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

ISSN 1729-2646
e-ISSN 2500-3909

THE JOURNAL PROMOTER:
"Journal "Reliability" Ltd

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

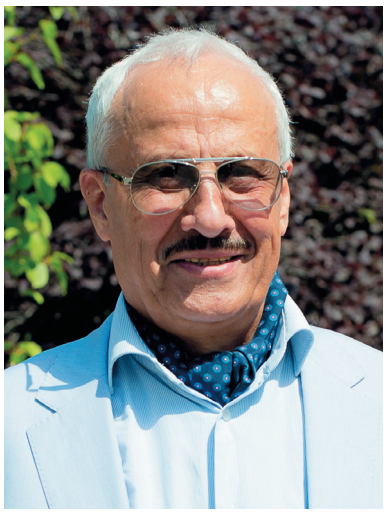
Official organ of the Russian Academy of Reliability

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

Papers are reviewed.
Papers are published in author's edition. The opinion of members of the editorial board may not coincide with the point of view of authors' publications. The reprint of materials is granted only with the written permission of the editorial board. Manuscripts are not returned.

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

CONTENTS



Dear colleagues,

For decades, technical system dependability has been a focus of attention of the expert community. The relevance of the subject grows with the miniaturization of components and the growth of their number in systems. Along with the structural dependability that deals with only the failure and recovery processes in technical facilities, functional dependability is of increasing importance in the context of general dependability. The method of functional dependability is built around the estimation of the accuracy of process performance. This method takes into consideration the algorithms of the tasks performed in the system. It is designed for the purpose of evaluating the effects of operator errors, program errors, faults, data errors on the results of the tasks performed in the system.

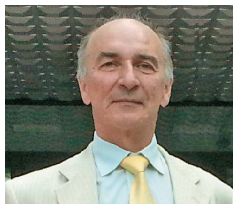
The dependability of technical systems is directly linked to their functional safety. The hazardous failure flow in a system's operation may be regarded as a multiply randomly rarefied failure flow of the components. Hazardous failures may cause critical or even catastrophic consequences to the system's operation. Therefore the problems of process-specific, technological and technology-related risks are closely related to the problems of functional safety and dependability of technical systems. Severe negative consequences in the operation of technical systems may be caused by computer attacks. The combination of functional safety and information security is within the domain of general safety that is covered by the Dependability journal.

Dependability is making steady progress. The Editorial Council now includes prominent researchers from Russia, Ukraine, Belarus, India, Israeland Serbia. The journal's global visibility is improving. Some of our authors reference their articles published in the journal, provide long lists of references to foreign publications in their papers. This practice increases the journal's citation indices and should help its inclusion into such international databases as Scopus.

I wish all of our authors great creative achievements, health and satisfaction with the results of their work.

Fault tree analysis in the R programming environment

Alexander V. Antonov, *JSC RASU, Moscow, Russia*
Evgeny Yu. Galivets, *JSC RASU, Moscow, Russia*
Valery A. Chepurko, *JSC RASU, Moscow, Russia*
Alexey N. Cherniaev, *JSC RASU, Moscow, Russia*


Alexander V. Antonov


Evgeny Yu. Galivets


Valery A. Chepurko


Alexey N. Cherniaev

Abstract. Aim. *Fault tree analysis (FTA) is one of the primary methods of dependability analysis of complex technical systems. This process often employs commercial software tools like Saphire, Risk Spectrum, Arbitr, etc. Each of them has both advantages and drawbacks. It must be noted that the primary purpose of the above software tools consists in performing qualitative fault tree analysis. The software systems additionally feature a number of statistical methods that, among other things, enable uncertainty analysis, interval estimation of indicators, as well as other statistical research. The number of such procedures is not large and is strictly limited by a certain array of proposed distributions and functions. In this paper, let us consider the possibility of solving the task of fault tree analysis by means of the R programming language. R was primarily created and is continuing to evolve as a statistical data processing tool. FTA in this environment is just one of 10 thousand packages. In other words, if compared to commercial packages with the FTA as the main function, the functionality of R is much wider and enables significantly higher quality of analysis. One of R's undeniable advantages is the freeware open-source environment. This paper aims to present a small number of primary procedures of R's FaultTree package that enable FTA: construction and display of fault trees, calculation of probability per nodes, determination of minimum cross-sections.* **Methods.** *R's FaultTree scripts were used for the calculations and FTA capabilities demonstration.* **Conclusions.** *Three examples are examined in detail. First, a tree is calculated based on known probabilities, then the time to failure distribution function of a technical system is identified. In the last example, FTA is performed for systems with elements that are described by different functional and service models. In conclusion, FTA capabilities of R are described that allow, for instance, taking into consideration common cause failures.*

Keywords: *fault tree, fault tree analysis, non-availability factor, evident failures, hidden failures, mean time between failure.*

For citation: *Antonov AV, Galivets EYu, Chepurko VA, Cherniaev AN. Fault tree analysis in the R programming environment. Dependability 2018;18(1): 4-13. DOI: 10.21683/1729-2646-2018-18-1-4-13*

Introduction

R is a programming language for statistical computing and graphics, as well as a free open-source computing software environment developed as part of the GNU project. Primarily, R was created by Ross Ihaka and Robert Gentleman (R is the first letter of their names), statistics researchers from the University of Auckland. The programming language and environment are supported and developed by the *R Foundation Company*. R entered into the winners list of the InfoWorld magazine contest in the nomination for the best open software for applications development in 2010.

R supports a wide range of statistical and numerical methods and is highly extensible through the use of packages. Packages are libraries that provide specific functions and subprograms or specific applications. A package is a set of functions, files with reference information and examples collected together in one archive used as an additional extension based on R. R is a programming language, thus own programs, or scripts, can be designed and specialized extensions, or packages, can be used.

A number of graphical interfaces such as RStudio, JGR, etc. were developed to simplify the process of working with R. R can perform simple calculations, edit tables with data and make simple statistical analysis (e.g. t-test, ANOVA or regression analysis) and more complex time-consuming computations, test hypotheses, construct vector graphics. Yet this is not the full list of R functions.

This article deals with the package for "constructing, calculating and displaying" fault trees, the FaultTree package. The author of this package is David J. Silkworth and the maintainer is Jacob T. Ormerod. FaultTree provides a set of functions for building tree structures as Dataframe objects. The fault tree includes logic nodes (primarily "AND" and "OR") that process input data and may direct output data "upwards" through the tree structure.

The method of fault tree analysis (FTA) was first used by Bell Labs for the US Air Force in 1962. Today, FTA is widely used to analyze failures of static systems.

FTA is a method for failures analysis in complex systems, in which undesired states of system failures are analyzed using Boolean algebra methods to combine a series of lower-level events (failures of the lowest level), which lead to the failure of the whole system. Fault tree analysis is widely used in various industries to calculate technical system dependability, identify the most unreliable elements subject to frequent failures. In this case chains of random events are defined, under which the system may fail, methods for reducing risks are identified and the frequencies of system failures are determined. Fault tree analysis is effectively used in the aerospace, nuclear power, chemical and processing industries, pharmaceutical, oil and gas and other high-hazard sectors.

The FaultTree is one of a huge number of packages of the R language, among which most are related to the qualitative statistical processing with easy application of different probability distributions. This abundance and at the same time flexibility of the language combined with the simplicity of scripting, make it quite an interesting solution for not only FTA, but for additional research that cannot be performed in known software products. The second example shows a method of FTA with the capability of dynamic analysis of object behavior when probability of events is functions of time. This probability allows obtaining not just a static (at a certain time) estimate of a system's failure probability but some time dependence of failure probability which allows, for example, reasonably determining a system's residual life not limited to exponential distribution. Not only standard laws, but also nonparametric distribution estimates can be used as initial distribution of system elements, which sets the R language apart.

Let us consider some basic features of the FaultTree package.

Calculation of the fault tree with known event probabilities

As an example, let us calculate with R the failure probability of a chain of 8 elements, each of which refers to non-recoverable objects and has specific failure probability (Fig. 1, Table 1).

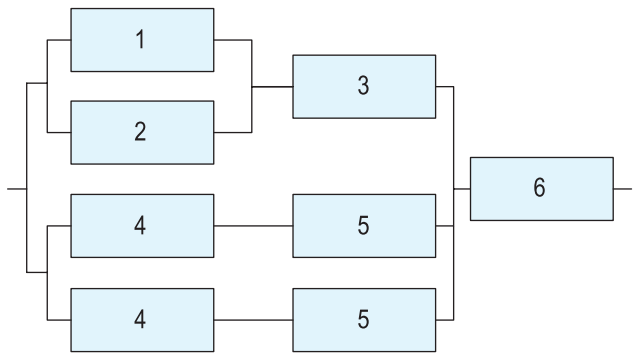


Figure 1. Chain diagram

Table 1. Failure probabilities of chain elements

Element	1	2	3	4	5	6
q_i	0,01	0,02	0,03	0,04	0,05	0,06

Note that the continuous set 4-5 is single redundant, i.e. in the lower part of the diagram there are two 4-5 sections connected in parallel.

In order to calculate the diagram it is required to connect the FaultTree package. This can be done in at least two ways: by directly connecting the package in the RStudio environment or by typing the following command in the generated script:

library(FaultTree).

Then, the tree is to be built by calling the free.make script which has several arguments, and the most important of which is the type of the generated tree rather than the type of the upper gate in the fault tree. In the current version of the FaultTree library, there are two basic types of the gate:

“or” and “and”. Let us focus on Figure 1. The chain is a serial connection of the element 6 and the complex subchain 1-5 consisting of elements 1, 2, …, 5. Therefore, the chain failure will occur if the element 6 of the subchain 1-5 fails (or both occur immediately). Thus, it necessary to choose the type of the upper gate “or”:

1. Tree1 <- ftree.make(type=”or”, name=”Example 1. Calculation”, name2=”on probabilities”).

In this script a data structure (dataframe) is created, i.e. a fault tree with the name (identifier) Tree1, which is essentially an “or” type gate. When the event tree is displayed graphically, this gate will be called “Example 1. Calculation in probabilities” (Fig. 2). Due to the fact that there is a limitation on the number of symbols in the title, long names sometimes have to be divided into two lines “name” and “name2”. The upper gate will be assigned the number 1 (red value inside the gate). Let us note, that the line numbering of the script is given only for the convenience of making comments in the article and is not used in the syntax of the R language.

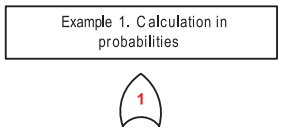


Figure 2. First step of the fault tree constructing. Upper gate of chain

The next step is to add two structures to gate 1: the event of “failure of element 6” and the “and” gate, which will be the upper gate in relation to the structure 1-5. The choice of this gate type is due to the fact that the structure 1-5 fails if both channels “1-3” and “4,5” simultaneously fail. Thus, the script will have the following commands:

2. Tree1 <- addProbability(Tree1, at=1, prob=.06, name=» Failure 6»),
3. Tree1 <- addLogic(Tree1, at=1, type= “and”, name= ”Failure 1-3”,name2=”and (4-5)*2”).

In the first line the event “failure 6” is added to gate 1. Let us analyze in detail the arguments of the addProbability sub-program. The first argument is tree identifier to which the event will be built. The second argument “at” indicates the number of the parent node of the tree Tree1 to which this structure will be added. The third argument sets the numerical value of the failure probability. The fourth value, as before, is the name of the event. Let us note that the arguments of any sub-programs in the R language are permutable and do not have to obey a certain order. However, from the point of view of program debugging and simplifying of errors search it is reasonable to adhere to a certain order of arguments. In the second line above, an “and” gate is added to gate 1 of Tree1, which will be a conjunction of the “1-3” failure channel and both “4, 5” channels.

Verifying the fault tree requires making a draft of the future fault tree and then occasionally check the correspondence of the tree with the draft. For graphic output of the tree the FaultTree package suggests using the ftree2html script, which obviously creates an image in the html format:

4. ftree2html(Tree1, write_file=TRUE),
5. browseURL(“Tree1.html”).

The first argument of the ftree2html sub-program is the identifier of the output fault tree; the second argument indicates that the file will be overwritten after each following run. The browseURL sub-program allows seeing the constructed tree using a browser, which by default is called up by the R environment. Figure 3 shows the constructed fault tree with two added structures.

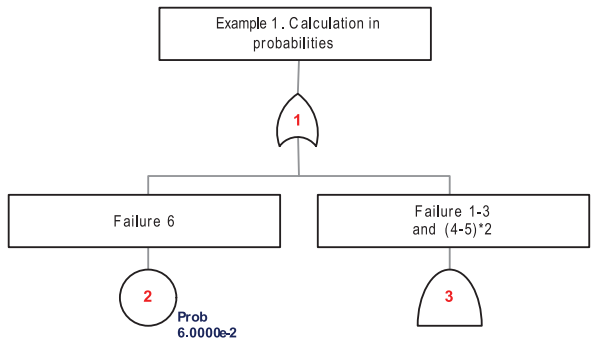


Figure 3. The second step of fault tree building

Note that the numbers 2 and 3 were automatically assigned to the simple event “failure of element 6” and the “and” gate respectively. During the permutation of script lines it is important to control the assigned numbers and remember that the permutation of lines can lead to a change of event numbers and possible occurrence of failure in the program code.

Next to the “failure of the element 6” event the numerical probability value of this event is shown. However, the other two gates are shown without the event probability.

Figure 4 shows the final version of the event tree with the calculated probabilities of each tree node.

The full version of the script for building such tree is shown below.

Example 1.

1. library(FaultTree)
2. Tree1 <- ftree.make(type=”or”, name=”Example 1. Calculation”, name2=”on probabilities”)
3. Tree1 <- addProbability(Tree1, at=1, prob=.06, name=”Failure 6”)
4. Tree1 <- addLogic(Tree1, at=1, type= “and”, name=” Failure 1-3”,name2=”and (4-5)*2”)
5. Tree1 <- addLogic(Tree1, at=3, type= “or”, name=” Failure 1 и 2”,name2=”or 3”)
6. Tree1 <- addProbability(Tree1, at=4, prob=.03, name=” Failure 3”)

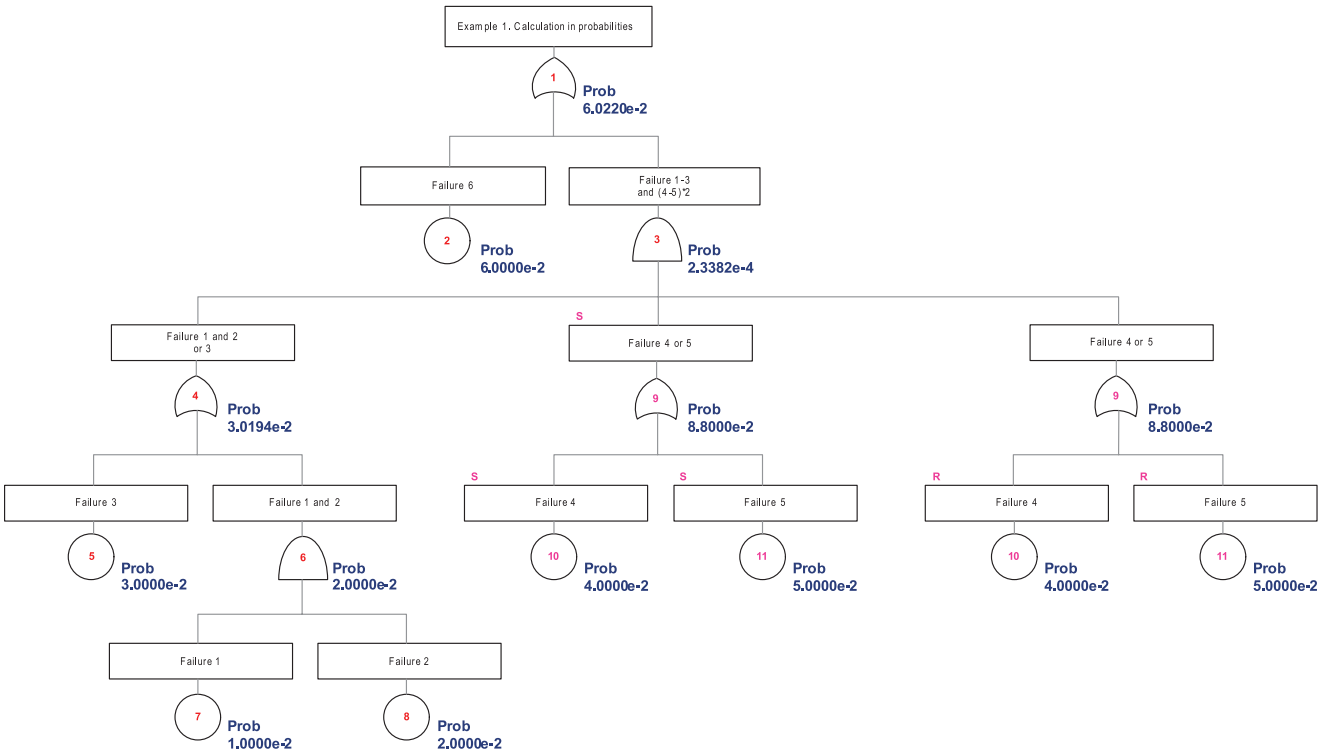


Figure 4. Final version of the fault tree with calculation in probabilities per nodes

7. Tree1 <- addLogic(Tree1, at=4, type= "and", name=" Failure 1 and 2")

8. Tree1 <- addProbability(Tree1, at=6, prob=.01, name=" Failure 1")

9. Tree1 <- addProbability(Tree1, at=6, prob=.02, name=" Failure 2")

10. Tree1 <- addLogic(Tree1, at=3, type= "or", name=" Failure 4 or 5")

11. Tree1 <- addProbability(Tree1, at=9, prob=.04, name=" Failure 4")

12. Tree1 <- addProbability(Tree1, at=9, prob=.05, name=" Failure 5")

13. Tree1 <- addDuplicate(Tree1, at=3, dup_id=9)

14. Tree1 <- ftree.calc(Tree1)

15. ftree2html(Tree1, write_file=TRUE)

16. browseURL("Tree1.html")

Let us pay attention to the 13th line. The FaultTree library has a very convenient function, which allows duplicating both the repeated event and whole data structure, i.e. event branches. As in our chain channel 4-5 was duplicated, the addDuplicate(Tree1, at=3, dup_id=9) structure duplication function was to be used. The first argument of this function, as before, is the identifier of the tree being built, at=3 is the number of the tree node to which the repeated data structure will be added, dup_id=9 is the upper node of the added data structure. Figure 4 shows letters S and R which mean branch-source (Source) and repeated branch (Repeat), accordingly. After the fault tree has been built, the sub-program ftree.calc(Tree1) is called up, which calculates the failure probability of each tree node according to the well-known probability calculation methods through transformation of logical dependencies.

Then let us consider the feasibility of identifying the failure probability of non-recoverable chain over time.

Calculation of the distribution function of the chain's time to failure

An analysis of the previous script allows assuming that it is not necessary to specify the probabilities as fixed numbers, i.e. they can be made time dependent. To do that, it is necessary to recalculate the probability of each elementary event inside the time loop and calculate the fault tree inside the loop estimating the probability of chain failure.

In order to identify the failure probability dynamics (essentially, the distribution function of time to failure of the chain element), three different approaches may be used, i.e. parametric, non-parametric and combined.

In the first case time between failures of each chain element is defined by a parametrical law of distribution with a specific set of parameters. Let us note that different random values distribution laws are widely used in R language that is designed for "statistical data processing" [1-3].

The second approach consists in non-parametric estimation of the distribution function of time to failure of each chain element. If a researcher has statistical information, which contains full time to failure (the experiment resulted in the failure of each test sample), it suffices to estimate the empirical distribution function. For this purpose the R language has the ecdf() function. In case of censored information it is possible to use the Kaplan-Meier estimate, the

script of which is also contained in the packages of the R language associated with survival analysis. It is possible to use kernel estimate of distribution function.

The third approach involves combined application of both the first (parametric) and the second (non-parametric) approaches, when the initial information is non-homogeneous, i.e. there are both statistical information and parametric estimate of the distribution law. In the dependability theory, the exponential law of distribution of time to failure has been widely used, and the failure rate is estimated based on the results of statistical tests. Methods of estimation are best developed for this distribution.

This article is not to question which is better, parameterization of distribution or non-parametric approach. We think that it is sufficient to use all information to the maximum extent without making unfounded conclusions regarding the distribution law.

Let us consider an example of finding the distribution function of time to failure for a structure. Let us first set forth the script and then analyze it.

