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 OOO Otmara.net. 2/1 bldg 2,
Verkhiaya Krasnoselskaya St., floor 2, premise II,
rooms 2A, 2B, 107140, Moscow, Russia.

Circulation: 500 copies.
Printing order
Papers are reviewed. Signed print 21.06.2021,
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»)

CONTENTS

Effectiveness retention ratio and its standardization

Victor A. Netes, *Moscow Technical University of Communications and Informatics, Moscow, Russian Federation*
v.a.netes@mtuci.ru

Victor A. Netes

Abstract. Aim. *To promote a better understanding, a wider and more correct application of the effectiveness retention ratio. That is the measure that is best suited for assessing the dependability of complex technical systems, in which partial failures are possible that put a system into intermediate states between complete up and down ones.* **Methods.** *The paper uses the methods of the probability theory and comparative analysis of texts of interstate (Euro-Asian), Russian and international dependability-related standards.* **Results.** *The principal contribution of Russian researchers to the creation and development of methods for applying effectiveness indicators to estimating the dependability of complex systems is pointed out. Shortcomings were identified in the basic dependability-related standards as regards the effectiveness retention ratio and related concepts. Namely, in terminology standard GOST 27.002–2015, the phrases that require improvement are indicated. They relate to the concepts of partial failure, partial up state and partial down state. A broader and more accurate definition of partial failure is suggested. It is noted that the relationship between partially up and partially down states are to be discussed and clarified. GOST 27.003–2016 that establishes the content and general rules for specifying dependability requirements contains wording errors in the classification of items according to the number of possible (taken into consideration) states and in the examples of possible variants of the effectiveness retention ratio in various branches of technology that are probabilities of task completion, etc. The paper suggests corrections to the appropriate wordings. It has been established that although the effectiveness retention ratio is not referred to in the international dependability-related terminology standard (IEC 60050-192:2015), it implicitly appears in two IEC standards (IEC 61703:2016 and IEC 62673:2013), in which it is assigned to availability measures.* **Conclusion.** *The paper's findings will be useful to experts involved in the assessment and standardization of complex technical system dependability. Their implementation will help improve interstate, Russian and international dependability-related standards.*

Keywords: *complex system, dependability, partial failure, effectiveness retention ratio, output effect, interstate (Euro-Asian), Russian and international standards.*

For citation: *Netes V.A. Effectiveness retention ratio and its standardization. Dependability 2021;2: 3-8. https://doi.org/10.21683/1729-2646-2021-21-2-3-8*

Received on: *12.02.2021* / **Revised on:** *12.04.2021* / **For printing:** *21.06.2021.*

Introduction

Conventional dependability measures that characterize reliability and availability are defined on the assumption that a technical item can be in one of two states: up or down. However, many complex systems are characterized by partial failures that put the item into an intermediate state with reduced (partial) operability. The main dependability measure for such systems is the effectiveness retention ratio (ERR) that was covered in a number of publications referred to below.

The purpose of this paper is to promote a better understanding of the ERR, its broader and more correct application. It is intended for experts involved in the assessment and standardization of complex system dependability. The author analyses the degree and correctness of how ERR is captured in interstate, Russian and international standards adopted over the recent years. The concepts of partial failure and partially up and down states closely associated with ERR are also examined. The conducted analysis revealed the shortcomings present in those standards. Appropriate corrections are suggested.

Background

The need to consider systems with more than two levels of operability became clear as early as in 1960s. That was mentioned in the classic monograph [1]. In particular, it states that "the concept of failure associated with a complete or significant loss of operability of a [complex] system appears to be quite artificial. <…> In such cases, dependability of a system should be understood as the stability of efficiency subject to the dependability of the parts the system is composed of" [1, p. 84]. However, this idea was not further developed in this book. In the general mathematical model, the dependability measures were defined on the basis of the phase space where a set of down states was specified.

The credit for the initial systematic description of the effectiveness calculation methods is due to I.A. Ushakov [2]. He has also done a lot to popularize this area of research. The appropriate sections were included in the commonly-used guidebooks [3–6]. However, his publications dealt with absolute effectiveness values determined with regard to dependability, whereas the other factors that affect effectiveness were practically ignored. Later, I.A. Ushakov arrived to the conclusion that a non-dimensional indicator should be considered that shows the relative decrease in the operating effectiveness of a system as its elements fail [7, p. 131], i.e., the ERR .

The first book that thoroughly examined the ERR , was [8]. It is well complemented by [9] that describes the process of ERR evaluation using computational and experimental method. These books are still relevant these days and can be recommended to anyone interested in the topic. An overview of further findings as regards the ERR calculation and evaluation was presented in [10].

Definition and meaning of the ERR

The ERR can be found in Russian dependability-related terminology standards as early as 1983. The definition has not changed much ever since, and in the current standard [11] is as follows: the ratio of the value of the effectiveness indicator of an item's intended use over a certain period of operation to the nominal value of this indicator calculated under the assumption that the item is not affected by failures during the above period. In the international standards, this measure is not explicitly defined.

If we denote the item's application effectiveness indicator as E and its nominal value is E_0, then the ratio defining the ERR denoted as R_{ef} is as follows: $R_{ef} = E/E_0$. It should be emphasized that this formula defines what the ERR is, but does not provide the method for its practical calculation [8].

The effectiveness of an item's intended use is understood as its property to create a certain useful result (output effect) over the period of operation under certain conditions [12]. The output effect is defined as the useful result obtained in the course of the item's operation. It can be defined in a number of ways. For instance, the output effect can be the revenue generated by an item's operation and be expressed in monetary units. However, natural measures are more commonly used. Below are examples of the output effect for various types of systems:

- production systems, the quantity of released products (in pieces, tons, cubic meters, hectolitres, etc.);
- various service systems, the number of successfully served users or requests;
- transportation systems, the quantity of transported goods (in tons, cubic meters, etc.) or number of transported passengers;
- information and communication systems, the amount of transmitted, collected or processed information.

Usually, the mathematical expectation (average value) of the output effect is used as the effectiveness indicator. The meaning of the ERR is quite simple. For instance, let output effect be income, while R_{ef}= 0.98. This means that, due to failures, the income generated by the item decreases on average by 2%.

Additionally, the probability of task completion can be taken as the effectiveness indicator. That is justified for intermittently operating and single use items [12]. The probability of task completion can also be represented as the mathematical expectation of the output effect. Indeed, if we set the output effect to 1 in the case the task has been completed , and 0 if otherwise, the mathematical expectation of such random value is equal to the probability that it takes the value of 1, i.e.,

the probability of task completion . In such situation, the ERR takes a direct probabilistic meaning. It is equal to the probability that the task completion will not be disrupted by failures [8].

The ERR can also apply to items all of whose states can be clearly divided into up and down. That being said, it usually comes down to such conventional dependability measures as availability, reliability, interval reliability [8]. In such situations, the ERR-based approach facilitates the correct selection of standardized measures .

Partial failure, partially up and partially down states

As noted above, the ERR is primarily required for systems that might be affected by partial failures. This concept is introduced in [11] in the note to the term "failure", where it is stated that a partial failure is characterized by the transition of an item into a partially down state. Unfortunately, [11] provides no explanation of what that means, yet sets forth the concept of "partially up state", i.e., a state of an item, in which it is capable of performing some functions, but at the same time is unable to perform some others. That definition is given in the note to the terms "up state" and "down state". Thus, there is an inconsistency.

The question regarding the relationship between the partially up and partially down states can be answered in different ways. In the author's opinion, those are essentially the same thing. For example, if, in a certain state, the output effect is 70% of the maximum value, then such state is 70% (partially) up and 30% (partially) down. That can be interpreted as the fuzzification of the failure criterion, i.e., the division of the whole set of states of an item into two complementary fuzzy subsets of up and down states (for the first time this idea was expressed in [13]). At the same time, some authors distinguish between the partially up and partially down states, believing that the former is closer to up state, and the latter is closer to down state [14, p. 53]. The issue therefore requires discussion and clarification.

Additionally, the definitions of partial failure and partially up/down state in [11] trace to the international terminology standard [15] and are only applicable to multifunctional items. However, those concepts should be considered for single-function items as well. For example, a process system may operate at reduced performance. Therefore, the associated wordings should be adjusted. In particular, a partially up/down state is to be defined as a state of an item with a reduced ability to function as required that is characterized by the loss of the ability to perform some, but not all, required functions or a reduced output effect. That will be close to the definition of the term "degraded state" in [15].

GOST 27.003-2016

The contents and general rules for specifying dependability requirements are set out in standard [12]. The ERR is among the dependability measures used in it. This standard was adopted to replace [16] and largely repeats its basic provisions. Unfortunately, among the modifications made to [12] some are positive, but some are erroneous.

Let us start with the positive changes. While [16] refers to products, [12] uses the more general term "item" (although this replacement was not done throughout the text and the word "product" is still found in the text). The relationship between these two concepts was thoroughly analysed in [17], so this matter is not addressed herewith. In [12], a useful note was added that explains the meaning of effectiveness and defines output effect (those were given above).

On the other hand, a frustrating mistake was made in one of the paragraphs of [12] that is important for understanding the scope of the ERR application. It was briefly mentioned in [18]. The matter is that among the primary features, based on which items are classified as part of dependability requirements specification, is the number of possible (taken into consideration) states of an item in terms of operability in operation. Based on that feature, [16] identified products of type I that, in the course of operation, can be in two states, i.e., up or down, and type II that, aside from the two above states, can be in a number of partially up/down states initiated by partial failure. Standard [12] dropped the nondescript types designated by Roman numerals, but the corresponding paragraph of the standard (6.3.2) contains a nonsensical wording stating that items are subdivided into those that are in up state and those in down state.

The correct wording of this paragraph is as follows: in terms of the number of possible (taken into consideration) states (operability-wise), items are classified as: items that, in the course of operation, can be in two states, i.e., up or down, and items that, apart from the two above states, can be in a number of partially up/down states initiated by partial failure.

Additional explanations concerning the ERR are given in Annex A that is identical to that in [16]. It states that the ERR is a generalized term denoting a group of measures used in a number of industries with their own names, designations and definitions. Unfortunately, several probabilistic measures are erroneously listed among the examples: "probability of specified output of a certain quality per work shift (month, quarter, year)" for process systems, "probability of mission program completion" by a spacecraft, "probability of typical mission (flight mission) performance within a given time" by a plane. The error is that dependability and ability to perform a task (program, mission, etc.) must be distinguished. That matter was discussed in

detail in [19]. Indeed, an item's ability to perform a task may depend on factors that are not related to its dependability. For example, a completely operable aircraft may fail to complete a task (flight mission) due to adverse weather conditions or improper actions by ground services. However, as noted above, the probability of task (program, mission, etc.) completion may be an effectiveness indicator used for determining the ERR .

GOST R 27.010-2019 (IEC 61703:2016) and IEC 62673:2013

Standard [20] is based on the IEC standard [21] and is its modified version. It contains item 6.1.2.4 entitled "Extending the concept of availability factor to items with multiple states". It examines systems whose states, as pointed out above, "cannot be classified as up and down only, and more accurate classification is required". It is noted that "this is especially common for the production of outputs, including oil, gas, electricity, water, etc." For such systems, a measure is defined that is described as "a generalization of the average availability factor and the mathematical expectation of performance often called the "production availability" of a system. More broadly, it is also called the item performance". A simple example is given for a production system, for which this measure is calculated along with the conventional availability factor.

In this case , the standard refers to monograph [22]. In its preface, the authors express their gratitude to their teacher and friend, I.A. Ushakov, but while presenting the basic concepts associated with multi-state systems, they use only one example out all his works, the one taken from [6].

In fact, the measure examined in the above item in [20, 21] is an ERR . Unfortunately, in [20], this fact is not even mentioned. It is clear that [20] is based on the IEC standard. However, that is a modified standard. The changes are that references to international standards are replaced with references to national standards. The above item 6.1.2.4 should also have been amended to indicate that it refers to ERR . The reference to [22] should be replaced with a reference to a Russian subject matter publication, preferably [8].

In general, the reference list in [20] should have been further modified. The American version of [1] in English should have been replaced with the original Russian version. A number of books on the list have been translated into Russian (by R. Barlow and F. Proschan, W. Feller, D.R. Cox). The Russian publications should have been referenced instead, which would be much more convenient for the Russian users of the standard.

As a side note, we would like to make another observation regarding many standards developed on the basis of international standards. We are talking about the discrepancy with other dependability-related standards in terms of terminology and notations. In particular, in [20], the availability factor is designated as A, although in Russia it is conventionally designated $K_г$, which is stipulated in standard [12]; for continuously operating item and intermittently operating item English abbreviations (COI and IOI) are used instead of Russian ones set in [12], etc. In such situations, one would want to follow suite of the authors of [23] and exclaim "What to believe?" It is clear that there is a conflict between the principles of continuity and proximity to international standards [24], but the standard developers must find a reasonable middle ground. For instance, the dependability measures and types of items could be designated according to both the international and Russian convention (as it is done for physical values in [25]).

Another IEC standard, in which the ERR is implied is [26] (you can learn about it in [27]). It is dedicated to the dependability of communication networks, the feasibility of the ERR's application to which was shown in [28–31]. In [26], it is recommended to use two measures, i.e., end-to-end network availability and full-end network availability designed to assess dependability from the point of view of the end users and network operator/service provider, respectively. The former is the availability factor of a node-to-node connection and the latter is the weighted sum of such availability factors for different pairs of nodes and actually turns out to be the ERR [27, 30, 31].

Conclusion

One of the achievements of the Russian school of dependability that should not be forgotten is the definition and development of the ERR calculation and evaluation methods. Our representatives in the IEC TC 56 should make efforts to incorporate this measure into international standards, especially since they already implicitly imply it. This challenge is motivated by one of the goals defined in Article 3 of the Federal Law FZ-162 "On Standardization", i.e., to promote the integration of the Russian Federation into international standardization systems as an equal partner.

Unfortunately, interstate standards contain inaccuracies as regards ERR . Specifically, in GOST 27.002-2015, the wording associated with the terms "partial failure" and "partially up/down state" are to be clarified. In GOST 27.003–2016, it is required to make corrections to the wordings in the classification of items in terms of the number of possible (taken into consideration) states and in the examples of possible ERR variants in various branches of technology that are probabilities of task completion, etc. The paper suggests the appropriate adjustments.

The Russian standard GOST R 27.010–2019 developed on the basis of an IEC standard does not fully comply with the above basic standards for dependability and ignores the Russian ERR developments. In general, speaking on the subject of Russian and interstate standards created on the basis of international ones, one should remember the words of I.A. Ushakov written by him while the draft of one of those documents was being discussed: "The basic idea of the domestic standard is not to follow blindly the letter of the IEC recommendations, but to ensure the most complete conformity to the spirit of these recommendations, yet be sure to capture the immense domestic experience in the theory and practice of dependability and over half a century of domestic technical documentation and scientific and technical literature." We would like to direct this message to all standard-makers.

References

1. Gnedenko B.V., Belyayev Yu.K., Solovyev A.D. [Mathematical methods in the dependability theory]. Moscow, Nauka; 1965. (in Russ.)
2. Ushakov I.A. [Efficiency of complex systems operation]. In: [On the dependability of complex technical systems]. Sov. radio; 1966. (in Russ.)
3. Kozlov B.A., Ushakov I.A. [Brief handbook for dependability calculation of electronic equipment]. Moscow: Sov. radio; 1966. (in Russ.)
4. Kozlov B.A., Ushakov I.A. [Handbook for dependability calculation of electronic and automation equipment]. Moscow: Sov. radio; 1975. (in Russ.)
5. Ushakov I.A., editor. [Dependability of technical systems: a handbook]. Moscow: Radio i sviaz; 1985. (in Russ.)
6. Ushakov I.A., editor. Handbook of dependability engineering. New York: John Wiley & Sons; 1994.
7. Ushakov I.A. [Course of systems dependability theory]. Moscow: Drofa; 2008.
8. Dzirkal E.V. [Specification and verification of dependability requirements of complex products]. Moscow: Radio i sviaz; 1981. (in Russ.)
9. Rezinovsky A.Ya. [Dependability testing of radioelectronic complexes]. Moscow: Radio i sviaz; 1985. (in Russ.)
10. Netes V.A. Effectiveness retention ratio: a dependability measure for complex systems. Dependability 2012;4:14-23.
11. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)
12. GOST 27.003-2016. Industrial product dependability. Contents and general rules for specifying dependability requirements. Moscow: Standartinform; 2018. (in Russ.)
13. Netes V.A. [Method of estimating complex systems dependability and its application to tree-like information networks]. *Proceedings of ZNIIS* 1976;2:17-23. (in Russ.)
14. Dedoborshch V.G., Sutorikhin N.B, editors. [Dependability and maintenance of software -controlled automatic trunk telephone exchanges]. Moscow: Radio i sviaz; 1989. (in Russ.)
15. IEC 60050-192:2015. International electrotechnical vocabulary. Chapter 192. Dependability.
16. GOST 27.003-90. Industrial product dependability. Contents and general rules for specifying dependability requirements. Moscow: Standartinform; 2007. (in Russ.)
17. Netes V.A. Item in dependability: definition and content of the concept. Dependability 2019;19(4):3-7.
18. Netes V.A. [How to regain trust? About the system of standards "Dependability in engineering"]. *Standarty i kachestvo* 2019;2:19-24. (in Russ.)
19. Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what "dependability" is. *Dependability* 2014;4:15-26.
20. GOST R 27.010–2019 (IEC 61703:2016). Dependability in technics. Mathematical expressions for reliability, availability, maintainability measures. Moscow: Standartinform; 2019. (in Russ.)
21. IEC 61703:2016. Mathematical expressions for reliability, availability, maintainability and maintenance support terms.
22. Lisnianski A., Frenkel I., Ding Y. Multi-state system dependability analysis and optimization for engineers and industrial managers. London: Springer-Verlag; 2010.
23. Yershov G.A., Semerikov V.N., Semerikov N.V. [What to believe? On the system of standards "Dependability in engineering"]. *Standarty i kachestvo* 2018;8:14-19. (in Russ.)
24. Netes V.A. The principles of dependability terminology standardization. *Dependability* 2020;2:19-23.
25. GOST 8.417–2002. State system for ensuring the uniformity of measurements. Units of quantities. Moscow: Standartinform; 2018. (in Russ.)
26. IEC 62673:2013. Methodology for communication network dependability assessment and assurance.
27. Netes V.A. [Communication networks dependability in the IEC standards]. *Vestnik sviazi* 2014;2:13-15. (in Russ.)
28. Netes V.A., Smetanin L.D. [Application of the effectiveness retention ratio for dependability analysis of communication systems]. *Elektrosviaz* 1988;12:9-12. (in Russ.)
29. Netes V.A. Choice of reliability indexes for access networks. *Last mile* 2019;8:52-55. (in Russ.)
30. Netes V. Dependability measures for access networks and their evaluation. Proc. of the 26th Conf. of Open Innovations Association FRUCT; 2020. P. 352-358.

31. Netes V. Modern network technologies and dependability. Proc. of the 3d Intern. Science and Technology Conf. Modern Network Technologies 2020. P. 104-113.

About the author

Victor A. Netes, Doctor of Engineering, Professor of the Department of Telecommunications Networks and Switching Systems, Moscow Technical University of Communication and Informatics, Moscow, Russian Federation, e-mail: v.a.netes@mtuci.ru.

The author's contribution

Netes V.A. analysed interstate, Russian and international dependability-related standards in terms of definitions and other wordings related to the effectiveness retention ratio and related concepts (partial failure, partially up and partially down states), identified existing shortcomings and suggested corrections.

Conflict of interests

The author declares the absence of a conflict of interests.

Specificity of the development of the damage process to network structures of pipeline transportation systems

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

Igor A. Tararychkin

Abstract. Introduction. *Industrial pipeline transportation systems are complex, potentially hazardous engineering facilities that ensure the delivery of specified amounts of a target product to consumers. The development of emergencies associated with the transition to the down state of a certain number of pipelines may result in the disconnection of some or all the product consumers from the source. If the system's linear elements transition to the down state in a random order, such a change of the network structure is called a progressive damage. A progressive damage is especially hazardous if, in the course of maintenance activities, a part of the system or a set of process pipelines is disconnected. The* **Aim** *of the work is to identify the change patterns of pipeline system resilience when affected by progressive damage and to develop practical recommendations for ensuring the resilience of such systems in operation and during maintenance operations.* **Methods of research.** *The resilience of systems as the capability to resist progressive damage was evaluated with an indicator that represents the average fraction of pipelines whose transition into the down state causes the disconnection of all consumers from the source of the product. The resilience values were defined by means of computer simulation. The network structure and the nature of the existing intersystem communications were defined using an adjacency matrix.* **Results.** *Damage to a transportation network structure is regarded as a result of a two-stage process. At the stage of target transformation, linear elements are purposefully excluded from a full graph-based structure, bringing the network to a certain initial state. At the second stage, the original structure is transformed according to the mechanism of progressive damage. Such approach allows correctly assessing the changes in the resilience of complex network structures and their ability to resist the development of the processes of damage. The paper sets forth calculated characteristics that allow predicting the behaviour of pipeline networks affected by emergencies. The existence of limit network structures is demonstrated that prove to be very vulnerable to the development of progressive damage.* **Conclusions.** *As the process of targeted transformation goes on, the ability of newly formed network structures to resist the development of progressive damage progressively diminishes. The lowest level of pipeline system resilience against the development of the process of progressive damage can be observed as the structure of the network nears the limit state. When preparing maintenance activities with scheduled exclusion of a number of linear elements from an active pipeline system, the proximity of the newly built network structure to the limit state should be assessed along with the resilience of the restored system to possible development of progressive damage.*

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

For citation: *Tararychkin I.A. Specificity of the development of the damage process to network structures of pipeline transportation systems. Dependability 2021;2: 9-16. https://doi.org/10.21683/1729-2646-2021-21-2-9-16*

Received on: *14.03.2021 /* **Revised on:** *30.04.2021 /* **For printing:** *21.06.2021.*

The operation of industrial pipeline transportation systems in nominal operating conditions is associated with the delivery of the required quantities of the target product from the source to individual consumers. Efficiently managing transportation flows and achieving specified process conditions is enabled by the complex network structure and redundant internal communications [1-4]. Such systems are utility facilities, whose condition is to be assessed and that must be repaired accordingly [5-7].

The operation of various pipeline systems [8-10] is associated with the development of degradation processes that define the probability of failure of individual structural elements [11]. Interactions with the environment are diverse [12,13] and create risks one needs to considered and be able to assess [14].

In general, the processes within the systems are multifactor, while their analysis and identification of current state of the network entities is a complex engineering problem [15]. Under such circumstances, emergencies imply the removal of individual pipelines (linear elements) from operation and redistribution of transportation flows within the system.

If the system's linear elements progressively transition to the down state in a random order, such a change of the network structure is called a progressive damage [16].

Progressive damage is a hazardous scenario that transforms an initial transportation network into a set of point elements disconnected from each other. This state of the network entity is characterized by a null-graph, i.e., a graph with no edges.

In practice, achieving such state is impossible, for obvious reasons. Nevertheless, researching the properties of network entities affected by progressive disruption of communications within a system and the reduction of the number of linear elements is of practical interest, while the established process patterns should be taken into account while planning repair and ensuring the stability of the restored pipeline transportation systems.

It is obvious, that resilience as the ability of a system to resist the development of progressive damage depends on the number of the consumers, nodes, linear elements and the nature of the communications between them. Comparing the resilience of different network entities is only possible if they are comparable, i.e., the number of the following is identical:

- end product consumers;
- transportation nodes;
- linear elements.

This means that the failure of even one pipeline does not allow comparing the properties of the original and newly formed system correctly due to differences in the quantitative composition of linear elements.

This circumstance makes it difficult to analyse and evaluate the impact of structural changes on the system's ability to resist the development of progressive damage. In this context, it is required to develop new methods of assessing the properties and behaviour of transportation systems affected by progressive damage.

The technical literature on the behaviour of pipeline systems in emergencies is often insufficient to assess the expected impact of project decisions, which requires further research.

The aim of the work is to identify the change patterns of pipeline system resilience when affected by progressive damage and to develop practical recommendations for ensuring the resilience of such systems in operation and during maintenance operations.

Structural changes in a transportation network as the outcome of a two-stage process

Let us assume that the solution of a certain design problem is associated with the requirement to assess the resilience to progressive damage of the network structures shown in Figure 1. Each of them includes a source of product A, as well as consumers B and C. The first one contains 8, while the second one contains 7 linear elements.

If, in the course of progressive damage, a linear element fails at each point of the system time, a comparison of the resilience of the examined facilities is not valid, as their ranges of system time values do not match. For that reason, the relationship between the number of linear elements in a network and the resilience of a system against progressive damage should be studied on the basis of a different conceptual approach.

