALOG-NRS is intended for the calculation of dependability indicators of non-repairable redundant systems;

– Part 2. DIALOG-RRS is intended for the calculation of dependability indicators of repairable redundant systems, as well as the nu mber of and cost of warranty repairs;

– Part 3. DIALOG-ZIP-NS is intended for STPA sets calculation for simple non-redundant systems;

– Part 4. DIALOG-ZIP-RS is intended for STPA sets calculation for any redundant systems.

The DIALOG-NRS SSS allows identifying the following dependability indicators:

a) probability of no-failure (PNF) within the specified time t, $R(t)$;

b) mean time to failure, T_f;

c) gamma-percentile time to failure with specified probability γ, T_γ;

d) ES failure rate at the end of the specified period of time t, $\lambda(t)$;

e) failure rate at the end of the specified period of time t, $a(t)$;

f) data for construction of the graph of PNF as the function of time;

g) data for construction of the graph of failure rate as the function of time;

h) data for construction of the graph of failure rate as the function of time.

The above dependability indicators were defined in [5].

The structure and performance data of the DIALOG-NRS SSS are described in [2].

The DIALOG-RRS SSS allows identifying the following dependability indicators of repairable ES and performs functions associated with ES operational dependability:

a) mean time between failures, T_{mn};

b) mean failure rate at the end of the specified period of time t, $w(t)$;

c) cumulative failure rate at the end of the specified period of time t, $w_c(t)$;

d) data for construction of the graph of mean failure rate as the function of time;

e) data for construction of the graph of cumulative failure rate as the function of time;

f) number of warranty repairs at the specified stages of ES operation within the specified time t;

g) cost of warranty repairs within the specified time t that included one or several stages of ES operation.

The DIALOG-ZIP SSS is intended for calculating the optimal SPTA set and its characteristics that primarily include two sufficiency indicators (SI):

- SPTA availability coefficient $C_{\text{a.SPTA}}$;
- mean spare parts (SP) supply delay time by an SPTA set Δt_{SPTA}.

In solving the direct problem of SPTA set optimization, the input data includes the required SI value ($C^{(\text{rq})}_{\text{aSPTA}}$ or $\Delta t^{\text{rq}}_{\text{SPTA}}$) and type of costs that are to be optimized (minimized) in order to achieve the target values of SI.

In solving the inverse problem, the input data include the cost limitation $C^{\text{lmt}}_{\Sigma\text{SPTA}}$ and specified SI ($C^{(\text{rq})}_{\text{aSPTA}}$ or $\Delta t^{\text{rq}}_{\text{SPTA}}$) that is to be optimized under the given cost limitation.

The DIALOG-ZIP-NS SSS allows calculating an optimal SPTA set and its characteristics for simple non-redundant products. For that purpose, within the SSS, a model of the SPTA structure is created, the input data for the model's operation being the product components' characteristics.

The DIALOG-ZIP-RS SSS allows calculating an optimal SPTA set and its characteristics for any redundant products. For that purpose, two models are used in SSS: the repairable system model created using the programs of the DIALOG-RRS SSS, and the SPTA model created in the DIALOG-ZIP-RS SSS. Both simulation models created through synthesis have event-oriented identical structure elements and single programming language, Fortran, which enables their joint operation with a significant reduction of program execution time as compared to other languages.

A product's failure flow to SPTA is generated by the system model. It can have any form and is defined by the structure of the redundant product and type of repairs at various stages of product operation. The failure flow can also vary in time as the redundant product degrades.

The DIALOG-ZIP-RS SSS can also be used for calculating STPA sets intended for non-redundant systems. However, if the product is a non-redundant system and the request to SPTA occurs immediately after the product's failure, due to the significantly lower labour intensity of input data preparation for SPTA set calculation the DIALOG-ZIP-NS SSS is used. In this case, model generation only requires the preparation of the SPTA structure description, while product failures are generated by a special program that is part of the DIALOG-ZIP-NS SSS.

The DIALOG-ZIP-NS and DIALOG-ZIP-RS are used for calculating SPTA sets of any structure:

– single SPTA sets (SPTF-S);
– group SPTA sets (SPTF-G);
– SPTA systems (SPTAS).

General provisions for SPTA set composition calculation

STPA set calculation is normally done using standard procedures described in regulatory documents [6-8].

In the general case, let us examine a product consisting of N_0 types of components (each i-th type of component can have k_i instances) and operating in cycles, when each repeating cycle with the duration of T_c consists of M stages with each j-th stage ($j = 1, \ldots, M$) having the duration of T_j and failure rate of the component of the i-th type of λ_{ij}.

The product's operating cycle includes stages of operation under various conditions, stages of inactivity, stages of maintenance, etc.

Then, the replacement rate of components of the i-th type is calculated according to formula

$$\Lambda_{si(\text{Cmp})} = k_i \cdot \left[\left(\sum_{j=1}^{M} T_j \cdot \lambda_{ij} \right) / T_c \right], \qquad (1)$$

where $\sum_{j=1}^{M} T_j = T_c$.

The input data per the product's components are entered into columns 1 and 2 of Table 1, the input data that are part of formula (1) are entered into columns 3 to 6 of Table 1 (in

Table 1. Calculation of replacement rate $\Lambda_{\text{R}i\text{(Cmp)}}$ for product components

Component number, i	Component name	Stage number, j	Duration of stage, T_j, h	k_i, pcs	$\lambda_{ij} \times 10^6$, 1/h	$\Lambda_{\text{R}i\text{(Cmp)}} \times 10^6$, 1/h
1	2	3	4	5	6	7
1		1 … M	+ … +	+ … +	+ … +	+ …
…	…	…	…	…	…	…
N_0		1 … M	+ … +	+ … +	+ … +	+ …

columns 4 to 6, symbols «+» are given instead of specific numbers). The value $\Lambda_{ri(\mathrm{Cmp})}$ for each *i*-th type of component calculated according to formula (1) is entered into column 7 of Table 1.

Four primary SPTA set replenishment strategies are normally used:

– scheduled replenishment (conventional index $\alpha_i = 1$);

– scheduled replenishment with emergency deliveries (ED) ($\alpha_i = 2$);

– continuous replenishment ($\alpha_i = 3$);

– replenishment to the level of emergency stock ($\alpha_i = 4$).

Beside the type (index α_i), each replenishment strategy is characterized by one (T_i) or two (T_i and β_i) numerical parameters with values:

– if $\alpha_i = 1$ $T_i = T_{\mathrm{rpl}i}$ is the period of scheduled replenishment of *i* supply, if $\beta_i = 0$, the parameter is not used;

– if $\alpha_i = 2$ $T_i = T_{ri}$ is the period of scheduled replenishment of *i* supply, $\beta_i = \mathrm{T}_{\mathrm{ed}i}$ is the time of ED of *i*-type SP;

– if $\alpha_i = 3$ $T_i = T_{\mathrm{d}i}$ ($T_{\mathrm{rpr}i}$) is the time of delivery (repair) of *i*-type SP, if $\beta_i = 0$, the parameter is not used;

– if $\alpha_i = 4$ $T_i = T_{\mathrm{d}i}$ is the time of delivery of *i*-type SP, $\beta_i = m_i$ is the emergency supply of the *i* type.

Each individual stock within an SPTA set can, in general, be replenished according to an individual strategy that differs from the others both in type (α_i), and the values of numerical parameters (T_i and β_i).

In case of scheduled replenishment with ED, the following ED data must be additionally specified:

– level of supply replenishment;

– itemized replenishment list;

– ED request time: in case of supply failure or use of the last SP (prefailure).

The SI of an SPTA set $C^{(\mathrm{rq})}_{\mathrm{aSPTA}}$ or $\Delta t^{\mathrm{rq}}_{\mathrm{SPTA}}$ is defined by the corresponding SI of each *i*-th supply Δt_{si} and C_{ai} ($i = 1 \ldots N_{\mathrm{o}}$) using the following formulas [8]:

$$\Delta t_{\mathrm{s.SPTA}} = \frac{\sum_{i=1}^{No} \Lambda_{si(\mathrm{Cmp})} \cdot \Delta t_{si}}{\sum_{i=1}^{No} \Lambda_{si(\mathrm{Cmp})}}; \qquad (2)$$

$$C_{\mathrm{s.SPTA}} = \prod_{i=1}^{No} C_{ai}. \qquad (3)$$

The theoretical formulas for calculation of the SI of Δt_{si} and C_{ai} derived using mathematical models proposed in [9] are shown in Table 2.

The following designations are used in the table:

A_i, average number of requests for *i*-th type SP received by the SPTA set over the time T_i

$A_i = k_i \cdot \Lambda_{si(\mathrm{Cmp})} \cdot T_i$; (4)

L_i, initial supply of the *i*-th type in SPTA;

m_i, minimum level of supply of the *i*-th type when replenishing to level m_i.

GOST 27.507-2015 [8, annex A] cites the results of SPTA-S set optimization per the required SI $C^{(\mathrm{rq})}_{\mathrm{aSPTA\text{-}S}} \geq 0.95$ for the Pamir-1 ES that consists of $N_{\mathrm{o}} = 30$ components. The optimization was performed using standard procedures and ROKZERSIZ and ASONIKA-K-ZIP software suites.

SPTA optimization using the DIALOG-ZIP SSS allows improving user options as compared to the above software suites through the following additional characteristics:

– SPTA SP failure logging;

– optimization of SP count and accounting for their characteristic features for purposed of ED if a replenishment strategy with $\alpha_i = 2$ is used;

– capability to use components with any type of redundancy (e.g. any type of redundancy from [2]);

– capability to include differently-structured products into ESs, when working with a SPTA-G group set.

The list of primary methods used while estimating the indicators and calculating the primary types of SPTA are shown in Table 3.

Structure of the DIALOG-ZIP-RS SSS

The DIALOG SSS includes the following parts intended for SPTA sets calculation:

– part 3. DIALOG-ZIP-NS for STPA sets calculation for simple non-redundant systems;

Table 2. SI calculation formula for i-th type supply in SPTA-S set

Replenishment strategy	Sufficiency indicators
Scheduled replenishment ($\alpha_i = 1$) $T_i = T_{\mathrm{R}i}$	$\Delta t_{si} = T_{ni}\left[\exp\left(-A_i\right)\cdot\sum_{\gamma=L_i+2}^{\infty}\frac{A_i^{\gamma-2}}{\gamma!}\left(\gamma-L_i-1\right)\right],\ C_{ai} = 1-\exp\left(-A_i\right)\cdot\sum_{\gamma=L_i+2}^{\infty}\frac{A_i^{\gamma-1}}{\gamma!}\left(\gamma-L_i-1\right)$
Scheduled replenishment with ED ($\alpha_i = 2$) $T_i = T_{\mathrm{R}i}$	$\Delta t_{si} = T_{\mathrm{ED}i}\left[\exp(-A_i)\cdot\sum_{\upsilon=1}^{\infty}\sum_{\gamma=\upsilon\cdot(L_i+1)}^{\infty}\frac{A_i^{\gamma-1}}{\gamma!}\right],\ \Delta t_{si} = 1-\frac{T_{\mathrm{ED}i}}{T_{ni}}\left[\exp(A_i)\cdot\sum_{\upsilon=1}^{\infty}\sum_{\gamma=\upsilon\cdot(L_i+1)}^{\infty}\frac{A_i^{\gamma}}{\gamma!}\right]$
Continuous replenishment ($\alpha_i = 1$) $T_i = T_{\mathrm{D}i}$	$\Delta t_{si} = T_{\mathrm{D}i}\cdot A_i^{L_i}\left[\left(L_i+1\right)!\sum_{\gamma=0}^{L_i+1}\frac{A_i^{\gamma}}{\gamma!}\right]^{-1},\ C_{si} = 1-A_i^{L_i+1}\left[\left(L_i+1\right)!\sum_{\gamma=0}^{L_i+1}\frac{A_i^{\gamma}}{\gamma!}\right]^{-1}$
Replenishment to level m_i ($\alpha_i = 1$) $T_i = T_{\mathrm{D}i}$	$\Delta t_{si} = T_{\mathrm{D}i}\cdot A_i^{m_i+1}\left[A_i^{m_i+1}+\left(L_i-m_i\right)\left(1+A_i\right)^{m_i+1}\right]^{-1},\ C_{ai} = 1-A_i^{m_i+2}\left[A_i^{m_i+2}+\left(L_i-m_i\right)\left(1+A_i\right)^{m_i+1}\right]^{-1}$

Table 3. List of methods of calculating and estimating SPTA indicators

№	Name of method	Designation and assignment of a method for each SPTA type		
		a) SPTA-S	b) SPTA-G	c) SPTAS
1	$A_{F.SPTA}$-based supply estimation	1a. Estimation of $A_{F.SPTA-S}$ value	—	1b. Estimation of $A_{F.SPTAS}$ value
2	$\Delta t_{S\cdot SPTA}$-based supply estimation	2a. Estimation of $\Delta t_{S\cdot SPTA-S}$ value	2b. Estimation of $\Delta t_{S\cdot SPTA-S}$ value	2b. Estimation of $\Delta t_{S\cdot SPTAS}$ value
3	Supply estimation based on the criterion of SPTA costs	3a. Estimation of C_{SPTA-O} value	3b. Estimation of C_{SPTA-G} value	3c. Estimation of C_{SPTAS} value
4	$A_{F.SPTA}$-based calculation of optimal supply	4a. Minimization of SPTA-S costs if the $A_{F.SPTA-S}$ requirements are met	—	4c. Minimization of SPTAS costs if the $A_{F.SPTAS}$ requirements are met
5	$\Delta t_{S\cdot SPTA}$-based calculation of optimal supply	5a. Minimization of SPTA-S costs if the $\Delta t_{S\cdot TPA-S}$ requirements are met	5b. Minimization of SPTA-G costs if the $\Delta t_{S\cdot TPA-G}$ requirements are met	5c. Minimization of SPTA-G costs if the $\Delta t_{S\cdot SPTAS}$ requirements are met
6	C_{SPTA}-based calculation of optimal supply	6a. SI optimization under the specified costs of initial SPTA-S supply	6b. SI optimization under the specified costs of initial SPTA-G supply	6c. SI optimization under the specified costs of initial SPTAS supply

– part 4. DIALOG-ZIP-RS for STPA sets calculation for any redundant systems.

This paper dwells on the calculation of the SPTF-S set using the DIALOG SSS.

The calculation method is based on the replacement of live tests of a "product – SPTA set" system with an imitation using event models. The models are submitted to statistical testing. For each test, the number of successful and failed requests to the SPTA set, SP delivery delays and other indicators are calculated. The following actions follow:

– summation of all requests to each supply within the specified number of tests;

– summation of all successful requests to a supply within the specified number of tests;

– summation of SP delivery delays;

– identification of the average numbers of requests to the supply, successful requests, delays of delivery, etc.;

– based on the results, the required indicators are calculated.

DIALOG-ZIP-RS creates a model that simulates the operation of the product, the SPTA and their interaction.

Such model can be used both for non-redundant and redundant products with any type of redundancy, in combination with any type of repairs at various stages of system operation.

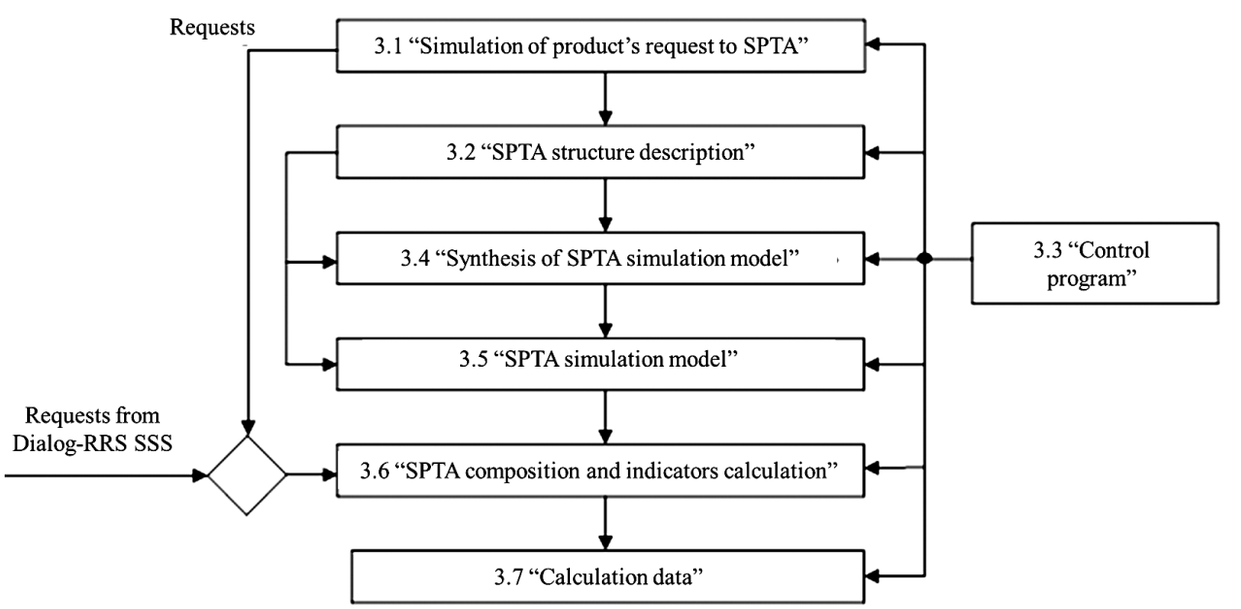


Figure 1 – Structure diagram of the DIALOG-ZIP-RS SSS programs interaction.

The SSS allows defining an optimal SPTA composition and obtaining the following indicators for SPTAs with any structure for redundant and non-redundant products with any types of repairs:

– availability coefficient and other indicators accounting for own failures of the SPs that are part of the SPTA;

– optimal SPTA composition by criterion of minimal cost under the given SI;

– optimal SPTA composition under limited given costs.

If SPTA requests are used that have been obtained through the generation of the simplest failure flow, such indicators can be obtained only for a non-redundant product and emergency full repairs.

The structure diagram of DIALOG-ZIP-RS SSS programs interaction is shown in Fig. 1.

In terms of their functionality, the DIALOG-ZIP-RS SSS programs are divided into three sections.

Section A. Input data.

Program 3.1 "Simulation of product's request to SPTA".

This program is intended for generating requests from product to SPTA set in case of non-redundant products. In case redundant products are employed, DIALOG-RRS SSS information is used.

The program creates random sequences of requests to each supply for a period of time equal to the planned simulation time. The time between requests to the supply is a discrete random value with an exponential distribution law and average value equal to the mean time between components failures.

Request times are generated using a subprogram that employs the logarithmic method for obtaining random discrete sequences with an exponential distribution law [10].

An example of a program that uses that method is shown in [3].

Program 3.2 "SPTA structure description".

The program serves to describe SPTA sets with any structure.

The obtained data are used in the process of automatic synthesis of the SPTA simulation model.

The program is also used for generating input data for the calculation of sufficiency indicators and SPTA set optimization. The data is represented in table form and is saved as a text file.

This data is further used in Program 3.4 "Synthesis of SPTA simulation model" and Program 3.5 "SPTA simulation model" for the purpose of calculations and optimization.

Section B. Indicator calculation and optimization.