Example 2.

```
1. library(FaultTree)
2. T=50
3. h=1
4. c1=”green4”
5. c2=”red2”
6. c3=”blue2”
7. t=seq(h,T,h)
8. n=length(t)
9. p1=pexp(t,0.01)
10. p2=pexp(t,0.02)
11. p3=pexp(t,0.03)
12. p4=pexp(t,0.04)
13. p5=pexp(t,0.05)
14. p6=pgamma(t,3,0.06)
15. p0=array(dim=n)
16. p7=array(dim=n)
17. TreePBF<-function(p1,p2,p3,p4,p5,p6){
18. Tree2 <- ftree.make(type=”or”, name=”Example 2. Calculation”, name2=”on probabilities”)
19. Tree2 <- addProbability(Tree2, at=1, prob=p6, name=”Failure 6”)
20. Tree2 <- addLogic(Tree2, at=1, type= “and”, name=” Failure 1-3”,name2=”and (4-5)*2”)
21. Tree2 <- addLogic(Tree2, at=3, type= “or”, name=” Failure 1 and 2”,name2=”or 3”)
22. Tree2 <- addProbability(Tree2, at=4, prob=p3, name=” Failure 3”)
23. Tree2 <- addLogic(Tree2, at=4, type= “and”, name=” Failure 1 и 2”)
24. Tree2 <- addProbability(Tree2, at=6, prob=p1, name=” Failure 1”)
25. Tree2 <- addProbability(Tree2, at=6, prob=p2, name=” Failure 2”)
26. Tree2 <- addLogic(Tree2, at=3, type= “or”, name=” Failure 4 or 5”)
27. Tree2 <- addProbability(Tree2, at=9, prob=p4, name=” Failure 4”)
28. Tree2 <- addProbability(Tree2, at=9, prob=p5, name=” Failure 5”)
29. Tree2 <- addDuplicate(Tree2, at=3, dup_id=9)
30. Tree2 <- ftree.calc(Tree2)
31. return(Tree2$PBF)
32. }
33. for (i in 1:n){
34. q=TreePBF(p1[i],p2[i],p3[i],p4[i],p5[i],p6[i])
35. p0[i]=q[1]
```

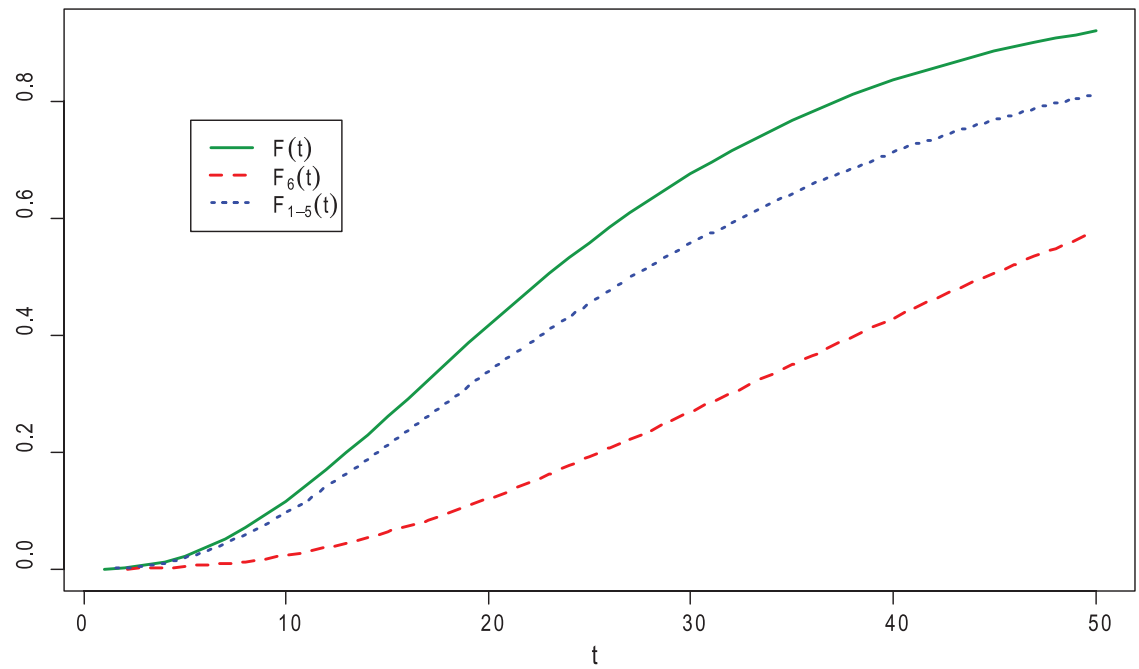


Figure 5. Distribution function of chain and its components

```
36. p7[i]=q[3]
37. }
38. plot(t,p0,type="l",lwd=2,col=c1,ylab="")
39. lines(t,p6,type="l",lwd=2,lty=2,col=c2)
40. lines(t,p7,type="l",lwd=2,lty=3,col=c3)
41. legend(locator(1), c(expression (F(t)), expression
(F[6](t)), expression (F[1-5](t))),
42. col = c(c1, c2, c3),
43. lty = c(1, 2, 3),
44. lwd = c(2, 2, 2))
```

The first line, as before, connects the FaultTree library. The maximum time T and the grid step h with which the distribution functions will be determined, are assigned on the time axis in the second and third lines. The colors of the displayed graphics are indicated in the 4-6 lines (Fig. 5). Note that there are several ways to specify a color in the R language and the color palette has a lot of colors. The quality of the applied vector graphics is undeniable, and it is possible to save pictures in different formats.

The numerical "temporal" array is created in the 7th line:

$$\vec{t} = (h, 2h, \ldots, T) = (1, 2, \ldots, 50).$$

The length of this array n=50 is determined in the 8th line.

The arrays of distribution functions of time to failure of each chain element (Fig. 1) are built in the 9th – 14th lines. So, time to failure of the first element has an exponential distribution with the rate λ=0.01. λ=rate=1/scale. The rate for the second element is 0.02, 0.03 for the third one, etc. The distribution function of time to failure of the 6th element corresponds to a gamma-distribution with the shape parameter 3 and rate λ=0.06.

Auxiliary arrays with the dimension n=50 are created in the 15th and 16th lines. The values of the distribution function of time to failure for the whole chain will be stored in array p0, and time to failure of the chain section 1-5 will be stored, for example, in array p7.

Lines 17 to 32 contain a function which computes the array of node probabilities of the fault tree. Six failure probabilities are the input parameters. Let us pay attention to the 31st line. The data structure of Tree2 contains many different factors, which becomes evident if we type the command Tree2 in the command prompt. So, the PBF factor contains the calculated failure probabilities of each tree node (Fig. 4). Thus, Tree2$PBF is an array of probabilities. Lines from 33 to 37 contain a simple loop, in which the fault tree will be calculated on a time grid with the step h=1. In this case, inside the loop, the failure probability of each element of the structure on the same time grid will be calculated. All calculated probabilities will be contained in the array q. Node 1 corresponds to the failure of the whole chain, node 3 corresponds to the failure the chain part 1-5, therefore q[1] and q[3] are the failure probabilities of the whole chain and its section 1-5 respectively. The graphical output of the results is in the 38th-44th lines (Fig. 5).

The advantage of the R language is the capability to build both parametric and non-parametric confidence intervals for the failure probability of the structure. In the parametric case it is necessary, as parameters of the law, to use such values of the confidence interval which provide the maximum and the minimal value of the failure probability. In the non-parametric case it is necessary to substitute the lower and upper bounds of the distribution function in accordance with the Clopper-Pearson method or their approximants, particularly, with the help of quintiles of the standard normal law. To determine the interval estimation of the failure probability of the structure, an insignificant script modification is required.

The next part of the article deals with the most important, in our opinion, situation related to the feasibility of calculation for the repairable as well as periodically maintainable equipment.

Calculation of the unavailability factor of the structure with repairable elements

Let us consider the following diagram (Fig. 6).

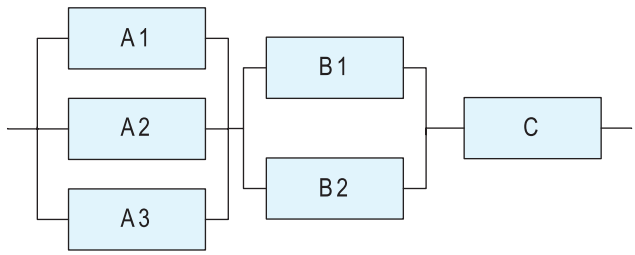


Figure 6. System diagram

Let us assume that the chain elements A1, A2, A3 are identical and operated under the same conditions; the same assumptions concern the elements B1, B2. All elements of the chain are repairable. The recovery time is T_r=8 h and does not depend on the number of repairable elements. In addition, let us suppose that the system has built-in diagnostic capability and the elements of the chain are under control. As a result, diagnostics can detect 90% of failures. Maintenance activities (preventive measures) are periodically carried out in a system with a period of τ=100 h, during which 10% of remaining "hidden" failures are detected. Let us assume that the mean time of the elements A is T_f(A)=1000 h, the mean time of elements B is T_f(B)=1500 h, the element C is T_f(C)=4000 h. Common cause failures (CCFs) are not taken into account.

To calculate an unavailability factor due to evident failures the addActive(DF, at, mttf, name) script is provided in the FaultTree library, where DF means the name of the fault tree, at is the tree node to which the event is attached, mttf is the mean time to failure, mttr is the mean time to recover, name is the name of the event in the failure tree.

In this case the non-asymptotic unavailability factor is used when calculating the failure probability [4-7]:

$$q = \frac{T_r}{T_r + T_f}, \quad (1)$$

where T_r=mttr is the mean time to recover, T_f=mttf is the mean time to failure.

To calculate an unavailability factor due to hidden failures the addLatent(DF, at, mttf, mttr, inspect, pzero, name) function is provided in the FaultTree library, in the arguments of which DF means the name of the fault tree, at is the tree node to which the event is attached, mttf is the mean time to failure, mttr is the mean time to recover, inspect is the control period, pzero is the optional argument equal to the probability that an element is restored at random times. As a default pzero=q means the asymptotic nonavailability factor (1). The name argument, as before, is the name of the event in the fault tree. In this case for calculating the failure probability the following approximate formula is used:

$$q = 1 - (1 - pzero) \cdot \left(1 - K_{nonav}\right), \quad (2)$$

where, as a default, pzero= $\frac{T_r}{T_r + T_f}$ T_r = mttr is the mean recovery time, T_f=mttf is the mean time to failure, $K_{nonav} = 1 - \frac{1 - e^{-\lambda\tau}}{\lambda\tau} = 1 + \frac{e^{-\lambda\tau} - 1}{\lambda\tau}$ is the asymptotic nonavailability factor for a periodically controlled element with instant recovery [6].

The program script will be as follows:

Example 3.

```
1. library(FaultTree)
2. Tree3 <- ftree.make(type=»or», name=»Example 3»)
3. Tree3 <- addLogic(Tree3, at=1, type= “or”, name= ”Failure C”)
4. Tree3 <- addLatent(Tree3, at=2, mttf=4000/0.1, mttr=8, inspect=100, name=”hidden”)
5. Tree3 <- addActive(Tree3, at=2, mttf=4000/0.9, mttr=8, name=”evident”)
6. Tree3 <- addLogic(Tree3, at=1, type= “and”, name= ”Failure B1,B2”)
7. Tree3 <- addLogic(Tree3, at=5, type= “or”, name= ”Failure B”)
8. Tree3 <- addLatent(Tree3, at=6, mttf=1500/0.1, mttr=8, inspect=100, name=”hidden”)
9. Tree3 <- addActive(Tree3, at=6, mttf=1500/0.9, mttr=8, name=”evident”)
10. #Tree3 <- addDuplicate(Tree3, at=5, dup_id=6)
11. Tree3 <- addLogic(Tree3, at=5, type= “or”, name= ”Failure B”)
12. Tree3 <- addLatent(Tree3, at=9, mttf=1500/0.1, mttr=8, inspect=100, name=”hidden”)
13. Tree3 <- addActive(Tree3, at=9, mttf=1500/0.9, mttr=8, name=”evident”)
14. Tree3 <- addLogic(Tree3, at=1, type= “and”, name= ”Failure A1,A2,A3”)
15. Tree3 <- addLogic(Tree3, at=12, type= “or”, name= ”Failure A”)
16. Tree3 <- addLatent(Tree3, at=13, mttf=1000/0.1, mttr=8,inspect=100, name=”hidden”)
17. Tree3 <- addActive(Tree3, at=13, mttf=1000/0.9, mttr=8, name=”evident”)
18. #Tree3 <- addDuplicate(Tree3, at=12, dup_id=13)
19. Tree3 <- addLogic(Tree3, at=12, type= “or”, name= ”Failure A”)
20. Tree3 <- addLatent(Tree3, at=16, mttf=1000/0.1, mttr=8,inspect=100, name=”hidden”)
21. Tree3 <- addActive(Tree3, at=16, mttf= 1000/0.9,mttr=8, name=”evident”)
22. #Tree3 <- addDuplicate(Tree3, at=12, dup_id=13)
23. Tree3 <- addLogic(Tree3, at=12, type= “or”, name= ”Failure A”)
24. Tree3 <- addLatent(Tree3, at=19, mttf=1000/0.1, mttr=8,inspect=100, name=”hidden”)
25. Tree3 <- addActive(Tree3, at=19, mttf=1000/0.9, mttr=8, name=”evident”)
26. Tree3 <- ftree.calc(Tree3)
27. Tree3_cs<-cutsets(Tree3)
28. ftree2html(Tree3, write_file=TRUE)
29. browseURL(“Tree3.html”)
```

Let us note that evident and hidden failures of the same element are connected by logical element “or”, while they should be connected with mutually exclusive element “or” – “xor”. Such logical element is not yet available in the current package version. However, the application of the simple “or” will lead to a minor failure in this situation.

Also note, that in the 4th line the addLatent function has the mttf=4000/0.1 argument, but in the 5th line the addActive function has mttf=4000/0.9 argument. This is due to the assumption that 90% of failures are evident failures and 10% are hidden failures, i.e.

$$\lambda = \lambda_{evid} + \lambda_{hidd}, \ \lambda_{evid} = 0,9\lambda, \ \lambda_{hidd} = 0,1\lambda.$$

In this case the mean time to failures of evident and hidden failures will be equal, accordingly:

$$T_{f,evid} = \frac{1}{\lambda_{evid}} = \frac{1}{0,9\lambda} = \frac{T_f}{0,9} \text{ and}$$

$$T_{f,hidd} = \frac{1}{\lambda_{hidd}} = \frac{1}{0,1\lambda} = \frac{T_f}{0,1}. \quad (3)$$

Lines 10, 18 and 22 are commented out. The 10th line duplicates lines from 11th to 13th, the 18th line duplicates lines from 19th to 21st, etc. In terms of script shortness, the variant with lines commented out is preferable. In line 27, the possibility of constructing minimal cut sets is first shown. The application of addDuplicate adds to the fault tree nodes with existing values, and in this case in the current package version cutsets sometimes yields incorrect cuts. Therefore, if it is intended to analyze the minimal cuts, it is better to duplicate events through repeated commands.

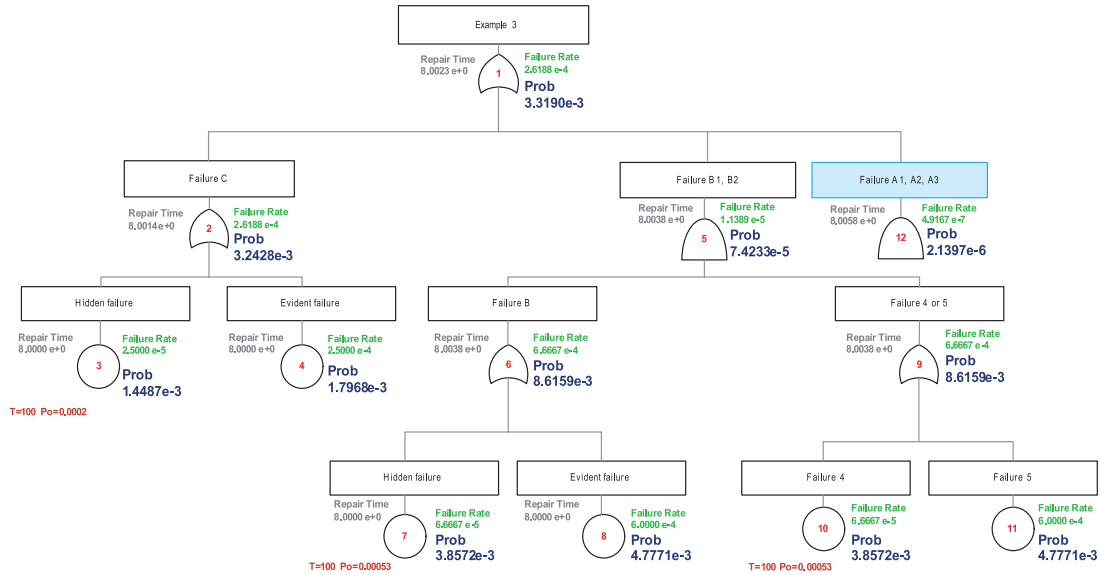


Figure 7. The fault tree for the example 3

Figure 7 shows the fault tree with "minimized" failures of the A1, A2, A3 elements due to large size of the fault tree. The created tree is interactive and allows minimizing branches, and in this case the complex event is highlighted in blue.

Note that now next to nodes, additional information has appeared along with the deduced failure probability.

Failure Rate is the rate which for such nodes as addLatent and addActive is calculated using the formula $\lambda_f = \frac{1}{T_f}$. For the logical node "or", corresponding to the series chain, the failure rate is the sum of failure rates of the descending node, i.e. $\lambda_{f-S} = \lambda_{f,1} + \lambda_{f,2} + \ldots$. For the logical element "or" the known approximate formula for the mean time between failures is used [11]:

$$T_{f-S} = \frac{K_{av}(p)}{\sum_{i=1}^{n} \lambda_{f-i} p_i \frac{\partial K_{av}(p)}{\partial p_i}}, \quad (4)$$

from which follows $\lambda_{f-S} = \frac{1}{T_{f-S}} = \frac{\sum_{i=1}^{n} \lambda_{f-i} p_i \frac{\partial K_{av}(p)}{\partial p_i}}{K_{av}(p)}$,

where $K_{av}(p)$ is the quorum-function or availability factor of the structure, λ_{f-i}, p_i is the failure rate and the probability of no failure (PNF) of the i[th] component of the complex system which consists from n elements. So, for n=2 the following formula is used

$$\lambda_{f-S} = \frac{\lambda_{f-1} p_1 (1-p_2) + \lambda_{f-2} p_2 (1-p_1)}{p_1 + p_2 - p_1 p_2}.$$

Repair time is the time which is set by the user for the addLatent and addActive nodes. For the logical node "and" in R the repair time should be equal to the repair time of the first attached node. For the logical element "or" the same formula (4) for the mean repair time is used [11]:

$$T_{R-S} = \frac{1 - K_{av}(p)}{\sum_{i=1}^{n} \lambda_{f-i} p_i \frac{\partial K_{av}(p)}{\partial p_i}} = \frac{1 - K_{av}(p)}{K_{av}(p) \sum_{i=1}^{n} \lambda_{f-i}}. \quad (5)$$

In this case the availability factor in the FaultTree is calculated by the following formula:

$$K_{av} = \prod_{i=1}^{n} \frac{T_{f-i}}{T_{f-i} + T_{R-i}}. \quad (6)$$

In formula (6) hidden failures are not taken into consideration. The probability of the hidden failure is defined by formula (2).

Let us note that in Figure 7, next to the nodes corresponding to the hidden failures, the control period T=100 and the probability value are indicated, which is defined by the following formula: pzero=P_0=$\frac{T_r}{T_r + T_f}$.

Thus, the value of the unavailability factor of the chain in the Example 3 is 3.319E-03, the failure rate is λ_{f-S} = 2.6188E-04 1/h, and the mean time between failures is $T_{f-S} = 1/\lambda_{f-S}$ =1/Tree$CFR=3818.535 h. To calculate the last value it is required to type the following command in the command prompt:

> 1/Tree3$CFR[1]

To define the minimal cuts in the command prompt it is required to type the following command:

> Tree3_cs

The minimal cut sets with one event, which lead to the chain failure, are given in the following matrix [[1]]:

Matrix [[1]]: $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$

This matrix contains one column and two rows. The number of columns is equal to the number of nodes in the cut, i.e. in the unit, and the number of rows determines the number of minimal cuts with one event; there are two such cuts. Matrix elements are the number of nodes, which lead to the chain failure. In this case, these are nodes 3 and 4 – hidden and evident failures of the C element.

Minimal cut sets with two events are given in matrix [[2]]. This matrix contains two columns and four rows. Minimal cut sets form a combination of events 7,10 is the hidden failure B1 and hidden failure B2, and 7,11 is the hidden failure B1 and evident failure B2, etc.