Let us examine the matter more in detail. The structure shown in Fig. 1b can be represented as a result of a transformation associated with the exclusion of a linear element from a more complex structure shown in Fig. 1a.

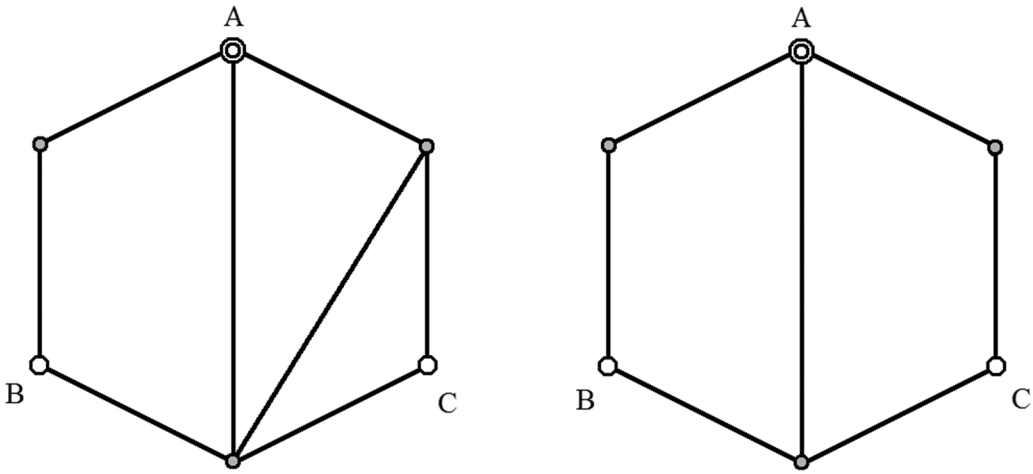
If we consider the process of progressive damage of each of these structures, it will be occurring from different starting positions and be characterized by different values of the resilience indicator.

The resilience indicator $0 \le F_W \le 1$ is understood as the average number of pipelines whose random failure causes disconnection of all consumers from the source of the target product [17].

In this context, it should be assumed that the first of the above structures will be more resilient on account of having a larger number of linear elements.

On the other hand, it can be assumed that the structure shown in Fig. 1a is the result of a transformation of a more complex structure shown in Fig. 2. Additionally, the structure of the network entity shown in Fig. 2 can become more complex as the result of development of new connections. If more new connections are added, the resulting complete graph [18], who's each node is connected by edges to all the others, is shown in Fig. 3. Such full graph-based structure is further called basic, while any of the examined network variants is the result of transformation of the same basic structure.

Given the above specificity, it would be convenient to consider the process of damage to a random network



a) b)

Fig. 1. Network structures of pipeline systems with identical numbers of nodes and consumers comprising 8 (a) and 7 (b) linear elements

structure as proceeding in two stages. At the first stage, the researcher intentionally excludes from the full graph-based network a part of linear elements, thereby bringing the basic structure to the initial one. Since the initial structure is the aim of the transformations, as it is complete, the target transformation is over.

At the second stage of transformation, the disruption of communications between individual nodes of the obtained initial structure occurs randomly by the mechanism of progressive damage.

Since structures with identical numbers of nodes have the same full graph, the range of system time values in the course of the two-step damage process turns out to be the same. This feature of network structures with equal numbers of nodes allows estimating the dynamics of the damage process from a single starting position. A special attention should be paid to the fact that a valid comparison of the resilience of network entities as part of the developed concept of two-stage damage is only possible for identical system time values.

As each of the above stages of damage has its own specific features, they should be examined and analysed separately.

Characteristics and specificity of the target transformation process

Target transformation involves sequential exclusion from the basic full graph-based network structure of a certain set of communications with gradual transition to the initial (target) structure.

The order of disruption of systemic communications in the course of target transformation is defined by the researcher or may be random. The dynamics of this process are characterized by system time t. As individual linear elements are excluded from the basic full graph-based structure, the system time takes on integer values and represents an event counter. Thus, before the onset of progressive damage, the original network structure is considered as the result of the

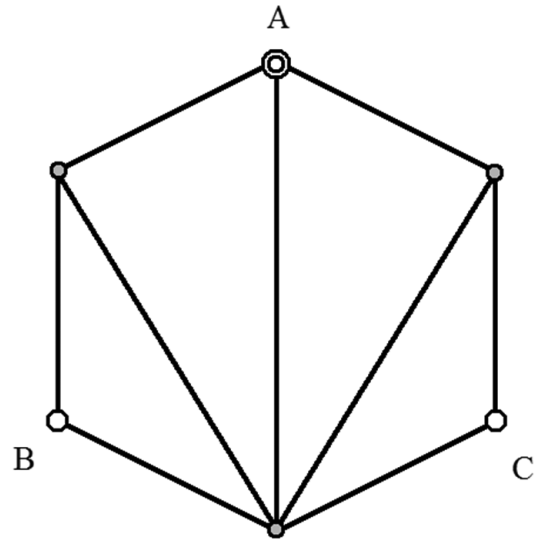


Fig. 2. Structure diagram of a pipeline system

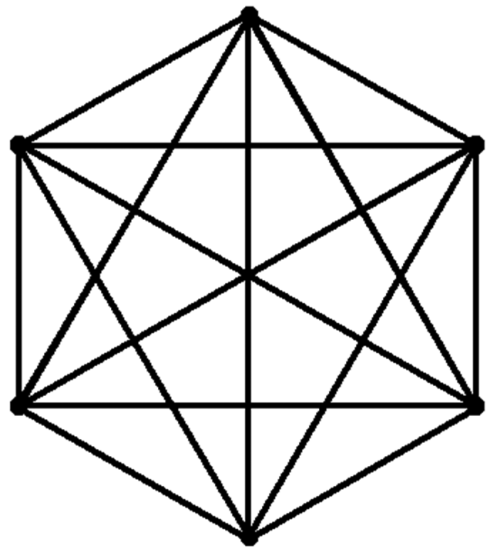


Fig. 3. Complete graph with 6 vertices and 15 edges

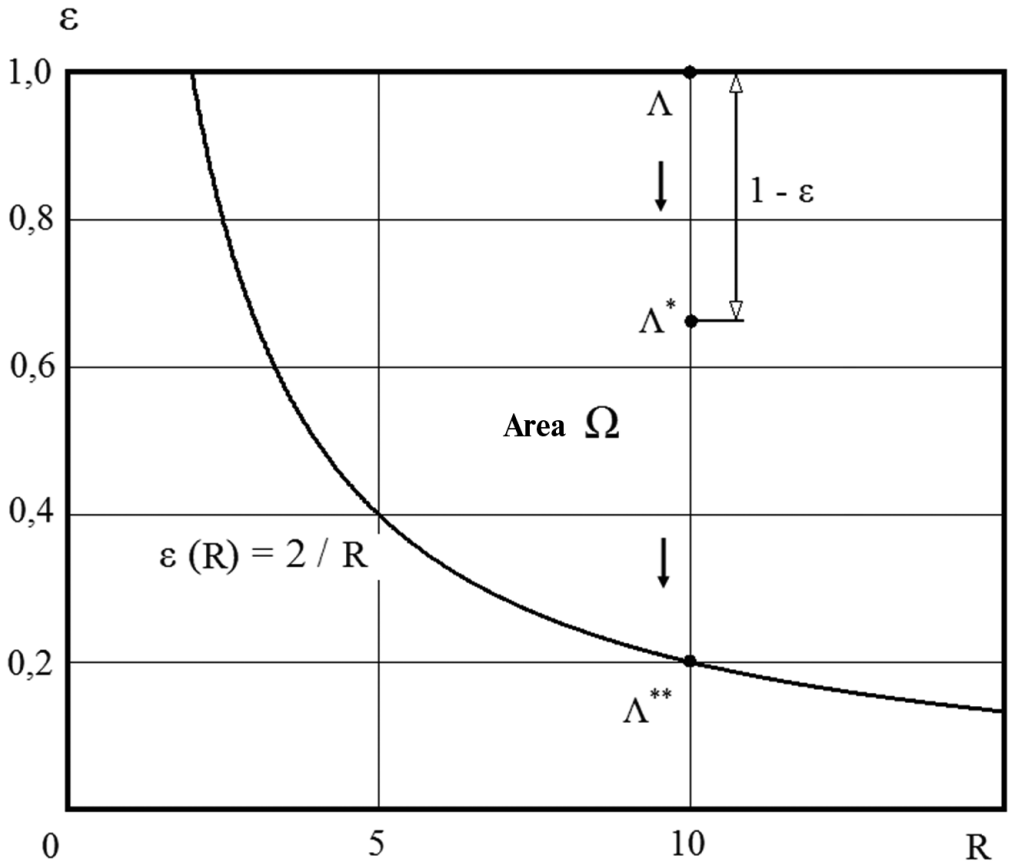


Fig. 4. The displacement of point Λ that characterizes the state of a network entity in the course of target transformation

preceding target transformation of the basic full graph-based object.

It is known that the full graph, at given number of vertices R, has the highest number of edges [19]:

$$Z_m = \frac{R \cdot (R-1)}{2}.$$

Then, the state of the original structure obtained as the result of purposeful removal of a certain number of edges from the full graph will be characterized by the communications completeness coefficient ε. Coefficient ε is the ratio of the number of communications Z between the graph vertices of the original structure to the number of communications in the full graph with the same number of vertices:

$$\varepsilon = \frac{Z}{Z_m} = \frac{2\,Z}{R \cdot (R-1)} \le 1.$$

Thus, coefficient ε is the share of the total number of communications in the full graph that must be disrupted in order to bring it to a state corresponding to the original network structure. It is obvious that for any full graph, regardless of the number of its vertices, ε = 1.

In the ε0*R* coordinate system, the process of target transformation of the full graph and its transition into the original structure will correspond to the displacement of point Λ across a series of intermediate steps into position Λ^* (Fig. 4).

Let us also note that the condition of network integrity in the process of target transformation results in restrictions on the lower threshold of values ε. Thus, the relationship between the number of linear elements Z and the number of nodes R for the limit structures with the "line" topology has the form:

$$Z = R - 1. \quad (1)$$

Further disruption of communications between the nodes of such entity will cause its separation into parts, which is unacceptable. Then, the condition of network integrity, taking into account dependence (1), leads to the following restriction:

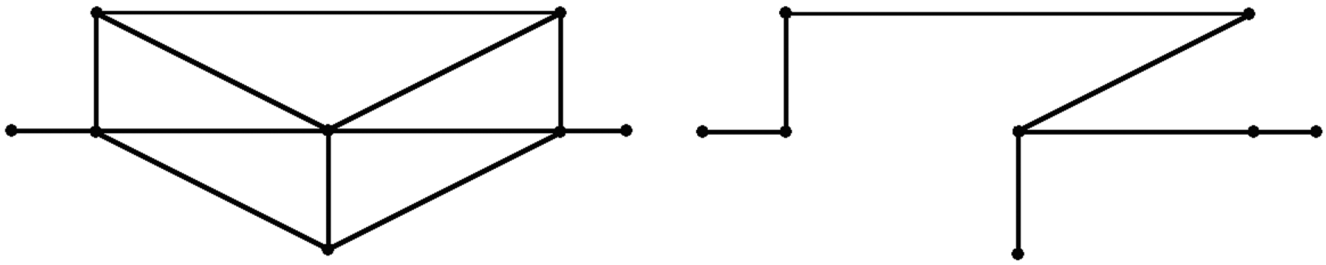
$$\varepsilon\,(R) \ge \frac{2}{R}.$$

Accordingly, the range of possible variation of the values of coefficient ε is determined as follows:

$$\frac{2}{R} \le \varepsilon\,(R) \le 1.$$

Area Ω, for which the combination of parameters ε and R corresponds to the above limitations and possibility of structural integrity upon the completion of the target transformation, is shown in Fig. 4.

In this context, let us consider the following example. Let us suppose that the initial network structure is characterized by the graph shown in Fig. 5a. It contains 12 edges and 8 vertices, while being the result of the target transformation of the full graph that consisting of 8 vertices and 28 edges.



a) b)

Fig. 5. Graphs that characterize integral network structures before (a) and after deliberate exclusion of 5 linear elements (b)

In the ε0*R* coordinate system (Fig. 6), this complete graph corresponds to point Λ, while the process of the target transformation that results in the formation of the initial network structure is associated with the transition of this point into position Λ^* by the system time t = 16.

If the resulting initial structure with the coefficient ε = 0,43 is later affected by progressive damage, it is obvious that it will be characterized by some resilience to this process. If the target transformation is continued to the point in time t = 21 with transition into the state shown in Fig. 5b, such process' potential would be fully exhausted.

The resulting limit structure is characterized by point Λ^{**} located on the boundary of area Ω (Fig. 6). Further elimination of linear elements from such structure is associated with the division of the network entity into parts or separation of nodes.

Thus, the lower threshold of coefficient $\varepsilon = \frac{2}{R} = 0{,}25$ is the limit value and its attainment in a real-life situation should be considered highly undesirable. This state of a network entity corresponds to the boundary of area Ω and is the maximum allowable in terms of its integrity.

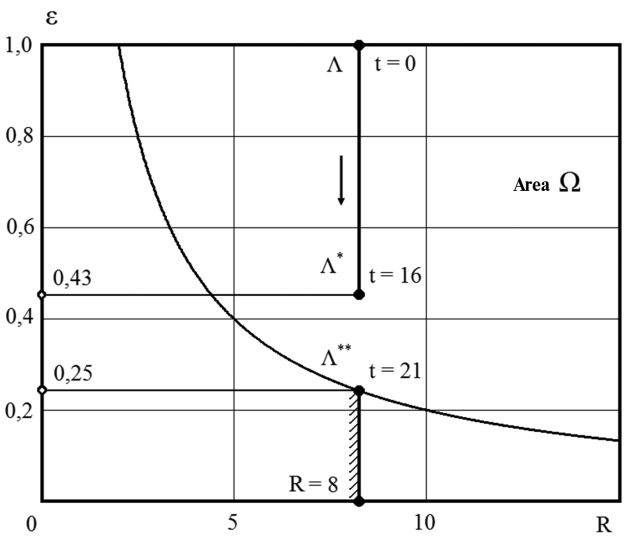


Fig. 6. A graphical representation of the target transformation process

The following formula is to be used for determining the proximity of the current network state to the limit state:

$$\eta = \frac{R(R-1) - 2Z}{(R-1)\cdot(R-2)}.$$

Coefficient η changes within the range of $0 \le \eta \le 1$. For a full graph-based structure η=0, and on the boundary of area Ω the value η=1. The range of possible application η should be divided into 3 value ranges according to the data of Table 1.

Thus, the calculation of values η for the analysed network structure helps form a general idea of its ability to resist the development of progressive damage.

Characteristics and specificity of progressive damage process

If we think of the network transformation process as a development of a two-stage process, it should be noted that a full graph-based structure is the most resilient against progressive damage. As linear elements are excluded from such basic structure and the process of target transformation develops, the ability of newly formed structural objects to resist the development of progressive damage decreases.

In this context, let us look into the development of the resilience of the ST0 full graph-based network structure with the source of product *A* and consumers *B*, *C*, *D* occurs (Fig. 7) as it gradually transforms into the limit state with a "line" topology.

Having eliminated 5 linear elements from the system, we will obtain the new ST1 structure outlined in Fig. 8a. For the structure designated ST1, the estimated resilience value is: $F_w = 0.769$. If the target transformation is continued and 4 more linear elements are eliminated from the system, the resulting structure designated ST2 will be as shown in Fig. 8b. Its calculated characteristics are given in Table 2.

Table 1. Verbal scale of network structure properties

Range of coefficient values η	$0 \le \eta < 0{,}5$	$0{,}5 \le \eta < 0{,}75$	$0{,}75 \le \eta \le 1$
Verbal scale of network structure properties	High resilience to progressive damage is ensured	The ability to ensure resilience to progressive damage is not high	The ability to ensure resilience to progressive damage is limited or very low

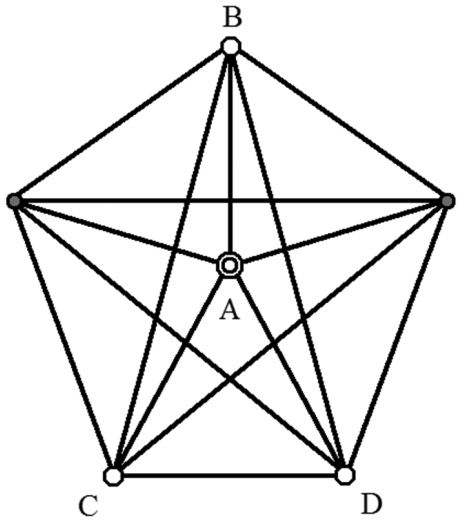


Fig. 7. Full graph-based structure ST0 with source A and consumers B, C, D

The elimination of two more linear elements results in the ST3 structure with the "ring" topology (Fig. 8c), after which only one linear element can be removed as part of target transformation (Fig. 8d).

As the result, the limit structure ST4 with the "line" topology is formed. The calculated characteristics of the above network structures are also shown in Table 2. It can be observed that the most significant decrease in the values of the resilience indicator in the process of target transformation is within the range $\eta = 0.7 \ldots 1$, i.e., as the network structure approaches its limit state.

The following specificity should be noted. For each of the examined structures, there are some variations due to possible changes in the mutual arrangement of the consumer nodes under the condition $\eta = \text{const}$.

For example, variations of the ST3 and ST4 structures can be related to a relocation of consumer node *C* (Fig. 9) with the value of η remaining unchanged. The interval estimates of the resilience values shown in Fig. 10 were obtained on the assumption of calculation error and the presence of some structural variations for fixed values of η.

The findings suggest that redundant intersystem connections have a positive effect on the resilience of pipeline systems to progressive damage, while the nature of such effect is non-linear. The most positive effect of the inclusion of additional connections into a system is observed if the network structure is close to the limit.

Conclusions

1. As the process of targeted transformation progresses, the ability of newly formed network structures to resist

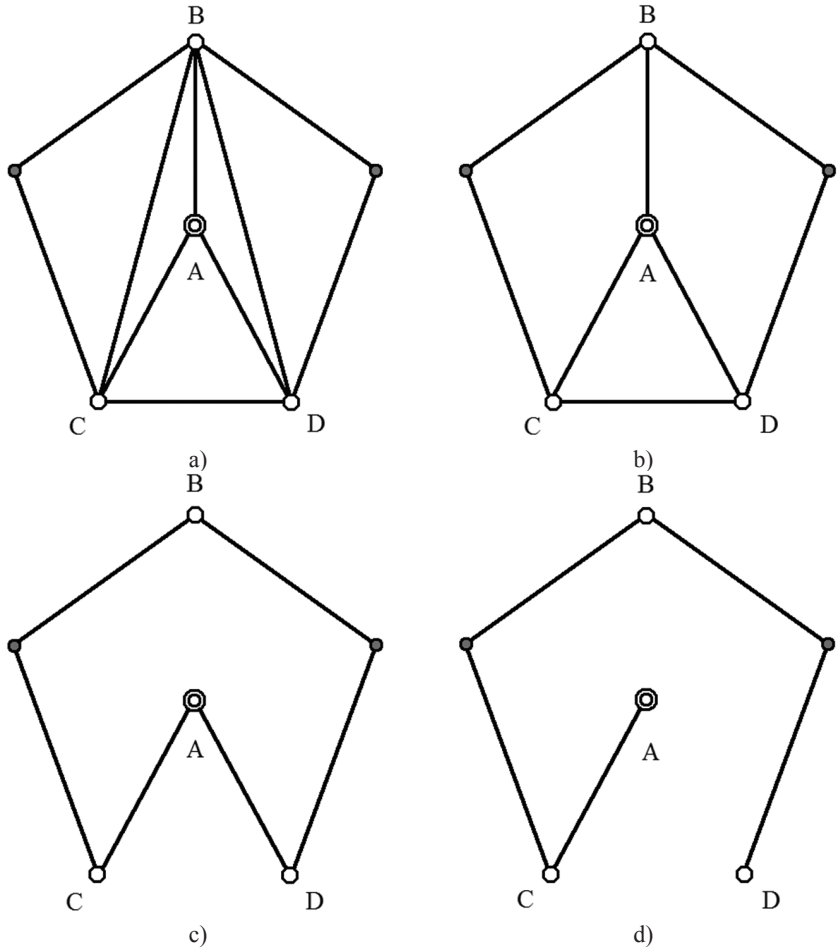
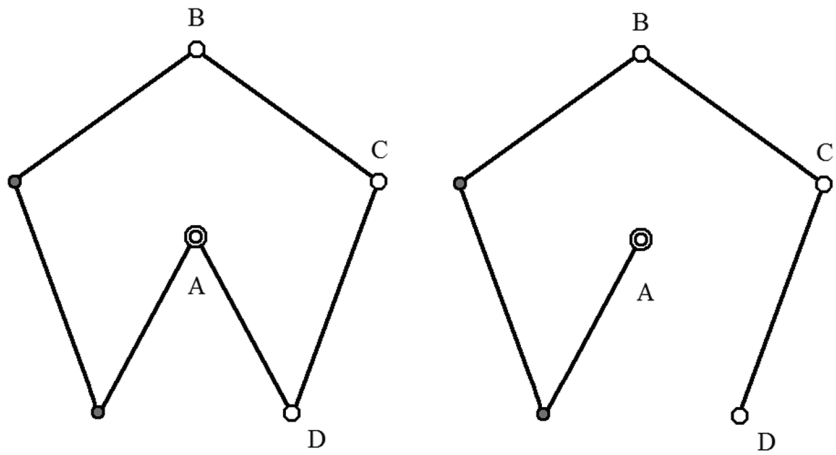


Fig. 8. Network structures designated ST1 (a), ST2 (b), ST3 (c), ST4 (d)

Table 2. Characteristics of network structures

Network structure designation	Characteristics of structures and process of targeted transformation						Note
	t	R	Z	ε	η	F_w	
ST0	0	6	15	1.0	0	0.800	The structure is based on a whole graph
ST1	5	6	10	0.667	0.5	0.769	
ST2	7	6	8	0.533	0.7	0.720	
ST3	9	6	6	0.4	0.9	0.581	
ST4	10	6	5	0.333	1	0.377	Limit structure composition



a) b)

Fig. 9. Variation of the ST3 (a) and ST4 (b) structures associated with the repositioning of consumer node C

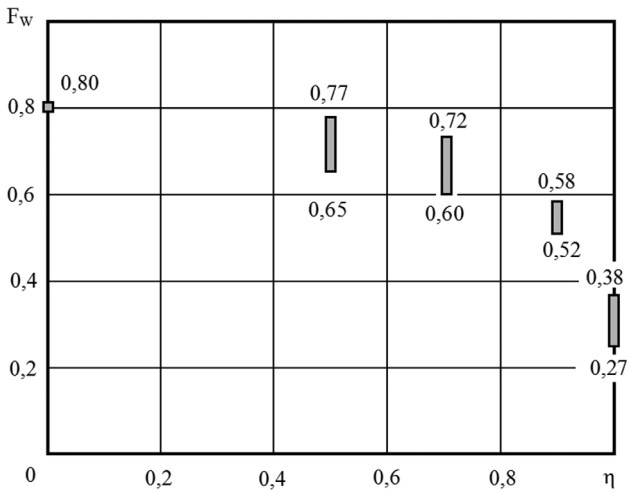


Fig. 10. Interval estimates of FW values for a set of comparable structures with fixed η values

the development of the process of progressive damage is continually diminished.

2. The lowest level of pipeline system resilience against the development of progressive damage can be observed as the structure of the network nears the limit state.

3. When carrying out maintenance activities associated with the exclusion of a number of linear elements from an active pipeline system, the proximity of the newly built network structure to the limit state should be assessed along with the resilience of the restored system to possible development of the process of progressive damage.

References

1. Sambasivan M., Gopal S. Handbook of oil and gas piping. A practical and comprehensive guide. Taylor & Francis Group; 2019.

2. Barker G. The engineer's guide to plant layout and piping design for the oil and gas industries. Elsevier Inc.; 2018.

3. Winston R., editor. Oil and gas pipelines. Integrity and safety handbook. John Wiley & Sons, Inc.; 2015.

4. Silowash B. Piping systems manual. The McGraw-Hill Companies, Inc.; 2010.

5. Nolan D.P. Handbook of fire and explosion protection engineering principles for oil, gas, chemical, and related facilities. Fourth edition. Gulf Professional Publishing. Elsevier Inc.; 2019.

6. Barkanov E.N., Dumitrescu A., Parinov I.A. Non-destructive testing and repair of pipelines. Springer International Publishing AG; 2018.

7. Kermani B., Chevrolet T. Recommended practice for corrosion management of pipelines in oil and gas production and transportation. European Federation of Corrosion Publications. CRC Press; 2017.

8. Bahadori A. Oil and gas pipelines and piping systems. Design, construction, management, and inspection. Elsevier Inc.; 2017.