Program 3.3 "Control program".

This program serves to run the DIALOG-ZIP-RS SSS and program execution control. The supervisor program obtains information on the results of other programs' operation, runs programs, sets operating modes of the simulation model, modes of information output and saving in Program 3.7 "Calculation data".

The programs can be executed automatically or with an operator's involvement. Upon his/her command the system's operation can be interrupted and later resumed. Programs' operating modes can be changed at launch, individual programs can be run repeatedly.

Program 3.4 "Synthesis of SPTA simulation model".

Using the data obtained from Program 3.2 "SPTA structure description" and utility files, the SPTA event simulation model is generated in the Fortran language with the parameters specified in the description of the SPTA structure. After translation, the model's executive file is generated.

Program 3.5 "SPTA simulation model".

The synthesized model is of the event-oriented type and has the form of source code and executable file. The model can be used on its own out of the DIALOG-ZIP SSS.

The model's operating principle is based on the simulation of the following sequence of events within the SPTA over the simulation time:

– requests from products for replacement of failed components;

– SPTA replenishment;

– requests for SP delivery;

– failure of SPs in SPTA.

As an event occurs, actions associated with the respective type of event are performed: supply contents are modified and subject to certain conditions SPTA resupply times are planned.

For the purpose of enabling event-specific actions special subprograms are used, where the supply, for which the actions are intended, is specified as a parameter.

Three operating modes are provided for the simulation model that are to be set by the supervisor program:

1. Calculation of indicators. In this mode, SI for the existing SPTA composition are calculated.

2. Calculation of zero supply. The initial supplies before optimization are calculated.

3. Calculation of optimal SPTA composition.

After the mode has been set, the simulation model is subjected to testing.

The parameters obtained from Program 3.2 "SPTA structure description" are used. The input data for the tests consists of the requests received from Program 3.1 "Simulation of product's request to SPTA".

Program 3.6 "SPTA composition and indicators calculation".

By processing the test results the program calculates SI or, in the optimization mode, along with the indicators data on the optimal SPTA composition are processed and displayed.

Section C Calculation data.

Program 3.7 "Calculation data".

The program serves to save the calculation data for each stage and total system operation time, as well as request flows and SPTA structure descriptions.

Simulation model operation requires the following characteristic to be defined:

- duration of a single test (simulation time);
- number of simulation model tests.

The duration of a single test in simulation time units is equal to the duration of the chosen period of time of "product – SPTA set" system operation, for which SPTA indicators are calculated. The duration of this period is equal to the simulation time that is defined in the SPTA structure description and can be changed when the model is launched.

The recommended minimal number of tests of model $n_{test}^{(\min)}$ is calculated when the SPTA set description is developed. The calculation is done based on the assumption that in order to ensure acceptable accuracy of calculation for components with minimal failure rate the number of the occurred failures over the whole time of testing must be at least 1000.

References

[1] Dykina T.K., Zayko Yu.G., Ivanov V.N. et al. [Design principles of a dialog simulation system for CS dependability research]. *Problemy upravleniya dvizheniem i navigatsii*. 1989;24:29-36. (in Russ.)

[2] Zayko Y.G., Iskandarova L.N., Trakhtomirov A.V. Simulation model to calculate the indices of reliability of redundant radio electronic systems. *Dependability*. 2016;16(3):8-17. (In Russ.)

[3] MacDougall M.H., Dietmeyer D., Duley J.R. Digital system design automation: languages, simulation and data base. Moscow: Mir; 1979.

[4] Schmidt B. GPSS-Fortran. Version II. Einfuhrung in die Simulation diskreter Systeme mit Hilfe eines FORTRAN-Programmpaketes. Berlin Heidelberg: Springer-Verlag; 1978.

[5] Polovko AM. [Fundamentals of the dependability theory]. Moscow: Nauka; 1964. (in Russ.)

[6] [RD V 319.01.19-98. Comprehensive quality control system. Military-purpose hardware, instruments, devices and equipment. Methods of estimation and calculation of supplies in SPTA sets. Brought into force on 15.06.1999]. Moscow: Technical committee for military standardization no. 319; 1998. (in Russ.)

[7] [GOST RV 27.3.03-2005. Dependability of military hardware. Estimation and calculation of supplies in SPTA sets. Brought into force on 01.01.2006]. Moscow: Standartinform; 2005. (in Russ.)

[8] GOST 27.005-97 Reliability in technique. Spare parts, tools and accessories. Evaluation and calculation of reserves. Brought into force on 03.01.2017. Moscow: Standartinform: 2016. (in Russ.)

[9] Golovin I.N., Chuvarygin B.V., Shura-Bura A.E. [Calculation and optimization of spare part kits of radioelectronic systems]. Moscow: Radio i sviaz; 1984. (in Russ.)

[10] Knuth D.E. The art of computer programming. Vol. 2. Seminumerical algorithms. Moscow: Mir; 1977.

About the authors

Boris A. Dolgopolov, Lead Engineer, RC Modul, Russian Federation, Moscow, e-mail: dolgopolov@module.ru

Yuri G. Zayko, Candidate of Engineering, Associate Professor, Senior Researcher, Head of Unit, RC Modul, Russian Federation, Moscow, e-mail: y.zayko@module.ru

Viktor A. Mikhailov, Doctor of Engineering, Deputy Director General for Onboard Equipment Development, RC Modul, Russian Federation, Moscow, e-mail: vmikh@module.ru

Alexander V. Trakhtomirov, Director, NPP AVT, Ukraine, Kharkov, e-mail: vehxbr39@ukr.net

The authors' contribution

Boris. A. Dolgopolov. Analysis of various aspects of optimal "product – SPTA" system creation, formalization of findings.

Yuri G. Zayko. General description of the DIALOG SSS. Analysis and definition of the requirements for the design of an optimal SPTA system, derivation of primary formulas, description of various options for SPTA design and use recommendations.

Viktor A. Mikhailov. General supervision of problem definition for designing an optimal system for RES maintenance with SPTA and selection of requirements for the design of an optimal SPTA system.

Alexander V. Trakhtomirov. Development of simulation, implementation and processing of results that allow assessing the operation of the "product – SPTA set" system. Description of the DIALOG-ZIP-RS SSS function.

The effect of gender differences on the reliability of aptitude screening of aviation specialists

Olga V. Arinicheva[1]*, Tatiana V. Ziuba[1], Alexey B. Malishevsky[1]
[1] *Saint Petersburg State University of Civil Aviation, Russian Federation, Saint Petersburg*
* *2067535@mail.ru*


Olga V. Arinicheva


Tatiana V. Ziuba


Alexey B. Malishevsky

Abstract. The Aim. *This paper examines the problem of reliability of aptitude screening currently in place in commercial aviation in terms of its indiscriminate applicability to males and females. The task consisted in evaluating some professionally important qualities in males and females, who have successfully completed aptitude screening while being admitted to the aviation school, and identify the presence or absence of differences between the obtained results. For that purpose, a research was conducted that involved 60 third-year traffic controller students of the Saint Petersburg State University of Civil Aviation (35 males and 25 females).* **Methods.** *The psychodiagnostic method included the Prognoz-1 and Prognoz-2 stress tolerance evaluation forms developed in the S.M. Kirov Military Medical Academy, H.J. Eysenck intellectual development test, A. Buss and A. Durkee hostility assessment forms. The authors' earlier findings were also used. Statistical processing was performed using correlation analysis and Pearson's chi-squared test.* **Results.** *The analysis of psychodiagnostic findings has shown the absence of positive differences in the intellectual development of males and females in the observed group. In general, the intelligence of the study participants was sufficiently high (121.17 average IQ for males and 123.04 for females). The assessment of the stress tolerance of the surveyed group using two different variants of the Prognoz forms also has not identified any significant differences between males and females (stress tolerance of females is somewhat lower, than that of males, but the identified difference is obviously not crucial). However, both among males (1 person) and females (1 person) participants were identified, for whom the prediction per both diagnostic method was "unfavourable". Positive differences between the examined males and females were identified in terms of tendency towards physical aggression (A. Buss and A. Durkee test).* **Conclusions.** *The psychodiagnostic method used as part of this work have not identified fundamental gender differences. An exception is the tendency towards physical aggression. In females this indicator is clearly lower, though there are girls who display high aggressiveness. Most experimental subjects demonstrated high stress tolerance and sufficiently high level of intellectual development. And while the examined group does not display clear differences in IQ (there are reasons to believe that the larger is the surveyed group the less significant are the positive differences between males and females in terms of intellectual development), however, the trend of female aviation specialists having overall higher IQ can be observed. The research must continue, extending the range of assessment methods, including alternative approaches that do not involve personality inventories, while simultaneously evaluating the extent of professionally important psychological qualities of aviation specialists, yet not with respect to gender, but in accordance with a candidate's identified gender type.*

Keywords: *aptitude screening, gender differences, intelligent, stress tolerance, aggressiveness.*

For citation: *Arinicheva OV, Malishevsky AV. The effect of gender differences on the reliability of aptitude screening of aviation specialists. Dependability. 2020;1: 39-46. https://doi.org/10.21683/1729-2646-2020-20-1-39-46*

Received on: 06.11.2019 / **Revised on:** 24.01.2020 / **For printing:** 20.03.2020

Introduction. One of the ways of reducing the destabilizing effect of the human factor (HF) on flight safety [1, 2] is competent organization of the aptitude screening (AS) of aviation specialists [3], which, as early as at the first stage, will allow identifying those who for some reason are unsuitable for work in aviation. That is especially true for operators, i.e. pilots and air traffic (AT) controllers.

Indeed, in emergency situations pilots display various behaviours. In one case [4] we can observe accurate, competent actions in a truly dire situation, in others [5-8] we can see panic and actions that cause catastrophic consequences.

N.V. Yakimovich, a well-known aviation psychologist, on the RRJ-95B RA-89098 crash: "After a destructive landing and onset of a massive fire that any second could cause an explosion onboard the aircraft, the pilots inevitably reached the final stage of stress and panicked. That is evidenced by the fact that upon landing the pilots stopped acting professionally and did not turn the engines off. Driven by the instinct of self-preservation, they rushed to save the passengers and their own lives. Human psyche is built upon natural laws and it is not always possible to overcome them. Therefore we cannot expect people to do the impossible, i.e. something they are unable to do while being in adverse mental states" [9]. We can of course agree with N.V. Yakimovich that we cannot ask people to do the impossible, but the fact remains. What is impossible for some people others can do. Damir Yusupov landed an airplane with failed engines on a corn field [4]. Certainly, some luck was at play, but the high professionalism and stress tolerance of the aircraft commander (ACC) are key. The report of the Interstate Aviation Committee (IAC) regarding the results of the An-148-100V RA-61704 crash [7] clearly states the following among the causes of the disaster: "individual psychological features of the pilots (for the ACC, reduced intellectual and behavioural agility, fixation on own point of view and inability (impossibility) to "hear" the hints of the second pilot; for the second pilot, disrupted rationality and sequence of actions), who in a stressful situation with inferior cockpit resource management came to the fore; loss of ACC operating capability in psychological terms (psychological incapacitation), which caused a complete loss of dimensional orientation and prevented due reaction to the hints and actions of the second pilot, namely after a PULL UP warning of EGPWS [7].

During the Boeing 737 disasters in Kazan [6] and Rostov-on-Don [8] the crews could not execute a go-around, even though the aircraft were in good working order. In both cases there was panic onboard. By contrast, while Tammie Jo Shults was piloting a similar Boeing 737 with a failed engine and decompressed cabin her voice did not even quiver. She successfully landed the damaged airplane [10]. In other words, all people are different in terms of their psychological resistance and other important psychological qualities. The AS aims to develop reliable selection criteria. If flight safety is indeed our primary goal, increasing AS reliability is certainly important and relevant.

Problem definition. The current Guidelines [3] that specified the procedure for aviation specialists AS is in fact an inferior version of the Soviet Guidelines [11]. The Report [12] explicitly states that some aspects specified in the Guidelines [11] were left out in the Guidelines [3]. The authors elaborated upon that issue in [2].

Another important aspect is that both the Guidelines [11] and, consequently the Guidelines [3], due to the industry situation of that time, were exclusively geared towards males. The authors analyzed a number of problems that has caused in [1].

The authors have absolutely no intention to question the fact that females can make great pilots. Not all of course, but not all males are able to be pilots either. As to the females who became outstanding pilots, beside the aforementioned Tammie Jo Shults, we can mention Amelia Mary Earhart and many prominent Soviet and Russian female pilots: L.V. Zvereva, V.S. Grizodubova, P.D. Osipenko, M.M. Raskova, M.L. Popovich, L.M. Ulanova, M.V. Popovich, S.E. Savitskaya, S.V. Kapanina and many others.

Another matter is whether AS for males is to differ from that for females. Common sense suggests that it should. At least for the reasons examined in [1]. But it is not all that simple. This paper aimed to examine some professionally important qualities in males and females and identify the differences (if any) in the obtained results.

Inputs and methods. A research of the effect of gender differences on the reliability of aptitude screening of aviation specialists involved 60 third-year students of the Faculty of Flight Operation of the Saint Petersburg State University of Civil Aviation (SPBGU GA) majoring in airspace management (ASM), i.e. future air traffic controllers. The group included 35 males and 25 females.

The used psychodiagnostic methods included:

- Prognoz-1 form for stress tolerance (ST) evaluation (N_1, ST in points) [13];
- Prognoz-2 form, also for ST evaluation (N_2, ST in points) [14];
- H.J. Eysenck test for intellectual development evaluation [15] (IQ, intelligence quotient);
- Buss-Durkee hostility inventory (for evaluation of A_P, physical aggression, A_{IA}, indirect aggression, A_{Ir}, irritation, A_N, negativism, A_R, resentment, A_S, suspicion, A_{VA}, verbal aggression and A_{SA}, self-aggression) [16];
- Thomas-Kilmann instrument (for identification of the mode of behaviour in a conflict: T_{CMPT}, competing, T_{CLBR}, collaborating, T_{CNPR}, compromising, T_{AVDN}, avoiding, T_{ACMD}, accommodating) [16];
- A. Assinger's test (for identifying levels of aggression, ε_{AA}) [16];
- V.I. Andreev's test (for identifying the proneness to conflict, $\sigma_{Andr.}$) [17];
- Cook-Medley scale (for identifying the levels of hostility γ_H, cynicism γ_C, aggression γ_A) [18].

Additionally, the analysis covered previously obtained data that were published by the authors in [19-22].

Table 1. Distribution of research participants in terms of intellectual development

Level of intellectual development		In general		Males		Females	
		ppl.	%	ppl.	%	ppl.	%
very low	70 > IQ	0	0	0	0	0	0
low	90 ≥ IQ ≥ 70	1	1.7	0	0	1	4.0
average	110 ≥ IQ > 90	13	21.7	8	22.9	5	20.0
high	130 ≥ IQ > 110	26	43.3	16	45.7	10	40.0
very high	IQ > 130	20	33.3	11	31.4	9	36.0

Table 2. Gender-based distribution of the intelligence quotient (IQ) in air traffic controller students (based on experimental data given in [27])

Air traffic controller students	IQ				
	very low	low	average	high	very high
	< 70	70-100	101-110	111-130	> 130
females	0	1	3	9	8
males	0	5	11	6	5

The findings were analyzed with the R programming language that is widely used as statistical software for data analysis and became a de-facto standard statistical program [23] (licensed under GNU GPL [24]). This work used correlation analysis methods [25] and Pearson's chi-squared test (χ^2) [25].

The research was conducted in accordance with primary bioethical rules [26] on a voluntary basis.

Results and discussion. The findings were not quite what was expected. Figure 1 and Table 1 show the distribution of research participants in terms of intellectual development. As it can be seen, the participants' intelligent is about the same.

The intellectual development of the examined participants is sufficiently high with the group's average IQ of 121.95. A the same time, the average IQ of males is 121.17, and that of females is 123.04. Positive differences were not identified (for the number of degrees of freedom $\nu = 2$ the empirical value χ^2_{emp} of Pearson's criterion [25] is lower than its critical value for level $p < 0.05$ $\chi^2_{emp} = 0.2095 < \chi^2_{0.05} = 5.991$).

If we compare the results of this study with those obtained by the authors earlier [22, 27, 28], we can observe a similar pattern, although some differences are present. Thus, another group of third-year SPBGU GA students majoring in ASM that took part in the experiment described in [27] showed similar results in the same test [15] (see Table 2): group's average IQ = 119.15, 115.00 and 124.48 for males and females respectively. Here, the differences between males and females proved to be significant ($\chi^2_{0.01} = 9.210 > \chi^2_{emp} = 7.8652 > \chi^2_{0.05} = 5.991$ for $\nu = 2$), but that is an exception rather than the norm.

Thus, [28] that cites data on 1294 SPBGU GA students in various majors who were surveyed using the Rudolf Amthauer test [29] examines the existence of differences in intellectual development of males and females. A the same time, the Pearson criterion helped identify clear differences

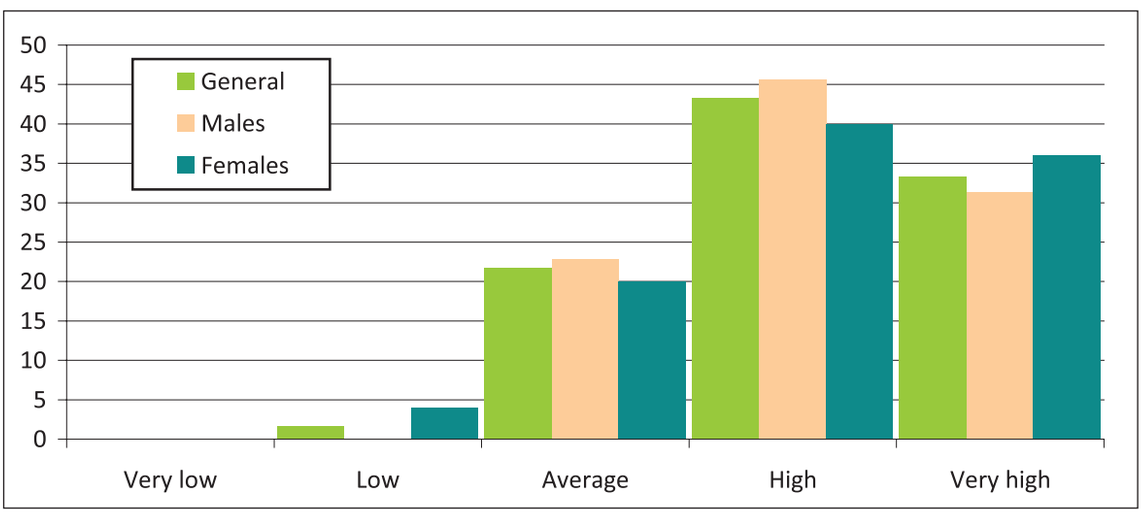


Figure 1. Distribution (%) of examined participants in terms of intellectual development (according to the Eysenck test)

Table 3. R. Amthauer test results of 1697 SPBGU GA students (for clarity, the distribution of intellectual development groups is shown in percentages) [22]

Students	IQ								Average score
	< 100	100-105	106-110	111-115	116-120	121-125	126-130	130 <	
Pilot students									
Males (245 ppl.)	4.49	7.36	11.02	21.63	26.12	16.73	11.02	1.63	114.74
Females (0 ppl.)	-	-	-	-	-	-	-	-	-
Air traffic control students									
Males (60 ppl.)	1.67	10.00	10.00	30.00	25.00	16.66	5.00	1.67	114.10
Females (25 ppl.)	-	-	8	16	24	40	12	-	118.08
Student technicians									
Males (371 ppl.)	2.43	2.96	6.47	28.84	29.38	21.56	6.74	1.62	115.73
Females (43 ppl.)	2.33	4.65	6.97	23.26	30.23	11.63	18.6	2.33	116.54
Transportation organization students									
Males (130 ppl.)	7.69	3.85	16.15	24.62	19.23	18.46	6.92	3.08	113.69
Females (125 ppl.)	4.00	4.80	8.80	21.60	30.40	21.60	8.00	0.80	115.17
Economics students									
Males (102 ppl.)	1.96	2.94	11.77	33.33	28.43	13.73	6.86	0.98	114.59
Females (330 ppl.)	1.52	3.03	11.21	28.78	32.12	17.58	4.55	1.21	114.97
Humanities students									
Males (44 ppl.)	-	-	6.82	45.45	22.73	22.73	2.27	-	115.41
Females (156 ppl.)	1.28	0.64	0.64	34.62	38.46	14.10	9.62	0.64	116.44
Law students									
Males (28 ppl.)	7.14	7.14	32.14	21.43	14.29	17.86	-	-	110.96
Females (38 ppl.)	13.16	13.16	13.16	39.47	13.16	5.26	2.63	-	109.08

in the case of air traffic controllers and air transportation organizers, while for engineering, humanities (Public Relations and Human Resources) and law students clear gender differences were not observed. It should be noted that the presence of positive differences in the sample of air traffic controllers appears to be more of a variance, as there were only 18 females in the sample with 50 males. As it follows from Table 3 that contains more complete data for this test from [22], for all categories except law students the IQ of females is somewhat higher.