Matrix [[2]]: $\begin{pmatrix} 7 & 10 \\ 7 & 11 \\ 8 & 10 \\ 8 & 11 \end{pmatrix}$

In matrix [[3]] different combinations of three events are given, which lead to the chain failure; obviously, these events are associated with elements A1, A2, A3.

Matrix [[3]]: $\begin{pmatrix} 14 & 17 & 20 \\ 14 & 17 & 21 \\ 14 & 18 & 20 \\ 14 & 18 & 21 \\ 15 & 17 & 20 \\ 15 & 17 & 21 \\ 15 & 18 & 20 \\ 15 & 18 & 21 \end{pmatrix}$

In specialized packages such as Saphire, Arbitr etc., along with the minimal cut sest, the probabilities of these cut sets and the impact on the general failure probability of the system are displayed. There is no such capability in the FaultTree package, but it can be done with the help of the R language tools. For example, using the following script:

```
1. m=length(Tree3_cs)
2. pr=Tree3_cs
3. for (i in 1:m){
4. n1=length(Tree3_cs[[i]][,1])
5. n2=length(Tree3_cs[[i]][1,])
6. for (j1 in 1:n1){
7. q1=Tree3_cs[[i]][j1,1]
8. prob=Tree3$PBF[q1]
9. if (n2>1) {
10. for (j2 in 2:n2){
11. q2=Tree3_cs[[i]][j1,j2]
12. prob=prob*Tree3$PBF[q2]
13. pr[[i]][j1,j2]=NA}}
14. pr[[i]][j1,1]=prob}}
```

If you type pr in the command prompt after executing script, the following information will be displayed:

```
> pr
[[1]]
[,1]
[1,] 0.001448669
[2,] 0.001796766

[[2]]
[,1] [,2]
[1,] 1.487810e-05 NA
[2,] 1.842618e-05 NA
[3,] 1.842618e-05 NA
[4,] 2.282040e-05 NA

[[3]]
[,1] [,2] [,3]
[1,] 1.929755e-07 NA NA
[2,] 2.387178e-07 NA NA
[3,] 2.387178e-07 NA NA
[4,] 2.953028e-07 NA NA
[5,] 2.387178e-07 NA NA
[6,] 2.953028e-07 NA NA
[7,] 2.953028e-07 NA NA
[8,] 3.653006e-07 NA NA
```

The first column shows the probability of the corresponding cut set. Additional columns have no important information. Analyzing the results, it may be concluded that two events negatively affect the system's dependability, i.e. evident and hidden failures of the C element.

In conclusion it should be noted that addLatent, addActive functions and others, which calculate the probability in accordance with some dependability model, can be uniformly replaced by addProbability with the failure probability calculated in advance.

Conclusion

This article demonstrates the capabilities of the actively developing R language for statistical data processing and its FaultTree package related to the construction and analysis of the fault trees. Fault trees are used to analyze the reliability of complex systems. Three examples are examined and analyzed in detail in this article. First, FTA is calculated with known failure probabilities of elements. Second, the dynamic fault tree is analyzed, i.e. the distribution function of time to failure of chain is identified. In the last example, FTA of the chain with repairable elements are examined.

References

1. Crawley MJ. The R Book. 2nd ed. Wiley Publishing; 2012.

2. Shipunov AB, Baldin EM, Volkov PA, Korobeynikov AI, Nazarov SA, Petrov SV et al. Nagliadnaya statistika. Ispolzuem R! [Illustrative statistics. Using R!]. Moscow: DMK Press; 2012 [in Russian].

3. Kabakov RI. R v deystvii. Analiz i vizualizatsiya dannykh v programme R [R in action. Analysis and visualization of data in R]. Moscow: DMK Press; 2014 [in Russian].

4. Antonov AV, Nikulin MS, Nikulin AM, Chepurko VA. Teoria nadiozhnosti. Statisticheskie modeli; Ouchebnoie posobie [Dependability theory. Statistical models: A study guide. Moscow: INFRA-M; 2015 [in Russian].

5. Gnedenko BV, Beliaev YuK, Soloviev AD. Matematicheskie metody v teorii nadiozhnosti [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965 [in Russian].

6. Beliaev YuK, Bogatyrev VA, Bolotin VV et al. Ushakov IA, editor. Nadiozhnost tekhnicheskikh system: Spravochnik [Dependability of technical systems: Reference book]. Moscow: Radio i sviaz; 1985 [in Russian].

7. Antonov AV, Nikulin MS. Statisticheskie modeli v teorii nadiozhnosti: Ouchebnoie posobie [Statistical models in the dependability theory: A study guide]. Moscow: Abris; 2012 [in Russian].

8. <https://ru.wikipedia.org/wiki/R_(язык_программирования)>

9. <http://www.openreliability.org/fault-tree-analysis-on-r/>

10. Mosleh A et al. Procedures Guidelines in Modeling Common Cause Failures in Probabilistic Risk Assessment (NUREG/CR-5485); 1998.

11. Programmnyy kompleks avtomatizirovannogo strukturno-logicheskogo modelirovaniya i rascheta nadezhnosti i bezopasnosti ASUTP na stadii proektirovaniya (PK ASM SZMA) [Software system for automated structural and logical modeling and dependability and safety calculation of ACS at the design stage (PK ASM SZMA)]. Technical documentation. Saint-Petersburg: OAO SPIK SZMA; 2003 [in Russian].

12. Smith CL, Wood ST, Galyean WJ, Schroeder JA, Sattison MB. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE). Version 8. Vol. 2, NUREG/CR-7039 INL/EXT-09-17009; June 2011.

About the authors

Alexander V. Antonov, Doctor of Engineering, Professor, Head of Division for Justifying Calculations of Design Solutions, JSC RZSU, Russia, Moscow, e-mail: AlVlaAntonov@rasu.ru

Evgeny Yu. Galivets, Deputy Director of Department, Head of Design Division, JSC RASU, Russia, Moscow, e-mail: EYGalivets@rasu.ru

Valery A. Chepurko, Candidate of Physics and Mathematics, Associate Professor, Chief Specialist of Division for Justifying Calculations of Design Solutions, JSC RZSU, Russia, Moscow, e-mail: VAChepurko@rasu.ru

Alexey N. Cherniaev, Candidate of Engineering, Deputy Technical Director, Director of Design Department, JSC RASU, Russia, Moscow, e-mail: AlNChernyaev@rasu.ru

Received on 04.08.2017

Original article
DOI: 10.21683/1729-2646-2018-18-1-14-19

Representation of superposition of two technical systems with a density function centroid

Evgeni P. Sorokoletov, *Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint Petersburg, Russia, e-mail: Sorokoletov.john@gmail.com*
Kirill N. Voynov, *Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint Petersburg, Russia, e-mail: forstar@mail.com*

Evgeni P. Sorokoletov

Kirill N. Voynov

Abstract. Aim. *The practice of dependability calculation and analysis occasionally deals with technical systems for which the dependability model is difficult or impossible to adequately describe with a set of serial and parallel connections and corresponding mathematical tools of multiplication of probabilities. The article examines the method of modeling the dependability of highly integrated systems through the analysis of the position of time to failure density function centroid f(t). This work is the continuation of a big research dedicated to the analysis of the properties of a density function centroid in highly integrated technical systems. In the first part it was shown that the centroid allows identifying the level of mutual influence of subsystems of a mechatronic system and identifying their contribution into the overall level of dependability of a whole product, where the primary criterion is the proximity of the partial centroid of the density function of each subsystem to the overall average centroid of the whole system. This paper assumes that the average centroid for a composition of density functions of product components does not depend on the way they are connected in the dependability model and thus can be used as the conditional reliability indicator for systems with fuzzy structural and functional connections.* **Methods.** *The research is based on graphs of time to failure density functions for conditional components of a complex technical system, such as electronics, mechanics and software. The diverse nature of the system's components is reflected through the variation of parameters of the Weibull-Gnedenko law. In order to simplify the calculation and presentation of the results, the analysis is conducted not in an integrated manner for 3 components, but for pairs. For each pair of subsystems density functions are calculated and plotted both for individual components, and for cases of their serial and parallel connection. Then, for each calculation case the centroid of the corresponding density function is generated with subsequent plotting and comparison of the average graphs.* **Results.** *The primary observation based on the results of the graph analysis is that the average centroid resulting from two partial centroids of the density functions of single systems (mechanics, electronics, software) has a high rate of correlation (over 0.99) and almost matches the average centroid generated out of two partial centroids of serial and parallel connection of the respective pairs of systems per each calculation case.* **Conclusions.** *The results of the research again show that the average centroid for a composition of density functions of different systems is equivalent to their superposition and can be used as a conditional average (or fuzzy) index of the overall level of dependability of highly integrated complex technical systems of which the structural and functional dependability model is difficult to represent with a set of serial and parallel connections and corresponding mathematical tools of multiplication of probabilities.*

Keywords: *function centroid, distribution density, dependability, Weibull distribution, highly integrated technical systems.*

For citation*: Sorokoletov EP, Voynov KN. Representation of superposition of two technical systems with a density function centroid. Dependability 2018;18(1): 14-19. DOI: 10.21683/1729-2646-2018-18-1-14-19*

Introduction

This paper is the continuation of research [1] dedicated to the analysis of the properties of density function centroid $f(t)$ of highly integrated technical systems. In the first part it was shown that the centroid allows identifying the level of mutual influence of subsystems of a mechatronic system and identifying their contribution into the overall level of dependability of a whole product. Further research deals with the question of whether it is allowable to use the centroid as the conditional average dependability indicator of highly integrated systems for cases when it impossible to adequately express the product model through a set of serial and parallel connections and corresponding mathematical tools [2].

With variable success and depending on the context and requirements the problem of dependability of such systems is solved by various means, e.g. logical and probabilistic method [3], fuzzy sets [4], as well as functional analysis [5, 6].The method presented in [1] and this paper can be ideologically classified as a fuzzy approach except for the fact that instead of state of failure/operability (or its frequency) the fuzzy measure is the structural and functional connection between the components.

1. Reference data and plan of research

The aim of the research is to study the behaviour of the density function centroid in cases of serial and parallel connection of elements. For that purpose pairs are made out of a random set of conditional technical systems with varied properties expressed through the variation of failure rate λ_0 and parameters of α and β of the Weibull distribution law (Table. 1):

$$\lambda(t) = \alpha\lambda_0 t^{\alpha-1}, \quad (1)$$

$f(t)$ is the time to failure density function

$$f(t) = \lambda_0 \alpha t^{\alpha-1} \exp\left(-\lambda_0 t^{\alpha}\right), \quad (2)$$

or for the case of Weibull distribution:

$$f(t) = \left(\frac{\alpha}{\beta}\right)\left(\frac{t}{\beta}\right)^{\alpha-1} \exp\left(-\left(\frac{t}{\beta}\right)^{\alpha}\right), \quad (3)$$

where λ_0 is the initial failure rate;

α is the parameter of the distribution shape;

β is the parameter of the breadth of distribution

$$\beta = \lambda_0^{-1/\alpha}. \quad (4)$$

Thus, 3 pairs of conditional systems are made for further research:

a) electronics + mechanics;

b) electronics + software;

c) mechanics + software.

Calculation is performed for the operation interval [0; 10000] hours with a 1000 h step.

For each pair of systems graphs of the following functions are calculated and plotted:

$f_i(t)$ is the time to failure density function for each single system;

C_i is the centroid of respective function $f_i(t)$;

$C\text{-}0_{i\_ini}$ is the average centroid for each pair of systems plotted based on the initial graphs C_i (see item 2);

$f(t)_{i\_ser}$ is the function $f_i(t)$ for the serial connection of the elements of the corresponding pair;

C_{i_ser} is the centroid of function $f(t)_{i\_ser}$ for serial connection (see item 4);

$f(t)_{i\_par}$ is the function $f_i(t)$ for the parallel connection of the corresponding pair;

C_{i_par} is the centroid of function $f(t)_{i\_par}$ for parallel connection (see item 6);

$C\text{-}0_{i\_sum}$ is the average centroid for each pair of systems generated based on the corresponding centroids C_{i_ser} of serial and C_{i_par} of parallel connection of systems (see items 5 and 7).

2.1. Calculation and generation of functions for pairs of systems

The time to failure density distribution functions $f_i(t)$ for each system are expressed according to formula (2-3) and described above (Table 1).

The function of centroid C_i for the corresponding density function $f_i(t)$ is generated according to the following model.

The first step is the definition of the time interval $[t_1; t_2]$ and limitation of the research area under the graph D_i. After the limits of the operation period and thus the area D_i have been defined, the subsequent analysis consists in the identification of the area S_i.

Table 1. Distribution law parameters of conditional technical systems

Parameter	Electronic components	Software (SW)	Mechanical components
λ_0, h^{-1}	1×10^{-4}	0.005	1×10^{-7}
α	1	0.5	1.8
β	10000	40000	7742.6368
$\lambda(t)$	$\lambda_{El}(t) = 0.0001$	$\lambda_{SW}(t) = 0.0025\cdot t^{-0.5}$	$\lambda_{Mec}(t) = 1.8\cdot10^{-7}t^{0.8}$
$f(t)$	$f_{El}(t) = 10^{-4} e^{-10^{-4}t}$	$f_{SW}(t) = 0.05\cdot0.5t^{-0.5}e^{-0.005t^{0.5}}$	$f_{Mex}(t) = 10^{-7}\cdot1,8t^{0,8}e^{-10^{-7}t^{1.8}}$

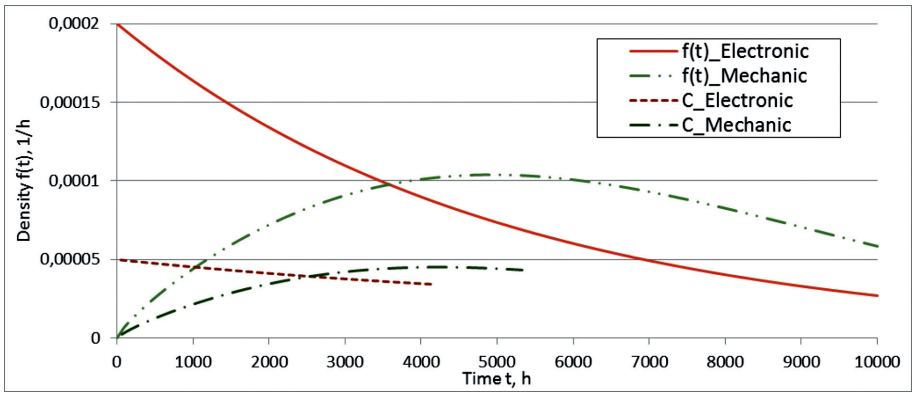


Figure 1. Density and centroid functions for the pair of systems Electronics + Mechanics

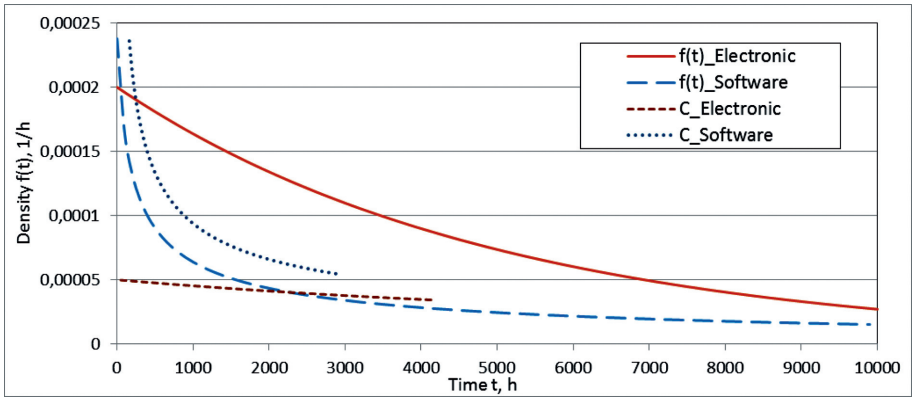


Figure 2. Density and centroid functions for the pair of systems Electronics + Software

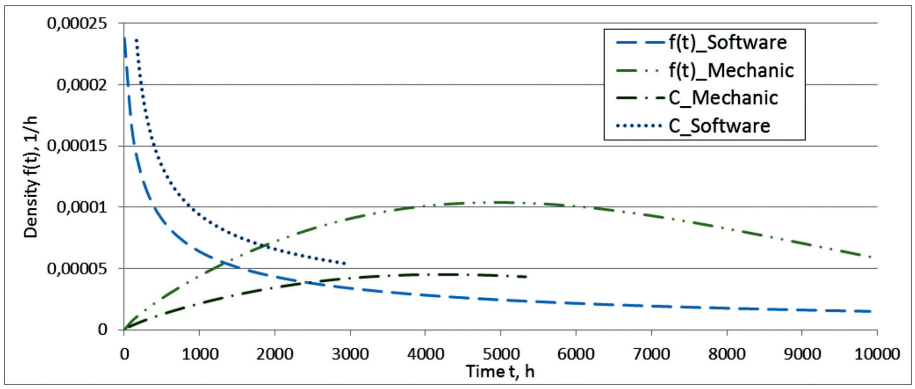


Figure 3. Density and centroid functions for the pair of systems Mechanics + Software

$$S_i = \iint\limits_{D_i} dfdt = \int\limits_{t_1}^{t_2} f_i(t)dt. \tag{5}$$

and calculation of the coordinates $(\overline{t}_i; \overline{f}_l)$ of the centroid of respective area D_i.

$$\overline{f}_l = \frac{1}{S_i}\iint\limits_{D_i} f\ dfdt; \quad \overline{t}_i = \frac{1}{S_i}\iint\limits_{D_i} t\ dfdt. \tag{6}$$

Such centroid calculation is performed for each operation interval for which a density function is generated (Fig. 1-3).

2.2. Calculation and generation of functions for serial and parallel connection

The value of the density functions for serial $f(t)_{i\text{–ser}}$ and parallel $f(t)_{i\text{–par}}$ connection of a pair of systems are identified by means of differentiation according to formula (8) of probability of no failure $P(t)$ for serial and parallel connection calculated based on the known formulas (9-10):

$$P(t) = \exp\left(-\lambda_0 t^{\alpha}\right) = \exp\left(-\left(\frac{t}{\beta}\right)^{\alpha}\right), \tag{7}$$

$$f(t) = -\frac{d}{dt}P(t) = \frac{d}{dt}Q(t), \tag{8}$$

$$P(t)_{ser} = P_1(t) \cdot P_2(t), \tag{9}$$

$$P(t)_{par} = P_1(t) + P_2(t) - P_1(t) \cdot P_2(t). \tag{10}$$

Thus, given the reference data (Table 1) and formulas (7-10) the time to failure density functions for serial and parallel connection of a pair of system is as follows (formulas 11-16, Fig. 4-6):

$$f(t)_{El+Mec_{ser}} = \\ = \left(1,8 \cdot 10^{-7} \cdot t^{0,8} + 10^{-4}\right) \cdot \exp\left(-t^{1,8} \cdot 10^3 t / 10^7\right), \tag{11}$$

$$f(t)_{El+Mec_{ser}} = \begin{bmatrix} 10^4 \cdot \exp\left(t^{1,8} \cdot 10^{-7}\right) + 1,8 \cdot 10^{-7} \cdot t^{1,8} \cdot \\ \cdot \exp\left(t \cdot 10^{-4}\right) - 1,8 \cdot 10^{-7} \cdot t^{0,8} - 10^{-4} \end{bmatrix} \times \\ \times \exp\left(-t^{1,8} \cdot 10^3 t / 10^7\right), \tag{12}$$

$$f(t)_{El+SW_{ser}} = \left(10^{-4} + 0,0025 \cdot t^{-0,5}\right) \cdot \\ \cdot \exp\left(-10^{-4} t - 0,005 t^{0,5}\right), \tag{13}$$

$$f(t)_{El+SW_{par}} = \begin{bmatrix} \exp\left(10^{-4} t\right) \cdot 0,0025 t^{-0,5} + 10^{-4} \cdot \\ \cdot \exp\left(0,005 \cdot t^{0,5}\right) - 0,0025 \cdot t^{-0,5} - 10^{-4} \end{bmatrix} \times \\ \times \exp\left(-10^{-4} t - 0,005 t^{0,5}\right), \tag{14}$$

$$f(t)_{Mec+SW_{ser}} = \left(1,8 \cdot 10^{-7} \cdot t^{0,8} + 0,0025 \cdot t^{-0,5}\right) \cdot \\ \cdot \exp\left(-10^{-7} t^{1,8} - 0,005 t^{0,5}\right), \tag{15}$$

$$f(t)_{Mec+SW_{par}} = \begin{bmatrix} \exp\left(10^{-7} t^{1,8}\right) \cdot 0,0025 t^{-0,5} + 1,8 \cdot 10^{-7} \cdot \\ \cdot t^{0,8} \cdot \exp\left(0,005 \cdot t^{0,5}\right) - 0,0025 \cdot t^{-0,5} - \\ -1,8 \cdot t^{0,8} \cdot 10^{-7} \end{bmatrix} \times \\ \times \exp\left(-10^{-7} t^{1,8} - 0,005 t^{0,5}\right). \tag{16}$$