9. Bai Q., Bai Y., Ruan W. Advances in pipes and pipelines. Flexible pipes. Scrivener Publishing LLC. John Wiley & sons, Inc.; 2017.

10. Mahmodian M. Reliability and maintainability of in-

service pipelines. Gulf Professional Publishing Publications. Elsevier Inc.; 2018.

11. Bolzon G., Gabetta G., Nykyforchyn H. Lecture notes in civil engineering. Degradation assessment and failure prevention of pipeline systems. Springer Nature Switzerland AG; 2021.

12. Antoniou A., Dimou A., Markogiannakis A., Karvelis P. Design of tanks foundation and onshore pipeline against earthquake-related geohazards in a coastal area in Northern Greece. *Pipeline Technology Journal* 2020;3:40-46.

13. Finley D., Daniels S., Kole K., Roeleveld M., Ogden P. Trial of a process for the identification of reduced depth of cover on buried pipelines. *Pipeline Technology Journal* 2018;3:42-47.

14. Singh R. Pipeline integrity handbook. Risk management and evaluation. Gulf Professional Publishing. Elsevier Inc.; 2014.

15. Ilkaev R., Seleznev V., Aleshin V., Klishin G. Seleznev V.E., editor. Numerical simulation of gas pipeline networks. Theory, computational implementation and industrial applications. Moscow: KowKniga; 2005.

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

17. Tararychkin I.A. Resistance of the pipeline transportation systems to damages of the network elements. *Occupational Safety in Industry* 2021;1:41-47. (in Russ).

18. Omelchenko A.V. [Graph theory]. Moscow: MTsNMO; 2018. (in Russ.)

19. Wilson R.J. Introduction to graph theory. Pearson Education Limited; 2010.

About the author

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

The author's contribution

The author suggested the concept of two-stage damage to the network structure of a pipeline transportation system that allows estimating the changes in the durability of the repaired systems and the possible consequences of structural changes associated with repair activities. The required calculation dependencies were obtained that allow predicting the behaviour of such systems in emergency situations.

Conflict of interests

The author declares the absence of a conflict of interests.

Intelligent centralized traffic management of a rapid transit system under heavy traffic

Leonid A. Baranov[1]*, Valentina G. Sidorenko[1], Ekaterina P. Balakina[1], Ludmila N. Loginova[1]
[1]*Russian University of Transport, Moscow, Russian Federation*
**baranov.miit@gmail.com*


Leonid A. Baranov


Valentina G. Sidorenko


Ekaterina P. Balakina


Ludmila N. Loginova

Abstract. Aim. *In today's major cities, increased utilization and capacity of the rapid transit systems (metro, light rail, commuter trains with stops within the city limits) – under conditions of positive traffic safety – is achieved through smart automatic train traffic management. The aim of this paper is to choose and substantiate the design principles and architecture of such system.* **Methods.** *Using systems analysis, the design principles and architecture of the system are substantiated. Genetic algorithms allow automating train traffic planning. Methods of the optimal control theory allow managing energy-efficient train movement patterns along open lines, assigning individual station-to-station running times following the principle of minimal energy consumption, developing energy-efficient target traffic schedules. Methods of the automatic control theory are used for selecting and substantiating the train traffic algorithms at various functional levels, for constructing random disturbance extrapolators that minimize the number of train stops between stations.* **Results.** *Development and substantiation of the design principles and architecture of a centralized intelligent hierarchical system for automatic rapid transit traffic management. The distribution of functions between the hierarchy levels is described, the set of subsystems is shown that implement the purpose of management, i.e., ensuring traffic safety and comfort of passengers. The criteria are defined and substantiated of management quality under compensated and non-compensated disturbances. Traffic management and target scheduling automation algorithms are examined. The application of decision algorithms is demonstrated in the context of uncertainty, use of disturbance prediction and genetic algorithms for the purpose of train traffic planning automation. The design principles of the algorithms of traffic planning and management are shown that ensure reduced traction energy consumption. The efficiency of centralized intelligent rapid transit management system is demonstrated; the fundamental role of the system in the digitalization of the transport system is noted.* **Conclusion.** *The examined design principles and operating algorithms of a centralized intelligent rapid transit management system showed the efficiency of such systems that ensured by the following: increased capacity of the rapid transit system; improved energy efficiency of train traffic planning and management; improved train traffic safety; assurance of operational traffic management during emergencies and major traffic disruptions; improved passenger comfort.*

Keywords: *centralized management, autonomous systems, intelligent management, functional lavels, subsystems, energy efficiency, disturbance prediction, genetic algorithms.*

For citation: *Baranov L.A., Sidorenko V.G., Balakina E.P., Loginova L.N. Intelligent centralized traffic management of a rapid transit system under heavy traffic. Dependability 2021;2: 17-23. https://doi.org/10.21683/1729-2646-2021-21-2-17-23*

Received on: *25.02.2021* / **Revised on:** *15.04.2021* / **For printing:** *21.06.2021.*

Introduction

Rapid transit systems conventionally include subways and a light rail systems separated from road traffic. Later, the commuter rail systems with stops within the city limits were included in the classification as well. In particular, the Moscow Central Circle (MCC) and the Moscow Central Diameters [1, 2] are classified as rapid transit. Given that the organization of traffic in metros, light rail and commuter rail has the same goal of providing comfortable and safe transportation of passengers, as well as the similarity of the underlying technologies, a centralized rapid transit traffic management system should be developed based on a single set of principles.

Centralized traffic management. Functional management levels. Management level subsystems

When traffic is heavy, which is typical for the rapid transit systems of major cities, designing autonomous unmanned vehicle control systems with automatic control of each train according to a predefined traffic schedule is not effective, as in such case the position of other trains on the line is not taken into account. "Harmful" mutual interaction of trains only takes place when it starts affecting the movement patterns automatically selected in the train control system [3]. Unlike autonomous systems, centralized systems receive information on the arrival and departure times of all trains across all stations, compare this information with a defined traffic schedule and condition control commands for each train, including the required station dwell times and travel times for the open line ahead. Such commands are implemented by unmanned vehicles. This mode of centralized systems operation is called disturbance-compensated management, when a deviation from the target schedule can be mitigated using available travel and station dwell time budget. We shall call compensated disturbances "minor faults". In this case, when the travel and station dwell time budget is not sufficient to mitigate the disturbances, unscheduled train turnovers are performed at stations with passing loops, if necessary, along with unplanned removal of trains to the yard, which leads to changes in the train pair count and sequence. Such situations are commonly called "major faults" [3, 4, 5]. In cases of major faults, algorithms are initiated for centralized fault management and traffic recovery upon elimination of the causes of the fault [5, 6], while traffic management is carried out based on the operational schedule. The purpose of post-fault management is to restore train traffic according to the initial target schedule, which enables the required night arrangement of trains [6, 7]. Thus, two functional management levels can be distinguished within the centralized system, i.e., upper and lower.

At the upper level, in accordance with the target or operational schedule and the received information on the arrival and departure of trains, the required travel times and dwell times for each train are calculated. At the lower level, the commands of the upper level are implemented. The most important upper-level management function is generating commands for train turnaround at terminals and stations with no passing loops. Such commands are delivered through centralized traffic control to the station interlocking system that controls the point operation. The operation of the upper functional level is supervised by the traffic controllers who receive information on the train locations through the supervisory control system. In addition, the traffic controllers are able to receive information from CCTV cameras at stations, turnaround points, etc. The role of the traffic controllers is especially important when major faults occur. At the upper functional level, a management scenario is automatically generated and its execution is approved by a traffic manager [6]. A mode is required, in which the traffic manager takes control. Traffic safety is ensured by track circuit-based systems (ARS in the Moscow metro) [8], or communications-based (CBTC-like) systems [9]. The advantage of the communications-based systems consists in the absence of position quantification of the "tail" of the train ahead (positioning of the "tail" of the train ahead based on the occupied track circuit), reduced operating costs associated with the maintenance and adjustment of track circuit equipment. In the case of communications-based train control, the positioning of the "tail" of the train ahead accurate to the length of the overlap determined by the maximum errors of travelled distance and speed measurement allows reducing the allowed headway [10], which is essential when traffic is heavy. At the same time, communications-based train control systems (like CBTC) do not ensure rail integrity control (the so-called "control mode"). Therefore, the application of CBTC-like systems requires additional equipment enabling rail integrity control [10]. Additionally, while deploying automatic traffic management systems on active lines it is important to ensure operational continuity of traffic safety systems. Therefore, the development of hybrid algorithms and equipment enabling the advantages of track circuit-based and communication-based systems appears to be promising. The commands of the traffic safety system are given the highest priority.

The upper functional level comprises the following subsystems:

– subsystem for minor faults, major faults, post-fault management [3];

– target schedule and turnover construction subsystem [11, 12];

– subsystem for selecting energy-optimal modes of train control with set specified travel times [13] and energy-optimal distribution of travel times [14]. The outputs of the above subsystems are used in the construction of target train schedules. It should be noted that solving the problem of energy-optimal train control for various travel times allows obtaining for each open line a dependence of traction power consumption as a function of the travel time that is required and sufficient for energy-optimal distribution;

– subsystem for archiving train orders and train sheets;

– database of failures and results of diagnostics of technical assets that enable train traffic, including rolling stock diagnostics data;

– subsystem for automatic management of rolling stock turnover at stations with passing loops;

– passenger information subsystem;

– subsystem for training of personnel involved in the traffic organization, a personnel training software and hardware system [15];

– subsystem for advanced training of traffic controllers, a traffic controller simulator [16, 17, 18].

The relevance of those software and hardware systems is much more significant than their direct purpose. Those systems include detailed line simulation models that are used in the analysis of new algorithms. The results of such simulation determine the effectiveness of their implementation. The simulator includes a system for calculating the performance criteria of the control system and an open library of control algorithms. Of special significance is the matter of integration of staff training systems of various services, which would allow using common criteria for training quality and methodology evaluation. The simulation models allow using machine learning for predicting hazardous failures of various system components [19].

Let us note a few advanced features of the upper functional level that allow using the term "intelligent system". The upper-level algorithms require generating commands for the trains on a line under uncertainty. The (n+1)-th train must be given the departure command and required travel time in such a way as to let it perform its movement with no interference on the part of the safety systems. Developing this solution requires knowing the deviation from the target value of the next station dwell time of the previous, n-th train while it has not yet arrived to the station. In this situation, an intelligent disturbance prediction algorithm is implemented that uses the delay statistics of previous trains [20]. A genetic algorithm is used for automatic construction of train and turnover schedule [21, 22]. Therefore, the term "intelligent system" is correct. The integration of various system functions, including management itself, collection and processing of diagnostic information, analysis of facility performance indicators and operation planning, archiving, etc., can be implemented using Big Data and artificial intelligence algorithms. In turn, the system's open architecture, availability of a database for collecting diagnostic information allows regarding it as a foundation for the digitalization of urban transportation systems.

At the lower functional level, the onboard control system solves the following tasks:

– train traffic safety;

– energy-optimal train control with the observance of all specified restrictions (including traffic safety indications) that ensures the observance of upper-level interstation travel times;

– targeted stops at stations;

– enforced permanent and temporary speed restrictions;

– closing and opening the doors, movement initiation, passenger information.

One of the vital tasks associated with ensuring safe and efficient traffic management is the measurement of traffic parameters, i.e., train speed and travelled distance. In subways, this problem is solved using wheel-mounted frequency-pulse rotation sensors and correction sensors installed on tunnel walls or in the track. In this environment, infra-red sensors have shown their efficiency. On the tunnel wall, an angle reflector is installed, while trains are equipped with infra-red transceivers [3]. The beam of the transmitter is directed toward the tunnel wall. It is reflected from the angle reflector and is received on the train, resetting the measurement error of the wheel-mounted frequency-pulse sensor. When two sensors are installed at a fixed distance from each other, the onboard computer calculates the wheel radius, thus enabling reduced error when measuring the travelled distance and speed outside the strobing signal points [3]. There is experience with RFID sensors installed between rails. The advantage of such sensors consists in the ability to transmit the sensor number, its coordinate, the number of the open line. At the same time, due to the bell-shaped direction diagram of the radio signal, the position of the detected correction point depends on the

speed of the train. The latter causes train positioning error. Reducing the train speed at the location of the RFID sensor when approaching the station in order to reduce the effect of the bell-shaped signal wave-form on the detection error results in longer traction time at a constant travel time and, therefore, overconsumption of traction energy. On average, a 1-second increase of braking time causes a 1-percent increase of traction energy consumption. The combined use of two types of sensors allows improving the dependability of the distance measurement link and to take advantage of the strengths of both sensors, i.e., the accuracy of correction point detection of the infra-red sensor and large amount of communicated information of the RFID sensors.

A technical vision system is required for detecting obstacles in the unmanned control mode in open areas accessible to people, animals, other modes of transport [23]. Control inputs generated by such system have the highest priority.

The presence of advanced computing facilities onboard the trains allows integrating the functions of automatic train control, train protection, collection of diagnostic information that is radioed to the station and further to the upper functional level.

Improving the energy efficiency of management processes

Let us focus on improving the upper-level traffic management algorithms. The main criteria for efficiency at the top level of the train management algorithm are:

– improved accuracy of target schedule performance with disturbance compensation;

– minimum time of target schedule recovery upon elimination of the causes of a major fault.

The minimization of the above criteria is to be achieved subject to the additional condition of minimized traction energy consumption.

In case of unmanned driving, the onboard travel time control facility can achieve the predefined range of travel time with high accuracy. This capability is used for improving the energy efficiency of management operations in the event of minor faults. The travel time of the (n+1)-th train across the open line ahead required for compensating for the late arrival of such train to the (j+1)-th station is chosen subject to the restrictions on the minimum dwell time in such a way as to enable the minimum headway based on the restrictions of the train control systems. The distinctive feature of the traffic management algorithm with disturbance compensation is the consideration for the dependence of the restrictions on the system status and predicted deviations of the dwell times of the train ahead based on the previous train delay statistics [20]. The dependence of the restrictions on the system status is defined by the regulating characteristic of the j-th open line $T_{uminj}[n+1] = [T_{xj}[n+1], T_{xj}[n]] + T_{cj}[n]$, where $T_{uminj}[n+1]$ is the minimum departure interval of the (n+1)-th train to the j-th open line from the (j-1)-th station, whereas the n-th train does not affect the operating modes of the (n+1)-th train through the traffic safety system; $T_{xj}[n]$, $T_{xj}[n+1]$ is the the travel times of the n-th and (n+1)-th trains across the j-th open line respectively; $T_{cj}[n]$ is the dwell time of the n-th train at the j-th station. When control is selected, the values $T_{cj}[n] = T^{r}_{cj}[n] + \Delta T^{pr}_{cj}[n]$, where $T^{r}_{cj}[n]$ is the dwell time of the n-th train at the j-th station according to target schedule; $\Delta T^{pr}_{cj}[n]$ is the predicted deviation of actual dwell time from the target value. The travel time of the (n+1)-th train across the j-th open line is chosen by the algorithm in such a way (provided that the requirements for the value $T_{uminj}[n]$ are met) as to enable the restriction on the allowable minimal dwell time and the minimal possible delay of the (n+ 1)-th train arriving to the j-th station. That also allows reducing the number of speed restrictions and stops of the following train between stations. Such algorithm, on the one hand, improves traffic safety by reducing the probability of trains running dangerously close to each other, and, on the other hand, reduces traction energy consumption not only by reducing the number of stops between stations, but also by increasing the running time of the following train.

Upon the elimination of the causes of a major fault, the control algorithm chooses – out of a variety of fastest-acting control algorithms – the one that minimizes the traction energy consumption through energy-optimal distribution of the travel times along the line. The problem of energy efficiency is taken into account while scheduling train traffic not only, as previously stated, by means of optimal distribution of travel times, but also by changing the way the number of trains on the line is increased at the beginning of to the peak hours. In conventional target traffic schedules, such transitions involved extended dwell times that ensured increased headway for the purpose of adding new trains to the operation. In the planning algorithm under consideration, the same effect is achieved through planned extension of travel times, which allows reducing the traction energy consumption. Thus, the energy efficiency of target train schedules is achieved by associating the traction energy consumption with the travel times under the selected energy-optimal control modes, distribution of train running time along the line, replacement of extended dwell times with increased travel times in transition mode.

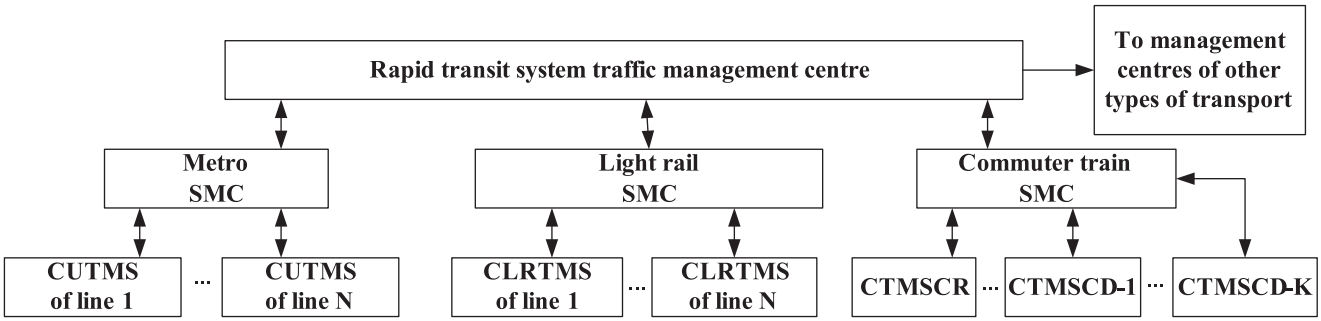


Fig. 1. System structure

The matters of information communication network design as part of centralized management systems, information protection are extremely important and define system efficiency. Such issues are not addressed in this article and require individual consideration.

Structure of the rapid transit traffic management system

A rapid transit traffic management system was examined above. The integration of such systems with the addition of a higher level of management is illustrated in Fig. 1, where the following designations are used:

– SMC, situation management centre;

– CUTMS of lines 1, …, *N*, centralized underground traffic management system of lines from 1 through *N*;

– CLRTMS of lines 1, …, *M*, centralized light rail traffic management system of lines from 1 through *M*;

– CTMSCR, centralized traffic management system of the central ring (MCC in Moscow);

– CTMSCD, centralized traffic management system of the central diameters from 1 through *K*.

The situational management centres (SMC) of various types of rapid transit receive information from subsystems of the upper functional level of centralized traffic management, in particular, from the hardware and software systems of line-level traffic management facilities. In normal mode, the received information is "compressed" and in a generalized form is displayed in situation management centres. If a train deviates from the target schedule by a fixed amount of time, the centre's personnel is informed accordingly by changing line colour and a tonal signal. They can then display a detailed image of the operational situation available to the traffic managers. The functionality of the situation management centre and its design principles were developed by the Russian University of Transport (RUT/MIIT) and the Moscow Metro [24]. Aggregated information from the SMC of various types of rapid transit systems is delivered to the metropolitan rapid transit management centre. At this level, the collected information will allow managing urban transportation in emergency situations, making coordinated advance managerial decisions in cases of planned closure of certain line sections. The metropolitan rapid transit management centre is to be associated with other transportation management centres. The concept of its construction requires considerable elaboration.

Conclusion

The examined design principles and operating algorithms of a centralized intelligent rapid transit management system showed their efficiency that is defined by the following:

– increased capacity of rapid transit systems through strict adherence to the target train schedule;

– improved energy efficiency of traffic planning and management through energy-efficient train management patterns, traction energy-optimal distribution of train running time along the line, replacement of the target train scheduling with extended station dwell times with the scheduling with modifiable target train running times during the periods of train pair count changeover, improved centralized management algorithms that take into account the dependence of control restrictions on the system state and prediction of possible disturbances, increased station-to-station train running times for the purpose of implementing the allowed headway by means of train separation systems;

– improved traffic safety through reduced probability of "hazardously close" distance between trains with stricter observance of station-to-station train running times and dwell times;

– operational traffic management during emergencies and major traffic disruptions through efficient algorithms of centralized management during traffic disruptions and after the elimination of their causes;

– improved passenger comfort through accurate execution of the traffic schedule.

Acknowledgements

The research was carried out with the financial support of RFBR, the Sirius University, JSC RZD and the Educational Foundation "Talent and Success" as part of the research project No. 20-37-51001.

References

1. [Passenger traffic on the MCC has reached 550 thousand people per day]. (accessed 18.03.2020). Available at: https//wwwm24.ru/news/transport/07122019/99787. (in Russ.)

2. Romensky D.Yu, Vakulenko S.P., Kozlov A.V. [Choice of the conceptual solution for organizing commuter rail traffic across the Moscow railway centre]. Molodye uchyonye razvitiyu natsionalnyy tekhnologicheskiy initsiativy 2020;1:568-570. (in Russ.)

3. Baranov L.A., Golovicher Ya.M., Erofeev E.V., Maximov V.M. Baranov L.A., editor. [Modern computer-based train separation systems for EMUs]. Moscow: Transport; 1990. (in Russ.)

4. Baranov L.A., Kozlov V.P. [Managing a subway line affected by traffic disruption]. VNIIZHT Scientific Journal 1992;5:29-31. (in Russ.)

5. Balakina E.P. Principles of algorithms construction of system of support decision making for a train dispatcher. *Science and Technology in Transport* 2008;2:23-26. (in Russ.)

6. Balakina E.P. Automatic devices function as traffic controller. World of Transport and Transportation 2008;2:104-109. (in Russ.)

7. Balakina E.P., Shcheglov M.I., Erofeev E.V. Metro line operational control algorithm for restoration traffic on a planned schedule. *Science and Technology in Transport* 1;1:23-25. (in Russ.)

8. Bestemiyanov P.F., Romanchchikov A.M. Traffic control using coordinate mode. World of Transport and Transportation 2008;1:104-108. (in Russ.)

9. IEEE 1474.1-2004 – IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements; 2004.

10. Baranov L.A. Evaluation of metro train succession time for safety systems based on radio channel. *World of Transport and Transportation* 2015;2:6-19.

11. Sidorenko V.G., Safronov A.I. [Constructing a target traffic schedule for a subway]. *World of Transport and Transportation* 2011;3:98-105. (in Russ.)

12. Iskakov T.A., Safronov A.I., Sidorenko V.G., Kyaw M.A. Approaches to quality assessment of subway traffic planning and management. *Automation on Transport* 2020;8:38-63. (in Russ.)

13. Baranov L.A., Melyoshin I.S., Chin' L.M. Energyoptimal dispatching of a regenerative braking train at the account of restrictions on phase coordinate. *Science and Technology in Transport* 2010;4:12-23. (in Russ.)

14. Baranov L.A., Kuznetsov N.A., Maksimov V.M. [Energy-optimal vehicle control]. *Electrical Engineering* 2016;9:12-18. (in Russ.).

15. Loginova L.N. The role of the system of automated knowledge test of train traffic controllers of metro in improvement of training quality. *Science and Technology in Transport* 2011;1:62-65. (in Russ.)

16. Baranov L.A., Sidorenko V.G. [Application of simulators in the improvement of the qualification of traffic department employees]. *Avtomatika, sviaz, informatika* 2003;2:17-20. (in Russ.)

17. Baranov L.A., Sidorenko V.G. [Simulator for train dispatchers of the Moscow Metro]. *Rail International* 2002;8:64-69. (in Russ.)

18. Baranov L.A., Balakina E.P., Sidorenko V.G. [Train dispatcher simulators in railway transportation]. Proceedings of the XVIII All-Russian Research and Practice Conference Train Traffic Safety. Moscow: MIIT; 2017. (in Russ.)

19. Shubinsky I.B., Zamyshliaev A.M., Pronevich O.B., Platonov E.N., Ignatov A.N. Application of machine learning methods for predicting hazardous failures of railway track assets. *Dependability* 2020;2:45-53.

20. Baranov L.A., Balakina E.P., Ikonnikov S.E., Antonov D.A. Centralized train traffic operation of urban railways of a modern megalopolis. *Science and Technology in Transport* 2020;1:30-38. (in Russ.)

21. Sidorenko V.G., Zhuo M.A. Application of genetic algorithms for underground electric trains scheduling problems. *Electronics and electrical equipment of transport* 2016;6:13-16.

22. Sidorenko V.G., Zhuo M.A. An investigation into the possibilities of genetic algorithm application to solve the underground electric rolling stock scheduling problem. *Electronics and electrical equipment of transport* 2017;6:37-40.

23. Okhotnikov A.L. Technical vision systems: development trends. *Zheleznodorozhny transport* 2020;9:44-51. (in Russ.)

24. Ershov A.V. Principles of construction of the situational centre on the Moscow underground. *Science and Technology in Transport* 2006;1:27-33. (in Russ.)