Another important psychological quality of an operator is the stress tolerance.

In the experiment described in [27] all the participants had the ST not lower than acceptable (see Table 4), although the scatter is quite significant, i.e. from 3 to 10. (Normally, in the data obtained in SPBGU GA this indicator is within 4 to 8; greater deviations are rare. Estimate 3 is sufficiently low. That is the limit, when the prediction is still favourable for operator activities.) No reliable differences between the samples of males and females in terms of ST estimates (E_{ST}) were identified based on the Pearson criterion ($\chi^2_{ST} = 0.7385 < \chi^2_{0.05} = 5.991$ for $\nu = 2$).

In this study (see Table 5 and Figures 2 and 3) both the male and female samples included one participant with $E_{ST} = 1$,

Table 4. Gender-based distribution of ST estimates (E_{ST}) in experiment participants described in [27]

E_{ST}	1	2	3	4	5	6	7	8	9	10
females	0	0	1	3	3	5	4	3	1	1
males	0	0	0	3	3	8	8	3	1	1

Table 5. Gender-based distribution of ST estimates (E_{ST}) for this study's participants

E_{ST}	1	2	3	4	5	6	7	8	9	10
Prognoz-1										
females	1	0	2	2	10	3	3	1	2	1
males	1	0	1	1	6	8	10	4	2	2
Prognoz-2										
females	1	0	1	0	3	5	4	5	0	6
males	1	1	0	0	0	5	7	11	4	6

i.e. with unfavourable forecast. It is difficult to say whether that is the case or the result of incorrect test performance (the issues of testing with the use of personality inventories were identified by the authors in a number of papers, e.g. [1,

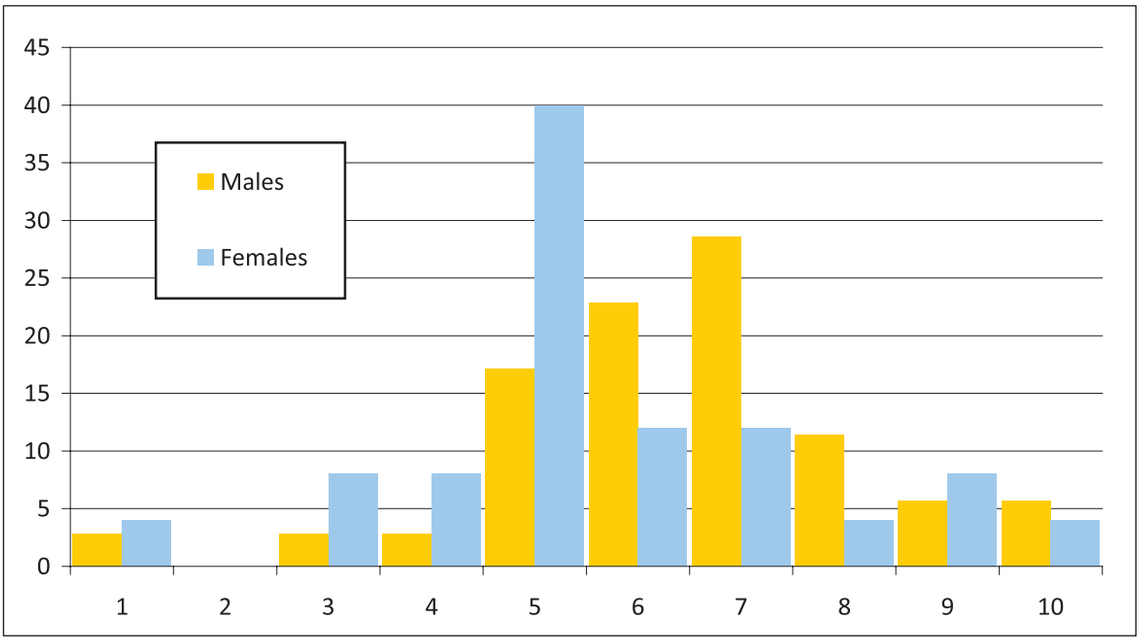


Figure 2. Distribution (%) of study participants by stress tolerance (E_{ST}, subject to the results of the Prognoz-1 form)

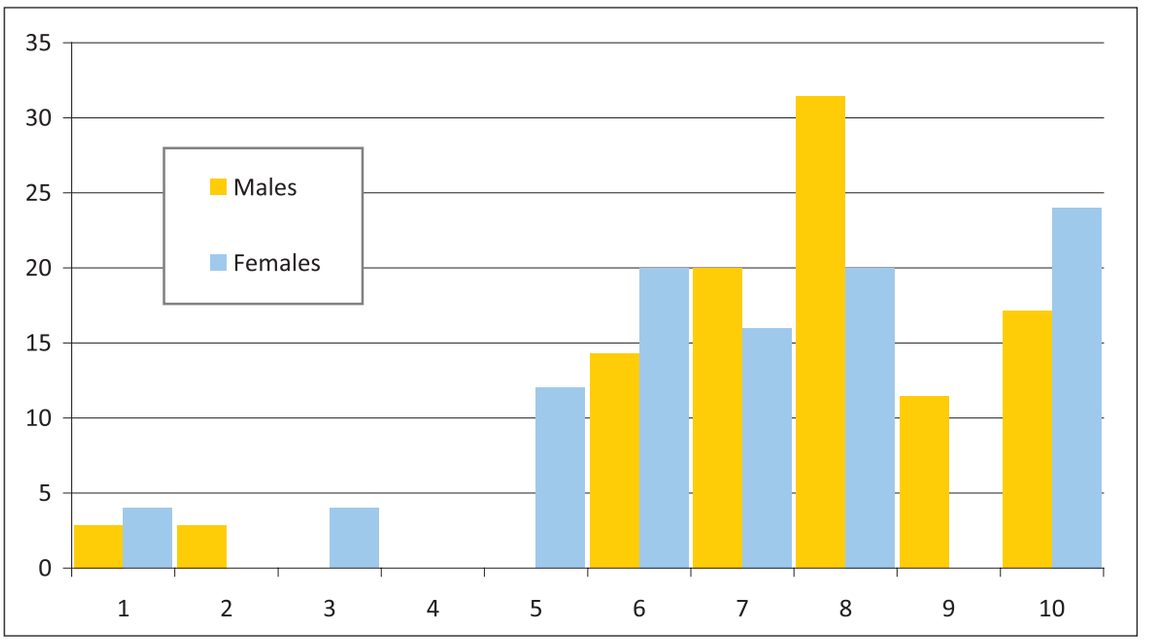


Figure 3. Distribution (%) of study participants by stress tolerance (E_{ST}, subject to the results of the Prognoz-2 form)

2, 20]), but the result is troubling. However, if we look at the big picture, the Prognoz-1 questionnaire produced the group-average result of $N_1 = 12.97$ ($N_1 = 11.89$ for males, $N_1 = 14.48$ for females), which corresponds to good ST ($E_{ST} = 6$). The Prognoz-2 questionnaire produced the group-average result of $N_2 = 15.08$ ($N_2 = 14.37$ for males, $N_2 = 16.08$ for females), which corresponds to high ST ($E_{ST} = 7$).

This study has also not identified positive differences by Pearson's criterion. The Prognoz-1 form produced the empirical Pearson's criterion of $\chi^2_{EMP} = 5.6327 < \chi^2_{0.05} = 5.991$ for $\nu = 2$. The Prognoz-2 form produced the empirical Pearson's criterion of $\chi^2_{EMP} = 1.7763 < \chi^2_{0.05} = 7.815$ for $\nu = 3$. In general, females have slightly lower stress tolerance than males, but the difference is clearly of little consequence.

Conclusions. The analysis of research findings showed that the psychodiagnostic methods used by the authors have not identified fundamental gender differences. An exception is the tendency towards physical aggression that was identified using the Arnold H. Buss and Ann Durkee test [16], where we have found positive differences using Pearson's chi-squared test ($\chi^2_{0.01} = 11.345 > \chi^2_{emp} = 11.1289 > \chi^2_{0.05} = 7.815$ for $\nu = 3$). In females this indicator is clearly lower (see Fig. 4), though there are girls who display high aggressiveness.

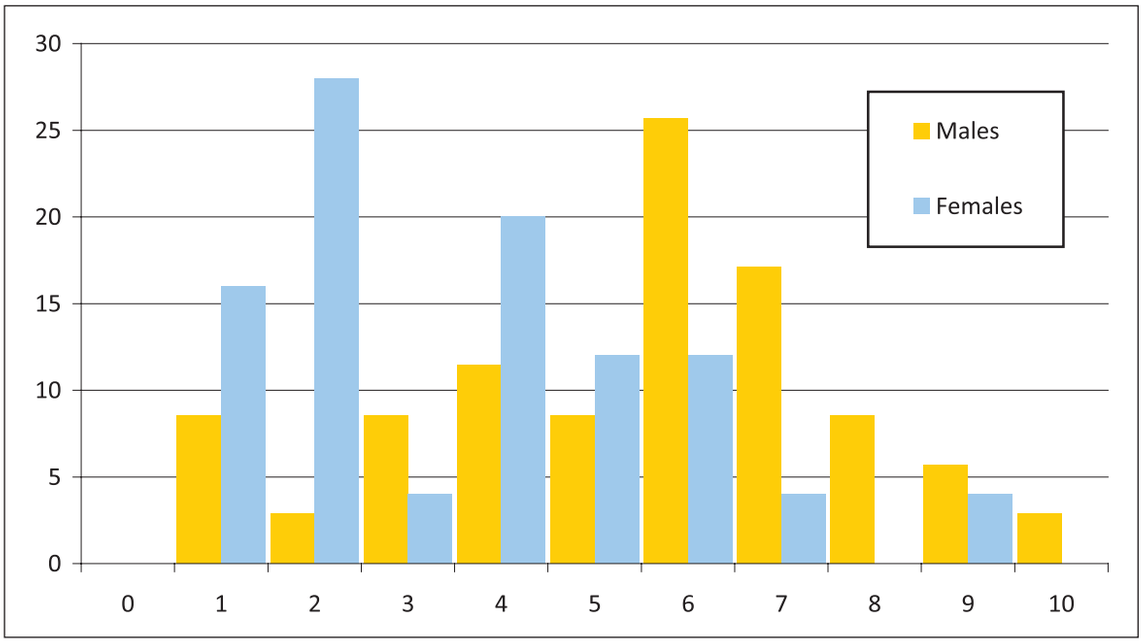


Figure 4. Distribution (%) of the test results of study participants on the Physical aggression (A_P) scale of the Arnold H. Buss and Ann Durkee test

Almost all students who took part in this research have sufficiently good stress tolerance, however, the presence of three persons with unfavourable predictions requires attention at the AS stage.

Most study participants displayed sufficiently high intellectual development. In general, it proved to be somewhat higher than average for the SPBGU GA students. (We are not referring to the results shown in Table 3, as the results of the Rudolf Amthauer and Hans Jürgen Eysenck tests slightly differ from each other. A sufficiently large body of data per the H.J. Eysenck test collected as part of the research, that was described in detail in [21], is shown in Table 6.)

This group does not display clear differences in IQ (there are reasons to believe that the larger is the surveyed group the less significant are the positive differences between males and females in terms of intellectual development), however, the trend of female aviation specialist having overall higher IQ can be observed. Possibly, females only engage in the competition in the aviation industry only if they feel they have a competitive advantage. But that remains only an assumption.

Conclusion. The scope of this paper does not allow discussing all the aspects of the problem, that were identified during the research. Although, in reason, we believe that AS for males and females who aim to become pilots and air traffic controllers should after all differ by a number of criteria, despite the fact that the analysis of the obtained results of a psychodiagnostic survey of students selected for training indicates that the existing AS procedure that is geared towards males, in most cases (except for some results, e.g. tendency towards physical aggression, as shown in this paper, or temperament, as it was shown in [27]) successfully select females based on "male" criteria, as in terms of the magnitude of surveyed personality characteristics, regardless of the candidates' gender, no differences were identified. The obtained results (as well as an analysis of global scientific research in this subject matter [30-34]) suggest that improving the reliability of AS requires researching

Table 6. Distribution of H.J. Eysenck IQ test results [21]

Sample \ IQ		70 and less points	71-90 points	91-110 points	111-130 points	over 130 points
Sample as a whole	603 ppl.	0	38	232	246	87
Males	344 ppl.	0	26	152	127	39
Females	259 ppl.	0	12	79	117	51
Pilot students	232 ppl.	0	17	110	92	13
Air traffic control students	141 ppl.	0	11	52	50	28
Transportation organization students	36 ppl.	0	2	13	16	5
Humanities students	194 ppl.	0	8	57	88	41

the differences in the expression of the necessary psychological and personality-specific professionally important qualities of aviation specialists not by criterion of gender, but rather in accordance with the identified gender-related personality type.

This research must be continued and as much as possible reoriented towards the search for methods that do not use personality inventory tests, e.g. as it was done in [27].

References

[1] Arinicheva O.V., Malishevsky A.V., Shkuntik M.S. [Topical issues related to the reduction of the effect of the human factor on the dependability of an aircraft system]. Problemy bezopasnosti poliotov. 2018;12:24-35. Available at: https://elibrary.ru/item.asp?id=37283956. (in Russ.)

[2] Arinicheva O.V., Malishevsky AV. [Disadvantages of the existing professional selection of pilots and matters of its improvement]. Transport: science, equipment, management 2016;6:41-51 [in Russian]. Available at: https://elibrary.ru/item.asp?id=26254884. (in Russ.)

[3] [Guidelines for psychological support of selection, training and professional activity of flying and control personnel of the commercial aviation of the Russian Federation]. Ministry of Transportation of the Russian Federation. Moscow: Vozdushny transport; 2001. (in Russ.)

[4] Paniushkin K. [Pilots landed an A321 with failed engines on a corn field]. www.1tv.ru; 2019 [accessed 25.10.2019]. Available at: https://www.1tv.ru/news/2019-08-15/370505-samolet_s_nerabotayuschimi_dvigatelyami_letchiki_a321_posadili_v_kukuruznoe_pole>. (in Russ.)

[5] [Preliminary report on the results of the investigation of aviation incident. RRJ-95B RA-89098 05.05.2019. Interstate Aviation Committee]. https://mak-iac.org; 2019 [accessed 25.10.2019]. Available at: https://mak-iac.org/upload/iblock/4e4/report_ra-89098_pr.pdf. (in Russ.)

[6] [Final report on the results of the investigation of aviation incident of Boeing 737-500 (53A) of Tatarstan Airlines on 17.11.2013 in Kazan International Airport. Approved by B.A. Goriunov, chair of accident board on 15.12.15]. Moscow: IAC; 2015. (in Russ.)

[7] [Final report on the results of the investigation of aviation incident. An-148-100V RA-61704 11.02.2018. Interstate Aviation Committee]. mak-iac.org; 2018 [accessed 25.10.2019]. Available at: https://mak-iac.org/upload/iblock/560/report_ra-61704.pdf. (in Russ.)

[8] [Air crash in Ristov-on-Don: 62 dead in a tragic accident]. avia.pro; 2016 [accessed 25.10.2019]. Available at: http://avia.pro/blog/aviakatastrofa-v-rostove-na-donu-flydubai?page=1. (in Russ.)

[9] Yakimovich N.V. [Pilots' errors are caused by stress. Whose actions predetermine pilots' stress?]. aviasafety.ru; 2019 [accessed 25.10.2019]. Available at: http://aviasafety.ru/23824/. (in Russ.)

[10] Southwest Airlines Flight 1380. Wikipedia.com [accessed 25.10.2019]. Available at: https://en.wikipedia.org/wiki/Southwest_Airlines_Flight_1380.

[11] Riapolov I.V., editor. [Guidelines for aptitude screening in commercial aviation]. Moscow: Vozdushny transport; 1986. (in Russ.)

[12] [Final report on the results of the investigation of aviation incident of Tu-154M RA85185 of Pulkovo Aviation Enterprise on 22.08.2006 near the village of Sukhaya Balka, Konstantinovsky Raion, Donetsk Oblast, Ukraine: Approved by A.N. Morozov, Deputy Chair of the Interstate Aviation Committee, chair of accident board on 12.02.2007]. Moscow: IAC; 2007. (in Russ.)

[13] Prokhorov A.O. [Practical lessons on the psychology of states: a study guide]. Saint Petersburg: Rech; 2004. (in Russ.)

[14] Berg T.N. [Stress tolerance and methods of its identification: a study guide]. Vladivostok: Maritime State University; 2005. (in Russ.)

[15] H.J. Eysenck. Check Your Own I.Q. Moscow: Eksmo-Press; 2003.

[16] Karelin A.A. [Large encyclopedia of psychological tests]. Moscow: Eksmo; 2007. (in Russ.)

[17] Andreev V.I. [Business rhetoric: a practical course of business communication and elocation]. Moscow: Narodnoye obrazovanie; 1995. (in Russ.)

[18] Fetiskin N.P., Kozlov V.V., Manuylov G.M. [Psychosocial diagnostics of personality and small groups development]. Moscow: Izdatelstvo Instituta Psikhoterapii; 2002. (in Russ.)

[19] Arinicheva O.V., Malishevsky A.V. Improving the reliability of aptitude screening of aviation specialists. Dependability. 2019;19(1):40-47. DOI: https://doi.org/10.21683/1729-2646-2019-19-1-40-47.