2.3. Constructing the average centroid

Generation of the average centroid of a system based on the partial centroids of the subsystems is performed using the formula (17)

$$\overline{f}_0 = \frac{\overline{f}_1 + \overline{f}_2 + \ldots + \overline{f}_n}{n}; \qquad \overline{t}_0 = \frac{\overline{t}_1 + \overline{t}_2 + \ldots + \overline{t}_n}{n}, \tag{17}$$

Let us construct and compare the following graphs for each pair of systems:

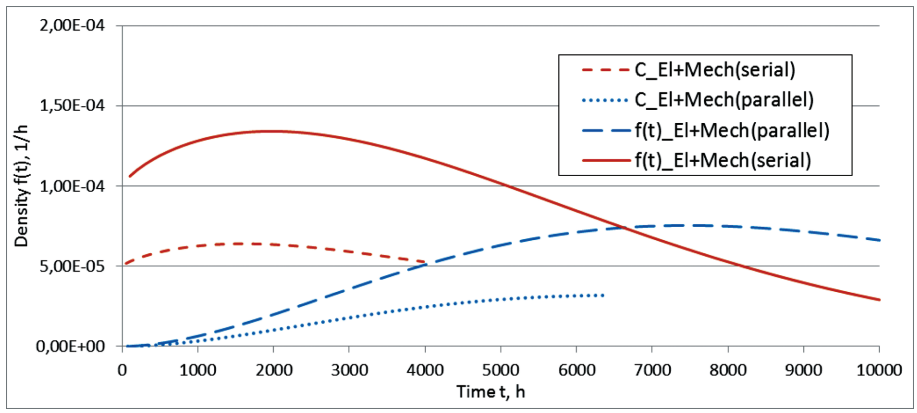


Figure 4. Density and centroid functions for serial and parallel connection of the elements of the pair Electronics + Mechanics

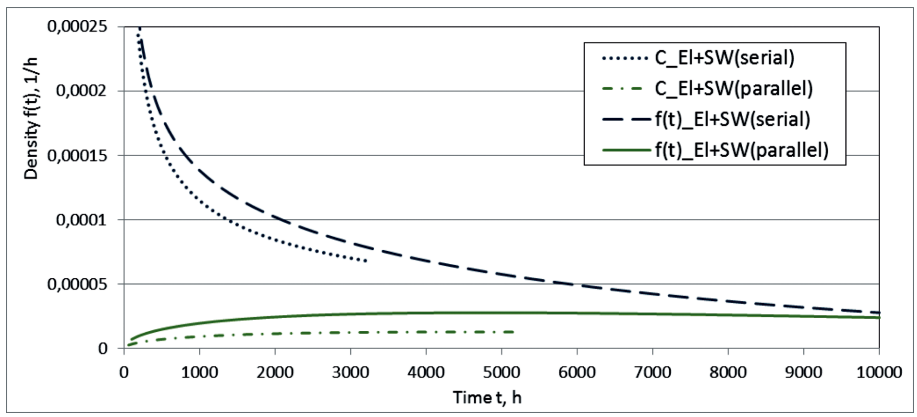


Figure 5. Density and centroid functions for serial and parallel connection of the elements of the pair Electronics + Software

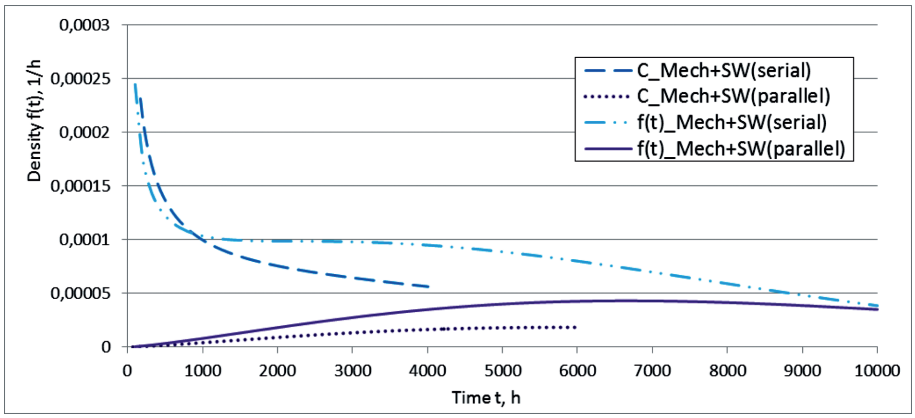


Figure 6. Density and centroid functions for serial and parallel connection of the elements of the pair Electronics + Software

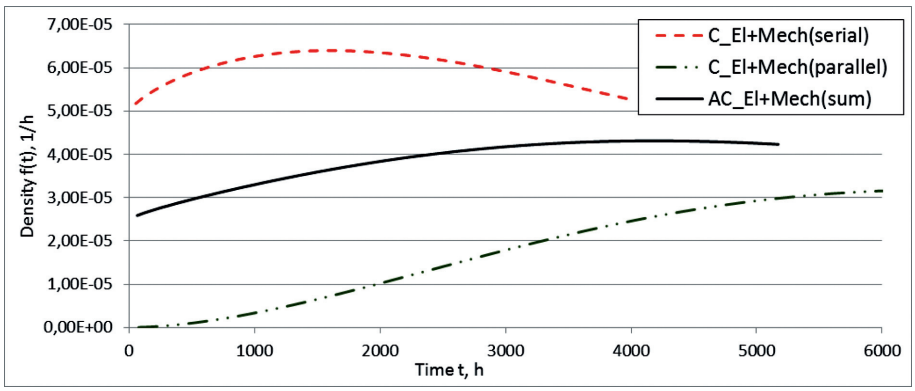


Figure 7. Generation of average centroids based on partial centroids of density functions for serial and parallel connection of the systems of pairs Electronics + Mechanics

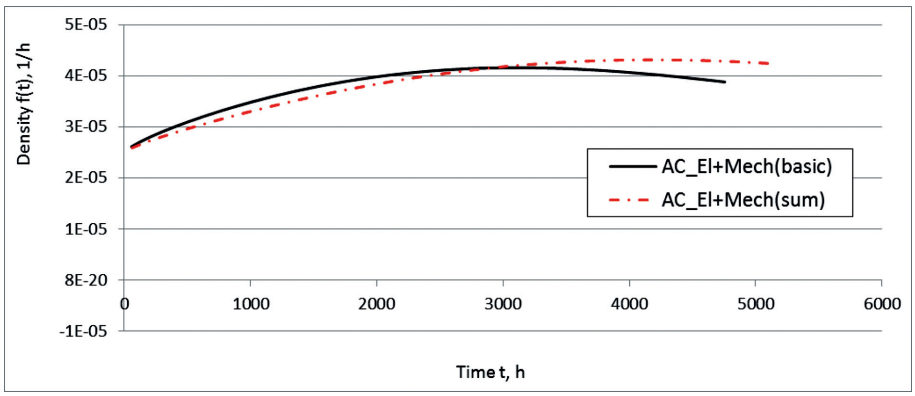


Figure 8. Functions of average centroids based on reference data and subject to serial and parallel connection of the elements of the pair Electronics + Mechanics

• Average centroid $C\text{-}0_{i\_ini}$ based on two partial centroids C_i of the initial density functions $f_i(t)$ for each system of the pair (Fig. 1-3).

• Average centroid $C\text{-}0_{i\_sum}$ based on two partial centroids C_{i_ser} and C_{i_par} of the calculated density functions for serial and parallel connections of the pair components (Fig. 4-6).

An example of average centroid generation based on the partial centroids is given below (Fig. 7). Functions of average centroids based on partial centroids of density functions for serial and parallel connection of the systems of pairs Electronics + Mechanics, Electronics + Software and Mechanics + Software are given in Fig. 8-10.

Conclusion

The primary observation based on the results of the graph analysis (Fig. 8-10) is that the average centroid resulting from two partial centroids of the density functions $f(t)$ of single systems (mechanics, electronics, software) has a high rate of correlation (over 0.99) and almost matches the average centroid generated out of two partial centroids of serial $f(t)_{i\_ser}$ and parallel $f(t)_{i\_par}$ connection of the respective pairs of systems.

Thus, that is another argument that the average centroid for a composition of density functions of different systems is equivalent to their superposition and can be used as a

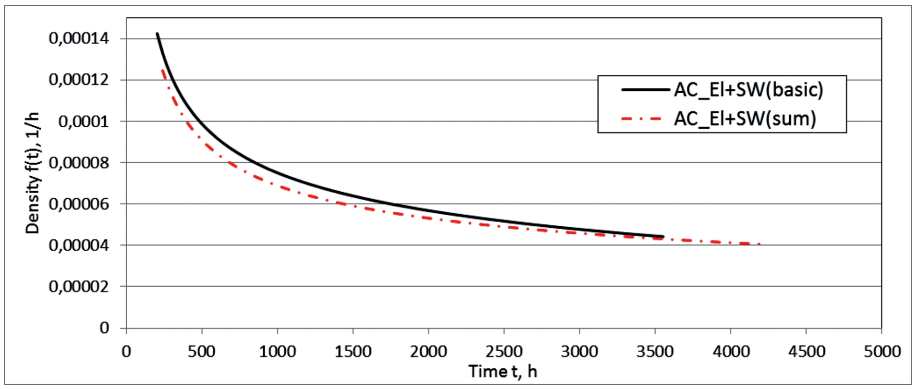


Figure 9. Functions of average centroids based on reference data and subject to serial and parallel connection of the elements of the pair Electronics + Software

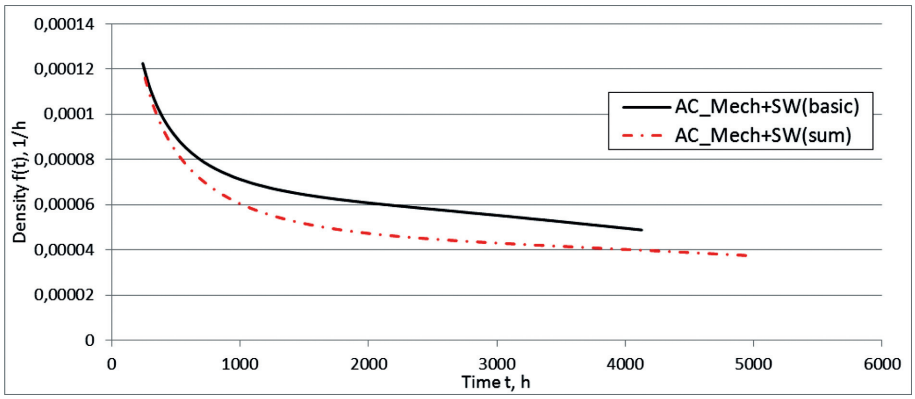


Figure 10. Functions of average centroids based on reference data and subject to serial and parallel connection of the elements of the pair Mechanics + Software

conditional average (or fuzzy) index of the overall level of dependability of highly integrated complex technical systems of which the structural and functional dependability model is difficult to represent with a set of serial and parallel connections.

References

1. Sorokoletov EP, Voynov KN. Research of the behavior of failure density centroid in redundant complex technical systems. Dependability 2016;16(4):3-10. DOI:10.21683/1729-2646-2016-16-4-3-10.

2. Voynov KN. Prognozirovanie nadezhnosti mekhanicheskikh sistem [Forecasting the dependability of mechanical systems]. Leningrad: Machinostroenie. Leningrad branch; 1978 [in Russian].

3. Riabinin IA. Nadezhnost i bezopasnost strukturno-slozhnykh sistem [Dependability and safety of structurally complex systems]. Saint Petersburg: Saint Petersburg University Publishing; 2007 [in Russian].

4. Chang JR, Liao SH. The reliability of general vague fault-tree analysis of weapon systems fault diagnosis. Soft Computing 2006;10:531-542.

5. Polovko AM, Gurov SV. Osnovy teorii nadiozhnosti [Introduction into the dependability theory]. BHV-Petersburg; 2006 [in Russian].

6. SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Pennsylvania: SAE International; 1996.

About the authors

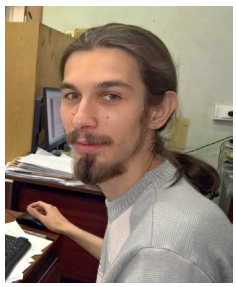
Evgeni P. Sorokoletov, Head of Fault Tolerance Engineering, Bi Petron, post-graduate student, Engineering Department, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint Petersburg, Russia, e-mail: sorokoletov.john@gmail.com

Kirill N. Voynov, Doctor of Engineering, Professor, Member of the Saint Petersburg Academy of Engineering, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint Petersburg, Russia, e-mail: forstar@mail.com

Received on 01.06.2017

Generation of PNF functions in matrix form for cold standby systems with heterogeneous elements

Dmitry M. Krivopalov, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia*
Evgeny V. Yurkevich, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia*



Dmitry M. Krivopalov

Evgeny V. Yurkevich

The importance of considering the particular features of the facilities that ensure redundancy of functional units is demonstrated in the context of design for dependability. With the growth of the number of types and quantity of involved elements the process of dependability calculation becomes more complex and time-consuming. Therefore, in order to simplify the calculations, assumptions are made. For instance, in redundant systems heterogeneous elements are used. However, this approach does not allow evaluating the dependability of a system that features essentially different elements.
The paper considers systems that include a random number of essentially different elements with cold redundancy. As a possible solution to the above problem, a method was developed and mathematically justified that allows representing in matrix form an analytic expression for calculating the probability of no-failure. It is shown that in this case a numeric evaluation of dependability is possible using rough computation with integration and differentiation.
The degree of approximation of such calculations is proposed to be defined by both the accuracy of the computer itself and the complexity of the system under consideration. In the context of design for dependability, when the process of recalculation is performed repeatedly this drawback is critical. In order to reduce the time of dependability calculation of the system under consideration, as well as to increase the accuracy of the results, the paper suggests a method of analytical solution for PNF calculation. As a result, the design mechanism of cold standby systems can be simplified, while their dependability evaluation can be done more accurately.
Therefore, in order to calculate the PNF of systems with a random number of elements in general by means of the numerical method, it is proposed to perform the number of serial integrations of the product of the function and derivatives an entity less than the number of the system elements. Given the particular nature of computer calculation and algorithm recurrence, PNF calculation of a system of as much as 5 or more elements may take significant time, while cumulated calculation error is inevitable.
The practical details of the task related to ensuring spacecraft operational stability under environmental effects are characterized by the importance of the factor of prompt decision-making regarding the generation of control signal aimed at ensuring homoeostasis of the onboard systems performance. The paper mathematically substantiated a method of representing an analytic expression for PNF calculation for a system of any number of elements in cold standby. Such representation can be used for mapping data in computer memory. Under known matrix coefficients this representation will allow avoiding integration and differentiation in PNF calculation, which significantly reduces calculation time and increasing the accuracy of the results.

Keywords: *design for dependability, technical systems, essentially different system components, cold redundancy, analytical expression, matrix coefficients, computation speedup, dependability estimation accuracy improvement.*

For citation*: Krivopalov DM, Yurkevich EV. Generation of PNF functions in matrix form for cold standby systems with heterogeneous elements. Dependability 2018; 18(1): 20-25. DOI: 10.21683/1729-2646-2018-18-1-20-25*

Introduction

Calculation of the probability of no-failure (PNF) is an integral stage of design for dependability. With the growth of the number of types and quantity of involved elements the process of dependability calculation becomes more complex and time-consuming.

In order to simplify the calculations, assumptions are made. For instance, in redundant systems heterogeneous elements are used. However, this approach does not allow evaluating the dependability of a system that features essentially different elements. (Such tasks arise when it is required to calculate the probability of faultless function performance, i.e. estimation of functional dependability [1]). In this case a numeric evaluation of dependability is possible using rough computation with integration and differentiation.

The degree of approximation of such calculations is defined by both the accuracy of the computer itself and the complexity of the system under consideration [2]. In the context of design for dependability, when the process of recalculation is performed repeatedly this drawback is critical.

In order to reduce the time of dependability calculation of the system under consideration, as well as to increase the accuracy of the results, the paper suggests a method of analytical solution for PNF calculation of cold standby systems, as those are some of the most dependable and most complexly calculated systems.

Method of numerical solution

The following recurrence formula is used to generally identify a cold standby system's PNF:

$$P_N(T) = P_{N-1}(T) + \int_0^T p_n(\tau, T) \cdot f_{N-1}(\tau) d\tau,$$

where $P_N(T)$ is the PNF of a system out of N elements over time T;

$P_{N-1}(T)$ is the PNF of a system out of (N-1) elements over time T;

$p_n(\tau,T)$ is the PNF of the n-th (initiated) element within the time period from τ to T;

$f_{N-1}(\tau)$ is the failure density distribution of the system out of (N-1) elements for the moment in time τ;

$$f_{N-1}(T) = -\frac{P_{N-1}(T)}{dT}.$$

Therefore, in order to generally numerically calculate the PNF of a system out of N elements it is required to perform (N–1) serial calculations of integrals of the function and derivatives $f_{N-1}(T)$. Given the particular nature of computer calculation and algorithm recurrence, PNF calculation of a system of as much as 5 or more elements may take significant time, while cumulated calculation error is inevitable.

Note: The formulas are used for practical calculation of dependability with the assumption that redundant elements do not lose dependability when switched off.

Analytical solutions

Let us consider a number of cases of cold redundancy in order to obtain analytical solutions and analyze the results.

A system out of 1 element

Let the element's failure rate be λ_1, then the system's PNF is:

$$P_1(T) = e^{-\lambda_1 T}.$$

The time function of PNF is as follows:

$$P_1(t) = e^{-\lambda_1 t}.$$

A system out of 2 elements

Two essentially different cases are possible.

The failure rate of the 2-nd initiated element is λ_1, then the system's PNF is:

$$P_2(T) = P_1(T) + \int_0^T p_2(\tau, T) \cdot f_1(\tau) d\tau,$$

$$p_2(\tau, T) = e^{-\lambda_1 (T-\tau)},$$

$$f_1(\tau) = -\frac{P_1(\tau)}{d\tau} = -\frac{e^{-\lambda_1 \tau}}{d\tau} = \lambda_1 \cdot e^{-\lambda_1 \tau},$$

$$P_2(T) = e^{-\lambda_1 T} + \int_0^T e^{-\lambda_1 (T-\tau)} \cdot \lambda_1 \cdot e^{-\lambda_1 \tau} d\tau =$$

$$= e^{-\lambda_1 T} + \lambda_1 \cdot e^{-\lambda_1 T} \cdot \int_0^T 1 d\tau = e^{-\lambda_1 T} + \lambda_1 \cdot e^{-\lambda_1 T} \cdot T = (1 + \lambda_1 \cdot T) \cdot e^{-\lambda_1 T}.$$

The failure rate of the 2-nd initiated element is λ_1, then the system's PNF is:

$$P_2(T) = P_1(T) + \int_0^T p_2(\tau, T) \cdot f_1(\tau) d\tau,$$

$$p_2(\tau, T) = e^{-\lambda_2 (T-\tau)},$$

$$f_1(\tau) = -\frac{P_1(\tau)}{d\tau} = -\frac{e^{-\lambda_1 \tau}}{d\tau} = \lambda_1 \cdot e^{-\lambda_1 \tau},$$

$$P_2(T) = e^{-\lambda_1 T} + \int_0^T e^{-\lambda_2 (T-\tau)} \cdot \lambda_1 \cdot e^{-\lambda_1 \tau} d\tau = e^{-\lambda_1 T} + \lambda_1 \cdot e^{-\lambda_2 T} \cdot$$

$$\cdot \int_0^T e^{(\lambda_2 - \lambda_1)\tau} d\tau = e^{-\lambda_1 T} + \lambda_1 \cdot e^{-\lambda_2 T} \cdot \frac{1}{\lambda_2 - \lambda_1} \cdot \left(e^{(\lambda_2 - \lambda_1) T} - 1 \right) =$$

$$= \frac{\lambda_2}{\lambda_2 - \lambda_1} \cdot e^{-\lambda_1 T} + \frac{\lambda_1}{\lambda_1 - \lambda_2} \cdot e^{-\lambda_2 T}.$$

The time function of PNF is as follows:

in case of matching elements:

$$P_2(t) = (1 + \lambda_1 \cdot t) \cdot e^{-\lambda_1 t};$$

in case of non-matching elements:

$$P_2(t)=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 t}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 t}.$$

A system out of 3 elements

The case when two identical elements are connected with a similar third one.