About the authors

Leonid A. Baranov, Doctor of Engineering, Professor, Head of Department of Management and Protection of Information, Russian University of Transport, Moscow, Russian Federation, e-mail: baranov.miit@gmail.com.

Valentina G. Sidorenko, Doctor of Engineering, Professor, Department of Management and Protection of Information, Russian University of Transport, Moscow, Russian Federation, e-mail: valenfalk@mail.ru.

Ekaterina P. Balakina, Candidate of Engineering, Senior Lecturer, Department of Management and Protection of Information, Russian University of Transport, Moscow, Russian Federation, e-mail: balakinaep@gmail.com.

Ludmila N. Loginova, Candidate of Engineering, Senior Lecturer, Department of Management and Protection of Information, Russian University of Transport, Moscow, Russian Federation, e-mail: ludmilanv@mail.ru.

The authors' contribution

Baranov L.A. Principles of system architecture, energy efficiency targets.

Sidorenko V.G. Train planning tasks, genetic algorithms.

Balakina E.P. Disruption prediction tasks. Management algorithms for cases of major traffic disruptions.

Loginova L.N. Traffic management algorithms for cases of compensated disruptions.

Conflict of interests

The authors declare the absence of a conflict of interests.

Original article
https://doi.org/10.21683/1729-2646-2021-21-2-24-27

Errors, faults and failures

Igor B. Shubinsky[1]*, Hendrik Schäbe[2]
[1]JSC NIIAS, Moscow, Russian Federation, [2]TÜV Rheinland, Cologne, Germany
**igor-shubinsky@yandex.ru*


Igor B. Shubinsky


Hendrik Schäbe

Abstract. Aim. *To harmonize the definitions of errors, faults, failures in the Russian and English languages. The Object of the paper is one of the most important subject matters of the dependability theory and functional safety. The Subject of the paper is the concepts and definitions of failures, errors, faults.* **Results of the research:** *analysis of the definitions of the concepts describing the dependability and functional safety of items in the Russian and international standards, such as GOST 27.002-2015, GOST R/IEC 61508-2012, IEC 60050, DIN 40041, as well as in publications by a number of authors. The analysis shows that failure is always associated with the loss of function, i.e., the ability to perform as required by all standards. It should be noted that wrong user expectation does qualify as failure. A failure should be distinguished from unintended functions. A fault is defined as a system's inability to perform the required operation to the full extent that, under certain conditions, may escalate into a failure. An error as a discrepancy between a calculated, observed or measured value or condition and a true, specified or theoretically correct value or condition is a deviation that is present and, under certain conditions, would probably turn into a failure. A typical example is non-critical software errors. The so-called systematic failures are actually errors that can turn into critical errors (failures). Let us note that the definitions in the IEC 60050 international electrotechnical vocabulary can be used, as they show general agreement, which is not surprising for an international standard.*

Keywords: *failure, malfunction, error, fault, damage, standard, term, dependability, functional safety, event, work.*

For citation: *Shubinsky I.B, Schäbe H. Errors, faults and failures. Dependability 2021; 2: 24-27. https://doi.org/10.21683/1729-2646-2021-21-2-24-27*

Received on: *20.10.2020* / **Revised on:** *10.04.2021* / **For printing:** *21.06.2021.*

1. Introduction

The development of dependability and safety-related terminology is at the focus of attention of many researchers (e.g., see works by Netes, Pokhabov, Plotnikov, Mikhailov [1-5]). Such terms are not always represented equally well in different languages. In this paper, we will attempt to examine possible definitions of the terms *error, fault, failure*. We will try to do that simultaneously in the English and Russian languages. That is not an easy task, since there are not so many well-translated papers or books. In any case, in this article the authors will attempt to describe their view of the terminology. Section 2 overviews a number of existing definitions and concepts. Section 3 provides a brief analysis of key terms and proposes definitions devised by the authors. Section 4 draws the conclusion.

2. Review of the existing concepts

Definitions of the terms *fault, failure* and *error* can primarily be found in the standards dealing with terminology and definitions. In IEC 60050 [7], the following definitions are recommended:

failure, loss of ability to perform as required,

fault, inability to perform the required function due to the internal state,

error, a discrepancy between the calculated, observed or measured value or condition and the true, specified or theoretically correct value or condition.

The GOST 27.002 interstate standard [8] sets forth the following definition:

failure, an event consisting in the disruption of an item's up state.

This interpretation is based on a monograph, the fundamental book on dependability written in 1965 by B.V. Gnedenko, Yu.K. Beliaev, Yu.D. Soloviev [9].

Failure is a partial or total loss or alteration of such properties of an item that significantly reduce the performance or cause the loss of operability.

It can be noted that this definition set forth in [9] may also define a fault. However, we must admit that over the past 55 years the terminology has somewhat evolved in a way the authors could not have anticipated. That is particularly the case with the definition of *error*.

The GOST 27.002 interstate standard [7] lacks the definition of error, but fault and defect are defined as follows:

fault is a state of an entity, in which it does not comply with at least one of the requirements specified in the respective documentation,

defect is each individual deviation of an entity from the requirements defined in the documentation.

The differences between the definitions are minor. Whereas a fault is any inconsistency with the requirements, a defect is each particular inconsistency. GOST 27.002 defines *damage* as an event consisting in the disruption of an entity's good state under condition of retained up state.

This definition of damage is very similar to that of fault according to the IEC 60050 dictionary [7].

As a third source, let us use the article by Gayen and Schäbe [10, 11] that was published in two languages, thus the terminology is coordinated. The authors partially borrowed the terminology from DIN 40041 [12] that, although still valid, is outdated and no longer supported. That explains some of the drawbacks.

Failure: a specific physical functional module stops performing a function within the specified load and environmental conditions.

This definition is associated with the loss of the expected function and corresponds to the above definitions. However, the application of the term does not go beyond the element. Such application of this concept at the system level can lead to confusion, as it does not necessarily characterize system failure. At the system level, it can be associated with a fault. However, the definition of fault in the same article explains that.

Fault is a lost or erroneous function or incomplete delivery of the desired function by module.

An important aspect of the discussion is the distinction between faults and failures. On the one hand, a fault is a partial loss of functional capacity or a complete loss of functional capacity associated with a module or subsystem not necessarily resulting in a system failure. On the other hand, a fault can also occur at the system level and reduce system performance. Therefore, it is important to distinguish between a system and a subsystem/unit. We must note that an event that may consist in a subsystem failure may be just a fault at the system level, as other subsystems can – at least partially – compensate for such subsystem failure to make it just a system-level fault.

Chillarege [13] considers a software failure/fault to be an event where the customer's expectations have not been met. In fact, that follows from the interpretation of failure as a complete or partial loss of system function, in this particular case caused by the software. Shubinsky [14] notes that in this case the software itself did not fail; the failure occurs at the system level. Only those parts of the software that are faulty are activated, or the part of the software unable to respond correctly to the system command is activated.

Randall [15] suggests a whole sequence as follows:

Failure → Fault → Error → Failure, etc.

Here, terms that repeat are associated with higher system levels. Randall uses the following definitions:

A system *failure* occurs when the delivered service deviates from the system's function, the latter being what the system is intended for.

This corresponds to the definition of failure given by other authors.

Error is the part of the system state that can cause a subsequent failure. An error affecting the service is an indication that the failure has already occurred. The known or assumed cause is an error.

So, for Randall, an *error* is a deviation as a component of a system's state. Additionally, he interprets it as a fault symptom and defines a fault as the cause of an error. This approach appears to be ambiguous. The author's understanding is that Randall rather describes a fault when he explains what an error is. Rees [16] also maintains that

failure is a loss of function, i.e., an element does not work if it has not done what we want and is in a good state if it has done what we wanted. More precisely, it is the function that fails.

Note that it is not a matter of whether a system is physically intact or otherwise. A failed system may be physically intact. A physically intact system may also fail due to hidden (unwanted or poorly designed functions, see, e.g., Deckers and Schäbe [17]) or undocumented functions that were integrated in the system unintentionally or intentionally.

Parhami [18] introduces a list of 7 states: *ideal*, *defective*, *faulty, error*, *poorly functioning*, *degraded*, *failure*. A system passes from state to state, from ideal to failure. In the authors' opinion, the designations of some of the states are ambiguous. A defect can also mean a fault, degradation or failure. Additionally, the question is how to interpret an error state. Is this term supposed to be used only to characterise a system affected by an error, where the error describes a deviation from the specifications, that was built into the system at the very beginning, i.e., a deviation? The authors believe that the number of states is to be reduced. While on the subject of failures, we should also mention the distinction made in IEC 61508 [6] and other functional safety standards between the concepts of "Accidental hardware failures" and "Systematic failures". First of all, let us define failure, fault and error according to IEC 61508 [6] part 4:

3.6.4: "a failure is the termination of a functional unit's ability to ensure the required function or the operation of such functional unit in any other way than the required one.

3.6.1: "a fault is an abnormal state that may cause a functional unit to completely or partially lose be ability to perform the required function".

3.6.11: "an error is a discrepancy between the calculated, observed or measured value or condition and the true, specified or theoretically correct value or condition".

By comparing these definitions with the definitions from other sources, it can be seen that failures are also regarded as events in which a system or its component unit does not ensure the performance of the desired function. Additionally, a fault is defined as a precursor of failure, i.e., an abnormal state, or a deviation, in this case. Nevertheless, the consequences will differ at the system level. That may include a partial loss of ability. Since the term "may" is used, it is also possible that, at the system level, there are no consequences, while there is only the requirement to repair the redundant unit.

3.6.5: "a random hardware failure is a failure that occurs at a random point in time that is the result of one or more possible hardware degradation mechanisms";

3.6.6: "a systematic failure is a failure deterministically associated with a certain cause that can only be eliminated by modifying the design or the process, operations, documentation, or other factors".

In these above two definitions, failures are distinguished depending on the mechanism that caused them. Accidental hardware failures are associated with the processes of ageing and degradation. Systematic failures are associated with design errors, etc. However, these failures also manifest themselves stochastically [19] when the failure mechanism is triggered, therefore they are deterministic only in the sense that one cause can be clearly defined. The time of occurrence is in many cases random. This randomness is caused by the environment that produces random external effects. To be precise, two sub-types should be distinguished:

a) the system contains an error, e.g., a software error. Another example could be a system that is unable to withstand certain high or low temperatures, although that is required. There is no ageing. Once an effect triggers such error, the system fails at a random time. The randomness is caused by the randomness of the external effect.

Due to erroneous processes, the system has a weakness. This weakness, for instance, consists in reduced resistance to loads, environmental effects, etc. An example is degraded mechanical parts that fail due to fatigue. Here, we can observe the triggering of the accidental failure mechanism caused by a design error that would otherwise have been eliminated through design solutions if the component was strong enough.

3. Analysis and conclusions

The analysis clearly shows how fault, failure and error should be interpreted.

Failure is always associated with a loss of function, i.e., a function as the ability to perform as required by all standards. It should be noted that this requirement may also be implicit, i.e., the system does not operate as expected. It should be noted that wrong user expectation does qualify as failure. Failures should be distinguished from sneaks (see, e.g., [17]).

Fault is defined as a system's inability to perform the required operation to the full extent that, under certain conditions, may escalate into a failure. The term "fault" may be translated into Russian in two different ways (failure, malfunction) that are used in parallel to each other depending on the document.

Error as a discrepancy between a calculated, observed or measured value or condition and a true, specified or theoretically correct value or condition, a deviation that is present and, under certain conditions, could turn into a failure. A typical example is non-critical software errors. The so-called systematic failures are actually errors that can turn into critical errors (failures). Let us note that the definitions in [6] can be used, as they show general agreement, which is not surprising for an international standard.

References

1. Netes V.A. Item in dependability: definition and content of the concept. Dependability 2019;19(4):3-7.

2. Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what "dependability" is. *Dependability* 2014;4:15-26.

3. Plotnikov N.I. Development of an alternative dependability terminology. *Dependability* 2020;3:21-26.

4. Pokhabov Yu.P. On the definition of the term "dependability". *Dependability* 2017;17(1):4-10.

5. Mikhailov V.S. On the terminology of dependability. *Dependability* 2020;2:24-27.

6. GOST R IEC 61508. Functional safety of electrical, electronic, programmable electronic safety-related systems. Moscow: Standartinform; 2014. (in Russ.)

7. IEC 60050 International Electrotechnical Vocabulary; 2015-02.

8. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

9. Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965. (in Russ.)

10. Gayen J.-T., Schäbe H. (Mis-)conceptions of safety principles. *Proceedings of ESREL 2008, Safety, Reliability and Risk Analysis* 2008;2:1283-1291.

11. Gayen J.-T., Shäbe H. [Correct and incorrect understanding of the principles of functional safety]. *Dependability* 3;3:63-74. (in Russ).

12. DIN 40041, Zuverlässigkeit; Begriffe (Reliability, terms). 1990-12 (outdated).

13. Chillaregge R. What is software failure. Commentary in IEEE Transactions on Reliability 1996;45(3).

14. Shubinsky I.B. [Functional dependability of information systems. Analysis methods] Moscow: Dependability Journal; 2012. (in Russ.)

15. Randall B. On failures and faults. Lecture notes in computer science. September 2003. DOI: 10.1007/978-3-540-45236-2_3.

16. Rees R. What is a failure. *IEEE Transactions on reliability* 1997;46(2):163.

17. Deckers J., Schäbe H. Using sneak circuit analysis in aerospace product assurance. *Qual. Rel. Eng. Int.* 1999;9:137-142.

18. Parhami B. Defect, fault, error,…., failure. *IEEE Transaction on Reliability* 1997;46(4):450-451.

19. Braband J., Schäbe H. Individual risk, collective risk, and F–N curves for railway risk acceptance. In: Mahboob Q., Zio E., editors. Handbook of RAMS in Railway systems – Theory and Practice. Boca Raton, Taylor and Francis; 2018. P.119-128.

About the authors

Igor B. Shubinsky, Doctor of Engineering, Professor, Deputy Director of Integrated Research and Development Unit, JSC NIIAS. Address: 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation, phone: +7 (495) 786 68 57, e-mail: igor-shubinsky@yandex.ru.

Hendrik Schäbe, Dr. rer. nat. habil., Head of Risk and Hazard Analysis, TÜV Rheinland InterTraffic, Cologne, Germany; e-mail: schaebe@de.tuv.com.

The authors' contribution

The authors' contribution consists in the analysis of the terms failure, fault and error and their use in the Russian and English languages. The authors' contributions are equal.

Conflict of interests

The authors declare the absence of a conflict of interests.

Original article
https://doi.org/10.21683/1729-2646-2021-21-2-28-30

Suggestions for improved dependability-related terminology

Boris P. Zelentsov, *Siberian State University of Telecommunications and Information Sciences, Novosibirsk, Russian Federation*
zelentsovb@mail.ru

Boris P. Zelentsov

Abstract. Aim. *This article aims to eliminate the shortcomings associated with the application of the conventional, yet insufficiently substantiated terms in the GOST 27.002-2015 interstate standard. Correct understanding and use of terms are of great significance for the activities of dependability experts.* **Methods.** *Shortcomings in terminology are eliminated by clarifying the definitions of the used terms. Several terms used in this standard were submitted to logical and terminological analysis that is based on statutory requirements and the semantic meanings of such terms. The premises were set forth in [8].* **Findings and conclusions.** *Definitions of several new terms, as well as those that do not meet the identified requirements are suggested: "dependability theory", "dependability estimation", "dependability calculation", etc. The expressed considerations could provide the foundation for the adoption of agreed (compromise) solutions.*

Keywords: *dependability, dependability-related terminology.*

For citation: *Zelentsov B.P. Suggestions for improved dependability-related terminology. Dependability 2021;2: 28-30. https://doi.org/10.21683/1729-2646-2021-21-2-28-30*

Received on*: 18.01.2021* / **Revised on:** *19.04.2021* / **For printing:** *21.06.2021.*

Introduction

The paper aims to formulate substantiated suggestions for clarifying certain terms and concepts of the standard [1]. The paper substantiates the definitions of a number of terms and concepts that, in the author's opinion, could provide the foundation for the adoption of agreed (compromise) solutions.

Source overview

In [10], the author correctly observed that technical standards require preliminary elaboration in terms of humanities. As the result, a set of agreed and consistent terms should be substantiated.

In [11], unorthodox approaches are set forth to the matters of technical item dependability in terms of design and development.

In [8], the requirements are defined for the used terminology in terms of internal logical consistency and specific terms are identified, whose use violates such requirements. Such terms include: "methods of dependability definition", "dependability estimation", "state of item".

In [8], the concepts are defined that are referred to in the name of the standard [1]: term, definition, dependability.

Term, a word or phrase that clearly designates a certain concept used in the field of dependability.

Definition, a wording that clarifies the meaning, content, essence, primary characteristic features of the terms using known and meaningful words.

Dependability is the property of an item to maintain in time the ability to perform the required functions in the specified modes and conditions of operation, maintenance, storage and transportation.

The definition of the term "dependability" is according to the standard [1]. It defines the essence of the term and its content as a property. This definition is unambiguous. No other interpretations, methods, variants, varieties of the definition of the term "dependability" must exist.

Methods

Besides the requirements of [8], the definitions of terms should include features that reveal the substance of the terms.

A new term – "dependability theory" – should be added to the basic concepts. This term is well-established and generally accepted. There is a number of monographs and textbooks entitled "Dependability theory". This term should also be used to define other dependability-related terms. Therefore, the term "dependability theory" should be included in the state standard.

Dependability theory: a set of scientific provisions that describe, substantiate and explain the principles, laws and correlations of phenomena in the field of dependability.

In [8], it was noted that the term "State" was used in the title of Section "3.2 States", yet it was not defined. Additionally, the term "State of item" is not defined either. The most appropriate terms associated with the states of items is "Technical state of item". The term and its definition are given in standard [2]:

Technical state of item (technical state, state of item, state): a set of properties of an item that is subject to changes in the course of its manufacture, operation, transportation and storage, characterized by parameter values and/or qualitative characteristics defined in the documentation.

In the author's opinion, the term "Technical state of item" should be made a basic concept and – along with its abbreviated forms – used in other sections of the standard.

Important terms are those that are associated with dependability calculation and its methods. The terms "dependability calculation" and "methods of dependability calculation" are used in reference and research literature, but they are not defined in the fundamental dependability-related standards. Let us definite those terms as follows:

Dependability calculation: mathematical calculations for the purpose of obtaining numerical values of dependability indicators of an item according to the rules established in the dependability theory.

Method of dependability calculation: a special technique or system of techniques for dependability calculation based on the laws substantiated in the dependability theory.

In accordance with standard [3], the terms are divided into two types, i.e., probabilistic and statistical. That means that dependability calculations can be based on the methods of the probability theory or mathematical statistics. Hence, the methods of dependability calculation are divided into two main classes, probabilistic and statistical. On the basis of the probability theory, the values of dependability indicators are calculated in terms of the properties of the entire assembly, while based on mathematical statistics, they are estimated according to sample observations of a certain set. Naturally, this does not rule out joint use of the probabilistic and statistical methods.

So, two classes of dependability calculation methods should be identified.

Probabilistic methods of dependability calculation: the methods of calculating dependability indicators based on the probability theory.

Statistical methods of dependability calculation: the methods of calculating dependability indicators on the basis of mathematical statistics.

Note 1. Those terms can be formulated differently, for example: methods of dependability calculation based on the probability theory/mathematical statistics.

Note 2. Those terms can replace the terms in [1]: the computational method for determining dependability, the computational and experimental method for determining dependability, the experimental method for determining dependability.

Note 3. The probabilistic and statistical methods can be used to calculate not only dependability indicators, but also various characteristics of random events and random values used in the field of dependability.

It should be noted that the term "statistical methods of dependability calculation" is used in [11].

Probabilistic methods are used to calculate the probability of random events and numerical values of dependability indicators that are numerical characteristics of random values. The dependability theory provides various probabilistic methods of dependability calculation that are set forth in monographs, manuals, textbooks and research papers. The standard [4] is dedicated to methods of dependability analysis (calculation). The specificity of methods based on the event tree and flow chart analysis have been examined, the Markovian, Petri net and other methods have been considered. The application of the Markovian methods is described in the standard [6], including the conditions of application, construction of state-transition diagrams, formulas for calculating the dependability of specific circuits. The standard [5] sets forth block diagrams on whose basis dependability is calculated, considers Boolean methods, the reduction method, etc. The subject matter of the author's research activities is the development of matrix methods of dependability calculation [9].

The standard [4] identifies statistical methods of assessing the probability of no-failure, defines the areas of their application and advantages. The statistical methods include Bayesian, Monte Carlo and others. The general terms associated with the statistical methods are set forth in standard [3]. The statistical methods are used for dependability indicator estimation.

The primary statistical terms include "estimate" and "estimation of dependability indicators".

Estimate of dependability indicator: the numerical value of a dependability indicator calculated from sample data.

Note: an estimate of dependability indicator is random and can take different values from sample to sample.

Estimation of dependability indicators: an operation that consists in obtaining (calculating) the numerical values of the dependability indicator from sample data.

Note 1. A dependability indicator is estimated based on statistical methods of dependability calculation.

Note 2. The purpose of an estimation is to obtain an estimate of a dependability indicator.

Discussion and conclusions

The paper sets forth specific suggestions for improving the dependability-related terminology. The author only considered a limited number of terms. The primary terms should include "dependability theory", "dependability calculation", "dependability calculation method". The definitions of the terms "technical state of item", "dependability estimate", "dependability estimation" were clarified.

The author hopes that the publication and discussion of the above suggestions will enable a stricter approach to the wordings of the dependability-related terminology standard.

References

1. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

2. GOST 18322-2016. Maintenance and repair system of engineering. Terms and definitions. Moscow: Standartinform; 2017. (in Russ.)

3. GOST R ISO 3534-1-2019. Statistics – Vocabulary and symbols – Part 1: General statistical terms and terms used in probability. Moscow: Standartinform; 2020. (in Russ.)

4. GOST R 51901.5-2005. Risk management. Guide for application of analysis techniques for dependability. Moscow: Standartinform; 2005. (in Russ.)

5. GOST R 51901.14-2007. Risk management. Reliability block diagram and boolean methods. Moscow: Standartinform; 2008. (in Russ.)

6. GOST R IEC 61165-2019. Dependability in technics. Methods. Moscow: Standartinform; 2019. (in Russ.)

7. Standardization recommendations R 50.1.075-2011. [Development of standards on terms and definitions]. Moscow: Standartinform; 2012. (in Russ.)

8. Zelentsov B.P. Comments on the contents of the dependability terminology standard. *Dependability* 2021; 1: 34- 37.

9. Zelentsov B.P. Matrix models of functioning of telecommunication equipment. *Vestnik SibGUTI* 2015; 4; 62-73. (in Russ.)

10. Plotnikov N.I. Development of the technology dependability automaton (substantiation of standardization regulation). *Dependability* 2020;4:21-24.

11. Pokhabov Yu.P. Dependability from a designer's standpoint. *Dependability* 2020;4:13-20.

About the author

Boris P. Zelentsov, Doctor of Engineering, Professor of the Department of Further Mathematics, Siberian State University of Telecommunications and Information Sciences, Novosibirsk, Russian Federation, e-mail: zelentsovb@mail.ru.

The author's contribution

The author conducted a terminological analysis of the fundamental dependability-related terminology standard and defined certain terms. The expressed considerations could provide the foundation for the adoption of agreed solutions in this area.

Conflict of interests

The authors declare the absence of a conflict of interests.

Safety model construction for a complex automatic transportation system

Alexey V. Ozerov[1]*, Alexey M. Olshansky[1]
[1]*JSC NIIAS, Moscow, Russian federation*
*a.ozerov@vniias.ru

Alexey V. Ozerov

Alexey M. Olshansky

Abstract. *The* **Aim** *of the paper is to consider approaches to the analysis of a safety model of complex multi-loop transportation systems comprising not completely supervised subsystems.* **Method.** *For the description of a safety model, the paper uses systems theoretic process analysis (STPA) methods and the principles specified in ISO/PAS 21448:2019 (SOTIF).* **Result.** *The paper shows drawbacks of the FTA and FMEA local risk analysis methods and demonstrates a demand for some universal approach based on the combination of STPA and control theory. It gives an overview of the major stages of such analysis for the safety model of complex transportation systems exemplified by the Moscow Central Circle, which provide a feedback for safety evaluation of a transport control system under development. The paper analyzes the feasibility of using a virtual model for control purposes in the form of a so-called "supervised artificial neural network".* **Conclusion.** *Today, railways are actively testing autonomous systems (with no driver onboard) that apply as their subsystems automatic perception modules using machine learning. The introduction of the latter into the control loop complicates the task of hazard analysis and safety evaluation of such systems using conventional FTA and FMEA methods. The construction of a safety model of such complex multi-loop transportation systems comprising not completely supervised subsystems that use machine learning methods with not completely predictable behavior requires the application of a systems approach to the analysis of unsafe scenarios along with the compilation of a scenario library and the formalization of a hazard model's description, pertaining to the boundaries of various control loops as well, in order to reduce the regions of unknown unsafe scenarios for autonomous transportation systems under development.*

Keywords: *railway transport, autonomy, safety model, STPA, machine learning, artificial neural network (ANN).*

For citation: *Ozerov A.V., Olshansky A.M. Safety model construction for a complex automatic transportation system. Dependability 2021; 2: 31-37. https://doi.org/10.21683/1729-2646-2021-21-1-31-37*

Received on: *23.03.2021* / **Upon revision:** *12.05.2021* / **For printing:** *21.06.2021*

1. Introduction

Today, many countries, including Russia, are testing automatic solutions in passenger rail transportation that aim for autonomy. Currently, full automation of passenger train control (with no driver or personnel onboard trains) has been only achieved for subways. According to UITP [1], 64 metro lines in 42 cities of the world operate in that mode.