[20] Arinicheva O.V., Malishevsky A.V., Akimov I.A. [Responsibility in the value system of aviation specialists]. Transport: science, equipment, management. 2018;6:20-25. Available at: https://elibrary.ru/item.asp?id=35093752. (in Russ.)

[21] Arinicheva O.V., Malishevsky A.V. [Predictors of conflict behaviour of aviation specialists]. Herald of the Saint Petersburg State University of Civil Aviation 2018;4(21):20-34. Available at: https://elibrary.ru/item.asp?id=36580852. (in Russ.)

[22] Arinicheva O.V. [Analysis of diagnostics of intellectual abilities of the future aviation professionals.] Transport: science, equipment, management 2017;2:15-22. Available at: https://elibrary.ru/item.asp?id=28422668. (in Russ.)

[23] Research & Statistical Support Services. University Information Technology. it.unt.edu [accessed 25.10.2019]. Available at: http://it.unt.edu/research.

[24] Free Software Foundation. https://fsf.org/ [accessed 25.10.2019].

[25] Bock D.E., Velleman P.F., De Veaux R.D. Stats: modeling the world. 4th Edition. Boston (USA): Pearson Addison Wesley; 2015.

[26] Ushakov E.V. [Bioethics: textbook and practical lessons for higher education]. Moscow: Yurait; 2018. (in Russ.)

[27] Arinicheva O.V., Gerasimenkova A.E., Malishevsky A.V., Chepik M.G. Possible ways of improving the reliability of aptitude screening of air traffic controllers. Dependability.

2018;18(1):38-45. DOI: https://doi.org/10.21683/1729-2646-2018-18-1-38-45.

[28] Arinicheva O.V. [Intelligence quotient: a selection criterion or an apocryphal indicator for assessment of intellectual abilities]. Herald of the Saint Petersburg State University of Civil Aviation 2015;1(8):49-63. Available at: https://elibrary.ru/item.asp?id=24346536. (in Russ.)

[29] Istratova O.N., Eksakusto T.V. [Psychological assessment: collection of best tests. 3-rd edition]. Rostov-on-Don: Feniks; 2006. (in Russ.)

[30] Dillon K.M., Wolf E., Katz H. Sex roles, gender, and fear. The Journal of Psychology. 1985;119(4):355-359. DOI: https://doi.org/10.1080/00223980.1985.9915454.

[31] Fowler S.L., Rasinski H.M., Geers A.L., Helfer S.G., France C.R. Concept priming and pain: an experimental approach to understanding gender roles in sex-related pain differences. Journal of Behavioral Medicine. 2011;34(2):139-147. DOI: https://doi.org/10.1007/s10865-010-9291-7.

[32] Muris P., Meesters C., Knoops M. The relation between gender role orientation and fear and anxiety in nonclinic-referred children. Journal of Clinical Child and Adolescent Psychology. 2005;34(2):326-332. DOI: https://doi.org/10.1207/s15374424jccp3402_12.

[33] Kolos Yu.V., Danilova M.V. Relationship between self-actualization, emotional and personality-related factors in students. Nauchnyie issledovaniia vypusknikov fakulteta psikhologii SPbGU. 2013;1(1):115-122. URL: https://elibrary.ru/item.asp?id=20255612.

[34] Azarnykh T.D. Post-traumatic stress, female sex and gender. Vestnik of Kostroma State University. Pedagogics. Psychology. Social work. Youth studies. Sociokinetics Series. 2014;20(3):160-164. Available at: https://elibrary.ru/item.asp?id=22287308.

About the authors

Olga V. Arinicheva, Candidate of Engineering, Senior Lecturer in Flight Operation and Safety in Civil Aviation, Saint Petersburg State University of Civil Aviation, e-mail: 2067535@mail.ru, address: 38 Pilotov St., 196210, Saint Petersburg, Russian Federation.mailto:2067535@mail.ru

Tatiana V. Ziuba, Candidate of Engineering, Senior Lecturer in Life Safety, Saint Petersburg State University of Civil Aviation, e-mail: zuba57@mail.ru, address: 38 Pilotov St., 196210, Saint Petersburg, Russian Federation.

Alexey V. Malishevsky, Candidate of Engineering, Associate Professor, Senior Lecturer in Flight Operation and Safety in Civil Aviation, Saint Petersburg State University of Civil Aviation, Russia, Saint Petersburg, e-mail: 9909395@bk.ru, address: 38 Pilotov St., 196210, Saint Petersburg, Russian Federation.mailto:9909395@bk.ru

The authors' contribution

Arinicheva O.V. Review and analysis of the state of the art of the problem under consideration, collection of psychodiagnostic data on flying and air traffic control personnel for statistical processing. The theoretical component of the work.

Ziuba T.V. Review and analysis of the state of the art of the problem under consideration, collection of psychodiagnostic data for statistical processing per aviation specialists not involved in operations.

Malishevsky A.V. Review and analysis of the state of the art of the problem under consideration, collection of psychodiagnostic data on flying and air traffic control personnel for statistical processing. Processing of the obtained results.

 Original article
https://doi.org/10.21683/1729-2646-2020-20-1-47-56

Comprehensive analysis of the strength and safety of potentially hazardous facilities subject to uncertainties

Nikolay A. Makhutov[1], Dmitry O. Reznikov[1]*

[1] *Mechanical Engineering Research Institute of the Russian Academy of Sciences, Russian Federation, Moscow*
* *mibsts@mail.ru*

Nikolay A. Makhutov

Dmitry O. Reznikov

Abstract. *Aim. This paper aims to compare the two primary approaches to ensuring the structural strength and safety of potentially hazardous facilities, i.e. the deterministic approach that is based on ensuring standard values of a strength margin per primary limit state mechanisms, and the probabilistic approach, under which the strength condition criterion is the non-exceedance by the target values of probability of damage per various damage modes of the standard maximum allowable values.* **Methods.** *The key problem of ensuring the structural strength is the high level of uncertainties that are conventionally subdivided into two types: (1) the uncertainties due to the natural variation of the parameters that define the load-carrying ability of a system and the load it is exposed to, and (2) the uncertainties due to the human factor (the limited nature of human knowledge of a system and possibility of human error at various stages of system operation). The methods of uncertainty mitigation depend on the approach applied to strength assurance: under the deterministic approach the random variables "load" and "carrying capacity" are replaced with deterministic values, i.e. their mathematical expectations, while the fulfillment of the strength conditions subject to uncertainties is ensured by introducing the condition that the relation of the mathematical expectation of the load-carrying capacity and strength must exceed the standard value of strength margin that, in turn, must be greater than unity. As part of the probabilistic approach, the structural strength is assumed to be ensured if the estimated probability of damage per the given mechanism of limit state attainment does not exceed the standard value of the probability of damage.* **Conclusions.** *The two approaches (deterministic and probabilistic) can be deemed equivalent only in particular cases. The disadvantage of both is the limited capability to mitigate the uncertainties of the second type defined by the effects of the human factor, as well as the absence of a correct procedure of accounting for the severity of consequences caused by the attainment of the limit state. The above disadvantages can be overcome if risk-based methods are used in ensuring structural strength and safety. Such methods allow considering uncertainties of the second type and explicitly taking into consideration the criticality of consequences of facility destruction.*

Keyword: *structural strength, safety, uncertainty, strength margin, probability of damage, risk.*

For citation: *Makhutov N.A., Reznikov D.O. Comprehensive analysis of the strength and safety of potentially hazardous facilities subject to uncertainties. Dependability. 2020;1: 47-56. https://doi.org/10.21683/1729-2646-2020-20-1-47-56*

Received on: *02.11.2019 /* ***Revised on:*** *12.02.2020 /* **For printing:** *20.03.2020*

1. Introduction

Structural strength represents the initial complex characteristic of a technical system, which is described as a combination of differentiated indicators of static, dynamic, cyclic strength and strength reliability, and determined by the ability of the system to withstand various limit states in real operating conditions. The fulfillment of the structural strength requirements of the potentially hazardous facilities (PHF) is the key element of ensuring technological safety [1, 2]. Structural strength is deemed to have been ensured when for all involved limit state mechanisms the following condition is satisfied:

$$Q_i^S / Q_i^O > 1 \ (\forall_i = 1,2,\ldots,m), \quad (1)$$

where Q_i^S and Q_i^O are the parameters of a load-carrying capacity with the *i*-th limit state mechanism associated with negative consequences in the form of economic losses and casualties; *m* is the number of limit state mechanisms. As the analysis of national and foreign information sources on the scenarios of technological accidents and disasters shows, this interpretation of the structural strength provides the basis for research, regulation and ensuring technological safety.

There are three main matters related to ensuring structural strength and safety of PHF for all life cycle stages:

- calculation and experimental analysis of the stress-strain states taking into account mechanical Q_m^O, thermal Q_t^O, aerohydrodynamic Q_{ah}^O, electromagnetic Q_{em}^O, radiation and chemical Q_r^O effects. In addition, local stress σ^O_{max} and strain e^O_{max} depend on operating number of load cycles N^O, time τ^O and temperature t^O:

$$\left\{\sigma^O_{max}, e^O_{max}\right\} = F_O\{P^O, Q_t^O, Q_{ah}^O, Q_{em}^O, Q_r^O, N^O, \tau^O, t^O\}; \quad (2)$$

- analysis of the laws of cyclic and elastic and elastic-plastic deformation within and outside the concentration zones for varying frequencies f_τ, stress amplitudes σ_a^O and deformations e_a^O, temperatures t^O and time τ^O:

$$\left\{\sigma^O_{max}, e^O_{max}\right\} = F_{1O}\{f_\tau, \left(\sigma_a^O, e_a^O\right), t^O, \tau^O\}; \quad (3)$$

- analysis of the criteria and conditions for the damage accumulation d^O, as well as the determination of the cyclic life N_C^O for the stages of the formation and development of cracks, and damages:

$$\left\{d^O, N_C^O\right\} = F_{2O}\{f_\tau, \left(\sigma_a^O, e_a^O\right), t^O, \tau^O\}. \quad (4)$$

The tasks of ensuring the structural strength of potentially hazardous facilities are solved under conditions of a high level of uncertainty regarding operation loading on the one hand, as well as load-carrying capacity of PHF elements at various stages of its operation cycle, on the other hand [3-5]. Uncertainty factors include: natural variety of object's parameters (geometrical dimension, mechanical characteristics of the material); stochastic nature of the degradation processes and loading modes; limited knowledge of the developments and processes in load-carrying elements; limited available statistic data; imperfection of the used mathematical model; inaccuracy of the available measurement equipment.

Structural strength of PHF at different stages of its life cycle can be ensured through two radically different approaches [3, 4, 7, 8]:

1) Deterministic (normative) approach to ensuring structural strength that is based on ensuring standard values of the strength margin per primary limit state mechanisms.

2) Probabilistic approach to ensuring structural strength that is based on reducing the probability of reaching the limit state to the level that is acceptable at the defined level of technology development.

For many centuries, the first approach has been developing. It implies that uncertainties during design, development and operation of technical systems were taken into consideration through the use of a system of strength margins for various limit state mechanisms. The second approach became widespread in the middle of the 20th century with the development of such disciplines as probability and reliability theories for assessing uncertainties using the probability of system reaching the limit state. This approach has become an important element in the development of the theory of technical risks and safety. A comparative assessment of the deterministic and probabilistic approaches and conditions for equivalence will be discussed below.

2. Uncertainties of the problem

The uncertainties related to ensuring structural strength of technical systems of PHF can be divided into two fundamentally different types [9-14]:

1) Uncertainties of natural, material and technical behavior caused by non-determination of parameters, events and processes of the real world. This type includes the uncertainties related to the variability of the system parameters and effects on it with the stochastic nature of the degradation processes of its characteristics, as well as the uncertainties caused by possible deviations from nominal values of impact intensity of external and internal force factors, operating modes, geometric dimensions of the system's elements, mechanical and physical properties of materials, environmental conditions, etc.

2) Uncertainties related to the human factor (in a broad sense) are divided into: (a) uncertainties related to the limited knowledge of the designer, manufacturer and operator regarding complex technical systems of PHF and operating conditions (in particular, the nature of the complex processes of reaching limit states of the system); (b) uncertainties caused by the possibility of personnel's actions leading to a violation of the existing standards for design, construction and operation of PHF, as a result of which system properties (behavior, characteristics) will be different from the design and planned (i.e. failures at the design, development and operation stages of the system); and (c) uncertainties caused

by the possibility of unauthorized action (sabotage/terrorism) against PHF under consideration.

As the limited knowledge of technical systems of PHF and neglect of important factors caused by it, as well as the violation of the established standards can be regarded as a kind of failures, then the group of uncertainties caused by the human factor can be called, for short, the uncertainties related to the failures made by designers, developers and operators of PHF, where the term *failure* is used in a broad sense.

The particularity of PHF protection against accidents and disasters is that their description requires the consideration of a vast number of factors. At the same time, a number of PHF operating modes become underdetermined [15]. This is due to the complex nonlinear interactions of the PHF components, the strong connection between the various subsystems, as well as the fact that PHF and environment change faster than they can be described and studied. Therefore, there is a situation of lack of information about the development of hazardous processes in PHF, and thereby, limitations for predicting their behavior and managing them. At the same time, it is impossible to describe in detail the principles of PHF operating and develop management rules in certain modes. A distinctive feature of the underdetermined systems is the inability of the full description of their behavior and prediction of their state under various conditions and in different operating modes. The distinction between fully determined and underdetermined systems becomes extremely important when developing a set of security measures.

Uncertainties of the first type are considered within the framework of the strength reliability theory. However, the experience in operating technical systems shows that the estimates of the system breakdown probabilities obtained via methods of reliability theory are significantly underestimated and differ from the values observed in practice by at least an order of magnitude. The main reason for this discrepancy is that the theory of the strength reliability does not take into account the uncertainties of the human factor, which are dominant in many cases. The second type of uncertainty is assessed within the framework of new approaches focusing on the study of the human factor.

3. Deterministic approach to ensuring structural strength

As part of the deterministic approach, the random parameters of load Q_i^S and carrying capacity Q_i^O are replaced with their mathematical expectations $E\{Q_i^S\}$ и $E\{Q_i^O\}$, and the fulfillment of the strength condition taking into account the uncertainties is ensured by adding into the right member of the inequality (1) of the standard allowable margin $[n_i]$, which must be greater than one:

$$n_i = \frac{E\{Q_i^S\}}{E\{Q_i^O\}} > [n_i] \; i = 1,2,\ldots,m. \qquad (5)$$

The matter of strength margin $[n_i]$ selection is very complex. The standard strength margin for the considered limit state is assigned based on: the experience of operating such systems; uncertainty level; socio-economic conditions in the country; the accuracy of the computational models and the level of damage expected in case the limit states are reached. Thus, the values of the strength margin are determined by both objective factors (the uncertainty level in relation to the loads and carrying capacity of the structure; the criticality of consequences associated with limit state achievement) and subjective circumstances (safety culture in particular sectors and in the country as a whole, threats perception by society). Current values of standard margins for structural elements of technical systems for various purposes vary within the ranges below (Table 1).

Table 1. Values of the standard strength margin

	Sector, type of technical system	Range of values [n]
1	Space technology	1.00…1.25
2	Aviation technology (airframe)	1.25…2.0
3	Equipment and pipelines of nuclear power plants	1.07…3.0
4	Vessels and machines operating under pressure	1.5…4.0
5	Metallurgical equipment	2.07…8.0
6	Railway transport	3.33…5.56
7	Handling machinery	1.3…1.6

The data presented in Table 1 shows that the values of the standard margins significantly vary (both within particular sectors and between sectors). This demonstrates not only the lack of a single methodological framework for their substantiation, but also the difference in the sector-specific PHF risk levels. The application of this approach when designing new (unique) objects is fraught with great difficulties and high uncertainty level, associated with the lack of experience in assigning allowable margins for limit states that can be implemented in the system.

It should be noted that PHF consisting of complex systems is characterized by the various limit states corresponding to different damage mechanisms (single overload, cumulative mechanism of fatigue, long-term, corrosion, thermal cyclic damage, etc.). In this case, the system of margins n_1, n_2, …, n_q for the basic limit state mechanism is used. The margins for various limit states also normally prove to be unconnected. Additionally, the system may have excess strength per some limit states and insufficient per others.

The results of experimental and calculation studies using samples, models and full-scale structures allow determining margins for stress n_σ, strain n_e, number of cycles n_N, time n_τ and defect (crack) size n_l:

$$\left\{n_\sigma, n_e, n_N, n_\tau, n_l\right\} = \left\{\frac{\sigma_S}{\sigma_{max}^O}, \frac{e_S}{e_{max}^O}, \frac{N_S}{N^O}, \frac{\tau_S}{\tau^O}, \frac{l_S}{l^O}\right\}, \qquad (6)$$

where "*S*" refers to the critical (limit) value of the corresponding characteristic of strength, durability and crack resistance, and "*O*" refers to the corresponding values in operation.

The generalized surfaces of the limit (hazardous) states of V^S are constructed based on expressions (2) – (4) (Fig. 1). The surface of the allowed states $[V]$ is determined upon the construction of the limit state surface by adding the margin coefficients $[n_i]$ for each of the specified limit parameters in accordance with the corresponding coordinate of the state space:

$$[V_i] = V_i^S / [n_i].$$

The condition for ensuring structural strength and safety is that the time varying vector of operational states V^O throughout all life cycle stages remains within the area of permissible states that is below the surface of the permissible states $[V]$.

Deterministic approaches are usually used at the initial stage of the design to determine the size of the most loaded sections of the designed structural elements, when there is no sufficient statistical material for the analysis with significant changes in the construction and their operating conditions. The task of ensuring the strength of the structural elements of technical systems has traditionally been solved through the application of deterministic approaches which allow compensating for the uncertainties by adding differentiated margins for the basic limit state mechanisms based on the experience of PHF design and operation. However, with the rapid development of technologies and implementation of new structural material, the possibilities of the normative deterministic approach are close to exhaustion.

4. Probabilistic approaches to ensuring structural strength

Probabilistic approaches to ensuring structural strength are based on reducing the probability of reaching limit states to a specified level. Within the framework of the probabilistic approach, structural strength is ensured if the calculated probability of damage by the *i*-th mechanism of reaching limit state $P_{Fi} = P\{Q_i^S/Q_i^O < 1\}$ does not exceed the standard value of damage probability $[P_F]$:

$$P\{Q_i^S / Q_i^O < 1\} \le [P_F], \quad \forall i = 1,2,\ldots,m. \qquad (7)$$

Probabilistic approaches are effective when significant amounts of initial statistical information on levels of operating loads and variability of the basic mechanical properties of carrying structural elements of PHF have been accumulated (or can be obtained). The above approaches, with their numerical implementation, allow determining the probabilistic initial characteristics of strength, service life and survivability and enable the quantification the most important damage parameters *U*, identification of the risk *R*, safety *S* and protection *Z*.

For high-risk PHF, the variations of τ^O, N^O reach 5-8 orders of magnitude, t^O reaches 4 orders of magnitude, l^O reaches 3 orders of magnitude, *P* reaches 10 orders of magnitude, *U* reaches 6 orders of magnitude, *R* reaches 3-4 orders of magnitudes [1, 2]. The value of margins $[n_i]$ vary within the same order ($1 \le [n_i] \le 10$).