The element's failure rate is λ_1, then the system's PNF is:

$$P_3(T)=P_2(T)+\int_0^T p_3(\tau,T)\cdot f_2(\tau)d\tau,$$

$$P_2(T)=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T},$$

$$p_3(\tau,T)=e^{-\lambda_1(T-\tau)},$$

$$f_2(\tau)=-\frac{P_2(\tau)}{d\tau}=-\frac{(1+\lambda_1\cdot\tau)\cdot e^{-\lambda_1\tau}}{d\tau}=\lambda_1{}^2\cdot\tau\cdot e^{-\lambda_1\tau},$$

$$P_3(T)=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+\int_0^T e^{-\lambda_1(T-\tau)}\cdot\lambda_1{}^2\cdot\tau\cdot e^{-\lambda_1\tau}d\tau=$$

$$=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+\lambda_1{}^2\cdot e^{-\lambda_1 T}\cdot\int_0^T\tau d\tau=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+$$

$$+\lambda_1{}^2\cdot e^{-\lambda_1 T}\cdot\frac{T^2}{2}=\left(1+\lambda_1\cdot T+\frac{\lambda_1{}^2}{2}\cdot T^2\right)\cdot e^{-\lambda_1 T}.$$

The case when two identical elements are connected with an element of another type.

The element's failure rate is λ_1, then the system's PNF is:

$$P_3(T)=P_2(T)+\int_0^T p_3(\tau,T)\cdot f_2(\tau)d\tau,$$

$$P_2(T)=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T},$$

$$p_3(\tau,T)=e^{-\lambda_2(T-\tau)},$$

$$f_2(\tau)=-\frac{P_2(\tau)}{d\tau}=-\frac{(1+\lambda_1\cdot\tau)\cdot e^{-\lambda_1\tau}}{d\tau}=\lambda_1{}^2\cdot\tau\cdot e^{-\lambda_1\tau},$$

$$P_3(T)=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+\int_0^T e^{-\lambda_2(T-\tau)}\cdot\lambda_1^2\cdot\tau\cdot e^{-\lambda_1\tau}d\tau=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+$$

$$+\lambda_1{}^2\cdot e^{-\lambda_2 T}\cdot\int_0^T e^{(\lambda_2-\lambda_1)\tau}\cdot\tau d\tau=(1+\lambda_1\cdot T)\cdot e^{-\lambda_1 T}+\lambda_1{}^2\cdot e^{-\lambda_2 T}\times$$

$$\times\left(\frac{1}{\lambda_2-\lambda_1}\cdot T\cdot e^{(\lambda_2-\lambda_1)T}-\frac{1}{(\lambda_2-\lambda_1)^2}\cdot e^{(\lambda_2-\lambda_1)T}+\frac{1}{(\lambda_2-\lambda_1)^2}\right)=$$

$$=\left(\frac{\lambda_2{}^2-2\lambda_1\lambda_2}{(\lambda_2-\lambda_1)^2}+\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot T\right)e^{-\lambda_1 T}+\frac{\lambda_1{}^2}{(\lambda_2-\lambda_1)^2}\cdot e^{-\lambda_2 T}.$$

The case when two non-identical elements are connected with a matching element.

The element's failure rate is λ_1, then the system's PNF is:

$$P_3(T)=P_2(T)+\int_0^T p_3(\tau,T)\cdot f_2(\tau)d\tau,$$

$$P_2(T)=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T},$$

$$p_3(\tau,T)=e^{-\lambda_1(T-\tau)},$$

$$f_2(\tau)=-\frac{P_2(\tau)}{d\tau}=-\frac{\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau}}{d\tau}=$$

$$=\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau}+\frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau},$$

$$P_3(T)=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T}+\int_0^T e^{-\lambda_1(T-\tau)}\cdot$$

$$\cdot\left(\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau}+\frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau}\right)d\tau=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T}+$$

$$+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T}+e^{-\lambda_1 T}\cdot\int_0^T\left(\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}+\frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{(\lambda_1-\lambda_2)\tau}\right)d\tau=$$

$$=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T}+e^{-\lambda_1 T}\times$$

$$\times\left(\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot T+\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)^2}\cdot e^{(\lambda_1-\lambda_2)T}-\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)^2}\right)=$$

$$=\left(\frac{\lambda_2{}^2-2\lambda_1\lambda_2}{(\lambda_2-\lambda_1)^2}+\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot T\right)e^{-\lambda_1 T}+\frac{\lambda_1{}^2}{(\lambda_2-\lambda_1)^2}\cdot e^{-\lambda_2 T}.$$

Note: The last two cases show that the formula of the PNF function does not depend on the order of element initiation in a cold standby system. It rather depends only on the type of the element.

The case when two non-identical elements are connected with a non-matching element.

The element's failure rate is λ_3, then the system's PNF is:

$$P_3(T)=P_2(T)+\int_0^T p_3(\tau,T)\cdot f_2(\tau)d\tau,$$

$$P_2(T)=\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T}+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T},$$

$$p_3(\tau,T)=e^{-\lambda_3(T-\tau)},$$

$$f_2(\tau) = -\frac{P_2(\tau)}{d\tau} = -\frac{\frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau} + \frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau}}{d\tau} =$$

$$= \frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau} + \frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau},$$

$$P_3(T) = \frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T} + \frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T} + \int_0^T e^{-\lambda_3(T-\tau)}\cdot$$

$$\cdot\left(\frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1\tau} + \frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2\tau}\right)d\tau = \frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T} +$$

$$+\frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T} + e^{-\lambda_3 T} \times\times \int_0^T \left(\begin{array}{l} \frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot e^{(\lambda_3-\lambda_1)\tau} + \\ +\frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2}\cdot e^{(\lambda_3-\lambda_2)\tau} \end{array}\right)d\tau =$$

$$= \frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 T} + \frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 T} + e^{-\lambda_3 T} \times$$

$$\times\left(\begin{array}{l} \frac{\lambda_1\lambda_2}{(\lambda_2-\lambda_1)\cdot(\lambda_3-\lambda_1)}\cdot e^{(\lambda_3-\lambda_1)T} - \frac{\lambda_1\lambda_2}{(\lambda_2-\lambda_1)\cdot(\lambda_3-\lambda_1)} + \\ +\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)\cdot(\lambda_3-\lambda_2)}\cdot e^{(\lambda_3-\lambda_2)T} - \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)\cdot(\lambda_3-\lambda_2)} \end{array}\right) =$$

$$= \frac{\lambda_2\lambda_3}{(\lambda_2-\lambda_1)\cdot(\lambda_3-\lambda_1)}\cdot e^{-\lambda_1 T} + \frac{\lambda_1\lambda_3}{(\lambda_1-\lambda_2)\cdot(\lambda_3-\lambda_2)}\cdot e^{-\lambda_2 T} +$$

$$+\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_3)\cdot(\lambda_2-\lambda_3)}\cdot e^{-\lambda_3 T}.$$

Let us consider in detail the resulting PNF functions.

The time function of PNF is as follows:

- one element with the rate of λ_1

$$P_1(t) = e^{-\lambda_1 t};$$

- for two elements:

two elements with the rate of λ_1

$$P_2(t) = (1+\lambda_1\cdot t)\cdot e^{-\lambda_1 t};$$

one element with the rate of λ_1, the second one with the rate of λ_2

$$P_2(t) = \frac{\lambda_2}{\lambda_2-\lambda_1}\cdot e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1-\lambda_2}\cdot e^{-\lambda_2 t};$$

- for three elements:

three elements with the rate of λ_1

$$P_3(t) = \left(1+\lambda_1\cdot t + \frac{\lambda_1^2}{2}\cdot t^2\right)\cdot e^{-\lambda_1 t};$$

two elements with the rate of λ_1, the third one with the rate of λ_2

$$P_3(t) = \left(\frac{\lambda_2^2 - 2\lambda_1\lambda_2}{(\lambda_2-\lambda_1)^2} + \frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1}\cdot t\right)e^{-\lambda_1 t} + \frac{\lambda_1^2}{(\lambda_2-\lambda_1)^2}\cdot e^{-\lambda_2 t};$$

three elements with the rates of λ_1, λ_2, λ_3, therefore

$$P_3(t) = \frac{\lambda_2\lambda_3}{(\lambda_2-\lambda_1)\cdot(\lambda_3-\lambda_1)}\cdot e^{-\lambda_1 t} + \frac{\lambda_1\lambda_3}{(\lambda_1-\lambda_2)\cdot(\lambda_3-\lambda_2)}\cdot e^{-\lambda_2 t} +$$

$$+\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_3)\cdot(\lambda_2-\lambda_3)}\cdot e^{-\lambda_3 t}.$$

The dependency shows that if «repeating» elements are present, the degree of polynomial ascends under the corresponding exponential. When a «non-repeating» element is initiated, the degree of polynomial does not ascend, yet the coefficients in the formulas rearrange. In order to represent the formulas in computer memory, let us develop the method of their representation.

Algorithm of analytic solution representation

In order to produce the general algorithm let us consider a random system out of 4 elements with the failure rate of λ_1, λ_2, λ_3, λ_4. As it was shown above, in general, the formula for calculating the probability of no failure can be made as a series containing exponents of the numbers $-\lambda_1 t$, $-\lambda_2 t$, $-\lambda_3 t$, $-\lambda_4 t$.

$$P_4(t) = A(t)\cdot e^{-\lambda_1 t} + B(t)\cdot e^{-\lambda_2 t} + C(t)\cdot e^{-\lambda_3 t} + D(t)\cdot e^{-\lambda_4 t}$$

The functions $A(t)$, $B(t)$, $C(t)$, $D(t)$ that are polynomials in powers of t, of which the number of summands is defined by the number of respective identical system elements. I.e. if in a system there are 2 elements with the failure rate of λ_1, the polynomial $A(t)$ contains 2 summands:

$$A(t) = a_0 + a_1 t$$

In general, the number of identical elements in a system is unknown. When elements are connected to the system, if a new type of element appears, a new exponential appears in the formula, while if the type of the initiated element matches the one of one of the already connected elements, the corresponding polynomial gets a new summand. For instance, for a system out of 4 elements, two «edge» cases are possible:

- 4 different elements. All the polynomials contain exactly one non-zero summand and have all types of exponentials;
- 4 identical types of elements. There is only one polynomial containing 4 elements and one type of exponential.

To describe such system, let us complement all the polynomials with zero coefficients so that they contain the maximum number of elements.

$$A(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3$$

$$B(t) = b_0 + b_1 t + b_2 t^2 + b_3 t^3$$

$$C(t) = c_0 + c_1 t + c_2 t^2 + c_3 t^3$$

$$D(t) = d_0 + d_1 t + d_2 t^2 + d_3 t^3$$

For clarity, let us represent the coefficients in matrix form:

	λ_1	λ_2	λ_3	λ_4
	–	–	–	–
t^0 |	a_0	b_0	c_0	d_0
t^1 |	a_1	b_1	c_1	d_1
t^2 |	a_2	b_2	c_2	d_2
t^3 |	a_3	b_3	c_3	d_3

Let us represent the matrix of initial coefficients as A, the matrix of failure rates as Λ and the matrix of degrees as T

$$A = \begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix},$$

$$\Lambda = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \end{pmatrix},$$

$$T = \begin{pmatrix} t^0 \\ t^1 \\ t^2 \\ t^3 \end{pmatrix}.$$

Let us also introduce the auxiliary function $F(A,t)$ that transforms the matrix according to the following rule:

$$B = F(A,t), \text{ where } B_{ij} = e^{-t \cdot A_{ij}}.$$

Then the system's PNF that is characterized by the matrix A can always be defined using the formula:

$$P(t) = A^{\mathrm{T}} \cdot T \cdot F(\Lambda,t)^T.$$

Example. The introduced PNF functions $P(t)$ are characterized by the following matrices with the respective auxiliary matrices T and Λ:

$$P_1(t) = e^{-\lambda_1 t},$$

$$A = (1),$$

$$P_2(t) = (1 + \lambda_1 \cdot t) \cdot e^{-\lambda_1 t},$$

$$A = \begin{pmatrix} 1 & 0 \\ \lambda_1 & 0 \end{pmatrix},$$

$$P_2(t) = \frac{\lambda_2}{\lambda_2 - \lambda_1} \cdot e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 - \lambda_2} \cdot e^{-\lambda_2 t},$$

$$A = \begin{pmatrix} \frac{\lambda_2}{\lambda_2 - \lambda_1} & \frac{\lambda_1}{\lambda_1 - \lambda_2} \\ 0 & 0 \end{pmatrix},$$

$$P_3(t) = \left(1 + \lambda_1 \cdot t + \frac{\lambda_1^2}{2} \cdot t^2\right) \cdot e^{-\lambda_1 t},$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ \lambda_1 & 0 & 0 \\ \frac{\lambda_1^2}{2} & 0 & 0 \end{pmatrix},$$

$$P_3(t) = \left(\frac{\lambda_2^2 - 2\lambda_1\lambda_2}{(\lambda_2 - \lambda_1)^2} + \frac{\lambda_1\lambda_2}{\lambda_2 - \lambda_1} \cdot t\right) e^{-\lambda_1 t} + \frac{\lambda_1^2}{(\lambda_2 - \lambda_1)^2} \cdot e^{-\lambda_2 t},$$

$$A = \begin{pmatrix} \frac{\lambda_2^2 - 2\lambda_1\lambda_2}{(\lambda_2 - \lambda_1)^2} & \frac{\lambda_1^2}{(\lambda_2 - \lambda_1)^2} & 0 \\ \frac{\lambda_1\lambda_2}{\lambda_2 - \lambda_1} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$P_3(t) = \frac{\lambda_2\lambda_3}{(\lambda_2 - \lambda_1)\cdot(\lambda_3 - \lambda_1)} \cdot e^{-\lambda_1 t} + \frac{\lambda_1\lambda_3}{(\lambda_1 - \lambda_2)\cdot(\lambda_3 - \lambda_2)} \cdot e^{-\lambda_2 t} + \frac{\lambda_1\lambda_2}{(\lambda_1 - \lambda_3)\cdot(\lambda_2 - \lambda_3)} \cdot e^{-\lambda_3 t},$$

$$A = \begin{pmatrix} \frac{\lambda_2\lambda_3}{(\lambda_2 - \lambda_1)\cdot(\lambda_3 - \lambda_1)} & \frac{\lambda_1\lambda_3}{(\lambda_1 - \lambda_2)\cdot(\lambda_3 - \lambda_2)} & \frac{\lambda_1\lambda_2}{(\lambda_1 - \lambda_3)\cdot(\lambda_2 - \lambda_3)} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Conclusions

The paper has developed and mathematically substantiated a method of representing an analytic expression for PNF calculation for a system of any number of elements in

cold standby. Such representation can be used for mapping data in computer memory. Under known matrix coefficients this representation will allow avoiding integration and differentiation in PNF calculation, which significantly reduces calculation time and increasing the accuracy of the results.

References

1. Shubinsky IB. Funktsionalnaia nadiozhnost informatsionnykh system. Metody analiza [Functional reliability of information systems. Analysis methods]. Moscow: Dependability Journal LLC; 2012 [in Russian].

2. Polovko AM, Gurov SV. Osnovy teorii nadiozhnosti [Introduction into the dependability theory]. Saint-Petersburg: BHV-Petersburg; 2006 [in Russian].

3. Krivopalov DV. Osobennosti dinamicheskogo programmirovania v nadiozhnostnom proektirovanii programmnotekhnicheskikh sistem kosmicheskikh apparatov [Special aspects of dynamic programming in design for dependability of hardware and software systems of spacecraft]. In: Proceedings of the Fifth international science and technology conference Topical matters of space-based Earth remote sensing systems. Moscow (Russia); 2017 [in Russian].

About the authors

Dmitry M. Krivopalov, engineer, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia, +7 926 840 06 58, e-mail: persival92@rambler.ru

Evgeny V. Yurkevich, Doctor of Engineering, Professor, Chief Researcher, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia, +7 495 334 88 70, e-mail: yurk@ipu.ru

Received on 29.08.2017

Ensuring resilience of pipeline transportation systems to damage to network structure elements

Igor A. Tararychkin, *V. Dal Lugansk National University, Ukraine, Lugansk*

Igor A. Tararychkin

The **Aim** *of the paper is to study the patterns of development of progressing damage affecting network structure elements of pipeline systems and to develop recommendations for ensuring the resilience of such engineering facilities. The progressing damage process is understood as the procedure of transition of linear elements (pipelines) of a system into the state of non-operability occurring in a random sequence. The capability of a system to resist progressing damage was evaluated with the resilience indicator F_w that represents the average fraction whose transition to the state of non-operability causes the disconnection of all consumers from the source of the product.* **Methods of research.** *The values of $0 < F_w < 1$ were identified by means of computer simulation. While performing a structural analysis of the systems the set of all linear elements was considered to be composed of five subsets G1, ..., G5 that connect point elements of various types.* **Results.** *It was established that elements belonging to different subsets have different effects on the system's resilience to progressing damage. The highest effect is created by the elements of subsets G1 and G2. These elements form the "core" of the network facility. The resilience to damage is least affected by the elements of subsets G4 and G5. They may be considered as a "remote periphery" of the network structure. The remote periphery interacts with the core by means of the elements belonging to subset G3. That is the "close periphery" that ensures communication between the core and the remote periphery. The effect of subset G3 elements on the resilience to damage turns out to be lower than that of the elements belonging to the core, yet higher than that of the elements of the remote periphery. Thus, the design of a pipeline system may be represented as a layered object. The core includes linear elements that interconnect the consumer and the source of the product. The higher the number of connections in the core, the higher the resilience of the network structure is.* **Conclusions.** *It was established that the resilience of network structures to progressing damage depends on their composition, while the set of all pipelines can be divided into five subsets of which the elements have different effects on the whole system's resilience. The network structure of a pipeline system may be represented as a layered object with a core, close and remote periphery. It was established that the resilience to damage largely depends on the quantitative composition and the nature of the interaction between the elements of different layers. "Tree"-type network elements are characterized by a low level of resilience to progressing damage. The resilience of such facilities can be improved by forming a core and introduction of additional linear elements into the system's composition.*

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

For citation: *Tararychkin IA. Ensuring resilience of pipeline transportation systems to damage to network structure elements. Dependability 2018;18(1): 26-31. DOI: 10.21683/1729-2646-2018-18-1-26-31*

Introduction. Pipeline transportation systems are used in a number of the sectors of economy and industry. They are part of the energy, engineering, metal, chemical, oil and gas industries. The operational properties of such complex engineering facilities depend on their structure that is made at the design stage subject to the expected characteristics of the whole system. While evaluating the probability of damage to the network structures of pipeline systems as a result of transition in the state of non-operability of individual linear elements, it should be noted that such processes may be due both to the development of internal processes within the system, and external reasons. Normally, when emergency situations arise and develop, the process of progressive transition of a number of pipelines into the state of non-operability can be observed. The process may be accompanied by the disconnection of some or all consumers from the source of the main product.

The process of further progressive transition of the system's linear elements (pipelines) into the state of non-operability in random order is called progressing damage [1]. The ability of a pipeline system to resist progressing damage primarily depends on its network structure and is characterized by such concept as resilience.

A structure's resilience to the development of progressing damage is evaluated in terms of the resilience indicator *Fw* that is the average fraction of the total number of linear elements (pipelines), whose transition into the state of non-operability causes the interruption of the delivery of the main product to all consumers.

The **Aim** of this paper is to study the patterns of development of progressing damage affecting network structure elements of pipeline systems and to develop recommendations for ensuring the resilience of such engineering facilities.

Resilience of pipeline transportation systems to damage to network structure elements

It does not appear to be possible to analytically identify the values of the resilience indicator for the given network structure. That is due to the requirement to generate a random sequence of damage to linear elements and evaluate the results of each fact of damage with subsequent generation of a database to enable the identification of F_w. At the same time, today's methods of mathematical simulations are best suited to such tasks [2].

Thus, in the process of software development in MathCAD the marked-out graph of the initial network structure was defined with a connectivity matrix [3]. Each act of graph edge damage that corresponds to transition of the system's individual pipeline into the state of non-operability was random in accordance with the MathCAD computing capabilities. The consequences of damage to network structure elements were evaluated subject to the existing connections between the source and the consumers of the product using reachability matrices [5].

The resulting set of reachability matrices was used to identify the percentage of linear elements of which the transition into the state of non-operability causes complete disconnection of all consumers from the source of the main product.

The above calculation algorithm was repeated multiple times in order to make a database required for the identification of the statistical characteristics of the random value $\boldsymbol{F}_w$.

In general, the pipelines of the transportation system connect various point objects, while the set of all linear elements can be divided into 5 subsets of which the characteristics are given in Table 1. The research findings show that elements belonging to different subsets have different effects on a working system's resilience to progressing damage.