The IEC 26690:2014 standard [2] specifies general requirements for an automatic control system for urban rail transport and proposes the following Grades of Automation (GoA) of systems (Fig. 1):

It is obvious that along with the increase of the GoA and shift to full automation of control, there appear additional safety risks that require evaluation and consideration in the process of developing the functional safety concept of this complex control system comprising a large number of subsystems.

Compared to subway systems where access to track is restricted and the boarding/disembarking process is eased up by using platform screen doors, urban railways have to resolve the issue through different means. Those include trackside and onboard perception (automatic obstacle detection) subsystems that use machine learning in decision making. Their introduction into the control loop significantly complicates the already complicated overall task of hazard analysis and safety evaluation of the multiple-loop control system associated with the safety of people. This task cannot be solved by means of the conventional FTA and FMEA hazard analysis methods only.

2. Problem definition

The aim of the paper is to outline a new analysis method for a safety model of complex multi-loop transportation systems comprising not completely supervised control loops, subsystems and modules. In a practical sense, this method could be used for safety evaluation of a driverless control system planned to be deployed on the Moscow Central Circle (MCC).

The key factors threatening the functional safety of a complex system may be described by the following list:

– Lost control commands or errors in transmission of external incoming information;

– Incomplete, incompatible, incorrect process model;

– Control algorithm errors (generation defect, errors of process scenario changes, problems of adaptability and trainability, inappropriate changes, errors in system state evaluation, system identification errors);

– Invalid, incorrect or missing control commands;

– Target or mechanism actions unfit for the process;

– Inadequate responses from sensors and observers;

– Invalid, incorrect or missing feedback;

– Feedback inaccurate measurements or delays;

– Delayed delivery of commands, input losses or errors;

– Component failures, unrecognized external noise/commands, their possible overlapping.

1. The basic premises for shaping a new approach to the construction of a safety model of complex transportation systems may be as follows:

2. Division into basic subsystems and error tree analysis for each subsystem does not take into account the interaction of these subsystems.

3. In a complex system, there may occur an event, when despite the constituent subsystems being operable, there may be incomplete interaction or multiple simultaneous delays due to external factors, which will cause an unintended reaction of the system in question.

Grade of automation	Train Operation	Setting Train in Motion	Driving and Stopping the train	Door Closure	Operation in event of disruption
GoA1	ATP with Driver	Driver	Driver	Driver	Driver
GoA2	ATP and ATO with Driver	Driver / Automatic	Automatic	Driver	Driver
GoA3	Driverless (DTO)	Automatic	Automatic	Attendant / Automatic	Attendant
GoA4	Unattendend (UTO)	Automatic	Automatic	Automatic	Automatic

Fig. 1. Grades of Automation (GoA) of operational modes in railway transportation

4. Complicated and time-consuming task of complete analysis of events in the system.

Insufficiency of a conventional redundant 2ooX system safety model when using ANNs in one or several subsystems. Necessity of applying additional safety measures, e.g., the implementation of a decision-making algorithm based on a digital twin. At the same time, the introduction of a digital twin (or virtual model) into a safety-critical system is an absolutely new and not yet well-proven approach to functional safety that is subject to further research (see Shubinsky et al., 2021 [3]).

3. STPA-based safety evaluation methodology

According to Qi Y. et al. (2020 [4]), the construction of a complex system safety model involves the development of a multi-level control system that includes the descriptions and apportionment of functional responsibilities between the system's components. The upper hierarchical level is a controller (control element) with a process model. The process model generates control commands through relations in the state space and a calculated control algorithm that is transmitted to the lower structures (target actuators). Through feedback devices, targets and other lower-level devices report about the execution of higher-level commands. The upper-level controller refers to the safety model and by comparing it with the received feedback, corrects the internal state of the model.

For such safety model, the probability of incidents comes down to situations where the internal state and feedback in the process model do not match. Such model is relevant to the functional structure of the system in question, while taking into account the relationship between subsystems as a sort of extension of multi-level control circuits.

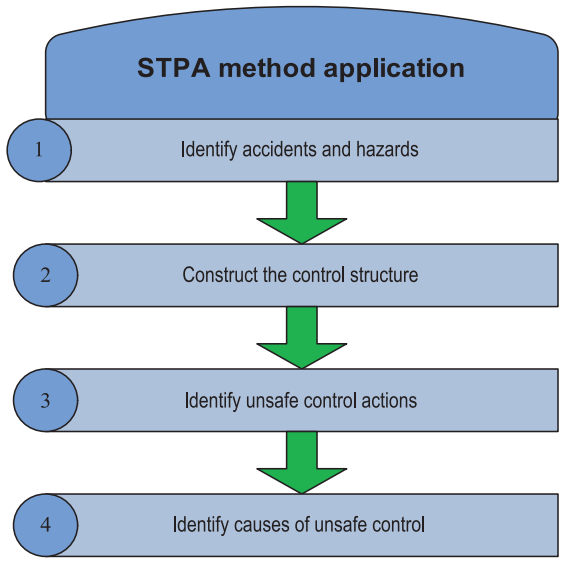


Fig. 2. STPA method application procedure

The proposed methodology is based on STPA methods assuming that we construct control and feedback circuits, target actuators, sensors and control processes and establish relationships between them that can be safety restrictions designed as systemically predefined cases (by the design and structure of such subsystems). By directly analyzing risks through an appropriate control process model, one has to evaluate safety requirements and all possible control solutions for each part of the system to identify potentially hazardous control actions and to improve the level of safety and restrictions that prevent hazardous behaviour caused by such control actions.

The STPA method (systems theoretic process analysis) appeared as a further development of the STAMP model (systems theoretic accident model and processes) proposed

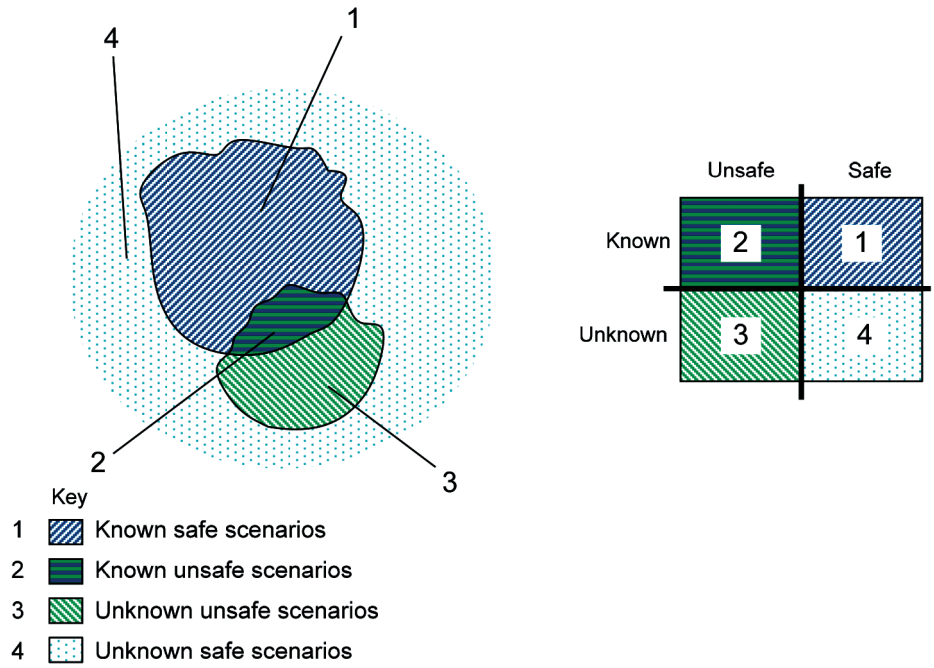


Fig. 3. Types of operational scenarios taken into account for a system's safety evaluation

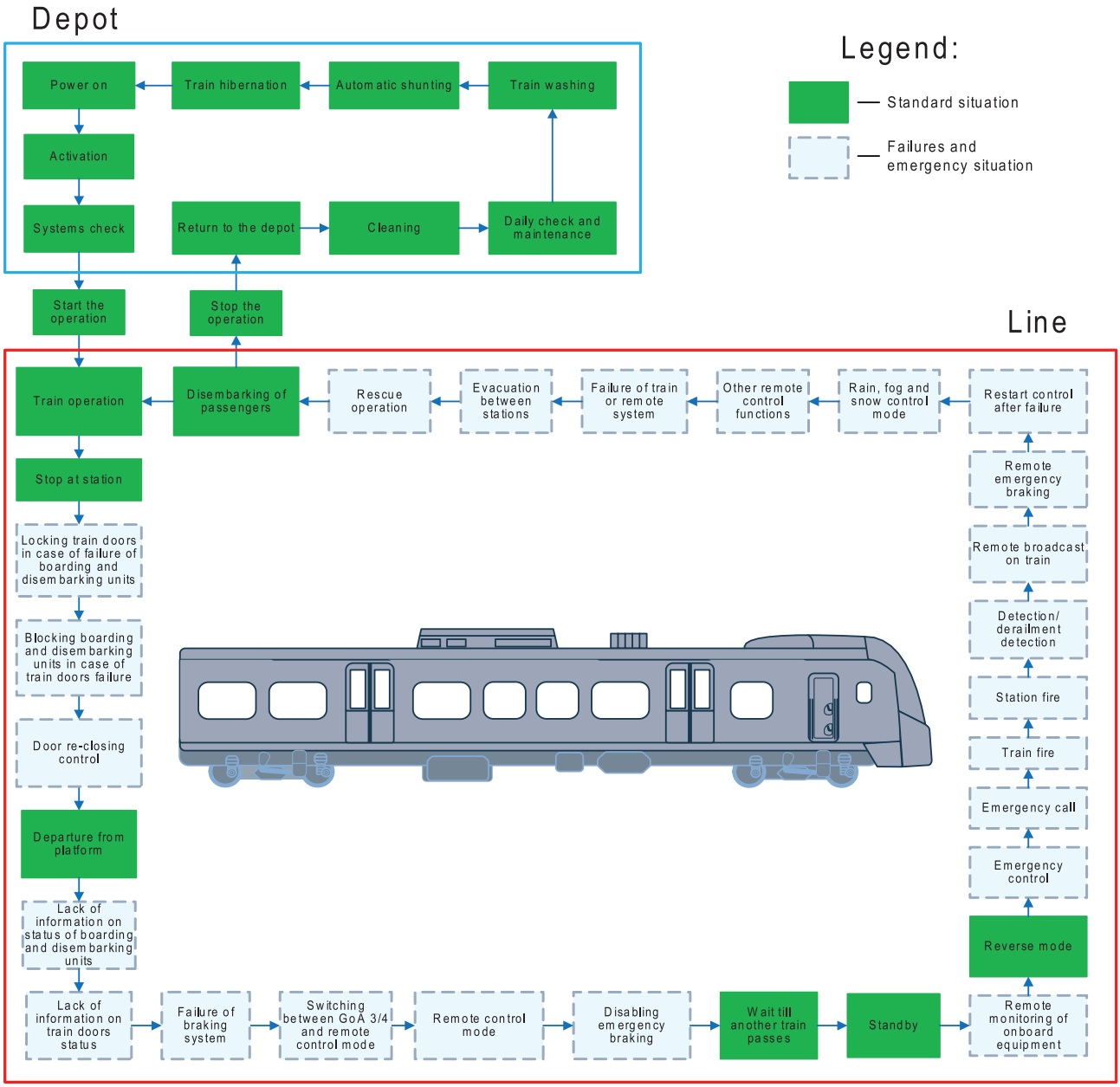


Fig. 4. Basic operational scenarios on urban railway such as the MCC

by Leveson (2004, [5]) and based on the control theory. The method is actively used in aviation, nuclear power and other industries associated with special safety requirements and complex systems. The method application procedure consists of 4 steps shown in Fig. 2 (see Chaima Bensaci et al., 2018 [6]):

Obviously, *at the first step*, we have to construct a scenario map for the entire complex system with scenario-to-scenario transition rules. Such scenarios could include all trigger events that lead to damage. In compliance with the ISO/PAS 21448:2019 (SOTIF) standard [7], one should take into account 4 scenario types presented in Fig. 3:

When constructing a safety model for a complex system, the objective is to get the maximum coverage for all scenarios and to bring the number of unsafe control scenarios to an acceptable level. As regards the MCC transportation system, we may propose a basic set of 1 and 2 type operational scenarios, which must be taken into account when constructing a safety model and compiling a general library of operational scenarios (Fig.4).

At the second step, it is required to construct a complete structural diagram of the control system under consideration. For instance, the MCC control system is designed as a multi-loop control system that implies two control modes, i.e., "autonomous" and remote ("remote control") (see Popov, 2020 [8]). In addition to the conventional track circuit-based train protection system, the control loop also includes radio communication between trackside and onboard train control and protection systems, as well as automatic obstacle detection by means of onboard and trackside perception modules that use ANNs and transmit relevant information to the remote control and supervision centre (RCSC). The overall

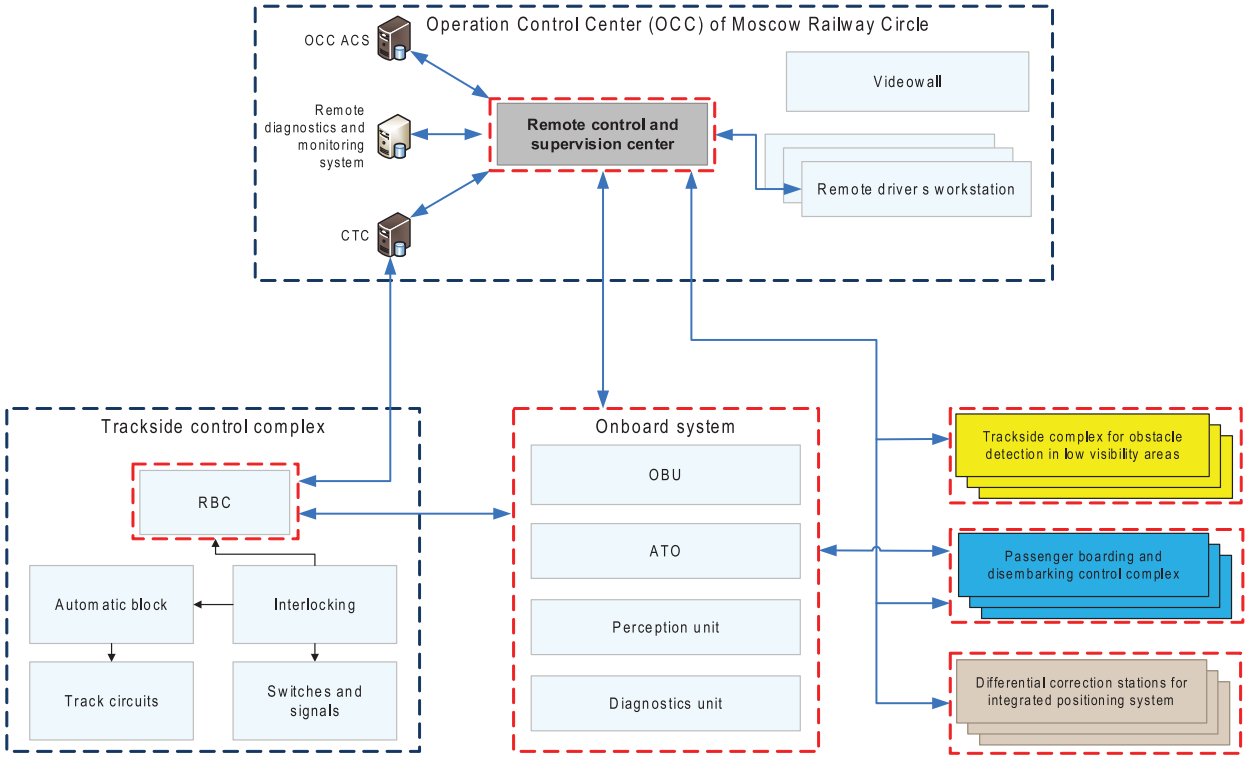


Fig. 5. The overall architecture of the MCC command and control system

architecture of the proposed MCC GoA3/4 control system is shown in Fig. 5 (red dash line indicates the subsystems making up the GoA3/4 control loop):

The presented control structure reduces the number of control layers as early as at the design stage and introduces some hierarchical order making the number of layers equal to two. The paper by Arnold (2004 [9]) clearly demonstrated that the systems with the number of layers equal to two can be sustainable provided that the upper-level control circuits are designed in a correct way. However, there should be further research and optimization of this structure to normalize relationship between control system complexes.

The third step of the study is the most time-consuming involving the definition and description of functional safety hazards according to the list of operational scenarios for each unit of the system at different hierarchical levels. Let us introduce the following notations for the purpose of analysis of the identified hazards: *Sc* is the total number of causal scenarios obtained through combinatorial means (which ensures 100% coverage of all devices and their combinations), *Mod* is the set of devices in the control loops that affect the functional safety of the system, *F* is the set of unsafe modes, *R* is the matrix of relationship between devices and unsafe modes, assuming that each device is incident with itself, i.e. the minimum sum of points in each device's line is 1.

In this case, subject to small modifications in terms of implementation in a particular programming language, the algorithm proposed by Yan F. et al. (2019 [10]) is applicable for the purpose of building a library of causal scenarios.

Therefore, with the introduced notation taken into account, we obtain the following sequence of actions to describe the functional safety hazards:

0. As the result of processing of a complete library of scenarios constructed according to the above syntax rules, one forms *Mod, F* sets.

1. *R* shall be constructed as a matrix (|*Mod*|, |*F*|). Note that the power of *F* set exceeds the total number of failure modes, since the same failure mode can be present in several scenarios. At the first stage, |*F*Yan F|>>|*M*| inequality shall be satisfied.

2. If *R* matrix line contains more than one entity, this means that at least one device out of *M* recorded in this line is involved in several failure modes.

3. Then identical columns shall be searched for. Their presence means that failure modes in them are the same. They can be included into one final scenario.

4. Thus, we have a library of relevant scenarios.

Such scenarios can be defined at all structural levels of the system under consideration. The general approach involves the following main stages of functional safety analysis:

1. Compilation of standard scenarios (see above), design of a hierarchical control structure, information flow diagrams.

2. Identification of hazard causes.

3. Development of safety measures.

The hierarchical control structure is a graphic representation of control layers, control commands from upper layers to lower layers and signals from lower layers, taking into account in the limit of sensors, doors, humans and microcontrollers. The selected units and devices are then described in

terms of normal and emergency behaviour as follows: "under normal conditions, N unit of X system provides (guarantees) a given property within the given range for the item."

A set of such statements as regards the elements of a hierarchical structure allows easily building a table of unsafe control actions. The table defines the description format: systems level hazards/control actions/not executed/executed incorrectly/control action is too early or too late/control action execution time is too short or too long.

The last 4 categories constitute unsafe scenarios (control actions). For each unsafe control action, the "cause – constraint" system is described, whereas the constraint describes the principles of safe behaviour in a particular situation under the selected unsafe control actions. For instance, the loop "train – Remote Control and Supervision Center (RCSC) – trackside obstacle detection system (TODS)" contains at least 2 sources of unsafe control actions, i.e., the signal from RCSC that may not arrive to the train, and TODS that may not send a request or send it too late. As the result, communication becomes a critical source of risk for the entire MCC transportation system.

A separate research will presumably be needed to cover unsafe scenarios that may take place at the boundary or at the overlap of the identified complexes "cause – constraints", or control loops. Special attention will have to be paid to the "overlap" of RCSC – TODS and "onboard perception unit (OPU) – RCSC" loops, as there is a probability of unsafe control actions from both loops when a train is in a low visibility area (TODS responsibility zone). Also, it should be kept in mind that neither loop is completely observable since both OPU and TODS use machine learning algorithms (VoVNet family convolutional ANNs), whose behaviour cannot be considered completely predictable.

It may result in a further review and change of the safety model of a transportation system under design by means of introducing an additional component in the model taking on the supervision and constraining function. As a constraining element, there are various alternatives being researched – from final state machine based on "hard" logics to supervising network. Fig. 6. shows a simplified control structure, a virtual model ("digital twin") that can be implemented as "supervised ANN".

Unfortunately, the supervisor in the form of the so-called "supervised ANN" has a delay (if an adequate solution does not appear at the second step, its search can last longer than two steps and even infinitely, till it is not stopped by a decision maker). Moreover, the supervisor's algorithms of acceptability estimation and decision-making must be fast enough in order that a total delay could be reasonable. It should be kept in mind that the confidence level *P* returned by a decision-making algorithm will always be less than 100%. We hope that further research will help solve these issues.

4. Conclusion

With the increase of the GoA and shift to full automation of control, for a transportation system there arise additional safety risks related to not completely predictable behaviour of the constituent subsystems due to the application of machine learning methods in them. The introduction of ANN-based perception modules into the control loop significantly complicates the task of hazard analysis and safety evaluation of such systems using conventional FTA

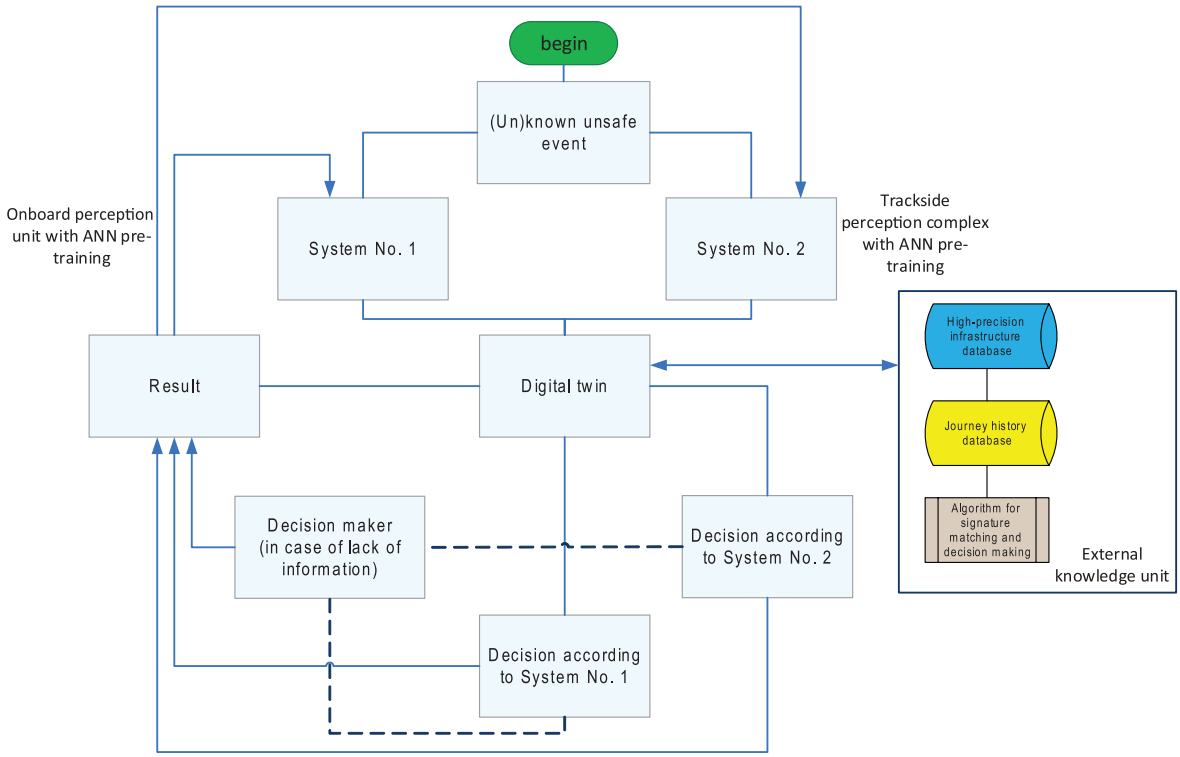


Fig. 6. Control structure with a virtual model

and FMEA methods. Evidently, the construction of a safety model of such complex multi-loop transportation systems requires the application of a comprehensive approach.