Probabilistic approaches to ensuring structural strength have been in development since the middle of the 20-th century, first within the framework of the classical strength theory, and later as part of the strength reliability theory. The limit permissible value of the damage probability $[P_F]$ is set depending on the value of damage that may occur in case of failure, taking into account the social significance of the object and its useful life. In particular, the Construction Industry Research and Information Association (CIRIA) proposed the following interpolation formula for estimating the maximum permissible calculated probability of damage [3] of complex engineering structures (dams, bridges, offshore platforms):

$$[P_F] = \frac{10^{-4}\xi_S \cdot \tau}{L \cdot k_{HF}}, \qquad (8)$$

where τ is the estimated useful life of the system; *L* is the average number of people who may die in case of a system failure; k_{HF} is the coefficient that takes into account damage associated with the human factor (usually, $k_{HF} = 10$); ξ_S is the coefficient of the system's social significance (see Table 2). Thus, the value $[P_F]$ is usually in the range of $1 \cdot 10^{-5} \ldots 1 \cdot 10^{-7}$.

Table 2. Coefficient of social significance for various types of technical systems

Type of system	ξ_S
Places of mass gathering (sport centers, shopping centers)	0.005
Dams	0.005
Residential buildings, office centers, industrial plants	0.05
Bridges	0.5
Drilling rigs, offshore installations	5

It should be noted that formula (8) takes into account the uncertainties associated not only with the random nature of the loads and carrying capacity of structures, but also with the uncertainties caused by the human factor. This is achieved by adding coefficient k_{HF}, which, as a rule, equals 10. The so-called theoretical maximum permissible probability of damage $[P_{F,T}]$ is often mentioned in regulatory documents; this probability is estimated without taking into account possible failures or unauthorized human actions and is significantly lower than $[P_F]$. It is generally accepted that these values differ by one order of magnitude.

Today, the probabilistic approach to ensuring structural strength is increasingly implemented into the practice of a

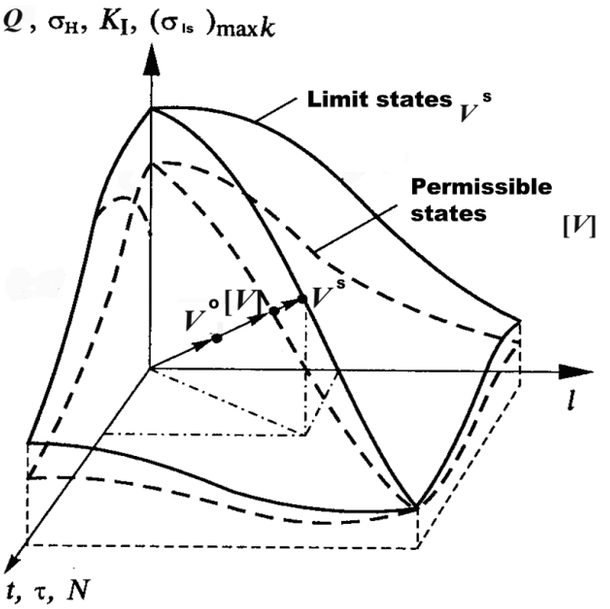


Figure 1 – Surface construction for limit and permissible states as part of assessing the strength, lifetime and survivability in a three-dimensional space of object states

number of industries, in particular, in the design of nuclear power facilities, hydraulic structures, offshore oil and gas platforms, shipbuilding, etc.

It should be noted that the social significance coefficient ξ_S of the system in formula (8) allows implicitly and highly approximately taking into account the scale of possible destruction consequences when deciding whether the considered system is protected. More comprehensive and mathematically correct way for considering destruction consequences is implemented as part of an integrated approach to ensuring strength and safety, which is based on the risk theory.

5. Comparison of deterministic and probabilistic approaches

It should be noted that designing and assuring the strength, life and safety of the PHF structural elements as part of the deterministic approach, which is based on margins, is less labour-consuming. Subject to this approach, in order to make sure that expression (5) is true, the relation $E\{Q_i^S\}/E\{Q_i^O\}$ should only be evaluated once, while the calculation by the probabilistic criterion (7) requires a multiple evaluation of Q_i^S/Q_i^O. Unfortunately, the deterministic approach, despite its simplicity, lacks analytical rigor and accuracy as well as uncertainty management. The human factor and experience in operating same-class systems in similar environmental conditions play a significant role in assessing the strength and life. The applicability of the deterministic approach when designing unique objects, for which there is no relevant statistical information, is very limited. Furthermore, the deterministic approach does not enable the optimization of the designed system, since it does not allow comparing the costs of its creation with a given margin and the positive

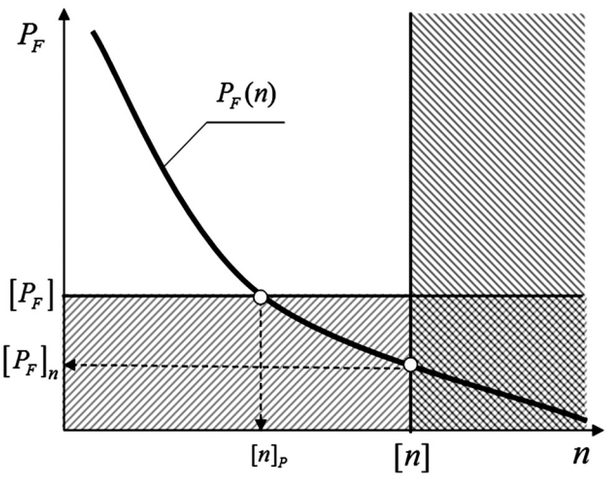


Figure 2 – Relationship between strength margin and damage probability

effect associated with an increase in strength that cannot be calculated without answering the question: *To what level can the probability of damage be reduced, if the fulfillment of the designated margin is ensured?* Thus, the deterministic approach does not allow selecting the optimal variant from a number of possible systems.

On the contrary, designing and ensuring structural strength by the criterion of dependability is a fairly rigorous mathematical procedure in terms of managing the load and carrying capacity-related uncertainties. This criterion allows making informed decisions when designing a system under uncertainty, making comparative assessments of strength and life for various parameters of the designed element and performing optimization. However, the probabilistic approach is labour-consuming and requires a highly qualified designer.

Therefore, it would be useful to combine the advantages of both approaches to obtain, when possible, the relationship between the strength margin and the probability of damage. For example, this would allow evaluating the safety of a structural element designed with a given strength margin according to reliability criteria. Another important task consists in comparing the areas of protected states Ω_n and Ω_P, obtained by the safety criterion and the reliability criterion, respectively.

Based on the general principles of the reliability and strength theory, it can be assumed that, at least in some cases, there is a monotonously decreasing function between the strength margin n and the probability of damage P_F (Fig. 2). When this assumption is true, deterministic and probabilistic approaches can be considered equivalent. Then, if the deterministic approach is used, the limit probability of damage $[P_F]_n$, corresponding to the normative margin $[n]$, can be determined. Similarly, if the probabilistic approach is used, the limit value of margin $[n]_P$, corresponding to the maximum allowable probability of damage $[P_F]$, can be determined.

Unfortunately, in the general case there is no one-to-one correspondence between the values of $[n]$ and $[P_F]$,

and, therefore, these two approaches cannot be considered equivalent. However, such functions can be obtained for a number of special cases.

Let us consider the equivalence of the deterministic and probabilistic approaches for cases of single static loading. Per the deterministic approach, the condition for ensuring strength (1) and (5) can be rewritten as:

$$n \geq [n], \tag{9}$$

where Q_S and Q_O are parameters characterizing static strength and load; $n=E\{Q_S\}/E\{Q_O\}$ is the actual margin, which should not be lower than the standard minimum allowable margin $[n]$. Thus, margin n is determined by the ratio between the mathematical expectations of the load and the carrying capacity values.

Obviously, the introduction of margins cannot completely eliminate the possibility of system damage. Therefore, when the deterministic approach is used, the question arises of what limit probability of damage $[P_F]$ corresponds to a given standard margin $[n]$.

In the deterministic approach, which is based on assigning margins, only the ratio between the characteristic values of the distributions is taken into account (in this example, between mathematical expectations of load and carrying capacity $E\{Q_C\}/E\{Q_Э\}$).

If the values of Q_S and Q_O are uncorrelated and normally distributed, probability of damage can be estimated using a well-known expression [3, 6]:

$$P_F = \mathrm{F}\left(-\frac{E\{Q_S\}-E\{Q_O\}}{\sqrt{\left(S\{Q_S\}\right)^2+\left(S\{Q_O\}\right)^2}}\right), \tag{10}$$

$F(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} exp\left(-\frac{t^2}{2}\right)dt$ is normal distribution function.

If coefficients of variation $v_{Q_O}=\frac{S\{Q_O\}}{E\{Q_O\}}$ and $v_{Q_S}=\frac{S\{Q_S\}}{E\{Q_S\}}$ are introduced, the required function takes the form:

$$P = \mathrm{F}\left(-\frac{n-1}{\sqrt{v_{Q_O}^2+v_{Q_S}^2\cdot n^2}}\right), \tag{11}$$

Thus, assuming the load and carrying capacity are normally distributed, and specifying the fixed values of variation coefficients v_{Q_S} and v_{Q_O} (which shall be considered invariant), the relationship between the probability of reaching the limit state and the strength margin can be built. Which is to say, in the case of normally distributed, uncorrelated Q_S and Q_O, if the variation coefficients v_{Q_S} and v_{Q_O} stay constant when the system parameters vary, then the probability of damage depends only on strength margin n.

In other words, formula (11) suggests that approaches based on assigning margins and reliability theory are equivalent when the coefficients of variation v_{Q_S} and v_{Q_O} do not change when the design parameters vary.

Figure 3 shows dependencies between probability of reaching limit state $P_F\left(n\,|\,v_{Q_O*}, v_{Q_S*}\right)$ and margin n for different values of load and strength variation coefficients v_{Q_S} and v_{Q_O} plotted in linear coordinates.

In strength reliability theory the system is considered protected if the calculated probability of local damage of the critical element is less than the standard value of the maximum permissible probability of damage: $P_F < [P_F]$.

According to (11), probability of damage P_F is a function of tree variables: central margin n, load variation coefficient v_{Q_S} and carrying capacity variation coefficient v_{Q_S}. Hence, there can be three methods of ensuring structural strength: increasing the margin, reducing the variation in strength, reducing the variation in load. The protection method is selected taking into account the specifics of the industry and operating conditions of systems. In those industries where there are no strict restrictions on the weight of

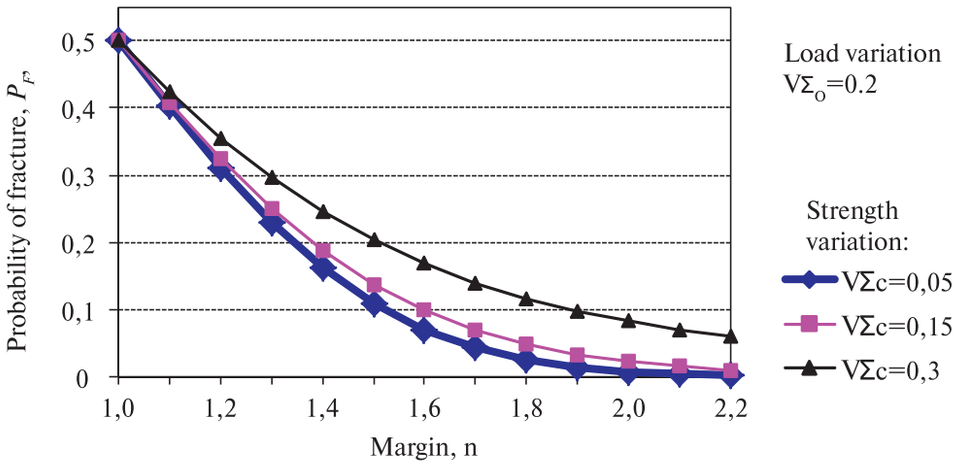


Figure 3 – Dependence of the probability of local damage on the margin for various combinations of load variation coefficients and strength at $v_{Q_O}=0$

structures (nuclear energy, construction), protection can be mainly achieved by increasing the margins n = 2…5. In aerospace systems, where the requirements of weight limitation are dominant and, therefore, the margins cannot exceed 1.2 ... 1.6, ensuring protection should focus on reducing load variations and on the basic mechanical properties of materials.

6. Methods of compensating for uncertainties in structural strength and safety assurance

Damage of PHF due to technical factors is considered in the framework of the classical strength reliability theory. The traditional method of compensating for uncertainties associated with the variability of the load and the carrying capacity parameters is to introduce margins n.

The introduction of margins cannot completely eliminate the possibility of system damage. Therefore, when the normative deterministic approach is used, the question arises of what probability of damage $P(F)$ corresponds to the calculated margin n (Fig. 4). The relationship between the margin and the probability of damage (accidents and catastrophes) when there is an exact or approximate relationship between these quantities was addressed in detail in [3, 4, 7, 8].

The probability of damage due to human factor may also depend on the margin. However, it should be noted that operator errors can not only change the relative position of the load distribution and carrying capacity curves, but also lead to a change in the system probabilistic model itself, creating new functions of limit states or changing the dimension of the state space. Moreover, increasing margins for the initial limit state cannot compensate for the uncertainties introduced by errors [9].

In accordance with the types of uncertainties discussed in Section 2 above, two types of causes of PHF damage (accidents, catastrophes) can be distinguished:

- damage F_V caused by the variability of the state function. The probability of such event is estimated as $P(F_V)$;
- damage F_E caused by the human factor (or errors in the broad sense of the term), the probability of which is estimated as $P(F_E)$.

The simplest scenario model, which takes into account the uncertainties of these two types, can be represented by an event tree (Fig. 5) containing generalized scenarios of damage (accidents, catastrophes) due to technical reasons and the human factor [10]. For this model, let us assume that damage F to the system as a whole can occur when the system reaches the limit states due to (a) the damage of individual elements due to the variability of the limit state function, and (b) the errors of designers, builders or users made at different stages of the life cycle. Then, event F can be seen as a combination of two events: F_V, damage due to the variability of the technical parameters, and F_E, damage due to error (human factor): $F = F_V \cup F_E$. In this case, the probability of system damage can be expressed as:

$$P(F) = P(F_V \mid \bar{E}) \cdot P(\bar{E}) + \left[P(F_E \mid E) + P(F_V \mid E)\right] \cdot P(E), \quad (12)$$

where $P(E)$ is probability of error; $P(F|E)$ is conditional probability of damage due to error if an error is made; $P(F_V|E)$ is conditional probability of damage due to the variability of the technical parameters if an error is not made; $P(\bar{E}) = 1 - P(E)$ is probability of no error.

Traditional reliability theory focuses on estimating the value of $P(F_V|\bar{E})$, which describes the probability of PHF damage when no errors were made. However, the experience of PHF operation suggests that from 70 to

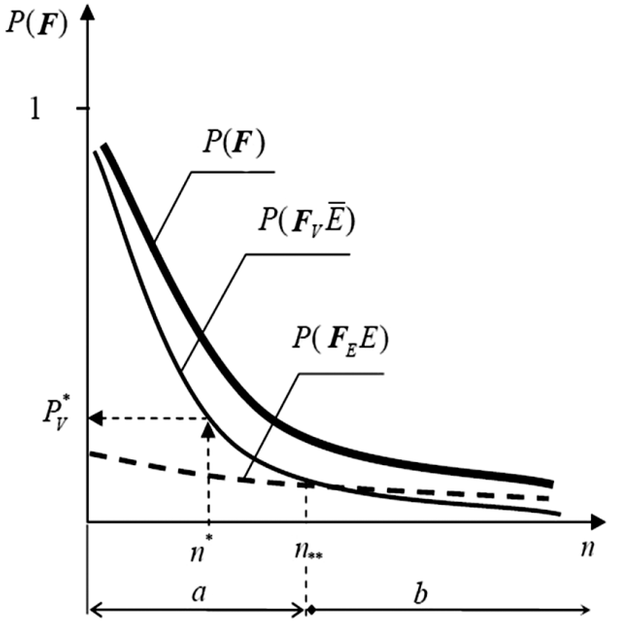


Figure 4 – The effect of the strength margin on the probability of damage of PHF [9].

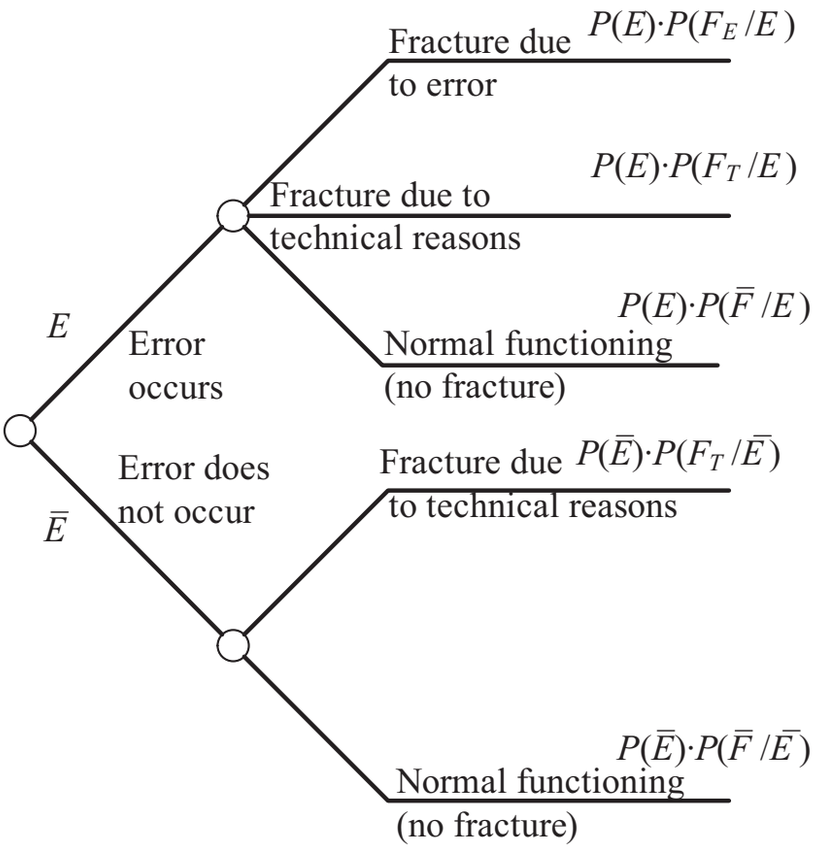


Figure 5 – Simple model for assessing the probability of damage of PHF, with account of the uncertainties caused by the variability of the state function and human errors [10].

90% of PHF damage is associated with the human factor [1]. The important thing is that both primary types of damage causes can be described by expression (12). It should be noted that the mechanisms of damage due to technical reasons can fundamentally differ from the mechanisms of damage due to human errors. Therefore, the structure of the scenario graph, which takes into account the human factor, should be substantially revised.