Thus, the quantitative composition of the subsets of the network structure shown in Fig. 1 is given in Table 2. It also shows the values of resilience indicator F_w identified by means of computer simulation. In the course of the research the initial network structure *SK* (Fig. 1) was transformed in such a way as to one by one exclude the elements belonging to subsets *G*1, …, *G*5. For the network objects *SK*1, …, *SK*5 that appear in the process the values of F_w were identified (Table 2).

The findings allow concluding that a network structure's resilience to progressing damage is most affected by the elements of subset *G*1. The elements of the other subsets have a lesser effect that progressively diminishes from *G*2 to *G*3 and further from *G*4 to *G*5.

Table 1. Designation of subsets of linear elements within the network structure

Designation of subsets of linear elements	Characteristics of point element connections	Conventional representation of the elements of corresponding subsets	Number of subset elements within the network structure
*G*1	Source – consumer		g_1
*G*2	Consumer – consumer		g_2
*G*3	Consumer – hub		g_3
*G*4	Hub – hub		g_4
*G*5	Source – hub		g_5

The simulation results show that the identified trends are also observed in more complex structural facilities with a large number of consumers and structural elements.

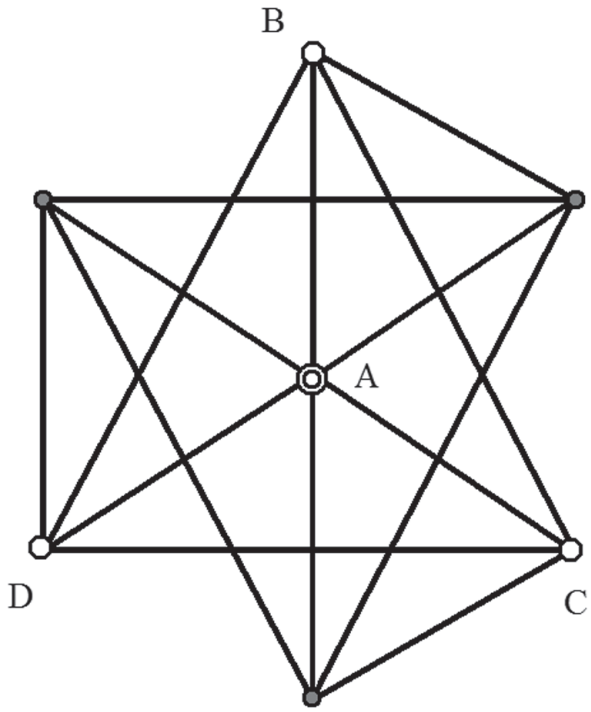


Figure 1. Structure of a system with conventional designation SK

In general, the analysis of the resulting data allows establishing the presence of the following patterns.

1. The network structure's resilience to damage is most affected by elements of subsets *G1* and *G2*. These elements form the "core" of the network facility.

2. The resilience to damage is least affected by the elements of subsets *G4* and *G5*. They may be considered as a "remote periphery" of the network structure.

3. The remote periphery interacts with the core by means of the elements belonging to subset *G*3. Their sum can be considered the "close periphery" that ensures communication between the core and the remote periphery. The effect of subset *G*3 elements on the resilience to damage turns out to be lower than that of the elements belonging to the core, yet higher than that of the elements of the remote periphery.

The findings allow concluding that, in general, the structure of a pipeline system may be represented as a layered object shown in Fig. 2.

The core includes linear elements that interconnect the consumer and the source of the product. The higher the number of elements in the core the higher is the resilience of the network structure.

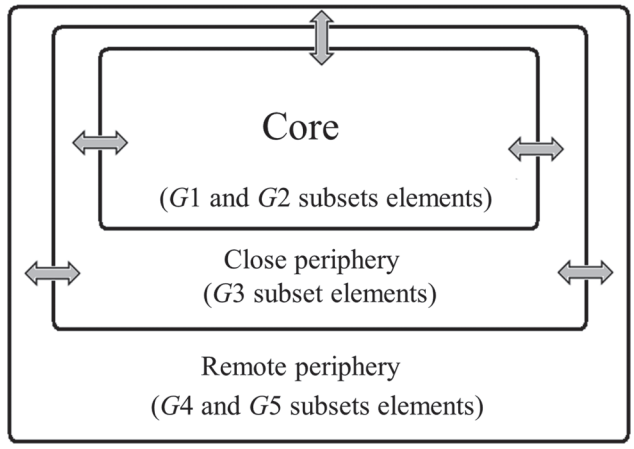


Figure 2. Diagram of a three-layer structural object

Resilience to progressing damage of network structures based on acyclic graphs

In many cases, the design and manufacture of pipeline transportation systems is associated with the requirement to distribute and deliver the main product to a large number of various consumers. The consumers, in turn, are grouped in a certain way in accordance with the adopted process flow cart. For example, an enterprise-level hub delivers specified quantities of main product to consumers in individual shops. In each shop, the product is distributed among aisles, areas and individual workstations (groups of production equipment).

Possible distribution of main product and diagram of its delivery to individual consumers distributed over different production sites is shown in Fig. 3. Such network structures are described with acyclic graphs also called "trees" [6].

The distinctive feature of such structures is that connection of any graph nodes is only possible in one way and only via specific edges. In other words, there is only one way from one node to another.

The use of levels in the description of "trees" allows establishing a hierarchy of individual elements and evalu-

Table 2. Model prediction of the progressing damage process for various network structures

Structure designation	Network structure composition					Resilience indicator F_w
	g_1	g_2	g_3	g_4	g_5	
*SK*1	0	3	3	3	3	0.586±0.006
*SK*2	3	0	3	3	3	0.660±0.006
*SK*3	3	3	0	3	3	0.677±0.008
*SK*4	3	3	3	0	3	0.741±0.005
*SK*5	3	3	3	3	0	0.748±0.007

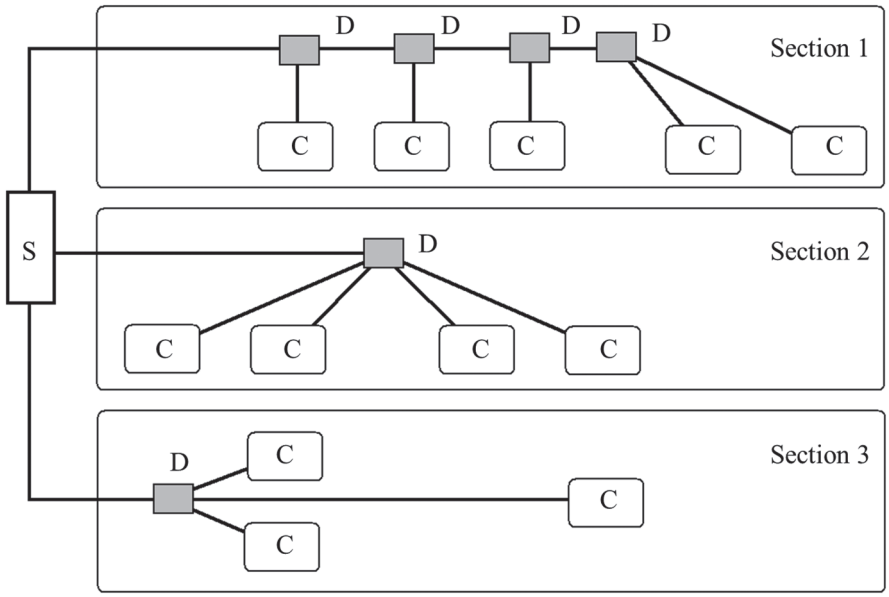


Figure 3. Diagram of product delivery from the source (S) through distributors (D) to individual consumers (C)

ating their role in the process of main product delivery to consumers.

While considering a "tree"-type facility in terms of potential development of progressing damage process it can be argued that such structure is quite vulnerable. The elimination of any linear element from its structure will cause a division of the network facility into separate parts.

In practice, such situations are quite dangerous, as any event involving the transition of linear elements into the state on non-operability will be accompanied by the disconnection of at least one consumer from the source. That means that "tree"-type structures are characterized by a low level of resilience to progressing damage.

In this context it is required to evaluate the resilience to progressing damage of network structures based on acyclic graphs, as well as establish the feasibility and efficiency of various measures aimed at improving the value F_w.

Let us examine the properties of the network structure of a tree-based pipeline transportation system shown in Figure 4. This structure is characterized by the following composition: $g_1 = 0$; $g_2 = 0$; $g_3 = 12$; $g_4 = 6$; $g_5 = 3$.

Its representation in the form of a layered facility is shown in Figure 5. As it can be seen, this structure is completely devoid of core elements. For that reason high values of resilience to progressing damage should not be expected from such facilities.

Given the above, the exclusion of one or more linear elements from the facility's composition causes a significant reduction of the whole system's operational capabilities. Additionally, due to the hierarchic nature of the connections between individual units the highest hazard is posed by damage to the elements belonging to the subset from $G5$ to $G4$.

Simulation of the process of progressing damage for the "tree"-type structure under consideration allows identifying

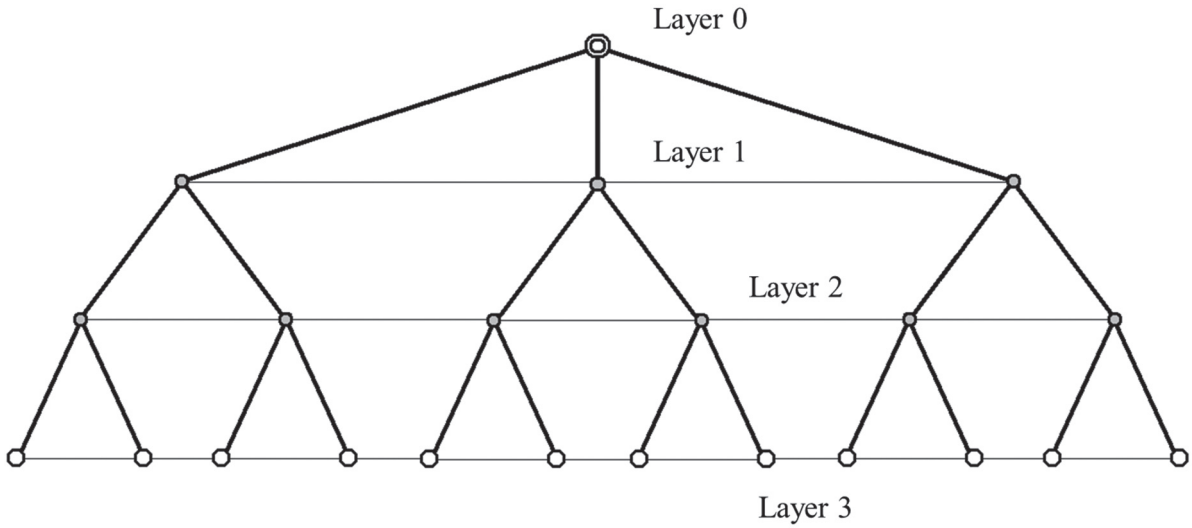


Figure 4. Diagram of a "tree"-based network structure

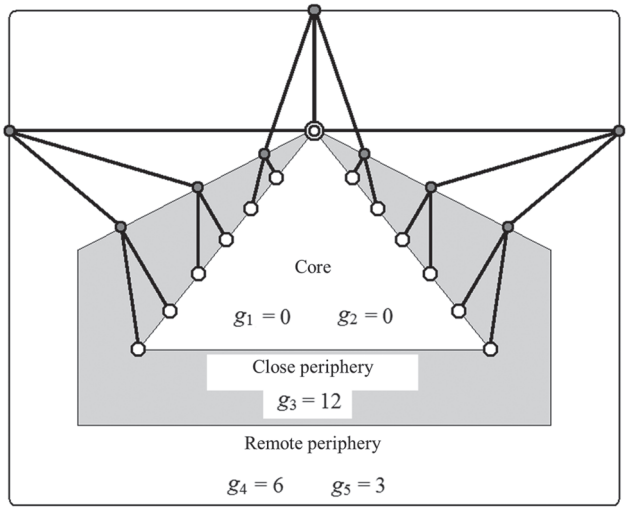


Figure 5. Representation of network structure in the form of a layered facility

the value: $F_w = 0.291$. The value F_w can be most efficiently increased by shaping a core of the network object.

In practice, that means the need for additional linear elements between the source and each consumer. However, if the number of consumers of the main product is large this solution is very difficult to implement.

Additionally, connections can be established between pairs of consumer units. From the practical point of view, the solution involving connections between individual consumers is the most acceptable. That entails the requirement to add to the structure shown in Figure 4 11 elements of subset *G*2 that interconnect consumers at Layer 3. The simulation of progressing damage of such facility allows obtaining the following value of the resilience indicator: $F_w = 0.447$.

As it can be seen, the use of the simplest method of increasing the value F_w for a "tree"-type structure is quite efficient and increases the resilience value by 54%.

If this growth is considered insufficient, the value F_w can be increased even further by means of the above measures.

However, it must be taken into consideration that the creation of new connections will be associated with both the growth of the number of linear elements and the overall complexity of the whole pipeline system. For that reason the adoption of the final solution in any case is a tradeoff.

Now, let us consider the structural diagram of a pipeline system with the "bus" topology (Fig. 6) that is a special case of the acyclic graph. Such network facility can be represented as a layered one with a "tree"-type structure and the following composition characteristics: $g_1 = 0$; $g_2 = 0$; $g_3 = 5$; $g_4 = 3$; $g_5 = 1$.

As it can be seen, the facility under consideration is devoid of core elements. That is the reason of low values of resilience to progressing damage.

Thus, the simulation of damage resulted in the following value of the resilience indicator: $F_w = 0.259$. That means that the delivery of the main product to all consumers will be interrupted if about 26% of all the system's pipelines are in

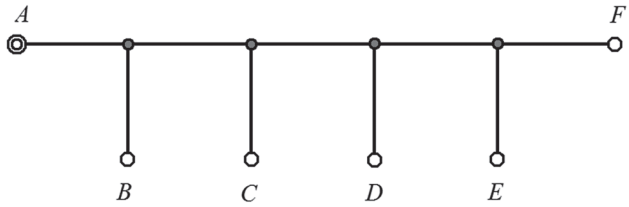


Figure 6. System elements connection in accordance with the "bus" topology

the state of non-operability.

One of the ways of improving the resilience to progressing damage is to connect all consumers of the main product with linear elements as shown in Fig. 7.

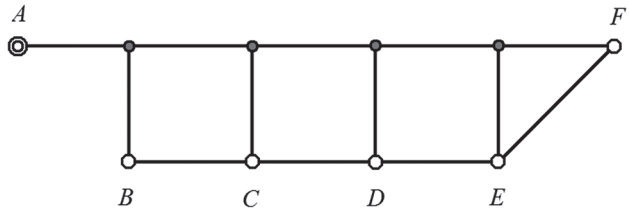


Figure 7. Diagram of the network structure with interconnected main product consumers

Simulation of the progressing damage process for this structure yields the value $F_w = 0.369$ which is 42% higher than the previously identified value for the "bus"-type network structure.

Other solutions aimed at improving the value F_w can be chosen if required. Additionally, all previously made recommendations regarding the resilience of structures based on acyclic graphs still hold as regards network structures with "bus"-type topology.

Conclusions

1. It was established that the resilience of network structures of pipeline transportation systems to progressing damage depends on their composition, while the set of all pipelines can be conventionally divided into 5 subsets of which the elements have different effects on the whole system's resilience to damage.

2. In general, the network structure of a pipeline system may be represented as a layered object with a core, close and remote periphery. It was established that the resilience to damage largely depends on the quantitative composition and possible interaction between the elements of different layers.

3. It was shown that "tree"-type network structures are characterized by a low level of resilience to progressing damage. The resilience of such facilities can be improved by forming a core and introducing additional linear elements into the system's composition.

References

1. Tararychkin I.A. Strukturnyy sintez truboprovodnykh transportnykh sistem, stoykikh k povrezhdeniyam

lineynykh elementov [Structural synthesis of pipeline transportation systems resilient to damage to linear elements]. Problemy sbora, podgotovki i transporta nefti i nefteproduktov [Matters of collection, preparation and transportation of oil and oil products] 2017; 1(107):96-106 [in Russian].

2. Strogaliov V.P, Lolkachiov I.O. Imitatsionnoe modelirovanie [Simulation]. 2nd ed. Moscow: Bauman MSTU Publishing; 2015 [in Russian].

3. Busacker R, Saaty T. Finite graphs and networks. Moscow: Nauka; 1973.

4. Okhorzin V.A. Kompiuternoie modelirovanie v sisteme Mathcad: oucheb. posobie [Computer modeling in Mathcad: a study guide]. Moscow: Financy i statistika; 2006 [in Russian].

5. Christofides N. Graph Theory: An Algorithmic Approach. Moscow: Mir; 1978.

6. Zykov A.A. Osnovy teorii grafov [Foundations of the graph theory]. Moscow: Vuzovskaya kniga; 2004 [in Russian].

About the authors

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

Received on 25.01.2017

Primary definitions of dependability of intense profession members

Nikolay I. Plotnikov, *Aviamanager Research and Design Institute of Civil Aviation, Novosibirsk, Russia*

Nikolay I. Plotnikov

Abstract.*Significance of the problem. The design of the activity of intense (extreme) profession members is due to the requirement to master new and previously unknown areas of industry and life. In the history of aviation, the matters of critical importance and calculation of required and sufficient properties of pilot and flight crew have been a subject of never-ending research for the purpose of regulation in the context of air transport operation. Up to the present moment, domain knowledge, theory and methods that would take into consideration the differences in the properties for standardization in flight operation management remain undefined. This problem of undefined domain knowledge and shortage of methods of calculation of the characteristics of civilian pilots and flight crew members are considered as extremely severe and still unsolved in the operation of civilian air transportation. Thus, the set of problems, the requirement for finding and developing new knowledge consists in the restriction of the available theories and methods of formalization, calculation of properties and management of human dependability. The relevance of this subject matter is reflected in fundamental and applied research conducted in Russia and abroad. This paper sets forth the primary definitions of dependability of intense profession members using the example of a commercial pilot. Definition of the problem of pilot dependability.Time scale is the universal foundation for the partition of the scope of the human operator (pilot) dependability concept. The primary property of human activity is the category of purpose. Purpose can be evaluated in structured subsumption of the concept of dependability. The technical substance of the category of purpose is structured with the definition of the nominal description of the objects: pilot (P), vehicle or aircraft (AC) and selected activity environment (E). The paper formalizes the definition of the human activity dependability problem. Axiomatics of pilot resource properties.The diverse nature of the human properties constitutes the fundamental problem of their description and standardization for the purpose of activity standards development. The properties have similarities, differences and independence. The paper sets forth axioms as the premises of the human resources theory under development. The premises are stated as axioms of equivalence, independence and completeness of properties, parameters and indicators of pilot resources. The practical significance of the axiomatics of the pilot resources properties consists in the fact that their formalized description allows obtaining algorithms for automated and expert technologies for flight operation management.Below are the formalizations of dependability definitions. Conclusion. The theoretical definitions of management efficiency and guaranteed management efficiency establish the concepts of discernibility of the space of successful activity outcomes. The axiomatics of pilot properties allow overcoming the fundamental difficulty of formalized description of the diverse nature of human properties and enables reliable consideration and calculation of the states for the purpose of flight operation management. The paper sets forth the definitions of pilot purpose, pilot dependability and dependability of three different kinds, i.e. individual, professional, operational, based on a fundamental temporal base of observation.*

Keywords: *pilot, purpose, management efficiency, guaranteed management efficiency, individual dependability, professional dependability, operational dependability.*

For citation:*Plotnikov NI. Primary definitions of dependability of intense profession members. Dependability 2018;18(1): 32-37. DOI: 10.21683/1729-2646-2018-18-1-32-37*

1. Introduction

In the history of aviation, the matters of critical importance and calculation of required and sufficient properties of pilot and flight crew have been a subject of never ending research for the purpose of regulation in the context of air transport operation.

The subject of dependability of individuals (pilots) and groups (crews) in today's research is at the level of concepts and is limited to statistical and empirical estimations. There is currently no dependability theory of complex objects, individuals and groups of people equivalent to the technology dependability theory, therefore the development of such theory is of relevance. The dependability of human activity and a technical object have the same U-shaped lifecycle profile [1, 2]. Therefore, the technology dependability theory can be justifiably used in the development of the human and organizational object dependability theory. Human dependability indicators are different in their nature, dynamicsand intensity of temporal variation.

The difficulty of pilot activity description consists in the absence of a single concept to define the activity. There is along list of concepts used to describe the properties of human activity: professionalism, occupational aptitude, availability, training, preparedness, dependability, responsibility, fitness for work, working efficiency, profession, qualification, experience [3, 4]. In general, the abundance of conceptual descriptions may be considered as a problem of identification of the object of activity.