This approach must include a mandatory systems analysis of unsafe scenarios along with the compilation of scenarios library and the formalization of a hazard model's description, pertaining to the boundaries of various control loops as well. The systems analysis may result in a further review and change of the safety model of a transportation system under design and the conclusion about the necessity of having an additional component in the model taking on the supervision and constraining function – e.g., by implementing a decision making algorithm based on a digital twin. At the same time, the introduction of a digital twin (or virtual model) into a safety-critical system is an absolutely new and not yet well-proven approach to functional safety that is subject to further research. We can only hope that further research will make it possible to prove the feasibility of constructing a "supervised artificial neural network" complying with the conventional safety requirements applied to mass transportation systems, or to develop some other adequate supervision and constraining algorithm.

In turn, the proposed method based on STPA and control theory may become a universal methodological platform for the simulation and design of autonomous transportation systems. As a logical extension, based on the presented approach there may later also follow some design and development of a specialized software for automated risk evaluation of systems and technological process under construction.

References

1. https://www.uitp.org/publications/world-report-on-metro-automation/.

2. IEC 26690:2014. Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts.

3. Shubinsky I.B., Schäbe H., Rozenberg E.N. On the functional safety of a complex technical control system with digital twins. *Dependability* 2021; 1:38-44.

4. Qi Y., Cao Y., Sun Y. Safety analysis on typical scenarios of GTCS based on STAMP and STPA. *IOP Conference Series: Materials Science and Engineering* 2020;768(4):042042.

5. Leveson N.G. A systems-theoretic approach to safety in software-intensive systems. *IEEE*

6. *Transactions on Dependable and Secure Computing* 2004;1(1):66-86.

7. Bensaci C., Zennir Y., Pomorski D. A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System. European Conference on Electrical Engineering & Computer Science. Bern (Switzerland); 2018.

8. ISO/PAS 21448:2019 (SOTIF). Road Vehicles – Safety of the Intended Function.

9. Popov P.A. [Development of Russian and foreign driverless operation technology]. *Automation, Communication and Informatics* 2020;9:6-12. (in Russ.)

10. Arnold V.I. "Hard" and "soft" mathematical models. MTSNMO Publishing house; 2004. (in Russ.).

11. Yan F., Zhang S., Tang T. Autonomous Train Operational Safety assurance by Accidental Scenarios Searching. IEEE Intelligent Transportation Systems Conference. IEEE; 2019. P. 3488-3495.

About the authors

Alexey V. Ozerov, Head of Department, JSC NIIAS, 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation; e-mail: A.Ozerov@vniias.ru

Alexey M. Olshansky, Head of Centre, JSC NIIAS, 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation; e-mail: A.Olshanskiy@vniias.ru

The authors' contribution

Ozerov A.V. analyzed major approaches, identified their benefits and drawbacks, developed a general scheme of command and control, basic operational scenarios, a control scheme with a virtual model.

Olshansky A.M. proposed the concept of "supervised artificial neural network" and the sequence of actions related to the description of functional safety hazards.

Conflict of interests

The authors declare the absence of a conflict of interests.

Original article
https://doi.org/10.21683/1729-2646-2021-21-2-38-45

Tendencies in the propagation of fires and ammunition explosions at fixed storage facilities

Vadim A. Zlobin, *Combined Arms Academy, Moscow, Russian Federation*
vadimzlobin@rambler.ru

Vadim A. Zlobin

Abstract. Aim. *To suggest an approach to identifying the common features of statistical series containing information on the time, place and external conditions of the development and propagation of emergency situations associated with fires and ammunition explosions at fixed storage facilities, to synthesize the function of partial risk indicator of such situations, i.e., the energy susceptibility to external effects of ammunition storage systems.* **Methods.** *The paper uses methods of mathematical analysis of statistical series and probability theory. For the first time ever, individual external conditions of emergency situations involving ammunition are analysed using statistical series (rate of insolation).* **Results.** *The paper has collected and classified statistical data on emergencies involving fires and explosions in ammunition storage facilities that took place in the current century in a number of countries of the world, whose emergency nature was confirmed by extensive media coverage. Using statistical series analysis, an exponential relationship has been established between the rate of fires and explosions and the total power saturation of the ammunition storage system.* **Conclusions.** *The frequency of emergencies involving fires and explosions depends on the overall power saturation of the storage system that is defined by the solar intensity in the area of the ammunition storage facility that depends on its latitude and season. The suggested approach allows, by analysing empirical data on the time and place of emergencies, identifying the specific survivability values of a hazardous storage facility characterizing the energy susceptibility of the system to the effects that trigger explosions and fires.*

Keywords: *ammunition, explosives, fire, explosion, factor, arsenal, survivability.*

For citation: *Zlobin V.A. Tendencies in the propagation of fires and ammunition explosions at fixed storage facilities. Dependability 2021;2: 38-45. https://doi.org/10.21683/1729-2646-2021-21-2-38-45*

Received on: *16.11.2020.* **Revised on:** *14.05.2021.* **For printing:** *21.06.2021.*

Introduction

The emergency of any phenomena of the real world is determined by comparing them with similar phenomena on the basis of the frequency of their onset and the extent of the transformation of the environment in the course of such events. The trends in the occurrence of rare events with potentially major consequences are the subject matter of the risk theory. The quality of risk assessment and analysis defines the efficiency of the management of complex potentially hazardous systems, including missile and ammunition storage facilities.

Today, along with analytical models, simulation, event and solution tree analysis, heuristic methods of knowledge acquisition, neural network programming and learning are widely used for assessing the risks associated with the behaviour of complex systems. The validity of the estimates obtained using a certain method of analysis of phenomena and synthesis of scientific knowledge depends on the quality and amount of the obtained information (initial data) and the quality of the analysis and synthesis mechanism. The higher is the number of factors taken into account as part of risk analysis, the more valid is the system behaviour model and higher is the accuracy of risk assessment. This approach allows synthesizing the emergency risk function in the form of a multiplicative convolution of partial indicators r_i.

$$R(r_1, ..., r_i, ..., r_n) = \prod_{i=1}^{n} f^{\alpha_i}(r_i).$$

In addition to the man-made, technology-related and natural factors that characterize the probability of events able to cause emergencies, the overall level of system susceptibility to energy effects that define the probability of emergency propagation in time and space should be examined as an additional partial indicator of the risk function.

In many previous studies [1-10], based on statistical data, the underlying causes of such fire and explosion emergencies (FEE) were analysed. This paper deals with environmental energy conditions that contribute to the propagation of fires and explosions. The primary source of energy for all processes on the Earth's surface is the radiant energy of the Sun called solar radiation. The energy of stellar radiation and heat coming to the surface of the Earth as the result of the processes taking place within it are negligible compared to solar radiation [11]. The formation of organic matter that constitutes the basis of combustible and explosive materials is essentially the process of accumulation in the course of billions of years of biotransformation of the primary source of energy within the molecular bonds of the substrate.

The purpose of the paper is to identify new correlations between a system's energy saturation and the frequency of FEEs at ammunition storage facilities.

1. Problem definition

The ability of explosive and flammable materials to initiate cascading combustion and explosions of other substances underlies the potential hazard of ammunition storage facilities. Stored ammunition is essentially accumulators of destructive energy connected by potential initiation relationships. The damage caused by the destructive operation of such energy depends on the energy potential of the chemical elements in the ammunition, the energy potential of the fire load at the storage facility (crating, structures, vegetation) and the degree of loss of control over the energy release. Thus, the level of emergency of the ammunition fires and explosions is defined not only by the level of intentional control input, but by the intrinsic properties of the system, its energy capacity. It is obvious that if a system's energy saturation is zero (absolute zero temperature), no chemical processes within materials are possible. Another boundary condition for the onset and propagation of FEEs is the energy saturation of the system reaching energy-releasing reaction in organic materials. For black powders, ignition becomes possible after hours-long exposure to temperatures in excess of 400° K. Thus, the frequency of explosions and fires at each storage facility is supposed to depend on the energy input into the system. Under known boundary energy conditions of reliable or impossible onset of the event of explosion and fire initiation, it is required to define the function of the effect of a system's energy saturation on the frequency of explosions and fires in order to determine the partial indicator of risk, i.e., the system's susceptibility to energy effects.

2. Overview of previous research

Normally, FEE is a consequence of factors of intentional or unintentional human influence (man-made factor), errors or failures of technology (technology-related factor) and stochastic natural effects (natural factor). Each of these factors depends on the spatiotemporal characteristics of the system.

In [1-9], it is noted that the "human factor" dominates in the causality of FEE. Thus, in [6], based on the analysis of a large set of statistical data, it is noted that the number of technology-related fires following a temperature increase goes down [$r = -0.72$], while the number of fires due to social causes increases [$r = 0.73$] instead. The number of fires caused by other factors is not associated with temperature dynamics.

The yearly distribution of incidents was examined in [1, 2]. Those works identified trends for higher frequency of incidents in fire hazard periods. For instance, out of 73 FEEs at ammunition storage facilities examined in [2] 93% took place during the warm season from March to October. The authors attribute that to the fact that most scheduled activities involving ammunition are carried out during the warm season, whereas they start in May and the end in October

[2, p. 32]. However, it should be noted that as the ambient temperature rises, within the system, the intensity of chemical processes increases, the energy threshold of initiation of combustion and explosion reactions decreases and the fire load on the storage facility premises grows. Thus, growing overall energy saturation of the system affects the frequency of explosions and fires.

3. Definition of input data

Achieving the designated goals involved examining the distinctive features of FEE development identified as part of the analysis of publicly available statistical data on the time, place and external conditions of mass explosions of ammunition at fixed storage facilities in a number of countries starting from 01.01.2001. The very fact that information on such incidents was covered in the media allows qualifying them as "extraordinary" and indicates that the examined energy connections are manifest in the sequence of mass explosions and fires.

The environmental temperature and humidity, the rates of thermal currents and static voltage in the air masses that affect the explosion and fire safety of the storage system, depend on the radiant energy of the Sun. The causality is clear: high temperature and low humidity dry out the fire load in the FEE area and increase the sensitivity of the explosives and powders to the initiating effects; the flows of oxygen-rich air facilitate the combustion reaction; the static voltage discharges, forming lightnings of hot plasma.

Almost all (90%) the radiation energy from the Sun is received by the Earth at the upper boundary of the atmosphere [11]. The amount of heat delivered by solar radiation per 1 cm^2 of a surface perpendicular to the beams of sunlight per 1 min of time is called solar intensity and is determined using the formula:

$$I = S/4\pi r^2,$$

where: S is the radiating power (radiant emittance) of the Sun equal to about $4 \cdot 10^{20}$ MW; r is the distance between the Earth and the Sun.

Given the average distance between the Earth and the Sun r = 149.600 mil km, the solar intensity is 1.98 cal/(cm^2 min) or 1.37 kW/m^2. This value is called the solar constant. The energy spectrum of solar radiation at the boundary of the atmosphere is close to that of the absolutely black body with the temperature of about 6000 K.

The distribution of solar radiation at the outer fringe and its change over time depend on the following causes:

1. Solar activity. In the peak years, the power of solar radiation can increase by 2%. As the solar activity grows, the Earth experiences increased intensity of magnetic and ionospheric disturbances affecting the man-made and technology-related factors of FEE;

2. Distance between the Earth and the Sun. Since the Earth's orbit is an ellipse, in January, the distance r_1 = 147.100 mil km, while in July, r_7 = 152.100 mil km. On the day of the winter solstice, the solar intensity is about 3.3% stronger than in spring and autumn, while on the day of the summer solstice it is 3.3% weaker.

3. The incident angle. The amount of incoming solar radiation (insolation) changes over time due to the deviation of the earth axis from the perpendicular to the orbit plane by 23°30'.

Thus, the cause of the annual and daily cycles of atmospheric phenomena is the rotation of the Earth around the Sun and the inclination of the Earth. If we designate the solar elevation as h_o, then a unit of the horizontal surface receives as much less radiation, as the surface area is larger than the flow area.

The solar intensity delivered to a surface at an angle of h_0 equals

$$I_h = I_0 \sin h_0,$$

where: I_0 is the rate of solar radiation per 1 min per 1 cm^2 of a perpendicular surface, h_0 is the flow incident angle. From astronomy, it is known that

$$\sin h_o = \sin \varphi \sin \delta + \cos \varphi \cos \delta \cos \psi \, cos,$$

where φ is the site latitude; δ is the solar declination; ψ is the local hour angle of the Sun.

Consequently, the heat inflow from solar radiation to a horizontal surface depends on:

1. Site latitude φ that largely defines the differences between the climate zones;

2. Solar declination δ that changes during the year from δ = 23.44°N to δ = 23.44°S, which defines the seasons;

3. Local hour angle of the Sun ψ that defines the daily variation of the solar intensity;

4. Distance between the Earth and the Sun r.

For the purpose of the analysis of the parameters of the evaluated system, the geographical coordinates of the potentially hazardous facilities are the initially specified spatial characteristics.

The values of the solar declination (δ), time of sunrise and sunset for specific dates can be determined using the solar calculator: http://www.timezone.ru/suncalc.php.

With an error of ±0.2º, the solar declination is calculated using the known formula (Wikipedia):

$$\delta = -\arcsin(0.39779 \cos(0.98565^\circ (N+N_{ds}))+ \\ +1{,}914^\circ \sin(0.98565^\circ (N-N_a)))$$

where: N is the sequence number of the estimated day from January 1; N_{ds} is the number of days since the December solstice before January 1 (N_{ds} = 10); N_a is the number of days after January 1 before the perihelion (N_a = 2).

The local hour angle of the Sun ψ is related to the latitude and solar declination with the formula:

$$\psi = \arccos(-\text{tg}\, \varphi \, \text{tg}\, \delta).$$

Table 1. Emergencies associated with fires and ammunition explosions

No.	Site	Latitude φ (degrees)	Date	JDN	Daily insolation Q (MJ/m^2)
1	2	3	4	5	6
1	Desselbrunn, District of Vöcklabruck, Austria	48.02	01.02.2018	32	12.635
2	Shirvan, Azerbaijan	39.92	26.07.2016	208	40.022
3	Giləzi, Khizi District, Azerbaijan	40.87	27.08.2017	239	34.957
4	Zemelan, Albania	41.32	06.05.2006	126	38.043
5	Gërdec, Albania	41.42	15.03.2008	75	26.792
6	Aïn Defla, Algeria	36.32	18.10.2015	291	24.974
7	Bashgah, Afghanistan	34.52	02.05.2005	122	38.331
8	Parwan, Afghanistan	35.02	23.03.2006	82	31.135
9	Chelopechene, Bulgaria	42.70	03.07.2008	185	41.771
10	Kostenets, Bulgaria	42.27	08.08.2014	220	38.144
11	Kostenets, Bulgaria	42.27	20.03.2015	79	27.434
12	Iganovo, Bulgaria	42.67	04.04.2015	94	31.076
13	Kazanlak, Bulgaria	42.62	25.04.2016	116	36.007
14	Maglizh, Bulgaria	42.60	27.05.2016	148	40.776
15	Hamburg, Germany	53.55	30.08.2002	242	30.118
16	Aden, Yemen	12.78	28.03.2015	87	37.158
17	Maharashtra, India	21.27	31.05.2016	152	39.728
18	Port of Tanjung Priok, Indonesia	-1.08	05.03.2014	64	37.934
19	Baghdad, Iraq	33.35	06.06.2018	157	41.279
20	Tokrau, Kazakhstan	46.83	08.08.2001	220	37.371
21	Arys, Kazakhstan	42.43	20.03.2009	79	27.358
22	Karaoy, Almaty Region, Kazakhstan	43.52	08.06.2009	159	41.596
23	Otar Station, Kazakhstan	43.55	27.08.2013	239	34.237
24	Arys, Kazakhstan	42.43	26.06.2014	177	41.994
25	Arys, Kazakhstan	42.43	24.06.2019	175	42.012
26	Hengyang, China	26.97	18.06.2014	169	40.848
27	Mbuji-Mayi, Democratic Republic of the Congo	-5.50	26.01.2014	26	38.373
28	Maputo, Mozambique	-25.23	22.03.2007	81	34.061
29	Lagos, Nigeria	6.45	27.01.2002	27	34.254
30	Podali, Khabarovsk Krai, Russia	50.55	17.01.2001	17	8.715
31	Nerchinsk, Chita Oblast, Russia	51.98	22.06.2001	173	41.797
32	Gusinoye Ozero, Buryatia, Russia	51.12	20.07.2001	201	39.885
33	Syzran, Samara Oblast, Russia	53.17	10.07.2002	191	40.881
34	Snegovaya Pad, Primorsky Krai, Russia	43.12	16.10.2002	289	21.853
35	Khabarovsk, Russia	48.48	13.06.2003	164	41.711
36	Norsk, Amur Oblast, Russia	52.33	18.06.2003	169	41.721
37	Kiparisovo, Primorsky Krai, Russia	43.47	13.07.2003	194	41.207
38	Achkhoy-Martan, Chechen Republic, Russia	43.18	07.12.2004	342	12.168
39	Kronstadt, Russia	60.00	17.05.2005	137	36.768
40	Ulan-Ude, Republic of Buryatia, Russia	51.83	16.06.2005	167	41.683
41	Yuzhnye Koryaki, Primorsky Krai, Russia	53.27	01.10.2005	274	20.459
42	Lodeynoye Pole, Leningrad Oblast, Russia	60.73	23.05.2008	144	38.208
43	Fokino, Primorsky Krai, Russia	42.97	30.09.2008	274	25.822
44	Karabash, Chelyabinsk Oblast, Russia	55.48	14.09.2009	257	24.647
45	Ulyanovsk, Russia	54.32	13.11.2009	317	8.711
46	Ulyanovsk, Russia	54.32	23.11.2009	327	7.089
47	Arga, Amur Oblast, Russia	51.27	28.10.2010	301	14.053
48	Dachny, Lipetsk Oblast, Russia	52.62	06.04.2011	96	27.590
49	Urman, Bashkortostan, Russia	55.47	26.05.2011	146	39.297

No.	Site	Latitude φ (degrees)	Date	JDN	Daily insolation Q (MJ/m^2)
50	Pugachiovo, Udmurtia, Russia	56.60	02.06.2011	153	40.199
51	Surgach, Primorsky Krai, Russia	45.52	18.05.2012	139	39.480
52	Koltubanovsky, Orenburg Oblast, Russia	49.02	11.06.2012	163	41.639
53	Orlovka, Orenburg Oblast, Russia	48.83	09.10.2012	283	20.290
54	Chapayevsk, Samara Oblast, Russia	52.98	18.06.2013	169	41.689
55	Bolshya Tura, Zabaykalsky Krai, Russia	51.62	29.04.2014	119	34.384
56	Pugachiovo, Udmurtia, Russia	56.60	04.05.2015	124	34.270
57	Urman, Bashkortostan, Russia	55.47	03.06.2015	154	40.432
58	Yuganets, Nizhny Novgorod Oblast, Russia	56.23	04.08.2016	217	36.005
59	Samara, Russia	53.18	18.10.2016	292	15.238
60	Khalino, Kursk Oblast	51.73	21.04.2017	111	32.268
61	Galichny, Khabarovsk Krai, Russia	50.72	29.07.2017	210	38.522
62	Primorskoye, Abkhazia (Russian Base)	42.58	02.08.2017	214	39.017
63	Pugachiovo, Russia	56.60	16.05.2018	136	37.198
64	Kamenka, Krasnoyarsk Krai, Russia	56.27	05.08.2019	217	35.997
65	Zheltukhino, Ryazan Oblast, Russia	53.75	07.10.2020	281	18.063
66	Parachin, Serbia	43.97	19.10.2006	292	20.621
67	Deir ez-Zor, Syria	35.33	08.10.2017	281	27.710
68	Damascus, Syria	33.52	02.09.2018	245	35.600
69	Abu Dali, Syria	34.43	14.06.2019	165	41.596
70	Mashrua ad-Dummar, Syria	33.52	15.06.2019	166	41.547
71	Shayrat, Syria	34.48	03.08.2019	215	39.559
72	Rmelan, Syria	36.48	21.06.2020	173	41.824
73	Al-Hasakah, Syria	36.48	16.07.2020	198	40.995
74	Novaki, Slovakia	48.72	03.03.2007	62	19.452
75	Juba, Sudan	4.85	23.02.2005	54	36.607
76	Sagamihara (US base), Japan	35.57	24.08.2015	236	36.663
77	Letterkenny, USA	39.93	19.07.2018	200	40.815
78	Abadan, Turkmenistan	38.05	08.07.2011	189	41.544
79	Diyarbakır, Turkey	37.90	16.09.2015	259	31.608
80	Kilis, Turkey	36.72	13.07.2017	194	41.250
81	Hakkâri, Turkey	37.57	09.11.2018	313	19.621
82	Reyhanlı, Turkey	36.27	09.08.2019	221	38.739
83	Kogon District, Bukhara Region, Uzbekistan	39.72	10.07.2008	192	41.407
84	Artemivsk, Luhansk Oblast, Ukraine	48.60	10.10.2003	283	20.421
85	Novobogdanovka, Zaporizhzhia Oblast, Ukraine	47.05	06.05.2004	127	37.235
86	Novobogdanovka, Zaporizhzhia Oblast, Ukraine	47.05	23.02.2005	54	18.258
87	Tsvitokha, Khmelnytskyi Oblast, Ukraine	50.23	06.05.2005	126	36.363
88	Novobogdanovka, Zaporizhzhia Oblast, Ukraine	47.05	19.08.2006	231	35.058
89	Lozova, Kharkiv Oblast, Ukraine	48.88	27.08.2008	240	32.352
90	Svatove, Luhansk Oblast, Ukraine	49.40	29.10.2015	302	14.941
91	Geyevka, Ukraine	49.50	08.03.2016	68	20.719
92	Khmelnytskyi, Ukraine	49.42	22.07.2016	204	39.658
93	Balakliia, Kharkiv Oblast, Ukraine	49.45	23.03.2017	82	24.865
94	Mariupol, Ukraine	47.12	22.09.2017	265	26.280
95	Kalynivka, Vinnytsia Oblast, Ukraine	49.43	26.09.2017	269	24.000
96	Balakliia, Kharkiv Oblast, Ukraine	49.45	03.05.2018	123	35.887
97	Ichnya, Chernihiv Oblast, Ukraine	50.85	09.10.2018	282	19.436
98	Gazost, France	43.02	07.10.2003	280	24.229
99	Salawa, Sri Lanka	6.92	05.06.2016	157	36.159
100	Latacunga, Ecuador	-0.27	07.11.2016	312	37.136

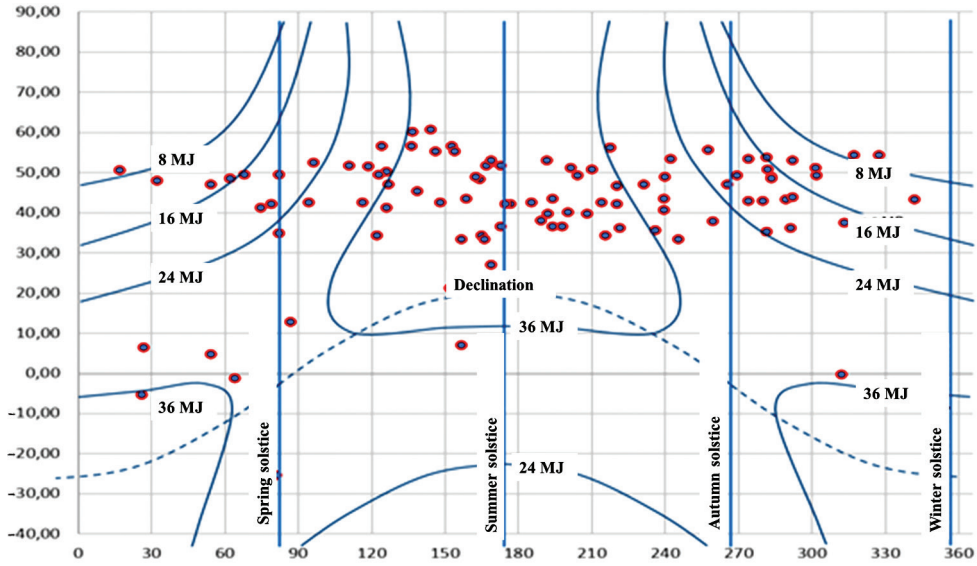


Fig. 1. Spatiotemporal distribution of FEE by day of year and by geographical latitude

The distance between the Earth and the Sun r is determined using the formula

$$r = \frac{r_0\left(1-E^2\right)}{1-E\cdot\cos\left(\frac{\pi}{2}-\arcsin\frac{\sin\delta}{\sin\varepsilon}\right)},$$

where: r_0 = 149.6 mil km is the average distance between the Earth and the Sun, E = 0.0167 is the Earth's orbit eccentricity, $\arcsin\frac{\sin\delta}{\sin\varepsilon}$ is the Sun's geocentric longitude.