Let us suppose that after a serious error the probability of system damage due to error is significantly greater, than the probability of damage due to the variability of load and carrying capacity parameters: $P(F_E|E) >> P(F_V|E)$. This assumption is true for sufficiently large margins. In this case, the value of $P(F_V|E)$ in expression (12) can be neglected in comparison with the value of $P(F_E|E)$, in other words, let us assume $P(F_V|E) \approx 0$. Then expression (12) can be rewritten in the form:

$$P(F) = P(F_V \mid \bar{E}) \cdot P(\bar{E}) + P(F_E \mid E) \cdot P(E) = \\ = P(F_V \bar{E}) + P(F_E E). \qquad (13)$$

The first summand in expression (13) determines the probability of damage due to technical factors, and the second summand determines the probability of damage due to errors made at different stages of the PHF life cycle.

The conclusions made are aligned with the available statistical data, which shows that the most effective way to increase reliability and safety of systems designed with a small margin and, therefore, operating in modes close to the exhaustion of their carrying capacity, is to increase the margin. At first, with an increase of margin n, the probability of damage decreases sharply (Fig. 4, section "a" of the $P(F_V)$ curve) [9]. However, as the margin grows, the rate of damage probability decrease begins to drop noticeably and, after the transition to the area of highly reliable systems (the conventional border of which is the margin of n_{**}), the probability of damage depends on a further increase in the margin very weakly (Fig. 4, section "b" of the $P(F_V)$ curve). This is due to the fact that at $n > n_{**}$ the main cause of damage is no longer the variability of the load parameters and carrying capacity, which can be compensated by introducing a larger margin, but errors during design, construction and operation, which cannot be effectively parried by increasing the margin (since these errors change the form of the limit states function or may even create new limit state mechanisms) (Fig. 4, $P(F_E)$ curve). Therefore, in this case reducing the probability of damage should be done by improving the operational strategy ξ, including technical monitoring measures, control procedures, routine maintenance and repair work, etc., allowing timely identification and elimination of errors, i.e. compensating for Type

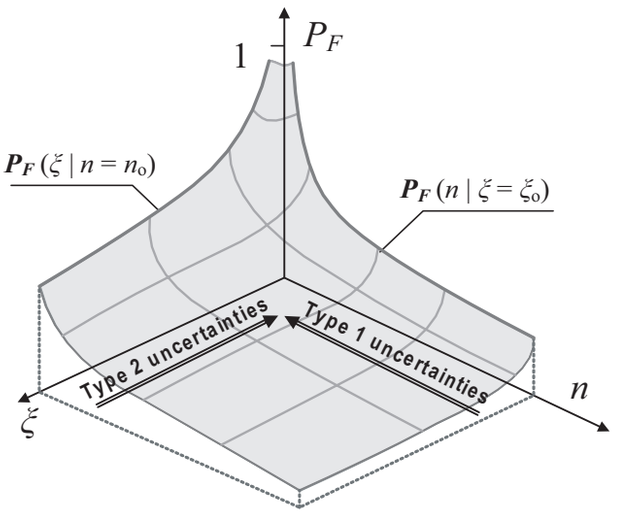


Figure 6 – Dependence of the probability of damage on the margin and the quality of the operation strategy

2 uncertainties[1]. Thus, the probability of PHF damage can be seen as a function of two generalized variables: margin n and quality of the operating strategy ξ (Fig. 6), which characterize two fundamentally different types of uncertainties associated with PHF operation [5].

The quantitative estimation of integral risks indicators for damage, accidents and catastrophes is at the core of traditional and new approaches to assessing the structural strength and safety of potentially hazardous facilities. Parameters such as strength margins and the probability of transfer of the carrying elements to the limit state and the corresponding damage must be considered in these approaches. Uncertainties associated with the variability of the system and the environment parameters and with the manifestation of the human factor at all stages of the objects' life cycle play an important role in the quantitative estimation of these parameters. Modern strength and safety theories allow both evaluating the role of these factors and developing methods for compensating for uncertainties.

References

[1] [Safety of Russia. Legal, socioeconomic and technological aspects]. Moscow: Znanie; 1998-20019; Vol. 1 to 55. (in Russ.)

[2] Makhutov N.A. [Strength and safety: Fundamental and applied research]. Novosibirsk: Nauka; 2008. (in Russ.)

[3] Elishakoff I. Safety Factors and Reliability: Friends and Foes? Dordrecht: Kluwer Academic Publishers; 2004.

[4] Ching J. Equivalence between reliability and factor of safety. *Probabilistic Engineering Mechanics*. 2009;24(2):159-171.

[5] Reznikov D.O. [Methods of uncertainty mitigation as part of ensuring the protection of complex technical systems and optimization of life cycle costs]. *Engineering and automation problems*. 2013;3:57-64. (in Russ.)

[6] Makhutov N.A., Reznikov D.O., Zatsarinny V.V. [Two types of emergency scenarios in complex technical system]. *Safety and emergency problems*. 2014;2:28-41. (in Russ.)

[7] Makhutov N.A., Reznikov D.O. The comparison of deterministic and probabilistic estimates of strength of structural elements of technical systems under serial loading. *Machinery manufacture and reliability*. 2014;5:384-388.

[8] Makhutov N.A., Reznikov D.O., Petrov V.P. et al. [Normative and probabilistic approaches to the assurance of critical facility protection]. *Safety in technosphere*. 2011;4:5-12. (in Russ.)

[9] Beeby A.W. Safety of structures, and a new approach to robustness. *The Structural Engineer*. 1999;77:16-21.

[10] Ellirtgwood B. Design and Construction Error Effects on Structural Reliability. *Journal of Structural Engineering*. 1987;113(2):409-422.

[11] Dhillon B.S. Human Reliability and Error in Transportation Systems. London: Springer-Verlag; 2007.

[12] Makhutov N.A., Reznikov D.O. Consideration of threats associated with the human factor when assessing the security of hazardous production facilities. *Occupational safety in industry*. 2015;1:60-67.

[13] Makhutov N.A., Akmetkhanov R.S., Dubinin E.F. et al. [The effect of the human factor on the safety of technical systems]. *Safety and emergencies problems*. 2014;3:80-98. (in Russ.)

[14] Makhutov N.A., Abramova N.A., Akimov V.A. et al. [Safety of Russia. The human factor in safety problems]. Moscow: Znanie; 2008. (in Russ.)

[15] Makhutov N.A., Reznikov D.O., Petrov V.P. Specific features of critical infrastructures safety ensuring. *Safety in technosphere*. 2014;3;1(46):3-14. (in Russ.)

[1] Here ξ is a generalized parameter characterizing the quality of the chosen PHF operation strategy, with $\xi = 0$ corresponding to the strategy, when PHF operation does not involve any control, maintenance and repair procedures, and $\xi = 1$ corresponding to the strategy that involves the highest possible control and repair level.

About the authors

Nikolay A. Makhutov, Doctor of Engineering, Professor, Corresponding Member, Russian Academy of Sciences, Lead Researcher, Federal State Publicly Funded Scientific Establishment Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), address: 4, Malyy Kharitonyevskiy Per., 101990, Moscow, Russian Federation, phone: (495) 930 80 78, e-mail: kei51@mail.ru

Dmitry O. Reznikov, Candidate of Engineering, Lead Researcher, Federal State Publicly Funded Scientific Establishment Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), address: 4, Malyy Kharitonyevskiy Per., 101990, Moscow, Russian Federation, phone: (495) 930 80 78, e-mail: mibsts@mail.ru

The authors' contribution

Makhutov N.A. generalized the data on the assignment of strength margins subject to various mechanisms of limit state attainment, substantiated the strength criteria of structural components and parts of machines in deterministic terms and developed the probabilistic approaches to the strength assessment subject to the spread of the mechanical characteristics of structural materials.

Reznikov D.O. compared the deterministic and probabilistic approaches to ensuring the strength and safety of technical systems, examined the applications of graphological methods in the assessment of strength-related dependability of technical systems subject to various types of uncertainty.

Original article
https://doi.org/10.21683/1729-2646-2020-20-1-57-67

On the method of risk synthesis in the safety management of structurally complex systems

Alexander V. Bochkov, *Gazprom Gaznadzor, Russian Federation, Moscow*
a.bochkov@gmail.com

Alexander V. Bochkov

Abstract. *The Aim of the paper is to show that the risk to critical infrastructure facilities (CIF) of structurally complex systems (SCS) should be considered as a multicomponent vector, whose set of parameters is subject to changes. Real safety estimation using the risk-oriented approach is impossible without a sufficient base of quantitative and qualitative characteristics of risk factors, as well as data on the status of facilities and processes that are exposed to such risk factors. Risk assessment always aims to estimate its quantitative indicators, which allows it to be used not only to assess industrial safety, but also to substantiate the economic efficiency of taken measures, conduct economic calculations of the required relief or compensation of lost health of workers and environmental damage.* **Method.** *The author suggests a method of risk synthesis (with game definition of the problem of countering possible external effects of various nature on CIF SCS) as one of the foundations of the design of advanced systems for monitoring safety threats to SCS. A special attention must be given to the effect of risk factors on the system of balanced safety and risk indicators, as prediction based on single indicators does not create a holistic image of the systems' status and development trends.* **Result.** *Key methodological premises were formulated: from general problem definition of safety management through the synthesis the model of a controlled facility and its external and internal connections, solution to the problem of selection of priority protection facilities in terms of assuring efficient operation and general safety of SCS. As the basis of advanced systems for monitoring safety threats and risks, the paper suggests the concept of risk management aiming to create the mechanism, method and tools for the synthesis, analysis and prediction of emergency risks.* **Conclusion.** *The proposed method can be applied to a wide range of tasks of primary analysis, synthesis and quantitative estimation of the CIF-related risks and safety management of SCS of various purpose.*

Keywords: *structurally complex system, critical infrastructure facilities, risk synthesis, safety, management.*

For citation: *Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. Dependability. 2020;1: 57-67. https://doi.org/10.21683/1729-2646-2020-20-1-57-67*

Received on: *13.12.2019 /* **Revised on:** *23.01.2020 /* **For printing:** *20.03.2020*

For psychological comfort some people would rather use the map of the Pyrenees while lost in the Alps than use nothing at all. They do not do so explicitly, but they actually do worse than that while dealing with the future and using risk measures. They would prefer a defective forecast to nothing.

Nassim Taleb

0. Introduction

Dependability and safety are key properties of critical and business-critical SCS, the requirements for which are on a constant rise. That is due to a number of factors.

First, the risks of emergencies and man-made catastrophes are increasing. For instance, according to the data announced at an ESREL conference, such accidents amount to 70% of the total number. Almost every tenth space launch results in an accident, causing economic and environmental consequences.

Second, the growing complexity of systems does not translate into improved reliability indicators of their components, which leads to reduced dependability and safety of SCS due to the absence of adequate structural solutions. Additionally, the diversity of components that can be used in a system design is growing as well, which, in turn, complicates the search for the ways of compensating for the above deficiency.

Third, the unique nature of such systems, be it with short or long periods of active use, causes a shortage of reliable information on the real values of reliability indicators reliability of the components and whole SCS. The gravity of this factor grows in proportion to the increasing complexity and stated reliability of components, e.g. large and ultra-large integration circuits. Additionally, the commercial nature of the manufacture of some elements and intense competition lead to the classification or unreliable information regarding their reliability.

On the other hand, the methods of today's complex technical systems dependability and risk theory, as well as the associated decision support technology, in the process of their development, operation and reengineering, do not provide suitable recommendations in terms of structural considerations, functionality and algorithms. The mathematical models of the classical dependability theory do not fully take into consideration the diversity of characteristics of components and therefore do not in fact allow obtaining exact solutions of optimization problems, which causes two types of risks. The risks associated with overstated dependability and safety indicators may cause an unacceptable growth of the actual value of failure and accident probability, while the risks of their understatement (as compared to the real ones) may lead to extra expenses at the stages of SCS development and operation, which is very important given the high cost of their manufacture and ownership.

The end of the XX century was marked by revolutionary changes in information processing that required a complete reconsideration of the basic principles of information management. Thus, while the information support of one or another type of activity used to revolve around the collection of rare data, today information is overabundant. In this context, the main problem consists in evaluating information by criteria of reliability, novelty, usefulness, as well as ensuring timely delivery of such information to the end user (decision-maker, DM) while observing the requirements for the specified scope and quality of data.

The tasks assigned to such entities of any company or nation due to their nature are beyond the capabilities of one person or even a whole team. Generating adequate managerial decisions requires complex, distributed among many employees procedures of search, storage and processing of required data, competent combination of scheduled activities and those imposed by the need for quick and effective reaction to the occurrence of unpredictable situations.

1. On the levels of system instability

The management of any organization follows the hierarchical principle. In a hierarchical management system, any subsystem of a certain level is subordinated to a higher-level system whose part it is and managed by. A management system is subdivided into subsystems until the resulting subsystem does not perform management functions, i.e. the bottom-level subsystem will be a subsystem that performs direct control of specific working tools, mechanism, device or processes. A higher-level management system controls manufacturing processes through lower-level subsystems (intermediate levels).

A company's management system also has a multilevel structure. Higher-level subsystems produce a flow of control information to lower-level subsystems. At the same time, lower-level subsystems send information on the current status of the controlled object to higher-level subsystems. The advantage of the hierarchical structure of company management consists in the fact that management problems are solved based on local decisions taken at the corresponding levels of the management hierarchy. The lower management level is the source of information for managerial decision-making at a higher level. The interlevel information flow gets smaller at each higher level, but at the same time, its semantic content increases.

All decisions taken as part of operations management are subdivided into routine and random. Routine decisions include those that are taken on the regular basis at certain intervals, so most procedures associated with the execution of such decisions can be automated. Random decisions are taken as the result of unforeseen circumstances and therefore are not subject to reliable information support.

For the top management of major industrial associations, specialized systems are created for execution supervision of higher-level directives and own decisions (indicative systems). That enables the managers to focus their attention on strategic matters, execution of long-term tasks and planned activities through quicker delivery of strategic information, wider and deeper analysis based on information grouping.

Thus, creating an optimal SCS safety management system requires the integration of research and development findings and information assets, as well as development of the method of comprehensive analysis of operational stability and basic procedures of a company's integrated risk management system. Such system will enable better substantiated decisions not only in terms of predicting emergencies and crises of various types and scale, but also as regards efficiency assessment of investment into safety and stable system operation. Comprehensive analysis of related risks will allow substantiating the required and sufficient safety levels of hazardous items and manufacturing facilities based on their importance in the context of a wide range of management problems.

Currently, there is a number of approaches to the assessment of critical (pre-critical) situations affecting a certain facility (system) that – from systems point of view – are based on the classification of the states of the examined partially-controllable dynamic facility (system) under risk and uncertainty or, in other words, the evaluation of the consequences of predicted scenarios of state development from the current to successor state.

From the point of view of systemology, the loss of stability of system development manifests itself at a number of hierarchically associated levels, each of which requires an individual and detailed analysis.

Level one is the "strength" level (a complex structure is to be composed of stable elements). It has to do with equipment ageing, personnel qualification lagging behind the development of modern technology and depletion of the resources the system's operation is based on.

Level two is the "dependability" level (retention of operability of the whole when some elements have failed). It is primarily ensured through element, unit and subsystem duplication.

Level three is the "survivability" level. It has to do with the system's ability to actively resist external threats.

Level four is the "self-organization" level. It is characterized by the adaptive properties of the system per "sublevels":

a) "homeostasis", meaning the retention of the "normal" system integrity and its vital functions;

b) "training", meaning the development of new methods of operation in order to ensure the ability to solve more complex tasks in the future;

c) "preadaptation" (prediction, intelligence), meaning the preventive development of optimized plans, mechanisms and resources for the purpose of resolving critical and pre-critical situations that have not occurred but may happen in the future;

d) "rebirth", meaning generation within the old system of a "new" system that operates according to "new" rules, in which the old system cannot exist.

Additionally, as it was noted above, a basic principle of situational management consists in the fact that a significant part of information is in the form of text messages in the mass media or other sources and is unplanned and unpredictable nature. As this information is unique and changes over time, a company's analytical units are often unable to evaluate its reliability, novelty and usefulness. For that reason, information in many cases is classified as "poorly formalized threats" (i.e. threats that are characterized by uncertainty and dynamic nature of input data and knowledge) that have the following properties:

– large amounts of symbolic information;

– the problem is not mathematically defined and lacks an algorithmic solution, or even if it does, the solution search space is too large and finding it within an allowable time and available resources is practically impossible;

– solving problems requires heuristics, i.e. affirmations based on experimental data, intuition. The aim of their application is to find a more rational solution, rather than the exact mathematical solution, by means of eliminating deliberately unsuitable solutions.

Despite the fact that, as of late, the proportion of poorly formalized threats (the advent of new information and social technologies, terrorist and war risks, changes in pricing policies, migration processes, etc.) has been growing, which inevitably reflects upon – among other things – integrated safety, assessment and analysis of such threats that are rather neglected.

However, we can observe growing experience with knowledge acquisition systems, models get developed that allow distinguishing between simple information noise and information attacks or designation of an incoming event. For instance, the vocabulary and frequency of messages before and after "critical" events. Information is normally multi-aspect, there are the so-called "problem classifiers", so, beside threat identification, knowledge of the fact which problems entail other problems as part of certain scenarios is accumulated and organized.

Only comprehensive analysis of related SCS and subsystem-related risks will allow substantiating the required and sufficient safety levels of hazardous items and manufacturing facilities based on their importance in the context of a wide range of management problems.

It should also be noted that the current practice of business mathematics is dominated by methods originating from the solution of certain physicotechnical problems. However, the "classical" science's postulate of impartiality of the laws of nature (their unconditional

reproducibility in real life) doesn't hold up against criticism. Practical solutions are often "one-off", "unrepeatable", therefore the "life" mathematics are methodologically in principle more complex than the mathematics for "physics".

With all due respect to physicotechnical and other scientific problems, the phenomena they study are subject to natural laws and are not ruled by someone's subjective actions and interests. Conscious intervention into the development of the "physical world" comes down – in mathematical terms – to the definition of certain "parameters" subject to unchanging general laws. The study of physical processes aims to identify and analyze hidden causal relations and thus only pertains to the analytical level of knowledge.

System analysis does not include either the assessment of new knowledge, or examination of the cognizer's actions based on new information. True analysis is impartial. It cannot dictate what the object of study must be like (what it "should" become) and what actions should be taken to modify it in a certain way. Thus, the criterion of conclusion of the system analysis as a stage of systemic knowledge is the ascertainment of consistency of the data obtained after the formalization of facts and correctness of the conclusion procedure.

However, the research of the majority of phenomena of the real world is motivated by the need for active conscious "partial" modification by the cognizer of the object of cognition, for instance, by the need to design objects that never existed before. At the same time, one must be able to predict the activities and their results accounting for the fact that "the others are wide awake", i.e. working against competition in a constant search for optimal (acceptable) solutions.