The competitive environment of the open global air transportation market is leveled against the standardization of airline activities. Air disasters of the last few decades highlight the primary causes, i.e. professional properties deficiency and excessive workload of flight crews in civil aviation operations [5]. This situation is caused by not only the pressure of the business environment, but also by the critical insufficiency of scientifically grounded methods of managing flight operations in terms of human resources.

Given the above, the set of problems, the requirement for finding and developing new knowledge consists in the restriction of the available theories and methods of formalization, calculation of properties and management of human dependability. The relevance of this subject matter is reflected in numerous fundamental and applied research conducted in Russia and abroad [6, 7, 8]. This paper sets forth the primary definitions of dependability of intense profession members using the example of a commercial pilot.

2. Logical foundations of the professional activity theory

The activity theory distinguishes the types of activities that can be performed by all or the majority of individuals in a society, and the professions with special requirements [3]. In this paper, professions with special requirements like the profession of commercial pilot are referred to as intense or extreme. The design of the activity of such profession members is due to the requirement to master new and previously unknown areas of industry and life or those having an enduring critical relevance to the outcome of an activity.

Identifying the properties of any object, whether material or immaterial, artificial or natural, is not a trivial task. We structure this task as follows: a) search for the concept that best generalizes and corresponds with the object's properties; b) search and establishment of the required base of structurization and observation (measurement, evaluation) of the property; c) identification of the term that best corresponds with the states (changes) of the property.

Let us clarify the task in terms of theory of concepts (subdiscipline of logic). Each concept has its scope and content. The evaluation of abstract concepts (categories) is done through the following axiomatic heuristic statement: a) evaluation of the type of concept in terms of scope; b) identification of the basis of its partition; c) contents and presence of attributes; d) establishment of relations of concepts [9, 10].

Logical classification of concepts. "The sum of single concepts designating such objects is the scope of concept". An example: the scope of the concept of "flight" includes the sum of individual concepts of "airplane", "bird". "The sum of attributes conceivable within a concept identical in all specimens of the class is the contents of the general concept [11, p. 92]. An example: the concept of class "flight" involves the attributes of movement in a three-dimensional space for all objects (specimens): aircraft, birds. The scope and contents of a concept are in inverse relations: while enriching the contents we decrease the scope and vice versa. The law works for reconcilable concepts, when an attribute characterizes a part of the scope of the initial concept, and for concepts having subsumption relations.

Types of concepts in terms of scope. A single concept contains one object or element: "Aeroflot", "Delta Airlines". Single concepts have no scope, as they signify one object rather than a class of objects. Single concepts have contents, as they have not less than one attribute. A general concept contains several or a set of objects, e.g. "airport", "airline". General concepts may be registering and infinite. In registering concepts a set of elements may be taken into consideration and recorded, e.g. "flight". In infinite concepts the set of elements is not limited, not estimable and has an infinite scope. For example, "aviation". This is explained in the diagram (Figure 1).

Types of concepts in terms of contents. In terms of contents, four pairs of concepts are distinguished. An abstract concept designates abstract ideal existence. An object's attributes form an independent object of thinking, a thought without an object, e.g. "risk", "dependability". A concrete concept designates a real object, e.g. "airplane", "aviation" (a set of real numerable objects). The concepts can be generalized or determined. General concepts may be both concrete and abstract. For example, the concept of "pilot"

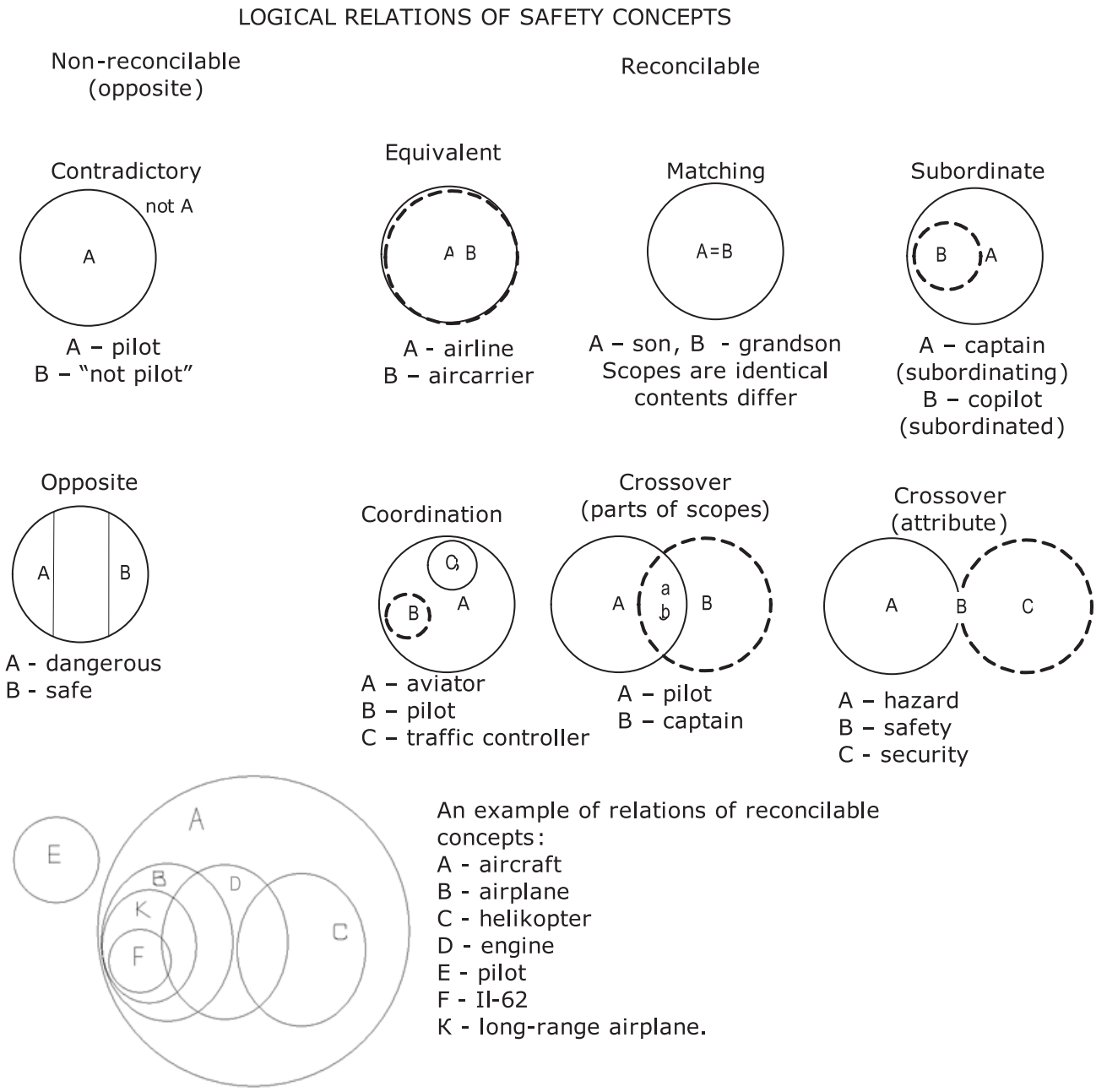


Figure 1. Logical relations of the safety concepts

is general and concrete, while the concept of "piloting" is general and abstract. A positive concept is a concept that includes attributes of object, a negative concept does not. An example: "hazard" and "safety". Coexisting concepts denote objects that designate the existence of the other, e.g. "pilot" and "aircraft". In independent concepts the objects are conceived separately: "city", "forest". A collective concept consists of a finite set of homogenous objects as a whole, e.g. "fleet", "crew", "air squadron". Non-collective concepts designate uncountable single objects, e.g. "sky", "safety", or a countable set of heterogeneous objects, e.g. "aviation".

As it is shown in [12], the main property of the pilot's activity is designated by the category of purpose (as the ability to control an aircraft in a three-dimensional space). The observer's position that defines the best possible discernibility of the object's properties is called the observation base. There are multiple types of observation bases: time, space, group and their combinations: time-space, time-group, space-group. The most universal observation bases are abstract concepts or categories, i.e. space and time (G. Klir) [13]. Therefore, this paper adopts the time scale as the basis for partition of the scope of the human operator (pilot) dependability concept. In our opinion the property of purpose can be evaluated in structured subsumption of the concept of dependability: individual, professional, operational. This partition enables the substantiation of the definition below.

3. General problem definition of dependability calculation of pilot properties and states

The technical content of the category of purpose is structured by the specified nominal description of objects: pilot (P), vehicle or aircraft (AC) and chosen activity environment (E) of the three-dimensional space. Attributes of observation become possible after the establishment of the following four types of subject-objectivity: self-observation by pilot of own activity P→P; observation of aircraft by pilot P→AC; observation of environment by pilot P→E; observation by pilot of the aircraft-environment interaction P→(AC↔E). The sum of these objects and relations is the common task of purpose of pilot's activity in flight A_{nom}:

$$A_{nom} = \left\{ \begin{array}{c} P \to P \\ P \to AC \\ P \to E \\ P \to (\mathrm{AC} \leftrightarrow \mathrm{E}) \end{array} \right\}.$$

The flight defined by the purpose is a process P_{fl} with the finite sum of n operations consisting of: (1) standardized P_{st}; (2) unexpected deviations from flight plan due to work environment P_{we}; (3) random changes of flight parameters P_m. The parameters of operations (1) and (2) are the parameters of purpose. The parameters of operations (3) are generated by the pilot based on the analysis of the parameters deviations $\Delta\omega$ from the nominal values ω_{nom}:

$$P_{fl} = n \sum_{i=1}^{\omega} (\omega_{nom} - \Delta\omega) V_{\omega_i},$$

where V_{ω_i} is the parameter change rate, $d\omega/dt$.

In accordance with the organization theory [14], the pilot's activity is described by the set A of allowed actions $y=(y \in A)$. The result of activity is $z\, A_0$, where A_0 is the set of allowed results. The connection between $(y \in A)$ and $(z \in A_0)$ is fuzzy and non-limiting. The pilot can compare the results having preferences $R_{A_0} \in$, where R_{A_0} is the preferences, $\Re_{A0}$ is the set of possible preferences. The possible R_{A_0} is in reciprocation with the value of parameter $r \in \Omega$ out of subset Ω of real axis $\Re^1$. While choosing action $y \in A$ the pilot is ruled by a) own preferences and b) the effect (estimation) of the chosen action on the activity result $z \in A_0$. The sum of (a) and (b) forms a law $W_I(\cdot)$ that characterizes the situation of which the information is reflected by variable I. The choice of action is defined by rule of individual rational choice that is dictated by the standards of flight operation, professional experience and identifies a set of preferable actions:

$$P^{W_I}\left(\Re_{A_0}, A, I\right) \subseteq A.$$

The objective function of control actions $u \in U$ equals:

$$K(B) = \max_{y \in P(u)} f_0(u, y).$$

D 1. The value $K(u)$, $u \in U$ is called efficiency of control.

D 2. If the pilot's actions entail the least preferable choice in the space of successful outcomes of activity, the value $K(u)$, $u \in U$ is called the guaranteed efficiency of control:

$$K(u) = \min_{u \in U} f_0(u, y).$$

Thus, the task of control is formulated: to find the allowable actions in the space of successful outcomes that lead to the best results, i.e. to optimal control: $K(u) \to \max$. The control model shown in this paper is the initial representation (statement) for the design of the resource system of pilot dependability. Subsequent formalization for the purpose of calculation of the properties and states of human resources in this class of tasks of the activity theory appears to be impossible using the tools of the classic set theory. The task is formalized in the pseudophysical activity model, i.e. relation between actions and outcomes of which the content is set forth in [4, 14].

4. Axiomatics of the properties of pilot resources

The diverse nature of the human properties constitutes the fundamental problem of their description and standardization for the purpose of activity standards development. The properties have similarities, differences and independence. For example, different and independent properties, e.g. professional experience, social maturity, individual's age are similar and commensurate in lifetime. The similarity of properties allows overcoming the mentioned problem by choosing a limited number of properties. The mutual similarity of properties allows using known indicator and parameter values to identify the values of unknown indicators and parameters in which the considered characteristics are examined "in isolation from all the other ones" [13, p. 348-354]. The substantiation may be in the form of theoretical postulates and axioms. For the first time this paper sets forth axioms as the premises of the new resources theory of human activity.

The logical conclusions of the suggested axioms are interrelated. The truth of the sum of conclusions is based on their consistency. The axioms are drawn from experience (empirical observation), formulated in heuristic statements, plausible judgments and conclusions. The following premises are stated as axioms of equivalence, independence and completeness of properties, parameters and indicators of pilot resources. The practical significance of the axiomatics of the pilot resources properties consists in the fact that their formalized description allows obtaining algorithms for automated and expert technologies for flight operation management.

The proposed axiomatics of the properties of a non-numerical object (human being) and complex object as formally reflected by measures of *regularity, continuity and distance.* The properties possess partial regularity Q of subset and defined as a binary relation over a set of states or a parametric set: $Q \subset V_i + V_i$ and satisfies the following requirement: reflectivity of $(x, y) \in Q$; antisymmetry when

$(x, y)\in Q$ and$(y, x)\in Q$, then $x=y$; transitivity, i.e. if $(x, y)\in Q$ and $(y, z)\in Q$, then $(x, y)\in Q$; if $(x, y)\in Q$, then x is the predecessor of y, while y is the successor of x; if $(x, y)\in Q$ and there is no $z\in Q$ such that $(y, z)\in Q$ and $(z, x)\in Q$, then x is the immediate predecessor of y, while y is the proximate successor of x; connection, i.e. for all $x, y\in V_1$ if $x\neq y$, then $(x, y)\in Q$ or $(y, x)\in Q$.

The axiomatics of properties enables the simplification of the design process and relatively simple calculations in adopted scales and units of time as shown in [11]. The system of pilot resources developed based on the described axiomatics of properties for the first time enables the acquisition of algorithms for automated and expert control systems [14].

5. Definition of resources (states) of pilot reliability

The resource of purpose is defined by the concept of dependability.

D 3. The ability to control an aircraft in a three-dimensional airspace is called the pilot's resource of purpose.

D 4. Dependability is the set of properties and states of the object within the metric of the standard activity space.

In [4, 13] dependability is structured in three forms: resources of individual dependability, resources of operational dependability, resources of professional dependability. The solution is substantiated by the single *basis*, i.e. discernibility of each group of resources in **time**.

D 5. *Individual dependability* is the sum of human evolutionary specific biological properties in the environmental conditions. Individual dependability has the meaning of specific evolution that is infinitely longer that an individual human life.

D 6. *Professional dependability* is the sum of human properties gained within a profession in the chosen professional environment. Professional dependability has the meaning of the duration of professional activity of an individual within the period roughly between 20 and 60 years.

D 7. *Operational dependability* is the sum of conditions and states of flight defined for the realization of managerial activity in the chosen purpose environment. Operational dependability is observed within the operational period of one year.

6. Conclusions

The category of purpose of activity names the object of WHAT exactly is performed as part of practical activity, while the category of dependability names HOW to observe (measure, evaluate) the object.

The next task is the detailed development of the categories of purpose and dependability in their linguistic, ontological and technical essence. The goal of linguistic analysis is to identify the objective semantics of words. The ontological task is to identify the subject area and the subject-objectivity.

The technical substance defines the terms, structure of activity and method of observation of the object. This approach constitutes the foundation of the presented method of technical modeling of pilot activity and implementation of the calculation and management design [15].

The theoretical definitions of management efficiency and guaranteed management efficiency establish the concepts of discernibility of the space of successful activity outcomes.

The theoretical foundations and deduced definitions allow developing expert systems and automated systems of prediction and prevention of flight accidents during organization and performance of air transportation operations [15] (Figure 2).

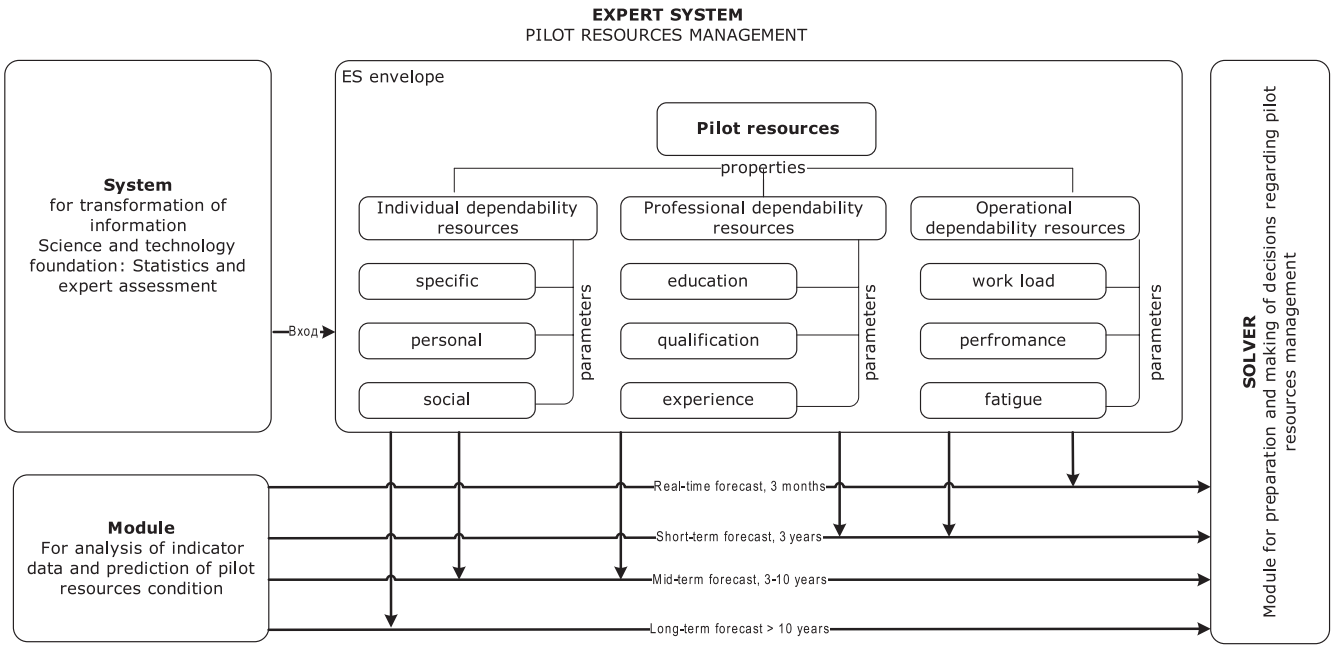


Figure 2. Pilot resources management ES

The axiomatics of pilot properties allow overcoming the fundamental difficulty of formalized description of the diverse nature of human properties and enables reliable consideration and calculation of the states for the purpose of flight operation management.

The paper sets forth the definitions of pilot purpose, pilot dependability and dependability of three different kinds, i.e. individual, professional, operational, based on a fundamental temporal base of observation.

Thus, new foundations may be developed for the activity theory and task definition of the property of activity of people of any profession may be formalized. For intense profession members the dependability category may be universal. For workers of education and science competence and qualification may be the right concepts. In professions involving physical labour that may be productivity and efficiency.

References

1. GOST R 53480-2009. Industrial product dependability. Terms and definitions. Moscow: Standartinform; 2010.

2. Golovko AM, Gurov SV. Osnovy teorii nadiozhnosti. Praktikum [Foundations of the dependability theory. A tutorial]. Saint Petersburg: PHV Peterburg; 2006 [in Russian].

3. Bodrov VA, Orlov VYa. Psikhologiya i nadezhnost': chelovek v sistemakh upravleniya tekhnikoy [Psychology and dependability: human being in control systems]. Moscow: RAS Institute of Psychology Publishing; 1998 [in Russian].

4. Plotnikov NI. Resursy pilota.Nadiozhnost. Monografia [Pilot's resources. Dependability. A monograph]. Novosibirsk: Research project center «AviaManager», CJSC; 2013 [in Russian].<http://aviam.org/images/sampledata/book/2015_prd.pdf>

5. Aviatsionnye proisshestviay, intsidenty i aviakatastrophy v SSSR i Rossii. Fakty, istoria, statistika [Aviation accidents, incidents and disasters in the USSR and Russia. Facts, history, statistics],<http://airdisaster.ru/>[in Russian].

6. Wiener EL, Kanki BG, Helmreich RL. Cockpit Resource Management. New York: Academic Press; 1993.

7. Makhutov NA, Faleev MI, Puchkov VA. Bezopasnost Rossii. Bezopasnost i zashchishchennost kriticheski vazhnykh obiektov [Security of Russia. Safety and security of critical facilities]. Vol. 2. Part 1 of 2. Moscow: MGF Znanie; 2012 [in Russian].