Calculating all the arguments that affect heat inflow allows determining the daily insolation in FEE area on the day of occurrence Q by the formula:

$$Q = \frac{I_0 T}{\pi\left(r/r_0\right)^2}\left(\psi\sin\phi\sin\delta+\cos\phi\cos\delta\sin\psi\right),$$

where: Q is the total daily insolation, MJ/m^2; I_0 is the solar constant equal to 1.37 kW/m^2;

T is the period of the Earth's daily rotation (equal to 86 400 s).

Table 1 shows the input data and calculated daily insolation values for each FEE site and time.

The spatiotemporal distribution of the analysed set of FEE is shown in Fig. 1.

4. Determining the dependence of the FEE rate of the energy saturation

Certain values of daily insolation in the area of storage facilities at the moment of FEE enable statistical analysis based on this energy feature of the general population of exploded storage facilities (see Fig. 1).

The frequency distribution of 100 FEEs by daily insolation is presented in Fig. 2.

The power approximation of the integral indicator of FEE frequency with the insolation thresholds with the certainty of R^2=0.9976 allows estimating the dependence of the prob-

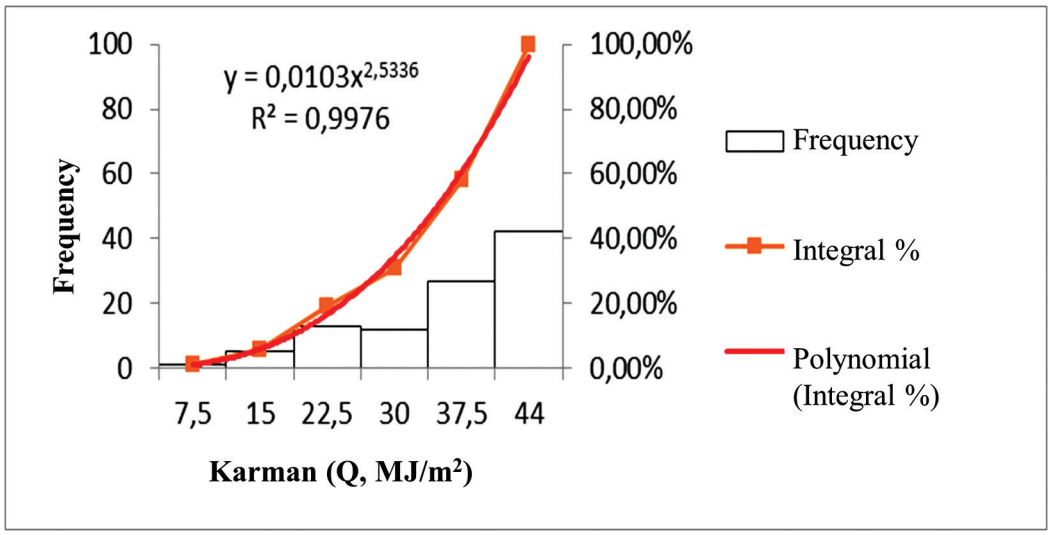


Fig. 2. Distribution of FEEs by daily insolation

ability of explosions and fires from the energy saturation of the environment.

Thus, the conducted analysis of empirical data allowed synthesizing the function of the partial risk indicator, i.e., a system's energy susceptibility to external effects r_e expressed through the value of daily insolation in a certain geographical region at a certain time

$$r_{\text{e}} = \frac{0,0103 \cdot Q^{2,534}}{0,0103 \cdot Q_{\max}^{2,534}} = \left(Q/44\right)^{2,534}.$$

The physical meaning of this indicator can be interpreted as the degree of correspondence of the environmental energy conditions with the conditions that most favour the development of FEEs.

Subject to the proposed partial risk indicator, the synthesized function of FEE risk (r_i) will be the product of four components:

$$r_i = r_{\text{val}}^a \cdot r_{\text{vul}}^b \cdot r_{\text{sc}}^c \cdot r_{\text{e}}^d,$$

where: r_{val}^a is the stock value indicator (affects the choice of the target of attack); r_{vul}^b is the stock vulnerability indicator (affects the attack effectiveness); r_{sc}^c is the indicator of social climate in the FEE area (indicates the aggressiveness of the social environment); r_{e}^d is an indicator of energy susceptibility (reflects the aggressiveness of the environment for the FEE development).

The specificity of using the convolution of indicators as multipliers is due to the fact that the human perception of expected losses has a logarithmic scale. In addition, the use of multiplicative convolution does not allow setting the partial indicators themselves that may have a natural expression, while only setting their weight coefficients: *a*, *b*, *c*, *d*.

5. Discussion of the results

A number of reasons can be associated with a rapid growth of the frequency of incidents as the insolation increases.

1. High-energy radiation (nuclear radiation) causes changes in the properties of powders. When affected by such radiation, destruction and structuring processes occur within them, ions and radicals may be generated that sharply increase the rate of chemical stabilizer consumption [5].

2. The cause of increased EA sensitivity to rising temperature is the weakening inter-molecular binding within the substance that facilitates the propagation of the initiating effects of wave, kinetic and thermal nature. As the temperature rises, the time it takes to heat the wooden package and gunpowder/ammunition to combustion temperature decreases, the depth of fragments penetration into the protective structures increases, wave attenuation in the environment weakens.

3. The power law dependence of the FEE on the level of insolation can be due to biological causes: growing fire load in ammunition storage facilities, intense growth and drying of vegetation, as well as the above-noted growing rate of operations involving ammunition. The existence of a dependence between the above and the comfortable climate conditions of work activity is beyond doubt.

4. Growing FEE frequency with rising insolation may be due to climate-related causes, e.g., increased frequency of thunderstorms, forest fires, peat fires, etc.

Conclusion

The conducted analysis of statistical data on incidents that caused fires and explosions at ammunition storage facilities allowed revealing a correlation between growing FEE frequency with rising environment temperature and the power law dependence of the susceptibility of items in the system to external effects on the overall energy saturation of the external environment.

The susceptibility to external effects reflects the correspondence between the actual external energy conditions and those that are most favourable for the propagation of FEE. This indicator should be used as an adjusting coefficient of the integral FEE risk indicator.

The inconsistency of the obtained findings regarding the effect of the environmental energy saturation on the emergencies involving ammunition explosions and regarding the low level of correlation between the frequency of forest fires and the air temperature stated in [6 – 9] defines the requirement to further examine the differences in the ways the environment's energy characteristics affect the more stochastic processes of mutual initiation of explosions and the more deterministic processes of fire front propagation.

References

1. [Development of basic technical solutions for the creation of hazardous facility safety training centres on the basis of an information, education and simulation environment: Report on the Instruktazhtsentr Research Project (final)]. Branch of the Combined Arms Academy of the AFRF; Penza. Activities Leader Alchinov V.I. Penza; 2010. (in Russ.)

2. Ivanov E.V. Emergency situations with explosions of ammunition: patterns of occurrence and progress. *Eastern-European Journal of Enterprise Technologies* 2016;1/10(79):26-35.

3. Liseychikov N.I. [Substantiation of the indicators of survivability of arsenals, bases and ammunition storage facilities]. *Nauka i voennaya bezopasnost* 2006;1:26-29. (in Russ.)

4. Sevryukov I.T., Ilyin V.V., Kozlov V.V. Assessing the Possibility of Emergency Situations When Storing the Distributed Groups of Ammunition. Vestnik IzGTU imeni M.T. Kalasnikova 2013;57:38-43. (in Russ.)

5. Pliushch A.A., Kurkov S.N., Elichev K.A. Operation of ammunition. A PAII textbook. Penza; 2004. (in Russ.)

6. Andreev Yu.A., Amelchugov S.P., Komarov S.Yu. [Development and prevention of fires in Siberia and the Far East]. *[Siberian Bulletin of Fire Safety]* 1999;1:22-46. (in Russ.)

7. Andreev Yu.A. [The effect of anthropogenic and natural factors on the development of fires in forests and communities: Doctor of Engineering Thesis]. Moscow; 2003. (in Russ.)

8. Baturo A.N. Laws of fires according to different groups of reasons. Vestnik Sankt-Peterburgskogo Universiteta GPS MCHS Rossii 2012;2:43-51. (in Russ.)

9. Glagolev V.A. [Estimation and prediction of vegetation fires in the Jewish Autonomous Oblast: Candidate of Geography Thesis]. Birobidzhan; 2015. (in Russ.)

10. Gorev G.V. [Estimation of a regions' climate-related disposition for forest fires (case study of the Tomsk Oblast): Synopsis of Candidate of Geography Thesis]. Tomsk; 2004. (in Russ.)

11. Lobanov V.A., Smirnov I.A., Shadursky A.E. [Practical course in climate science. A study guide. Part I]. Saint Petersburg: RSHU; 2011. (in Russ.)

About the author

Vadim A. Zlobin, Candidate of Engineering, Doctoral Student, Combined Arms Academy of the Armed Forces of the Russian Federation, Moscow, Russian Federation, e-mail: vadimzlobin@rambler.ru.

The author's contribution

Based on statistical data on emergencies involving ammunition fires and explosions in a number of countries of the world, the author suggested an approach to identifying the common features of statistical series containing information on the time, place and external conditions of the development and propagation of emergency situations associated with ammunition fires and explosions at fixed storage facilities and synthesized the function of partial risk indicator of such situations, i.e., the energy susceptibility to external effects of ammunition storage systems, identified the dependence between the rate of fires and explosions and the overall power saturation of an ammunition storage systems.

Conflict of interests

The author declares the absence of a conflict of interests.

 Original article
https://doi.org/10.21683/1729-2646-2021-21-2-46-52

Risk-oriented approach to life cycle contract implementation of weapons and military equipment

Vitaly A. Dubovsky[1]*, Natalia I. Dubovskaya[2], Andrey S. Nikolaev[3]

[1] General of the Army A.V. Khrulev Military Academy of Logistical Support, St. Petersburg, Russian Federation,
[2] Institute of Military System Research of Logistics Support of the Armed Forces of the Russian Federation, General of the Army A.V. Khrulev Military Academy of Logistical Support, St. Petersburg, Russian Federation,
[3] ITMO University, Saint Petersburg, Russian Federation
**dubovskiy@inbox.ru*


Vitaly A. Dubovsky


Natalia I. Dubovskaya


Andrey S. Nikolaev

Abstract. Aim. *Today, the development and operation of weapons and military equipment is characterized by fast-growing customer requirements, which, in turn, leads to their increased technical complexity and cost. It is obvious that maintaining the required physical and operational characteristics of high-technology weapons and military equipment by the users is not always possible due to a number of reasons, including insufficient capabilities of the service units that do not have the required personnel, assets and competences. In turn, the manufacturers involved in the delivery of the government defence order are also interested in shaping long-term relations with the customer allowing to build a platform for sound progress. One of the possible solutions for such interaction between the customer and the contractor used worldwide and in Russia is public-private partnership in the form of life cycle contracts. Despite the obvious advantages, its introduction into the practice of weapons and military equipment life cycle is hampered by a number of adverse factors (insufficiencies in the regulatory framework and technical standards, poor level of information technology deployment in LC management) that need to be overcome in terms of both scientific and practical considerations. It is perfectly clear that developing a tool that would allow mitigating a full spectrum of problems as part of this study would be an extremely challenging task. Given the above, the paper aims to examine risks as one of the aspects of this complex problem that implies the development of a new approach to the interaction of the parties involved in a life cycle contract for weapons and military equipment, taking into account the current conditions, interests, goals and objectives. It involves comprehensive analysis of uncertainty and the whole spectrum of possible risks associated with the weapons and military equipment life cycle processes.* **Methods.** *The managerial decision-making is based on the decision tree method that allows dividing the complex decision-making problem into component tasks and obtaining quantitative risk estimates, thus developing an adequate system of measures for the prevention of event risks and reduction of their negative consequences.* **Results.** *Based on the proposed methodological framework, a risk management algorithm has been developed, a matrix has been defined for assessing risks and their impact on the temporal and technical characteristics, as well as the costs of a project.* **Conclusion.** *The suggested approach is universally applicable and can be used by both the officials of military authorities in the process of scientific support of LCC implementation, and by the management of defense contractors as they develop their interaction with the military authorities responsible for the creation and operation of weapons and military equipment.*

Keywords: *public-private partnership, risk management, decision tree.*

For citation: *Dubovsky V.A., Dubovskaya N.I., Nikolaev A.S. Risk-oriented approach to life cycle contract implementation of weapons and military equipment. Dependability 2021;2: 46-52. https://doi.org/10.21683/1729-2646-2021-21-2-46-52*

Received on: *12.02.2021* / **Revised on:** *26.04.2021* / **For printing:** *21.06.2021.*

1. Introduction

The widespread economic integration of public organizations and business entities inevitably involved the military agencies of the Russian Federation. Outsourcing has become the most widely used process [1] implying the transfer of a number of non-core functions from units of the Ministry of Defence of the Russian Federation (MOD RF) to private companies. It normally involves activities associated with catering, supply of uniforms and gear, etc. In turn, the involvement of weapons and military equipment (WaME) manufacturers into the after-sales service is defined in accordance with service contracts that set forth a limited scope of WaME maintenance operations. Additionally, the operator remains responsible for the technical condition and operational capability of the WaME. Such situation is unacceptable, since the legal aspect contradicts the technical one and requires an alternative solution that would take into account the interests of all involved stakeholders.

Back in February 2013, at a meeting with defence contractors, the Minister of Defence of the Russian Federation made a case for life cycle contracts (LCC). A Decree of the President of the Russian Federation followed. Among other things, it defined the objective of developing a system for managing a complete industrial cycle of weapons, military and special equipment.

It should be noted that the matter of LCC application in various industries is not new. As of today, there is a fair number of Russian [2-7] and foreign publications [21-24] dealing with the subject matter that are usually either general in their nature or address the solution of risk management problems in individual industries [8-10] and local issues of engineering products LCC management [11-15]. In practical terms, the most interesting is [16] that makes an overview of the experience of LCC application in developed countries as part of public procurement and the analysis of the prospects of LCC development in Russia [17], where the author examines a set of problems in the context of WaME-related matters.

Despite the highest relevance of the issue and the large number of studies dedicated to finding the solution, it must be stated that there is no adequate theoretical foundation for an efficient application of WaME LCC.

A certain optimism is associated with the fact that all WaME LC stakeholders are interested in finding a solution. Each of them pursues their own pragmatic interest. Thus, the procurement agency of the MOD RF receives a specifications-compliant item that is able to fulfil the tasks assigned to the Armed Forces of the Russian Federation; the contractor, on the basis of long-term obligations involving guaranteed contractual funding, is able to invest in business development, while the operating agency is able to obtain WaME with required physical and operational characteristics with the assistance of third parties.

Such organization of interaction involves reassigning the responsibilities among the WaME LC stakeholders. That means that the technical availability of WaME is the responsibility of not only the operator, but the contracted company. In this case, the manufacturer will be interested in creating more dependable WaME, which would later allow minimizing the cost of maintenance and repair. For its part, the customer, the MOD RF, undertakes to comply with the terms of the contract, including the financial ones. That will obviously entail a paradigm shift in the way the MOD RF interacts with the military industrial complex (MIC), whose effectiveness will largely define the quality of the weapons systems.

Conceptually, such method of interaction is good for each of the WaME LC stakeholders, yet in practice the situation is not as trouble-free, since there are a number of serious organizational and legal barriers that prevent the process. They were examined in sufficient detail in [5, 17].

LC contracts proved to be efficient in many industries, including defense procurement in a number of foreign countries [18, 19]. But the specificity of the current internal processes of MOD RF defines a number of factors that cause differences between the public customer and the defence contractors.

Let us consider one of them. The existing system of interaction is designed mainly for the peacetime conditions and normal operation of WaME, which allows observing the scheduled dates of creation, delivery, maintenance, reasonably planning the delivery of required spare parts and accessories, frequency of maintenance personnel arrival, etc.

Implementing the WaME LC processes under special conditions will be affected by significant uncertainty, whose sources will consist in the following: stochastic demand for the required quantities of WaME; impossibility to accurately predict the locations of intended use; existence of a large number of factors that cannot be foreseen and predicted even in the probabilistic setting; violation of service schedules, premature life depletion, as well as a high probability of permanent loss of WaME. A separate issue is the operation beyond the normal operation period and subsequent disposal.

Thus, LCC will be implemented in an environment of uncertainty and risk. These two categories are interconnected.

Let us define *uncertainty* as incomplete and inaccurate information on the conditions of LC processes implementation, including the associated costs and results. Uncertainty involves the presence of factors that make the outcomes of actions non-deterministic, while the degree of such factors' effect on the outcomes is difficult to predict. Its sources include the lack of knowledge, many external and internal environment factors and their possible combinations affecting the WaME LC processes.

Risk is a potential, measurable probability of an adverse situation and associated severity of consequences in the form of non-compliance with customer requirements, failures and faults, contractor's losses, unfavourable circumstances, including act of God.

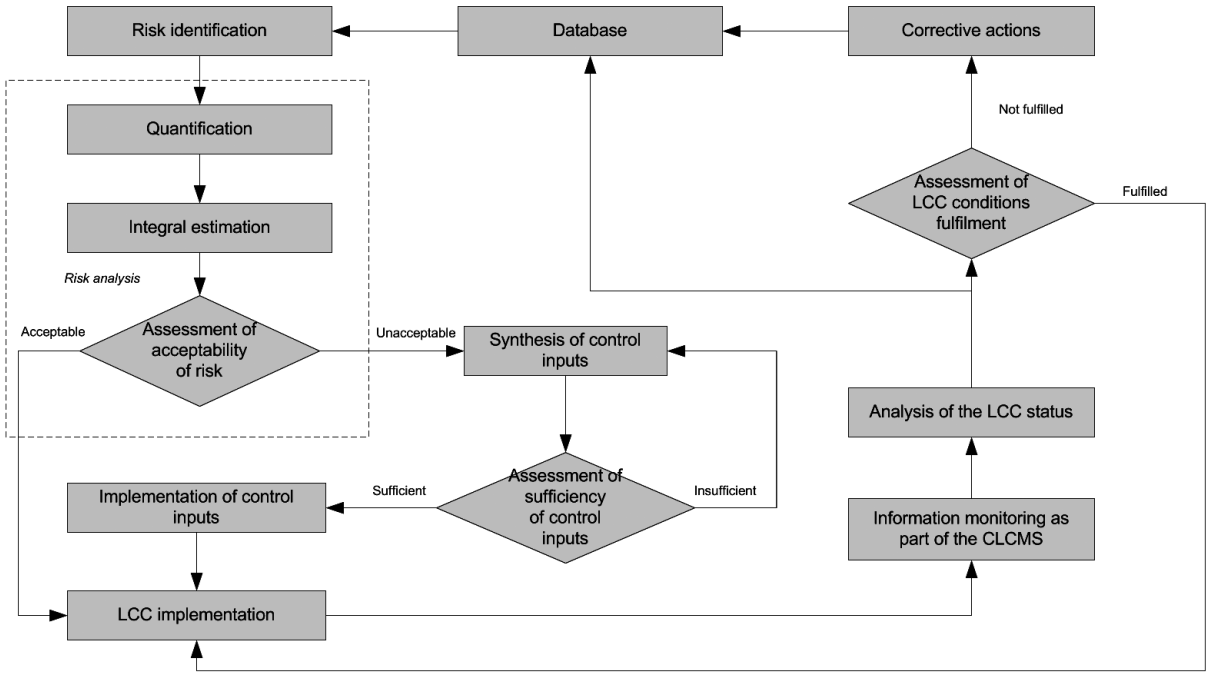


Fig. 1. A generalized risk management algorithm as part of WaME LCC implementation

The existence of a large number of risks arising from LCC implementation is currently one of the main outstanding issues. In this context, it appears relevant to develop a mechanism for the LCC implementation based on procedures enabling the identification, analysis of possible risks and development of appropriate managerial decisions for their minimization.

2. Methods

Following this reasoning, it is required to identify the primary risks associated with LCC implementation. That will later allow decomposing them, performing their qualitative and quantitative analysis. Figure 1 shows a generalized risk identification and management algorithm that illustrates a conceptual approach to their mitigation.

It is quite obvious that identifying a complete list of risks associated with the WaME LC process is extremely difficult, therefore the groups of the most likely risks were classified and then detailed to a level, at which they could be quantified and described as a particular event (set of events) with specific consequences.

In accordance with the established indicator of LC management efficiency, we will assume that the ultimate goal of LCC will be to ensure the required availability value within the budgetary limitations. As the efficiency criterion we will use the minimization of the integral risk indicator of LCC implementation, including the following types of risks [8]:

technical risk that characterizes the discrepancy between the performance characteristics and the performance specifications, which leads to deteriorating combat and operational performance;

economic risk that characterizes actual expenditures overrunning the planned values and leading to increasing LC cost indicators;

temporal risk that characterizes the discrepancies between the actual periods of activities and the scheduled dates causing failure to comply with the customer's requirements.

Factors of the above risks are identified and analysed according to the key LC characteristics, including: customer's requirements, logistics, cost and time parameters.

In this context, let us note that the uncertainty drives the risk and should be regarded as its main source. Therefore, analysing and subsequently managing risks is to be the focus of attention for preventive actions by the LC participants, as the elimination of the consequences of past events, including risk events, is more about situational management. That means that researching uncertainty would allow creating an empirical basis for subsequent identification and risk management in the course of LCC implementation.

An LCC is essentially a complex, long-term project, therefore a major part of managerial decisions requires thorough substantiation. The decision tree method is a convenient tool for such situations. It allows visualising and structuring complex decision-making problems amidst uncertainty and risk (see Fig. 2).

The method is based on decision points and consequence points of such decisions. Their number is not limited, therefore, so is the number of branches on the tree. Each decision point can produce a branch that represents a candidate decision in the given situation. For convenience, a brief description of the possible action is given. Let us denote the possible actions in the decision tree as a_1 and a_2, the execution of each of which can result in consequences from the set b_i, $i = 1, 2, 3, \ldots, n$. In turn, each of

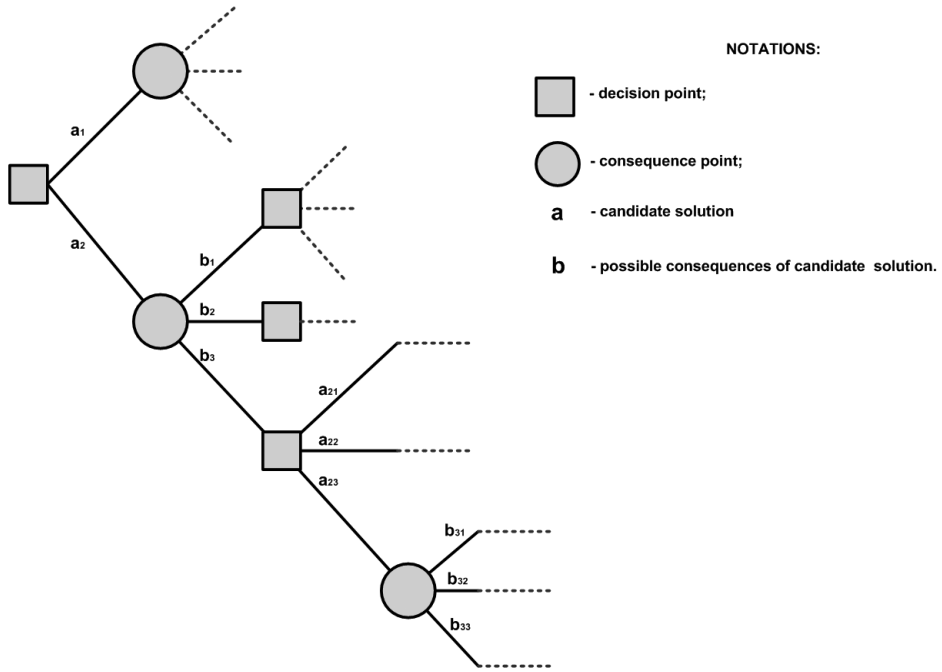


Fig. 2. General view of the decision tree

the possible consequences leads to the next decision point. That shows the convenience of this approach that allows segmenting the complex decision-making problem to the required level of detail, thereby ensuring total coverage of the subject area.

The next step involves quantifying the risk of events. A quantitative estimation of the risks of LCC implementation is required for substantiated planning of activities allowing to prevent or eliminate the negative consequences of the risk events. If their probability is high, adequate activities should be organized, which may require large amounts of resources.

Expert and statistical methods are now the most widely used, but the reliability of the application of the former depends largely on the competence of the experts, and the latter requires the availability of sufficient statistical data, which is not always possible in the case of LC contracts. Of some interest are the methods of sensitivity analysis, scenarios and stability testing that have some advantages and disadvantages.