2. Notes on the optimality

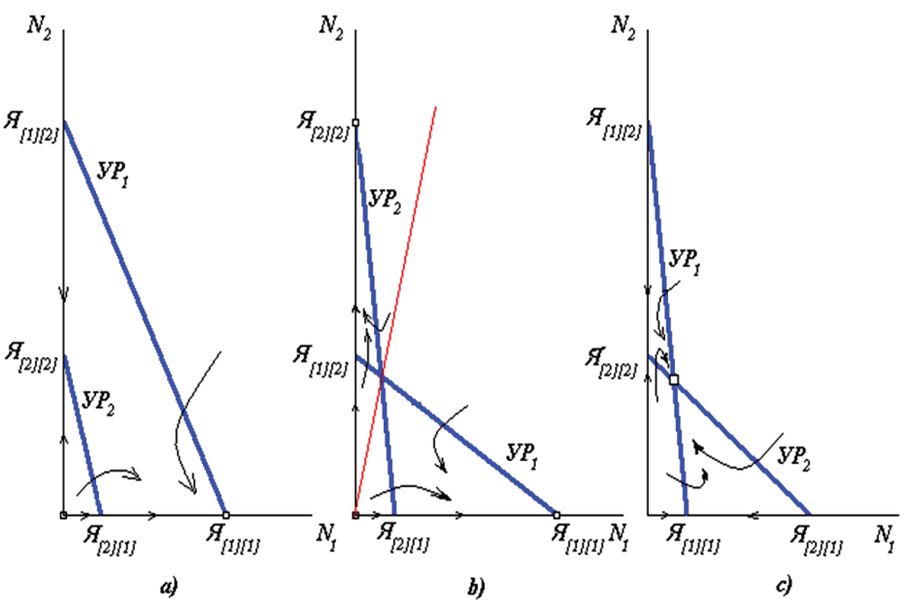
In order to answer the question of "What is optimal?", some methodological work is required. Ideas related to the meaning of optimality in conflicts (i.e. in the context of different interests) emerged and have been developing since a while. In many studies the concept of conflict and optimality in conflict is at the focus of attention in the sense that their non-consideration devoid the whole research of a subject matter. It is enough to mention such phenomena as military conflicts, political struggle, economic confrontations, etc. The presence of competition essentially modifies any predictions, including such regarding certain areas of business.

Let us elaborate on the above using the example of a system of Lotka–Volterra equations used in the research of "convergent evolution" (selection of the most promising directions of development), for instance:

$$\begin{cases} dN_1/dt = \varepsilon_1 \times N_1 - \gamma_{12} \times N_1 \times N_2 - \gamma_{11} \times N_1^2 = УР_1(N_1, N_2) \times N_1; \\ dN_2/dt = \varepsilon_2 \times N_2 - \gamma_{21} \times N_2 \times N_1 - \gamma_{22} \times N_2^2 = УР_2(N_1, N_2) \times N_2. \end{cases} (1)$$

The first coefficients in the right members of the equations ε_1 and ε_2 are the rate of capital growth of two competing directions, the second ones γ_{12} and γ_{22} are the level of interspecific competition (effect of external competitors, or "them"); the third ones γ_{11} and γ_{22} are the indicators of intraspecific competition (effects of internal competitors, or "us"; the development of own production alleviates product shortage, i.e. reduces the commodity prices, thus reducing the rate of production). Here N_1 and N_2 are the dimensions of the competing capitals.

Let us designate as $Я_{[a][b]}$ the crossing coordinates of linear equations $УР_a(N_1, N_2)$ with the axes of variables $(0, N_b)$:



$УР_1$ and $УР_2$ are isoclinic lines of the vertical and horizontal tangents respectively
Figure 1- Phase portraits of Lotka–Volterra equation.

$$Я_{[1][1]} = \frac{\varepsilon_1}{\gamma_{11}},\ Я_{[1][2]} = \frac{\varepsilon_1}{\gamma_{12}},\ Я_{[2][1]} = \frac{\varepsilon_2}{\gamma_{21}},\ Я_{[2][2]} = \frac{\varepsilon_2}{\gamma_{22}}. \quad (2)$$

Depending on the value of those four coefficients and initial values of capital $N_1(0)$ and $N_2(0)$, system (1) allows for three types of solutions that describe three different outcomes of competitive activity (Fig. 1).

Case (a). If $Я_{[1][1]} \succ Я_{[2][1]}$ and $Я_{[1][2]} \succ Я_{[2][2]}$ are simultaneously true, then the first type of business certainly outcompetes its opponent regardless of the "starting" conditions (see. Fig. 1a). The scenario of "selection" of the strongest is realized, the weakest party has no chance to survive.

Case (b). If $Я_{[1][1]} \succ Я_{[2][1]}$ and $Я_{[2][2]} \succ Я_{[1][2]}$, again there is only one winner, but which of the two is the matter of the initial conditions (see. Fig. 1b).

In this case the antagonism between the competitors is so intense that self-restraint does not play a significant role. Case (b) is different from the previous one in that the "weakest" party gets a chance to win through "numerical superiority": a certain "startup capital" that places the winner on the preferable side relative to the separatrix that passes through the point on the phase plain (0,0) and point of intersection of the isoclinic lines of the vertical and horizontal tangents. This case describes a market situation when the key factor consists in the sufficiency of the "critical mass" of the startup capital to nip the competitor in the bud, not allow it to grow up to the level when it has to be dealt with (by sharing the market).

Case (c). The intraspecific competition for both competitors is so intense (each one is preoccupied with the problem of slowing capital expansion due to "internal problems") that the competition among "us" is higher than the pressure of "them" (if $Я_{[2][2]} \prec Я_{[1][2]}$ and $Я_{[1][1]} \prec Я_{[2][1]}$).

In this case both competing parties can coexist on a market for long periods of time (see. Fig. 1c). There is only one stable solution, under which the reproduction rates of new elements in the competing parties offsets the suppression created by the cumulative effect of the factors of internal and external competition.

Such models are, for instance, used for predicting the future development of relatively uniform competing technologies (for instance, due to them having different owners) that have a common "enemy". For instance, for the gas industry such is the nuclear energy, possibly other alternative types of energy, chemical industry that produces materials that substitute gas that is used in synthesis processes, etc.

As we can conclude from the analysis of even the above simplified analytical model, using the tools of "technical analysis" of economic data is not always correct. At least when the dominating factor is not the dynamics of the preceding success, but rather the factors that define the competitive advantage of old (proven) technology as compared to the developing new technology (belonging to both "us" and "them"), when they compete for the same consumer, whose capabilities are limited, methods are required for analyzing competing systems.

3. Algorithm of risk function synthesis

In [2], the author proposed an algorithm for solving the task of resources allocation for critical infrastructure protection against terrorist attacks based on subjective expert estimates. Let us show how quality expert estimates can enable quantitative estimation of a threat by using an algorithm that was previously designated risk synthesis.

So, let us examine a certain (k-th) SCS facility.

As the result of a supposed effect of certain intensity the facility will be damaged by being completely or partially disabled. Let us denote it as X.

Given that not each effect inevitably causes destruction, the protection profile of the k-th facility can be described with an interval representation by defining four matrices:

$$Q_{\min}^{[k]}(i,j),\ Q_{\max}^{[k]}(i,j),\ X_{\min}^{[k]}(i,j),\ X_{\max}^{[k]}(i,j), \quad (3)$$

where $i(i=0,1,\ldots,I^{[k]})$ is the level of protection of the k-th facility (zero level (i=0) corresponds to the current protection status).

The matrix elements are to be interpreted as: if the above facility k with protection level i is subject to an effect with the intensity level j, then with the probability of $Q_{\min}^{[k]}(i,j)$ to $Q_{\max}^{[k]}(i,j)$ the SCS will sustain damage with the magnitude of $X_{\min}^{[k]}(i,j)$ to $X_{\max}^{[k]}(i,j)$.

It is clear that values (3) will be growing as the level of effect j is on the rise and will decrease as the facility's protection level i is growing.

It is obvious that protection at any level requires certain material expenditure both on the part of the item's owner, and the Government. Let us designate the cost of achieving and maintaining the protection of facility k at the i-th level as $Y^{[k]}(i^{[k]})$.

As the total funds allocated for the protection of all facilities are limited, the following inequality must be fulfilled:

$$\sum_k Y^{[k]}\left(i^{[k]}\right) \le Y, \quad (4)$$

where Y is the sum of all costs of protecting a facility, provided that for each facility k protection system variant $i^{[k]}$ is chosen.

In case of natural effects, that unlike man-made effects do not have the benefit of aim and type, i.e. the nature is indiscriminate (like technology failures), the "optimal" protection profile of facilities could be achieved through the sequential execution of the following algorithm:

Step 1. Evaluation of probability $\lambda^{[k]}(j)$ of effect on each k-th facility of the j-th intensity level;

Step 2. Calculation of the median level of the risk effect on the k-th facility of the -th intensity level under the $i^{[k]}$-th protection facility variant:

$$R\left[k;i^{[k]}\right]=\sum_{j=0}^{J}\left\{\begin{array}{l}\lambda^{[k]}(j)\times\left(\dfrac{Q_{\min}^{[k]}\left(i^{[k]},j\right)+Q_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\times\\ \times\left(\dfrac{X_{\min}^{[k]}\left(i^{[k]},j\right)+X_{\max}^{[k]}\left(i^{[k]},j\right)}{2}\right)\end{array}\right\};\quad(5)$$

Step 3. Identification of the magnitude of the prevented risk per unit of protection investment, $\theta[k,i^{[k]}]$:

$$\theta\left[k,i^{[k]}\right]=\frac{R\left[k,i^{[k]}\right]}{Y^{[k]}(i^{[k]})};\quad(6)$$

Step 4. selection for each k-th facility of the maximum value of $\theta[k,i^{[k]}]$:

$$\theta\left[k,i^{*[k]}\right]=\max_{i^{[k]}}\left\{\theta\left[k,i^{[k]}\right]\right\},\quad(7)$$

i.e. the selection of variant $i^{*[k]}$ ensures the maximum reduction of the risk per unit of investment for the k-th facility.

Step 5. Ranking the facilities placing them in the descending order per the value of indicator $\theta[k,i^{*[k]}]$ and counting out the first $\tilde{K}$ facilities with the total costs of protection within the allocated sum Y with the $(\tilde{K}+1)$-th facility falling short of funds.

The essence of the above procedure is simple and clear: there is no point in funding additional protection of the assets that are not threatened (threat values $\lambda^{[k]}(j)$ are low). It is also unnecessary to additionally protect a facility, whose temporary inoperability has practically no effect on the overall losses of the facility's owner ($X_{\max}^{[k]}\left(i^{[k]},j\right)$ are low). And finally, additional protection is unnecessary in facilities that are already protected so well, that losses can be reduces, but that would require unreasonably high costs (i.e. values of $\theta[k,i^{*[k]}]$ are low).

The key factor of the above algorithm is the ranking facilities by the criterion of minimization of the mathematical expectation of losses per unit of funds invested in their protection (their stable operation).

Formula (5) clearly suggests the need for collection and assessment of data per three components:

- values of loss caused by the effects $X_{\min}^{[k]}(i,j)$, $X_{\max}^{[k]}(i,j)$;
- indicator of "aggressiveness of the operating environment" $\lambda^{[k]}(j)$;
- dependence of risks on the types of facilities k.

The values of losses X caused by the fact that SCS are not autonomous business entities must reflect the systemic impact (or socio-economic multieffect) that significantly grows depending on which of the affected facility's product consumers will be most harmed by its inoperability.

Subsequently, one must consider not the medium, but the upper boundaries of the damage indicators and additionally examine a fourth component, i.e. the indicator of importance of continuous operation of the facility due to the cascading increment of the consequences of the facility's lost operability to other businesses.

And finally, a fifth component needs to introduced in order to ensure correct ranking of facilities affected by terrorist attacks. This requirement is due to the fact that if an effect is active and targeted, has values and priorities unknown to security experts and governmental agencies that shift the values of $\lambda^{[k]}(j)$ away from the "industry average". Sometimes, such "additional" values are peculiar. Terrorists, for instance, have a tendency for excessive bloodshed, hostage-taking, ritualized murders, etc. The systemic importance of protecting certain facilities often increases when they are visited by top public officials, Government members, especially attending the inaugurations of politically-significant industrial facilities of not only international, but also regional importance within the country. One can spend a lot of time analyzing the factors that require taking into consideration the specificity of certain criminal activities, but what matters is the fact that criminals act out of their own ideas regarding the effectiveness and feasibility of attacks. Thus, the priorities of target selection shift. What matters to terrorists is not only and not so much the economic warfare, the damage to the facility's owner (as a competitor, as a "tool" to influence the authorities of another nation, etc.), but other aims to be reached by doing damage to a specific SCS' facilities.

The fifth component will help take those circumstances into consideration. Coefficient $\mu^{[k]}$ that initially equals one for all facilities and that, in the DM's or experts' opinion, may be increases in such a way as to increase the priority of exactly the k-th facility for inclusion on the list of facilities equipped with additional measures of protection for reasons that are not taken into consideration according to the common rules. To some extent, the significance of the new indicator $\mu^{[k]}$ is made clearer by the following integration diagram of models.

So, let $\tilde{Z}$ be the estimate of the total resources at the disposal of the forces interested in disrupting SCS facilities safety. If $\tilde{Z}<Z$, then the defending party underestimates the potential effects, if $\tilde{Z}>Z$, then, on the contrary, the effect is being overestimated.

Further, let us examine active intrusion as the most unpredictable case. Let us assume that at the moment of attack planning the intruder has his/her own idea of the amount of resources allocated by the system's owner to the protection of own facilities, i.e. he/she aware of how the "zero option" he/she knows could change.

Intruders are able to choose targets and sets of facilities they will attack. Let the choice be based on their own model of expected damage, i.e., they have at their disposal four similar (3) matrices for each facility: $\tilde{Q}_{\min}^{[k]}(i,j)$, $\tilde{Q}_{\max}^{[k]}(i,j)$, $\tilde{X}_{\min}^{[k]}(i,j)$, $\tilde{X}_{\max}^{[k]}(i,j)$ and own idea of the amount of resources $\tilde{Y}$ been invested by the owner into SCS facilities protection. Similarly, if $\tilde{Y}<Y$, then the

adversary underestimates the facility protection capabilities, if $\tilde{Y}>Y$, then he/she overestimates them. Obviously, an intruder can also either overstate or understate estimate $\tilde{Q}^{[k]}_{\min}(i,j)$, $\tilde{Q}^{[k]}_{\max}(i,j)$, $\tilde{X}^{[k]}_{\min}(i,j)$, $\tilde{X}^{[k]}_{\max}(i,j)$, however, using their freedom of choice they select such set of target facilities and such preparations for attacking specific facilities that would do maximum possible damage.

Let us designate as $\delta^{[k]}(i,j)$ the characteristic function that means that against the *k*-th facility with expected level of protection $i(i=0,1,\ldots,I^{[k]})$ an attack of level $j(j=0,1,\ldots,J^{[k]})$ has been chosen. If for all $i(i=0,1,\ldots,I^{[k]})$ the values of $\delta^{[k]}(i,j)$ are equal to zero, the -th facility will not be exposed to an attack of level *j*. If for all *j* and all *i* the values of $\delta^{[k]}(i,j)$ are equal to zero, the *k*-th facility under the intruder's assumed objectives definitely drops out of the list of targets.

If for some $\tilde{i}$ value $\delta^{[k]}\left(\tilde{i}, j\left(\tilde{i}\right)\right)=1$, we assume that facility *k* with the level of protection 0 has been chosen as the target with level of competence $j\left(\tilde{i}\right)$.

The above properties are written with a set of equations:

$$\begin{cases} \forall k \forall i \forall j \delta^{[k]}(i,j) \times \left(1-\delta^{[k]}(i,j)\right)=0, \\ \forall k \left(\sum\limits_{i=0}^{I_k}\sum\limits_{j=0}^{J}\delta^{[k]}(i,j)-1\right)\times\left(\sum\limits_{i=0}^{I_k}\sum\limits_{j=0}^{J}\delta^{[k]}(i,j)\right)=0. \end{cases} \quad (8)$$

Given that

$$\forall j \sum_{i=0}^{I_k}\sum_{k}\delta^{[k]}(i,j)=N_j \quad (9)$$

and complementing (8), (9) with a set of constraints we obtain the estimate of the total damage sustained by the facility:

$$\tilde{R}=\sum_{k}\sum_{i=0}^{I_k}\sum_{j=0}^{J}\left\{\begin{array}{c}\delta^{[k]}(i,j)\times\left(\frac{Q^{[k]}_{\min}\left(i^{[k]},j\right)+Q^{[k]}_{\max}\left(i^{[k]},j\right)}{2}\right)\times \\ \times\left(\frac{X^{[k]}_{\min}\left(i^{[k]},j\right)+X^{[k]}_{\max}\left(i^{[k]},j\right)}{2}\right)\end{array}\right\}. \quad (10)$$

Let us denote $\tilde{R}$ by $\tilde{R}(Var_I, Var_J)$ and emphasize that $\tilde{R}$ depends on both the facility protection solution Var_I, and the type of attack Var_J. Let us find the maximum of $\tilde{R}$ for all types of attack that comply with the restrictions provided that all additional protection solutions are considered as parameters:

$$\tilde{R}^*\left(Var_I\right)=\max_{Var_J}\left\{\tilde{R}(Var_I,Var_J)\right\}. \quad (11)$$

Thus, we postulate that the adversary (nature) choses the option that is the worst for the defending party. Subsequently, the problem of protection comes down to limiting the attack options. Such measures of facility protection strengthening are found that minimize $\tilde{R}^*\left(Var_I\right)$. In other words, the problem of safety management comes down to finding the equilibrium values of $\tilde{R}^{**}$:

$$\tilde{R}^{**}=\min_{Var_I}\left\{\tilde{R}^*(Var_I)\right\}. \quad (12)$$

The proposed problem definition is typical for the games theory. The solution is a Nash equilibrium, saddle value (Var_{I^*}, Var_{J^*}):

$$\tilde{R}^{**}=\tilde{R}\left(Var_{I^*},Var_{J^*}\right). \quad (13)$$

In this point the defending party is not interested in modifying its equipment strategy Var_{I^*}, as outside this strategy the adversary becomes able to perform more "sensitive" attacks. An active attacker is also not interested in modifying its plan $Var_{J^*}(Var_{I^*})$, as any changes reduces the potential total damage to the SCS facilities and, indirectly, to the nation.

In theory, this definition of the problem has very large dimension and combinatorial complexity, but is quite solvable due to the monotonicity of the criteria and linear nature of the sets of constraints.

The main difficulties of this problem are more about information technology that mathematics:

- for each *k*-th facility it is required to have estimates of the potential consequences of attacks of varied intensity *j*, which is often practically impossible;
- for the whole SCS, it is required to consider risks for the facilities along with other possible, if poorly formalized threats. Optimization of protection is more efficient, the more accurate is the assessment of the potential attack capabilities (those are not uniform both in terms of technology and geographical distribution).

In the light of the above problem definition that takes into consideration the integrated effect the understanding of the efficiency estimation of protection systems changes radically. For cases of active attacks, due to the limited resources at the disposal of the criminal underworld, it should be expected that attacks will be retargeted from well-protected facilities (with low expected effectiveness) to less protected facilities (with high effectiveness, but lower immediate damage). It is obvious that it is not rational to additionally protect facilities that noone attacks. It is possible that there are no attacks exactly because the protection measures are regularly enhanced.

Another key element of the problem under consideration is that the search for effective solutions on both sides is largely about the availability of information:

- a criminal, while preparing for an attack, theoretically looks for accomplices that would help choose a target, that would be attainable given the available competences and equipment;
- the protection system would be able to perform greater concentrated countermeasures if it was aware of the criminals' intentions.

For that reason, in the description of the above procedure for the case of active attack it is repeatedly emphasized that this only refers to assessments on both sides. Due to the inevitable uncertainty of the assessments, the problem of definition of the strategy and tactics of enhancement of SCS facilities protection against possible unlawful acts, including terrorist attacks and sabotage, should be solved by "coarsening" the game formulation [3]. While doing so, the adversary's capabilities are to be "idealized", possible losses are to be overstated by means of, for instance, using median instead of maximum estimates.

In conclusion, let us note that the risk assessment must involve the identification of the relations between the analyzed safety indicators and the high-level indicators (for instance, strategic target indicators) and their effect on the attainment of the target values of such indicators. The supervision of the monitored facility is to be organized in such a way as to enable timely execution of managerial decisions, if facility status is approaching hazard. This problem comprises several tasks, as in vertically integrated companies there are several centers of decision-making at various levels of management. This problem may be efficiently solved by means of methods for the estimation of reliability of target indicator attainment and methods of cluster analysis [3, 4].

4. On the indicators of pre-critical situations

The calculation of the parameters that describe the levels of competition, aside from strategy coded forecasts, require the creation of a monitoring system for "poorly formalized" threats to stable operation and development of SCS, i.e. development of the indicators of pre-critical situations.

Obviously, the development of pre-critical situation indicators is a most complex multilevel task, for which there is no single comprehensive solution, therefore further development of the system for standardization and methodological support of SCS safety management would involve the consideration of a number of additional areas of research in pre-critical situation indicators that is to be conducted within "particular" research paradigms using various theoretical approaches and models:

– datalogical approach;

– energy (balance sheet) approach;

– balance sheet approach (program-based planning);

– system status indication based on group behaviour models of system elements;

– system status indication based on the measurement of the correlations within the dynamics of system component indicators;

– system status indication based on "gray box" models (neural network, support vector machines, etc.).

Let us provide brief descriptions of the above approaches.

Datalogical approach. As part of this approach, the "critical situation" entity C is described as a logical function, the integration of possible "reference" implementations with the "OR" operator:

$$C = \bigcup_n C^{[n]}. \tag{14}$$

Each critical situation $C^{[n]}$ is described with a certain sufficiently large subset of datalogical characteristics (similarly to keywords in a text). Such descriptions, in general, are ambiguous; "synonyms", omissions of "implied" characteristics, etc. are possible. Normally, characteristics are subdivided into three categories: indicators of the status of the investigated system X, indicators of the "neutral" (natural) environment p and indicators of the potential adversary's ("competitor"'s) activities Y:

$$C^{[n]} = F^{[n]}\left\{\begin{matrix} X^{[n,1]},...,X^{[n,K(n)]}; p^{[n,1]},..., \\ p^{[n,L(n)]}; Y^{[n,1]},...,X^{[n,M(n)]} \end{matrix}\right\}. \tag{15}$$

A pre-critical situation (threat of critical situation) is diagnosed as an incomplete set of indicators close to one or several "reference" sets of function arguments $F^{[n]}$. At the same time, it is assumed that the solving system is able to estimate the probability of threat escalation into critical situations. That requires models of natural phenomena and models of competitor behaviour in response to the implementation of certain managerial decisions.

A similar approach is developed within the theory of conflicting structures and theory of heuristics in multi-step position games [5], in the decision theory [6], in some areas of artificial intelligence application [7] (medical diagnostic systems and other pattern recognition systems). In any case, this approach implements a certain automation of hypothesis formation [8] and some mechanisms of "reference" pattern "smearing" [9].

The descriptions of the pre-critical situation models are formalized as event/failure trees/networks that illustrate the logic of scenario development [10]. The synonymy (competition or replacement of risks) is simulated in the form of mutually nested contraction functions of information features $F^{[n]}$, from the contractions of primary features to larger aggregative features [6]. In case of large numbers of primary features, the feature dictionaries are often organized hierarchically [11].

The description of event trees is the prerogative of experts, however, interest has been growing lately in describing complex poorly formalized expert decisions using "genetic" algorithms and other heuristic methods that combine the search for the best description of a complex system (pre-critical situation) and limited logic of evolutionary selection [12].

Energy (balance sheet) approach. The activities of any company include three components: the resource-related component, the science and technology (manufactur-

ing) component and the foreign economic (market) component.

Given the above, the amount of sold goods can be evaluated using the following formula

$$C=E \times C_{eff} \times C_{plan}, \quad (16)$$

where E is the energy required for manufacturing the goods; efficiency coefficient (C_{eff}) ($0 \leq C_{\text{eff}} \leq 1$) reflects the efficiency of the manufacturing process (scientific and technological level of the manufacturer); plan quality coefficient (C_{plan}) lower than one indicates that the product has been manufactured but found no demand (or sold at a lower price), for instance, due to competitors' actions (emergence of alternative sources of energy), or foreign political (economic) circumstances (nonpayment risk, relocation of energy-intensive, polluting industrial facilities to developing countries, etc.).

This approach allows developing indicators of critical situation threats in terms of the probability of production capacity disruption. In this approach, a special attention is given to identifying the "bottlenecks" that define the top rates of goods flow (Gause's principle, Powell's bottleneck, etc.), whose indicators are used in the performance analysis of autopoietic systems accounting for "intraspecific" and "interspecific" competition [13].

Balance sheet approach (program-based planning). Methods of project management (scheduling) can help calculate the dependencies of the probabilities of certain activities completion from the amounts of allocated resources R and time T. Due to physical reasons there are minimal values T_{min} and R_{min}, below which activities cannot be completed in principle. For that reason, in order to improve the probability of activity completion, time and resource margins are created that are assumed to enable work performance in accordance with the approved schedule and within the allocated funds depending on the remaining work effort.

While analyzing the dynamics of time and funds consumption, it is advisable to employ as indicators the data that attest to the approach of the work completion indicators not situated on the "critical" paths in the activity charts to the critical activity indicators. The threat of overabundance of new critical paths for resources and/or time may indicate a pre-critical situation.

All the above approaches imply increasing level of detail of the description of system dynamics within the adaptive control paradigm. In other words, the level of deviation from the chosen work schedule of the considered system are analyzed as if only "external" factors (nature, competition) put the system out of balance, and it is required to measure the probability of crossing a certain barrier of stability.

However, situations may arise when maintaining the balance is impossible or unnecessary, and the system structure is to be reorganized in search of a "new way of living".

System status indication based on group behaviour models of system elements. As of late, prediction of the behaviour of economic system often involves "field" models based on Langevin and Fokker-Plank equations. Such equations describe the dynamics of system elements as a certain "particle hive" that is affected by two types of factors, i.e. factors of drift that shift the center by the action of external forces, and diffusion factors that reflect the freedom of particle migration with the hive. Within the models, hive disintegration or deterioration indicators are developed. Model indicators are estimative in their nature, as they are primarily based on the validity of the law of large numbers (theory of large deflection under random walks).

We can note a close relationship between the "field" models and applied catastrophe theory [14]. For instance, the work shows the proximity between such indicators as "increased large deviations – reduction of time of controlled indicator deviation outside the "corridor", reduction of the "rate of system relaxation to equilibrium states", "deterioration of the Hessian stability matrix".

System status indication based on the measurement of the correlations within the dynamics of system component indicators. Under this definition, critical situations are classified based on the variation of stable (for instance, correlation, causal, associative, information) relations between system elements. The analysis of interconnected economic behaviour of large subsystems (subsidiaries) can be enhanced by the application of findings of gender (family) relations analysis, as well as Gumilyov's mathematical theory of complementarity of ethnic groups [15].

System status indication based on "gray box" models (neural networks).Neural network classification of complex system states is based on the identification of information features and connections between them that correspond to the most common structures of critical situations. Decision rules are obtained by means of programming by example.

As the distribution laws of critical situations are unknown, a large number of parameters and examples are required for their description, therefore the "critical situation – non-critical situation" classification involves certain simplifications.

The following neural network solutions are most efficient for stochastic process simulation: probabilistic neural networks [16], Kohonen self-organizing maps [17] and algorithms with dynamic adaptation to modifiable statistics that describe the coordinates of the "reference" critical situations in the form of growing neural gas that propagates across the description space of examples [18].

Conclusion

All of the above, as well as the requirements of the systems approach to the study of the problems identified in the paper, naturally leads to the requirement to simulate the safety system of SCS as an evolutionary system [19].

Any object of research complimented, if necessary, with some connections to other evolving items, for instance, subjects of research, can be interpreted as such system. The realization of this fact stimulates a more and more active development of this line of research in a variety of fields of study [19-23].

Expert estimates show that the cumulative effect of the application of all available means of situational analysis (identification of hazardous activity, safety declaration, emergency action planning, community awareness of possible emergencies) in terms of reduction of accident rate and unplanned losses may be as high as 10 to 15 %. For instance, the speedy adoption by the European Union of the primary provisions of the Seveso Directive (1982) [24] allowed reducing the accident rate in developed countries 4 to 8 times (from 400 accident, including 75 major ones, in 1983 to 70, including 21 major ones, in 1989). The proposed information and organization measures will become more efficient if all components of the process safety management system responsible for the prediction, prevention and localization of negative consequences are in compliance with single regulations and standards. Subsequently, a process is required of gradual updating of the information, regulatory, predictive and analytical support of process safety activities both at the corporate and institutional levels.

In general, monitoring of the operation of the complex system that is a corporation is a key task of safety management. This monitoring can be compared to preventive therapeutic measures. Unlike in supervisory control that aims to quickly react to the ever-evolving situation, localize the occurring emergencies, sometimes perform (again, using a medical analogy) "surgical" intervention, the monitoring center (in the future, a network of centers for collection of reliable information on the changes occurring within SCS) is to predict the onset of negative trends in the SCS environment, in its internal processes in order to suggest remedial actions that could prevent the transformation of the identified threats into emergencies and crises.

References

[1] Bochkov A.V. On the nature of risk in the safety management of structurally complex systems. Dependability. 2019;4:54-66. URL: https://doi.org/:10.21683/1729-2646-2019-19-4-54-66.

[2] Bochkov A.V., Ushakov I.A. Solving the task of resources allocation for critical infrastructure protection against terrorist attacks based on subjective expert estimate. *Dependability*. 2015;1:88-96. Available at: https://doi.org/10.21683/1729-2646-2015-0-1-88-96

[3] Bochkov A.V., Zhigirev N.N., Lesnykh V.V. Dynamic Multi Criteria Decision Making Method for Sustainability Risk Analysis of Structurally Complex Techno-Economic Systems. Reliability: Theory & Applications. 2012;1;2(25):36-42.

[4] Bochkov A.V., Zhigirev N.N. Ram M., Davim J., editors. Development of Computation Algorithm and Ranking Methods for Decision-Making under Uncertainty. Advanced Mathematical Techniques in Engineering Science. CRC Press. Series: Science, Technology and Management. 2018;May, 17:121-154.

[5] Lefebvre V.A. Conflicting structures. Moscow: Sovietskoie radio; 1973.

[6] Muschick E., Muller P. Methods of engineering decision-making. Moscow: Mir; 1990.

[7] Popov E.V., Fomin I.B., Kisel E.B. et al. [Statistical and dynamic expert systems]. Moscow: Finansy i statistika; 1996. (in Russ.)

[8] Hajek P., Havranek T. Mechanizing hypothesis formation. Moscow: Nauka; 1984.

[9] [Fuzzy sets and possibility theory]. Moscow: Radio i sviaz; 1986. (in Russ.)

[10] Podinovsky V.V., Nogin V.D. [Pareto-optimal solutions of multicriterion problems]. Moscow: Nauka; 1982. (in Russ.)

[11] Jambu M. Classification automatique pour l'analyse des données. Moscow: Finansy i statistika; 1988.

[12] Price K.V. Genetic Annealing. Dr. Dobb's Journal. 1994;19(11):117.

[13] Ebeling W., Engel A., Feistel R. Physik der Evolutionsprozesse. Moscow: Editorial URSS; 2001.

[14] Gilmore R. Catastrophe theory for scientists and engineers. Moscow: Mir; 1984.

[15] Guts A.K., Korobitsyn V.V. [Mathematical models of social systems: Study guide in 2 volumes]. Omsk: OmSU; 2000. (in Russ.)

[16] Specht D. Probabilistic Neural Networks. Neural Networks;1990:1.

[17] Kohonen T. Self-Organizing Maps. Springer-Verlag; 1995.

[18] Fritzke B. Tessauro G., Touretsky D.S., Leen T.K., editors. A growing neural gas network learns topologies. Advanced in Neural Information Processing Systems 7. Cambridge (MA): MIT Press; 1995.

[19] Glushkov V.V., Ivanov V.V., Yanenko V.M. [Simulation of evolutionary systems]. Moscow: Nauka. Main office of physics and mathematics; 1983. (in Russ.)

[20] Nikolis G., Prigozhin I. Chizmazhev Yu.A., editor. [Self-organization in nonequilibrium systems]. Moscow: Mir; 1979. (in Russ.)

[21] Reutov A.P., Savchenko R.G., Suslov R.M. [System model as a relation of generalized properties: order, dependability and efficiency]. In: [Matters of cybernetics (system development management)]. Moscow: 1979. (in Russ.) Moscow: 1979. 26 – 34.

[22] Romanovsky Yu.M. [Self-organization processes in physics, chemistry and biology]. Moscow: Znanie; 1981. (in Russ.)

[23] Ganti T. A theory of Biomedical supersystems and its application to problems of natural and artificial biogenesis. Budapest: Akademiai; 1979.

[24] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major accident hazards involving dangerous substances. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018&from=en (accessed 17.02.2017).

About the author

Alexander V. Bochkov, Candidate of Engineering, Deputy Head of Unit for Analysis and Ranking of Controlled Facilities, Administration, Gazprom gaznadzor, Russian Federation, Moscow, e-mail: a.bochkov@gmail.com

The author's contribution

The author suggested a method of risk synthesis (with game problem definition of countering possible external effects of various nature on critical infrastructure facilities) as one of the foundations of the design of advanced systems for monitoring safety threats to structurally complex systems. Key methodological premises were formulated: from general problem definition of safety management through the synthesis of a model of a controlled facility and its external and internal connections, solution to the problem of selection of priority protection facilities in terms of assuring efficient operation and general safety of structurally complex systems.

Gnedenko e-Forum

International Group on Reliability

http://www.gnedenko.net

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc.

Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications".

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.

Join Gnedenko Forum!

Welcome!

More than 500 experts from 44 countries worldwide have already joined us!

To join the Forum, send a photo and a short CV to the following address:

Alexander Bochkov, PhD

a.bochkov@gmail.com

Membership is free.

REQUIREMENTS OF EDITION ON EXECUTION OF PAPERS IN JOURNALS OF PUBLISHING GROUP OF IDT PUBLISHERS

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 109029, Moscow, Str. Nizhegorodskaya, 27, Building 1, office 209, LLC "JOURNAL DEPENDABILITY" or e-mail: dependability@bk.ru (in scanned form).

The letter should be attached to a paper text containing the summary and keywords, information on authors, bibliographic list, and one complete set of figures. All listed items are to be presented in an electronic form (on CD or via the e-mail address provided above).

Attention! Titles of papers, names of authors, summary and keywords must be presented, in Russian and English languages, according to the requirements of the Higher Attestation Commission. The information on each author should contain the following standard data:

- Surname, name, patronymic;
- Scientific degree, academic status, honorary title;
- Membership of relevant public unions, etc.;
- Place of employment, position;
- The list and numbers of Journals of IDT Publishers in which papers of the author have been previously published;
- Contact information.

Texts should be presented in Word 97-2003 format in a 12-point typeface; the text should not be formatted. Paragraphs should be arranged by pressing the "return" key. The text of the paper should be double-spaced on pages of A4; on the left there should be a margin of 2 cm; pages should be numbered, the «first line indent» is obligatory.

All alphabetical designations represented in figures should be explained in the body text or in a legend. Inconsistencies between designations in figures and in the text are inadmissible. Numbering should only be applied to those formulas and equations that are referred to in the text.

Simple formulas appearing directly in the text (for example, m^2, n^2t, $c = 1 + DDF - A_2$), and the Greek letters and symbols, for example, β, © may be typed using the Symbol font. When it is not possible to type directly in the text editor, use the "Microsoft Equation" formula editor (available with the complete installation of Microsoft Office) or the "Mathtype" formula-editing program. Representation of formulae in the text in the form of images is not admissible. Photos and figures for papers should be provided in individual files with extension TIF, EPS or JPG with a resolution of not less than 300 dpi. The list of literature referred to in the paper (bibliography) is presented according to order of citation and provided at the end of paper. References to the literature in the text are marked by serial numerals in square brackets.

To authors that are published in journals of "IDT Publishers".

In addition to the journal, information on each author will be presented at the techizdat.ru site in the «Authors» section on the individual web page.

Authors of papers for publication have the opportunity to send an electronic photo and additional material to appear on this individualised Internet-business card. At their own discretion, authors can present more details about themselves, interesting examples and stories of solutions to technical problems, about contemporary problems according to subjects of corresponding journal, etc. This material should not exceed 1000 characters including spaces.

SUBSCRIPTION TO THE JOURNAL «DEPENDABILITY»

It is possible to subscribe to the journal:

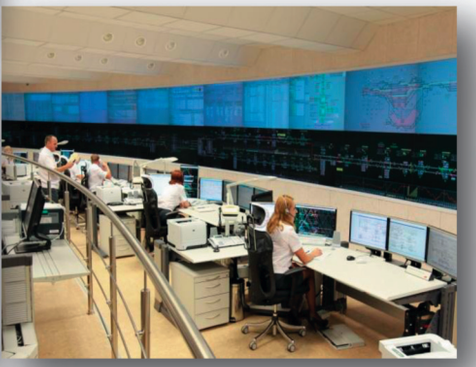
- Through the agency «Rospechat»
  – for the first half of the year: an index 81733;

- Under the catalogue "Press of Russia" of the agency «Books-services»:
  – for half a year: an index 11804;

- Through the editorial office:
  – for any time-frame
  tel.: +7 (495) 967-77-05; e-mail: dependability@bk.ru

THE JOURNAL IS PUBLISHED WITH PARTICIPATION AND SUPPORT

OF JOINT-STOCK COMPANY RESEARCH & DESIGN INSTITUTE
FOR INFORMATION TECHNOLOGY, SIGNALLING AND TELECOMMUNICATIONS
ON RAILWAY TRANSPORT (JSC NIIAS)



JSC NIIAS is RZD's leading company in the field of development of train control and safety systems, traffic management systems, GIS support technology, railway fleet and infrastructure monitoring systems

Mission:

transportation

- ❑ efficiency,
- ❑ safety,
- ❑ reliability

Key areas of activity

- Intellectual control and management systems
- Transportation management systems and transport service technology
- Signalling and remote control systems
- Automated transportation management centers
- Railway transport information systems
- Geoinformation systems and satellite technology
- Transport safety systems
- Infrastructure management systems
- Power consumption and energy management systems
- Testing, certification and expert assessment
- Information security
- Regulatory support

www.vniias.ru