In this context, it is proposed to quantify risks as the product of the frequency of the risk event P by the magnitude of damage S when realized and to represent them as expression

$$R = P \cdot S.$$

Given its obvious simplicity, this approach is quite justified. The fact is that WaME LC is a rather complex and lasting project, therefore it does not appear to be pos-

Table 1. Risk matrix

Frequency (points)	Degree of damage (points)				
	Insignificant **(0.05)**	Small **(0.1)**	Medium **(0.2)**	Significant **(0.4)**	High **(0.8)**
A. Frequent **(1)**	**1a** Low **0.05**	**2a** Moderate **0.1**	**3a** Moderate **0.2**	**4a** High **0.4**	**5a** Unacceptable **0.8**
B. Remote **(0.8)**	**1в** Low **0.04**	**2в** Low **0.08**	**3в** Moderate **0.16**	**4в** Moderate **0.32**	**5в** Unacceptable **0.64**
C. Probable **(0.6)**	**1c** Low **0.03**	**2c** Low **0.06**	**3c** Moderate **0.12**	**4c** Moderate **0.24**	**5c** High **0.48**
D. Improbable **(0.4)**	**1d** Negligible **0.02**	**2d** Low **0.04**	**3d** Low **0.08**	**4d** Moderate **0.16**	**5d** High **0.32**
E. Practically incredible **(0.2)**	**1e** Negligible **0.01**	**2e** Negligible **0.02**	**3e** Low **0.04**	**4e** Low **0.08**	**5e** Moderate **0.16**

sible to take into account the full range of possible risks. But at the same time, each stakeholder involved in these processes should understand the extent of the possible damage from the realization of a particular risk event throughout the project.

3. Results and discussion.

Risk estimates are normally represented quantitatively with the dimensionality of the consequence measurements taken relative to the observation period, but in some cases the obtained estimates may be represented qualitatively, e.g., as "low" or "high" (Table 1). When assigning probability estimates, especially if quantitative values cannot be obtained, they can be accompanied by more detailed comments.

For the purpose of visualizing the risk estimates and further substantiating the LCC solutions, a matrix is built that consists of five columns (corresponding to the scale of event occurrence) and five lines (corresponding to the degrees of possible damage), at the intersection of which the corresponding integral estimates are formed.

In dark grey are shown high and unacceptable risk values that indicate that the project has no further positive outlook, in light grey are shown negligible and low risk values that do not require any action on the part of the responsible officials. In turn, the estimates in grey boxes require appropriate risk reduction activities. In respect to the complete life cycle, their set is quite large and will differ depending on the specific conditions and LC stage. In the fundamental publication [8], the authors quite aptly note that the existing approaches to risk management are strictly specific in their nature, i.e., take into consideration either the financial and economic aspects of the manufacturing processes, or the research and development or engineering and manufacturing potential of the defence contractors. Following on that conclusion, it could be justifiably noted that the specificity of LCC adds a number of factors to the assessment of the risks caused by the divergence of the goals of the LC stakeholders. Therefore, given the requirements of the WaME customer, risks should be assessed subject to their impact on the execution periods, technical characteristics and financial costs of the parties (Table 2) that define the selection of one or another project execution option.

Such situations are discussed in sufficient detail in system engineering studies and normally come down to rethinking the resource allocation, synchronization of parallel activities and optimization of logistics. In general, the possible options are: project termination in case of high and unacceptable risks; risk reduction in case of moderate risks; project continuation in case of low and minor risks.

4. Conclusions

Summing up the conducted study, the following conclusions should be made:

1. The introduction of the LC contracts in the practice of WaME development and operation, first, is one of the most common forms of private-public partnerships that has been successfully proven in many sectors of the economy, and,

Table 2. Definition of the risk's impact on the project

Degree of damage	Impact on delivery dates	Impact on technical characteristics	Impact on financial costs
Insignificant	minimal or none	minimal or none	minimal or none
Small	minimal deviations in intermediate points of the graph. Shift of secondary reference points of the graph	insignificant performance degradation; effect on the program is minimal or none	increase of program budget or production cost by more than 1% of the allocated funds
Medium	shift of the intermediate points of the graph, deviations unable to affect the progress of the program in general	moderate performance degradation that has an insignificant effect on the progress of the program	increase of program budget or production cost by 1 to 5% of the allocated funds
Significant	critical non-compliance with program execution schedule. Key reference points shifting over 2 months away and/or intermediate reference points shifting over 6 months away	significant degradation of performance undermining program implementation	increase in program budget or production cost 5 to 10% of the allocated funds
High	impossibility to clear the established reference points within the established time limits	critical degradation of performance; impossibility to achieve key parameters or minimal allowed performance values; risk of program failure	more than 10% program cost overrun

second, is an objective necessity of the military organization of the nation due to the growing technical complexity of the WaME.

2. In the current economic conditions, developing an LCC system for the entire range of WaME is probably one of the few ways allowing to ensure the preparedness of the Armed Forces of the Russian Federation to fulfil their intended mission. Given the global experience, it can be stated that, today, there is no other way to achieve that.

3. The establishment of a long-term system of LCC-based interaction between the defence contractors and the departments of the MOD RF is to be preceded by a thorough analysis of all possible conditions for their implementation, which would allow identifying a significant part of possible risks and create the required conditions for their minimization.

References

1. Kurbanov A.Kh. [Outsourcing: theory, methodology, specifics of application in a military organization]. Saint Petersburg: Kopi-R Group; 2011. (in Russ.)

2. Gasyuk D.P., Dubovsky V.A., Dubovskaya N.I. [Topologization of the factors defining the development of a complete life cycle management system of an army missile system]. In: [Topical issues of protection and security. Proceedings of the XXIII All-Russian Research and Practice Conference of the RARAN]. Saint Petersburg Academy of Rocket and Artillery Sciences; 2020. P. 108-115. (in Russ.)

3. Nikolaev A.S. [Improving the practices of customs authorities within the risk management system]. In: [Anthology of research papers of young scientists of the ITMO University. Proceedings of the XLVI Science, Training and Methodology Conference]; 2017. P. 217-219.

4. Burenok V.M. Problems of the management system of the weapons entire lifecycle. *Armament and Economics* 2014;2(27):4-9. (in Russ.)

5. Dubovsky V.A., Kurbanov A.Kh., Plotnikov V.A. Methodical basis of monitoring of functioning full life cycle contract systems in the interests of the military organization of the state: organizational, technical and logistical aspects. *Military Enginery. Scientific and Technical Journal. Issue 16. Counter-terrorism technical devices* 2019;11-12(137-138): 15-22. (in Russ.)

6. Gasyuk D.P., Dubovsky V.A., Gurianov A.V. The problem of justification of appearance full life cycle management systems ground forces missile system. *Izvestia RARAN* 2020;2(112):29-33. (in Russ.)

7. Nikolaev A.E. Improvement of the mechanism for the management of development of scientific and technological potential of the defence industrial complex. *Naukivedenie* 2015;7(5). Available at: http://naukovedenie.ru/PDF/231EVN515.pdf. DOI: 10.15862/231EVN515. (in Russ.)

8. Drogovoz P.A., Raldugin O.V. Information and technological factors of developing cooperation in the military-industrial complex and risk-based approach to its formation while creating the system of aerospace defense. *Economic Strategies* 2016;7(141):76-89. (in Russ.)

9. Babenkov V.I., Gasyuk D.P., Dubovsky V.A. Method of risk assessment at the weapons and military equipment samples life cycle stages. *Armament and economics* 2020;3(53):59-65. (in Russ.)

10. Popovich L.G., Drogovoz P.A., Kalachanov V.D. [Managing innovation and investment in military industrial companies in the context of diversification: a monograph]. Moscow: Vash Format; 2018. (in Russ.)

11. Kharitonov A.V. [Life cycle contract]. *[State order: management, placement, security]* 2014;37:70-77. (in Russ.)

12. Yusupov R.M., Sokolov B.V., Patushkin A.I. et al. Research problems analysis of artificial objects lifecycle management. *SPIIRAS Proceedings* 2011;1(16):37-109. (in Russ.)

13. Kirov A.V. Key aspects of determination appearance of the system for managing the total life cycle of products. *Fundamental Research* 2016;9:31-34. (in Russ.)

14. Tereshina N.P. Podsorin V.A. [Life cycle management of railway technical systems: textbook for higher education establishments]. Moscow: VEGA-Info; 2012. (in Russ.)

15. Gasyuk D.P., Drogovoz P.A., Dubovsky V.A. [Functional simulation of life cycle processes of armaments and military equipment]. *Vestnik Akademii voennykh nauk* 2020;3(72):105-112. (in Russ.)

16. Rakuta N.V. Lifecycle contracts in public procurement. Issues of state and municipal administration. *Public Administration Issues* 2015;2:53-78. (in Russ.)

17. Elizarov P.M. [Life cycle contracts for commercial products and armaments and military and special equipment: similarities and differences]. *Tekhnologii PLM i ILP*. Available at: http://cals.ru/sites/default/files/downloads/emagazine/Emag_5_contracts_ZC_GP_and_BBT.pdf.

18. Kruglov M.G. [On the life cycle management system of armaments, military and special equipment in the US]. *Menedzhment kachestva* 2014;3:174-191. (in Russ.)

19. Grigin N.V. Organization of materiel procurements in the US Department of Defence and leading NATO countries. *Transactions of the Krylov State Research Centre* 2017;2(380):148-160. (in Russ.)

20. Yang Y., Hou Y., Wang Y. On the development of public-private partnerships in transitional economies: An explanatory framework. *Public Administration Review* 2013;73(2):301-310. DOI: 10.111/j.1540-6210.2012.02672.x.

21. Williamson O.E. Public and private bureaucracies: A transaction cost economics perspective. *Journal of Law Economics and Organization* 1999;15(1):306-342.

22. Tang L., Shen Q., Cheng E. A review of studies on public-private partnership projects in the construction industry. *International Journal of Project Management* 2010;28:683-694.

23. Saussier S., Staropoli C., Yvrande-Billon A. Public-private agreements, institutions, and competition: when economic theory meets facts. *Review of Industrial Organization* 2009;35:1-18. DOI 10.1007/s11151-009-9226-z.

About the authors

Vitaly A. Dubovsky, doctoral student, General of the Army A.V. Khrulev Military Academy of Logistical Support, Ministry of Defence of the Russian Federation, 8 Makarova Emb., 195197, Saint Petersburg, Russian Federation, e-mail: dubovskiy@inbox.ru.

Natalia I. Dubovskaya, junior researcher, General of the Army A.V. Khrulev Military Academy of Logistical Support, Ministry of Defence of the Russian Federation, Institute of Military System Research of Logistics Support of the Armed Forces of the Russian Federation, 8 Makarova Emb., 195197, Saint Petersburg, Russian Federation, e-mail: dubovskaya87@list.ru.

Andrey S. Nikolaev, Candidate of Economics, Head of the Technology Committee, Association of Technology and Innovation Support Centres, Associate Professor, Faculty of Technological Management and Innovations, ITMO University, 11/2 Tchaikovskogo St., 191187, Saint Petersburg, Russian Federation, e-mail: nikand@itmo.ru.

The authors' contribution

Dubovsky V.A. defined the basic idea of the research, developed a generalized risk management algorithm.

Dubovskaya N.I. analysed subject-matter literature, drawn up the paper's conclusions.

Nikolaev A.S. contributed to the discussion of the research methods and the obtained results.

Conflict of interests

The authors declare the absence of a conflict of interests.

GNEDENKO FORUM

INTERNATIONAL GROUP ON RELIABILITY

The Gnedenko Forum was founded in 2004 by an unofficial international group of experts in the dependability theory for the purpose of professional support of researches from all over the world who are interested in studying and developing the scientific, technical and other aspects of the dependability theory, risk analysis and safety in the theoretical and practical domains.

The Forum exists on the Internet as a non-for-profit organization. It aims to involve into joint discussion and communication technical experts interested in developing the dependability theory, safety and risk analysis regardless of their home country and membership in whichever organization.

The Forum acts as an impartial and neutral entity that delivers scientific information to the press and public as regards the matters of safety, risk analysis and dependability of complex technical systems. It publishes reviews, technical documents, technical reports and research essays for the purpose of dissemination of knowledge and information.

The Forum is named after Boris V. Gnedenko, an outstanding Soviet mathematician, expert in the probability theory and its applications, member of the Ukrainian Academy of Sciences. The Forum is the platform for distribution of information on educational grants, academic and professional positions related to dependability, safety and risk analysis all over the world.

Currently, the Forum has 500 members from 47 countries.

Since January 2006, the Forum has been publishing its quarterly journal, Reliability: Theory & Applications (www.gnedenko.net/RTA). The Journal is registered in the Library of Congress (ISSN 1932-2321) and publishes articles, reviews, memories, information and literature references regarding the theory and application of dependability, survivability, maintenance, risk analysis and management methods.

Since 2000, the Journal is indexed in Scopus.

Membership in the Gnedenko Forum does not imply any obligations. It is only required to send your photograph and a brief professional biography (resume) to a.bochkov@gmail.com.
Templates can be found at http://www.gnedenko.net/personalities.htm.

www.gnedenko.net

DEPENDABILITY JOURNAL ARTICLE SUBMISSION GUIDELINES

Article formatting requirements

Articles must be submitted to the editorial office in electronic form as a Microsoft Office Word file (*.doc or *.docx extension). The text must be in black, on a A4 sheet with the following margins: 2 cm for the left, top and bottom margins; 1.5 or 2 cm for the right margin. An article cannot be shorter than 5 pages and longer than 12 pages (can be extended upon agreement with the editorial office). The article is to include the structural elements described below.

Structure of the article

The following structural elements must be separated with an *empty line*. Examples of how they must look in the text are shown *in blue*.

1) Title of the article

The title of the article is given in the English language.

Presentation: The title must be in 12-point Times New Roman, with 1.5 line spacing, fully justified, with no indentation on the left. The font face must be bold. The title is not followed by a full stop.

An example:

Improving the dependability of electronic components

2) Author(s)' name.

This structural element for each author includes:

In English: second name and first name as "First name, Second name" (John Johnson).

Presentation: The authors' names must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be bold. The authors' names are separated with a comma. The line is not followed by a full stop.

An example:

John Johnson[1], Karen Smith[2*]

3) The author(s)' place of employment

The authors' place of employment is given in English. Before the place of employment, the superscripted number of the respective reference to the author's name is written.

Presentation: The reference to the place of employment must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal. Each place of employment is written in a new line. The lines are not followed by a full stop.

An example:

[1] Moscow State University, Russian Federation, Moscow

[2] Saint Petersburg Institute of Heat Power Engineering, Russian Federation, Saint Petersburg

4) The e-mail address of the author responsible for maintaining correspondence with the editorial office

Presentation: The address must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, all symbols must be lower-case. Before the address reference, symbol * is written. The title is not followed by a full stop.

An example:

*johnson_j@aaa.net

5) Abstract of the article

This structural element includes a structured summary of the article with the minimal size of 350 words and maximum size of 400 words. The abstract is given in the English language. The abstract must include (preferably explicitly) the following sections: Aim; Methods; Results/Findings; Conclusions. The abstract of the article should not include newly introduced terms, abbreviations (unless universally accepted), references to literature.

Presentation: The abstract must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, except "**Abstract**", "**Aim**", "**Methods**", "**Conclusions**", that (along with the full stop) must be in bold. The text of the abstract must not be paragraphed (written in a single paragraph).

An example:

Abstract. Aim.Proposing an approach … taking into consideration the current methods. **Methods.** The paper uses methods of mathematical analysis,…, probability theory. **Results.** The following findings were obtained using the proposed method … **Conclusion**. The approach proposed in the paper allows…

6) Keywords

5 to 7 words associated with the paper's subject matter must be listed. It is advisable that the keywords complimented the abstract and title of the article. The keywords are written in English.

Presentation: The text must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal, except "**Keywords:**" that (along with the colon) must be in bold. The text must not be paragraphed (written in a single paragraph). The text must be followed by a full stop.

An example:

Keywords: dependability, functional safety, technical systems, risk management, operational efficiency.

7) Text of the article

It is recommended to structure the text of the article in the following sections: Introduction, Overview of the sources, Methods, Results, Discussion, Conclusions. Figures and tables are included in the text of the article (the figures must be "In line with text", not "behind text" or "in front of text"; not "With Text Wrapping").

Presentation:

The titles of the sections must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be bold. The titles of the sections (except the Introduction and Conclusions) may be numbered in Arabic figures with a full stop after the number of a section. The number with a full stop must be separated from the title with a no-break space (Ctrl+Shift+Spacebar).

The text of the sections must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with a 1.25-cm indent. The font face must be normal. The text of the sections must be paragraphed. There must be no indent in the paragraph that follows a formula and contain notes to such formula, e.g.:

where *n* is the number of products.

An example:

1. State of the art of improving the dependability of electronic components

An analysis of Russian and foreign literature on the topic of this study has shown that …

Figures (photographs, screenshots) must be of good quality, suitable for printing. The resolution must be at least 300 dpi. If a figure is a diagram, drawing, etc. it should be inserted into the text in editable form (Microsoft Visio). All figures must be captioned. Figures are numbered in Arabic figures in the order of their appearance in the text. If a text has one figure, it is not numbered. References to figures must be written as follows: "Fig. 3. shows that …" or "It is shown that … (see. Fig. 3.)." The abbreviation "Fig." and number of the figure (if any) are always separated with a no-break space (Ctrl+Shift+Spacebar). The caption must include the counting number of the figure and its title. It must be placed a line below the figure and center justified:

Fig. 2. Description of vital process

Captions are not followed by a full stop. *With center justification there must be no indent!* All designations shown in figures must be explained in the main text or the captions. The designations in the text and the figure must be identical (including the differences between the upright and oblique fonts). *In case of difficulties with in-text figure formatting, the authors must – at the editorial office's request – provide such figures in a graphics format (files with the* *.tiff, *.png, *.gif, *.jpg, *.eps extensions).

The tables must be of good quality, suitable for printing. The tables must be editable (not scanned or in image format). All tables must be titled. Tables are numbered in Arabic figures in the order of their appearance in the text. If a text has one table, it is not numbered. References to tables must be written as follows: "Tab. 3. shows that …" or "It is shown that … (see. tab. 3.)." The abbreviation "tab." and number of the table (if any) must be always separated with a no-break space (Ctrl+Shift+Spacebar). The title of a table must include the counting number and its title. It is placed a line above the table with center justification:

Table 2. Description of vital process

The title of a table is not followed by a full stop. *With center justification there must be no indent!* All designations featured in tables must be explained in the main text. The designations in the text and tables must be identical (including the differences between the upright and oblique fonts).

Mathematical notations in the text must be written in capital and lower-case letters of the Latin and Greek alphabets. Latin symbols must always be oblique, except function designators, such as sin, cos, max, min, etc., that must be written in an upright font. Greek symbols must always be written in an upright font. The font size of the main text and mathematical notations (including formulas) must be identical; in Microsoft Word upper and lower indices are scaled automatically.

Formulas may de added directly into the text, for instance:

Let $y = a \cdot x + b$, then…,

or written in a separate line with center justification, e.g.:

$$y = a \cdot x + b.$$

In formulas both in the text, and in separate lines, the punctuation must be according to the normal rules, i.e. if a formula concludes a sentence, it is followed by a full stop; if the sentence continues after a formula, it is followed by a comma (or no punctuation mark). In order to separate formulas from the text, it is recommended to set the spacing for the formula line 6 points before and 6 points after). If a formula is referenced in the text of an article, such formula must be written in a separate line with the number of the formula written by the right edge in round brackets, for instance:

$$y = a \cdot x + b. \quad (1)$$

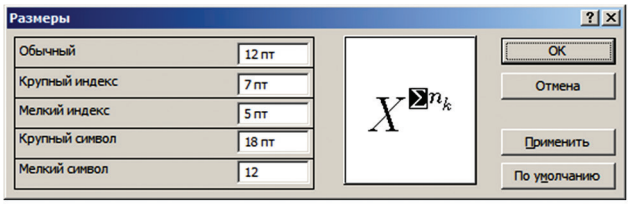
If a formula is written in a separate line and has a number, such line must be right justified, and the formula and its number must be tab-separated; tab position (in cm) is to be chosen in such a way as to place the formula roughly at the center. Formulas that are referenced in the text must be numbered in Arabic figures in the order of their appearance in the text.

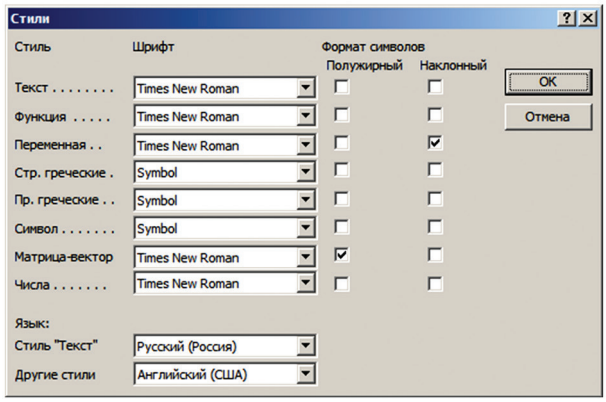
Simple formulas should be written without using formula editors (in MS Word, Latin should be used, as well as the "Insert" menu + "Special Characters", if Greek letters and mathematical operators are required), while observing the required slope for Latin symbols, for example:

$$\Omega = a + b \cdot \theta.$$

If a formula is written without using a formula editor, letters and +, –, = signs must be separated with no-break spaces (Ctrl+Shift+Spacebar).

Complex formulas must be written using a formula editor. In order to avoid problems when editing and formatting formulas it is highly recommended to use Microsoft Equation 3.0 or MathType 6.x. In order to ensure correct formula input (symbol size, slope, etc.), below are given the recommended editor settings.





When writing formulas in an editor, if brackets are required, those from the formula editor should be used and not typed on the keyboard (to ensure correct bracket height depending on the formula contents), for example (Equation 3.0):

$$Z = \frac{a \cdot \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_i \right)}{n+m}. \quad (2)$$

Footnotes in the text are numbered with Arabic figures, placed page by page. Footnotes may include: references to anonymous sources on the Internet, textbooks, study guides, standards, information from websites, statistic reports, publications in newspapers, magazines, autoabstracts, dissertations (if the articles published as the result of thesis research cannot be quoted), the author's comments.

References to bibliographic sources are written in the text in square brackets, and the sources are listed in the order of citation (end references). The page number is given within the brackets, separated with a comma and a space, after the source number: [6, p. 8].

8) Acknowledgements

This section contains the mentions of all sources of funds for the study, as well as acknowledgements to people who took part in the article preparation, but are not among the authors. Participation in the article preparation implies: recommendations regarding improvements to the study, provision of premises for research, institutional supervision, financial support, individual analytical operations, provision of reagents/patients/animals/other materials for the study.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

9) References

The References must include only peer-reviewed sources (articles from academic journals and monographs) mentioned in the text of the article. It is not advised to references autoabstracts, dissertations, textbooks, study guides, standards, information from websites, statistic reports, publications in newspapers, websites and social media. If such information must be referred to, the source should be quoted in a footnote.

The description of a source should include its DOI, if it can be found (for foreign sources, that is possible in 95% of cases).

References to articles that have been accepted, but not yet published must be marked "in press"; the authors must obtain a written permission in order to reference such documents and confirmation that they have been accepted for publication. Information from unpublished sources must be marked "unpublished data/documents"; the authors also must obtain a written permission to use such materials.

References to journal articles must contain the year of publication, volume and issue, page numbers.

The description of each source must mention all of its authors.

The references, imprint must be verified according to the journals' or publishers' official websites.

Presentation:

References must be written in accordance with the Vancouver system.

The references must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with a 1.25-cm indent on the left. The font face must be normal. Each entry must be numbered in Arabic figures with a full stop after the number. The number with a full stop must be separated from the entry with a no-break space (Ctrl+Shift+Spacebar).

10) About the authors

Full second name, first name (in English); complete mailing address (including the postal code, city and country); complete name of the place of employment, position; academic degree, academic title, honorary degrees; membership in public associations, organizations, unions, etc.; official name of the organization in English; e-mail address; list and numbers of journals with the author's previous publications; the authors' photographs for publication in the journal.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

11) The authors' contribution

Detailed information as to each author's contribution to the article. For example: Author A analyzed literature on the topic of the paper, author B has developed a model of real-life facility operation, performed example calculation, etc. Even if the article has only one author, his/her contribution must be specified.

Presentation:

The information must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

12) Conflict of interests

A conflict of interests is a situation when people have conflicting and competing interests that may affect editorial decisions. Conflicts of interests may be potential or conscious, as well as actually existing. The objectivity may be affected by personal, political, financial, scientific or religious factors.

The author must notify the editorial office on an existing or a potential conflict of interests by including the corresponding information into the article.

If there is no conflict of interests, the author must also make it known. An example of wording: "The author declares the absence of a conflict of interests".

Presentation:

The text must be in 12-point Times New Roman, with a 1.5-line spacing, fully justified, with no indentation on the left. The font face must be normal.

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