8. Ivanov AI, Ivaniushchenko AS, Narbut SR, Perevozchikov NI, Solovtsov NE, Cheltsov BF. Metodologicheskie osnovy ispytaniy slozhnykh sistem. Bezopasnost poletov letatelnykh apparatov pri ispytaniyakh i ucheniyakh raznorodnykh sil [Methodological foundations of complex systems testing. Flight safety of aircraft during testing and training of all-arms forces]. Moscow; 2003 [in Russian].

9. Getmanova AD. Ouchebnikpologike [Logic textbook]. 2nd edition. Moscow: Vlados; 1995 [in Russian].

10. Goncharov SS, YershovYuL, Samokhvalov KF. Vvedenie v logiku i metodologiyu naouki [Introduction into the logic and methodology of science]. Moscow: Interpraks, Novosibirsk: RAS SB Institute of Mathematics; 1994 [in Russian].

11. Lossky NO. Logika [Logic]. Obelisk; 1923 [in Russian].

12. Plotnikov NI. Osnovaniya teorii nadezhnosti cheloveka-operatora (pilota) [The bases of human operator (pilot) dependability theory]. Dependability 2015;2(53):94-97.

13. Klir G. Architecture of Systems Problem Solving. Moscow: Radio i sviaz; 1990.

14. Novikov DA. Teoriya upravleniya organizatsionnymi sistemami [Theory of management systems control]. 2nd edition. Moscow: Fizmatlit; 2007 [in Russian].

15. Plotnikov NI. Metod otsenki riskov dlya bezopasnosti poletov aviakompanii na osnove upravleniya i prognoza resursov pilota [A method for evaluating the air safety risks of air-lines based on pilot resources management and prediction]. In: Avtomatizirovannaya sis-tema prognozirovaniya i predotvrashcheniya aviatsionnykh proisshestviy pri organizatsii i proizvodstve vozdushnykh perevozok. Promezhutochny etap № 4: Adaptatsiya razrabo-tannykh algoritmov i programmnykh sredstv AS [Automated system for prediction and pre-vention of air accidents in organization and performance of air transportation. Intermediate, stage 4 Adaptation of developed AS algorithms and programs]. Science and engineering re-port, 2010-218-02-068, official registration no. 01201150118 dd 12.01.2011, identification no. 194. Ulianovsk; 2012: 154-238, 1048-1258 [in Russian]..

About the author:

Nikolay I. Plotnikov, Candidate of Engineering, Senior Researcher, Director General, Aviamanager Research Project Center, Novosibirsk, Russia, e-mail: am@aviam.org.

Received on 07.08.2017

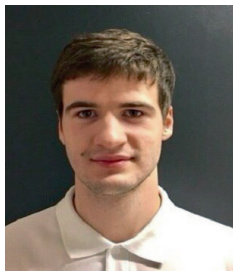
Possible ways of improving the reliability of professional psychological selection of air traffic controllers

Olga V. Arinicheva, *Flight Operation and Safety in Civilian Aviation Department, Saint Petersburg State University of Civil Aviation, Saint Petersburg, Russia*
Alina E. Gerasimenkova, *Saint Petersburg State University of Civil Aviation, Saint Petersburg, Russia*
Alexey V. Malishevsky, *Flight Operation and Safety in Civilian Aviation Department, Saint Petersburg State University of Civil Aviation, Saint Petersburg, Russia*
Mikhail G. Chepik, *Saint Petersburg State University of Civil Aviation, Saint Petersburg, Russia*


Olga V. Arinicheva


Alina E. Gerasimenkova


Alexey V. Malishevsky


Mikhail G. Chepik

Abstract.Aim. *The paper examines one of the possible ways of improving the reliability of professional psychological selection of air traffic controllers using diagnostic methods based on not subjective, but rather objective principles.* **Methods.** *The research used the following: Tobii REX fixed eye tracker and a specialized computer product developed by the All-Russian Scientific Research Institute of Radio Equipment and intended for the analysis of various aspects of eye movements in the process of exercise, as well as a range of psychodiagnostic methods: level of subjective control identification test, Buss-Durkee Hostility Inventory, MM-1 socionic test, H.J. Eysenck's intelligence test, H.J. Eysenck's personality inventory test, MMYa-1 general mode test, K. Thomas' conflict mode questionnaire and the Prognoz questionnaire for neuropsychicstability evaluation of experimental subjects. Statistical processing of the findings was done using the Bravais-Pearson correlation coefficient and Pearson's chi-squared test.* **Results.** *The experiment involved 48 third year students of the Saint Petersburg State University of Civil Aviation (SPBGU GA) majoring in Organization of Airspace Management. In terms of its psychological characteristics, the group is quite typical for this major of SPBGU GA. The results of psychodiagnostics do not correlate well with the results of this experiment, while among each other, in general, they match the theoretical assumption. The lower the neurotism which characterizes the balance of the nervous system, the better is the neuropsychicstability. The better is the neuropsychicstability, the higher the internality of any kind, especially general internality and internality for failure. People with good neuropsychicstability are also less inclined to aggressive behaviour, both in general as regards all of its kinds, and especially self-aggression. As expected, subjects with high levels of general internality turned out to be positively not inclined to such type of behaviour in conflict as "avoidance" that is the quintessence of irresponsibility. Also, people with high internality turned out to be not inclined to aggressive behaviour. The experiment exposed quite contradictory patterns of eye movement in the subjects.* **Conclusions.** *All the findings are of certain interest. Therefore, despite them being somewhat contradictory, it appears to be advisable to continue the research using the Tobii REX eye tracker. The identified shortcomings in the experiment organization allowed making corrections to the plan of further research based on the use of the Tobii REX eye tracker and aimed at improving the reliability of professional psychological selection.*

Keywords: *professional psychological selection, air traffic controller, dependability, eye tracker, neuropsychicstability, intelligence quotient, temperament.*

For citation: Arinicheva OV, Gerasimenkova AE, Malishevsky AV, Chepik MG. Possible ways of improving the reliability of professional psychological selection of air traffic controllers. Dependability 2018;18(1): 38-45. DOI: 10.21683/1729-2646-2018-18-1-38-45

Introduction. The efficiency of an air traffic management system is determined by its sophistication, dependability and reliability of technical facilities as well as organization, discipline and professional training of dispatchers and maintenance staff. The efficiency depends on the performance indicators of the components, i.e. accuracy, dependability and completeness of displayed information on the state of airspace, performed tasks, etc. [1].

The human factor is the main negative factor that reduces air traffic safety. Every year, a number of dangerous incidents related to the air traffic management (ATM) occur around the world. For example, on August 2, 2016 there was a hazardous proximity between two IndiGo airline planes in India. The planes passed so close to each other that four passengers and two flight attendants required medical aid due to the shock. As of July 10, 2016 in India alone 17 similar situations were registered in 2016, 25 in 2015, 31 in 2014 [2]. In Russia 24 incidents related to violation of the aircraft separation interval occurred in 2015 (35 such incidents occurred in 2014) [3]. Among the causes of incidents related to violations of the aircraft separation interval those related to ATM personnel are predominant. 9 incidents related to violations of aircraft separation interval occurred in the first half of the 2016 (6 incidents occurred in the same period in 2015). Seven of the incidents in 2016 were the result of ATM personnel errors, two incidents were due to aircraft crew errors. Moreover, in the first half of 2016 there were 17 cases of airborne collision avoidance systems or proximity warning systems actuations in situations not directly related to violation of separation intervals [4]. The Interstate Aviation Committee also identifies "Permission to fly and perform air traffic control (ATC) granted to flying personnel and dispatchers without the necessary experience and training" as one of the typical problems [5].

Aim of the study. There are various ways of gradually reducing the negative impact of the human factor on air traffic safety [6-9]. One of them is further improvement of the professional psychological selection (PPS) of air traffic controllers. Correct organization of aviation specialists PPS, including selection of air traffic controllers, is highly important for further improvement of flights safety. Essentially, it is the first barrier that prevents people who for various reasons are not suitable for work in aviation from joining. "PPS is a set of measures aimed at ensuring quality personnel selection based on assessing the compliance of psycho-physiological (individual) qualities and personal characteristics with the professional activity requirements" [10]. The existing PPS of pilots and ATC dispatchers [11], according to the authors of [12], has a number of major drawbacks and needs to be improved. These issues were addressed in [12, 13] and in other papers. In particular, the article [12] considered the shortcomings of such tests as the "personality questionnaire" used in aviation specialists PPS. It should be noted that tests like the "personality questionnaire" are generally not very reliable. The main problems of these tests are the possibility of falsification of answers as well as the decrease in data validity due to the respondents' attitudes or different understanding of questions [14]. Falsification of answers, which should be kept in mind when conducting certain surveys (in particular, PPS – *authors' note*), is only typical for some of the diagnostic situations. It is more complicated with the attitudes that are implemented when respondents answer the questionnaire [14]. In addition to the attitudinal factors, the reliability of the answers is significantly influenced by the respondents' intellectual appraisal of the questions (different understanding of the questions). It was shown that the ambiguity, difficulty of the questions lead to the variability of answers during a repeated survey, which indicates low *reliability*. At the same time, it appears that the questions, the answers to which remain constant in the repeated survey, often have low discriminatory power [14]. Therefore, a way of improving the reliability of ATC dispatchers PPS could be the wider use of diagnostics methods based on not subjective, but rather objective principles.

Methods. In order to explore such possibilities A.E. Gerasimenkova, I.Yu. Girenko, A.A. Dibrov, E.Yu. Lysanova and M.G. Chepik under the supervision of A.V. Malishevsky and O.V. Arinicheva conducted the following experiment using Tobii REX fixed eye tracker in November 2016. Data analysis and processing was carried out with the aid of a specialized computer product (developed by A.P. Plyasovskikh, All-Russian Scientific Research Institute of Radio Equipment) intended for the analysis of various aspects of eye movements during the exercise. The results of the experiment were partially described by the authors in [15-17].

Results and discussion. 48 third year students of the Saint Petersburg State University of Civil Aviation (SPBGU GA) majoring in Organization of Airspace Management participated in the experiment. In the first session of the exercise participants had to keep their eyes fixed on a green square that moved around the screen. In the second session the task remained the same but other squares of different colors appeared, creating distraction. It was assumed that the characteristics of attention distribution and switching in the second session would be worse. The differences in the characteristics of attention were then compared with the results of psychodiagnostics of the same sample of students.

A special computer program determined the time that the gaze was in each of the four areas of the screen. Ideally, the gaze should be fixated in each area for 25% of the total time of the exercise. Afterwards, we calculated sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (Σ_A and Σ_B), as well as the total sum (Σ_Σ) and the difference between those two sums (R_Z).

$\Sigma_\Sigma = \Sigma_B + \Sigma_A$; $R_Z = \Sigma_B - \Sigma_A$,

where: $\Sigma_A = t_{A1}^2 + t_{A2}^2 + t_{A3}^2 + t_{A4}^2$;

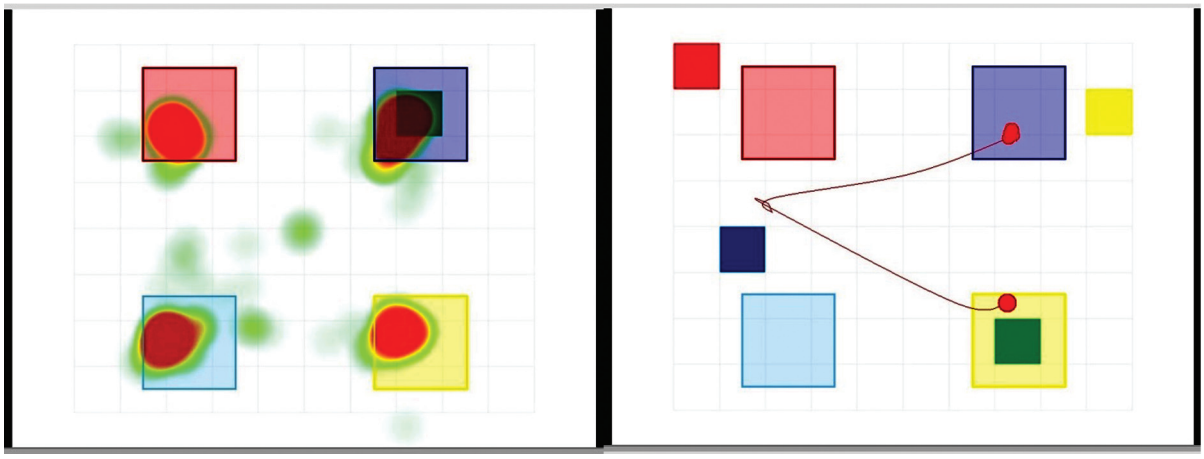
$\Sigma_B = t_{B1}^2 + t_{B2}^2 + t_{B3}^2 + t_{B4}^2$;

$t_{A1} = |25\text{-}T_{A1}|$; $t_{A2} = |25\text{-}T_{A2}|$;

$t_{A3} = |25\text{-}T_{A3}|$; $t_{A4} = |25\text{-}T_{A4}|$;

$t_{B1} = |25\text{-}T_{B1}|$; $t_{B2} = |25\text{-}T_{B2}|$;

$t_{B3} = |25\text{-}T_{B3}|$; $t_{B4} = |25\text{-}T_{B4}|$;



a) b)

Figure 1. Fragments of the subject's gaze visual display example of the subject's gaze heat map; b) example of an initially wrong gaze path (the top left position is area 1, then the numbering is clockwise).

T_{A1}, T_{A2}, T_{A3}, T_{A4} is the time spend by the gaze (%) in area 1, area 2, area 3 and area 4 accordingly (in the first session, i.e. with no distraction);

T_{B1}, T_{B2}, T_{B3}, T_{B4} is the time spend by the gaze (%) in area 1, area 2, area 3 and area 4 accordingly (in the second session, with distraction).

The gaze heat map (e.g. Fig. 1(a)) shows that the subjects fixated gaze within the given areas rather successfully. However the results were somewhat contradictory since a significant number of participants (22 of 48) performed a more difficult task more successfully. Although, the gaze path in Fig. 1(b) clearly shows that the subjects reacted to the distraction on many occasions.

In addition, 8 of the results were obviously incorrect. Possible reasons are: either the participants turned their heads, or the device was poorly calibrated for the subjects. After incorrect data was excluded, the results on the remaining 40 subjects were as shown below (Table 1). The correlations between the sum of sums of squared deviations from the ideal time spent by the gaze in each area in each session (Σ_Σ) and the sums of squared deviations in each session (Σ_A and Σ_B) are practically the same.

However, this sum of sums (Σ_Σ) practically does not depend on the deviations from the ideal time spent by the gaze in the upper areas (t_{A1}, t_{A2}, t_{B1}, t_{B2}) and very significantly depends on similar deviations in the lower areas (t_{A3}, t_{A4}, t_{B3}, t_{B4}). The correlation between the absolute value of the difference of the sums of squared deviations from the ideal time spent by the gaze in each area in each session ($|R_Z|$) and the sum of squared deviations in the first session (Σ_A) is practically non-existent, but the correlation with the sum of squared deviations in the second session (Σ_B) is very strong and very highly significant. Interestingly, the bottom left area (t_{B4}) makes the main contribution to this result. It is difficult to say what this means. It is quite possible that the correlation data is associated with the computer monitor being placed too low relative to the eyes of the subjects.

In addition to the above exercise, all subjects underwent a fairly extensive psychodiagnostic examination with the use of 8 different tests:

Table 1. Intercorrelations between results of the experiment

	Σ_Σ	$\lvert R_Z \rvert$	Σ_A	t_{A1}	t_{A2}	t_{A3}	t_{A4}	Σ_B	t_{B1}	t_{B2}	t_{B3}	t_{B4}
Σ_Σ		+0.5784	+0.9089	-0.0163	+0.1334	+0.6403	+0.5747	+0.9039	+0.0070	-0.0580	+0.6382	+0.5316
$\lvert R_Z \rvert$	$P \geq 0.999$		+0.2983	+0.0802	-0.1759	+0.1577	+0.3072	+0.7562	-0.1007	+0.0857	+0.3582	+0.6460
Σ_A	$P \geq 0.999$	$P < 0.95$		+0.0567	+0.2312	+0.7171	+0.5232	+0.6432	-0.0244	-0.1171	+0.5691	+0.2834
t_{A1}	$P < 0.95$	$P < 0.95$	$P < 0.95$		+0.2001	-0.1919	-0.2994	-0.0880	+0.3520	+0.1288	-0.1801	-0.2010
t_{A2}	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$		-0.0570	-0.2142	+0.0077	+0.3872	-0.2141	+0.0677	-0.1154
t_{A3}	$P \geq 0.999$	$P < 0.95$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$		+0.2250	+0.4402	-0.2644	-0.0459	+0.5434	+0.1563
t_{A4}	$P \geq 0.999$	$P < 0.95$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$	$P < 0.95$		+0.5186	+0.0046	+0.0879	+0.1764	+0.4682
Σ_B	$P \geq 0.999$	$P \geq 0.999$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$	$P \geq 0.99$	$P \geq 0.999$		+0.0378	+0.0137	+0.5881	+0.6854
t_{B1}	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P \geq 0.95$	$P \geq 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$		+0.2495	-0.2519	-0.3923
t_{B2}	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$		-0.1235	-0.2223
t_{B3}	$P \geq 0.999$	$P \geq 0.95$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$	$P \geq 0.999$	$P < 0.95$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$		+0.2352
t_{B4}	$P \geq 0.999$	$P \geq 0.999$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P < 0.95$	$P \geq 0.99$	$P \geq 0.999$	$P \geq 0.95$	$P < 0.95$	$P < 0.95$	

Table 2.Correlations obtained during psychodiagnostic examination in the group of participants of the experiment

First value	Second value	r_{corr}	Correlation strength	Significance of correlation	
N_{NPS}	n	+0.4923	moderate	$P \geq 0.999$	very highly significant
N_{NPS}	I_{Gen}	-0.4395	moderate	$P \geq 0.99$	highly significant
N_{NPS}	I_A	-0.3778	moderate	$P \geq 0.99$	highly significant
N_{NPS}	I_F	-0.4594	moderate	$P \geq 0.999$	very highly significant
N_{NPS}	I_{FR}	-0.4042	moderate	$P \geq 0.99$	highly significant
N_{NPS}	I_I	-0.3506	moderate	$P \geq 0.95$	significant
N_{NPS}	A_I	+0.4171	moderate	$P \geq 0.99$	highly significant
N_{NPS}	A_{Ir}	+0.3868	moderate	$P \geq 0.99$	highly significant
N_{NPS}	A_G	+0.4270	moderate	$P \geq 0.99$	highly significant
N_{NPS}	A_{Gen}	+0.4067	moderate	$P \geq 0.99$	highly significant
E	A_R	-0.3086	moderate	$P \geq 0.95$	significant
E	β_{Com}	+0.3468	moderate	$P \geq 0.95$	significant
E	$S_{E/I}$	+0.4654	moderate	$P \geq 0.999$	very highly significant
n	A_I	+0.4135	moderate	$P \geq 0.99$	highly significant
n	A_{Ir}	+0.3416	moderate	$P \geq 0.95$	significant
n	A_R	+0.3736	moderate	$P \geq 0.99$	highly significant
n	A_G	+0.4669	moderate	$P \geq 0.999$	very highly significant
I_{Gen}	β_{Av}	-0.4333	moderate	$P \geq 0.99$	highly significant
I_{Gen}	S_{LIE}	+0.3419	moderate	$P \geq 0.95$	significant
I_{Gen}	$S_{R/I}$	+0.3314	moderate	$P \geq 0.95$	significant
I_A	α_S	-0.3213	moderate	$P \geq 0.95$	significant
I_A	α_T	+0.3763	moderate	$P \geq 0.99$	highly significant
I_A	A_A	-0.3514	moderate	$P \geq 0.95$	significant
I_A	A_R	-0.3257	moderate	$P \geq 0.95$	significant
I_A	A_{Gen}	-0.3616	moderate	$P \geq 0.95$	significant
I_A	β_{Av}	-0.3457	moderate	$P \geq 0.95$	significant
I_F	A_A	-0.3018	moderate	$P \geq 0.95$	significant
I_F	A_{Ir}	-0.3436	moderate	$P \geq 0.95$	significant
I_F	A_S	-0.3246	moderate	$P \geq 0.95$	significant
I_F	A_{Gen}	-0.4214	moderate	$P \geq 0.99$	highly significant
I_F	β_{Av}	-0.3038	moderate	$P \geq 0.95$	significant
I_{FR}	A_{Gen}	-0.4144	moderate	$P \geq 0.99$	highly significant
I_P	β_{Av}	-0.4597	moderate	$P \geq 0.999$	very highly significant
I_I	A_{Gen}	-0.4772	moderate	$P \geq 0.999$	very highly significant
α_S	S_{LIE}	+0.3379	moderate	$P \geq 0.95$	significant
α_P	S_{LSE}	-0.4059	moderate	$P \geq 0.99$	highly significant
r	A_{Gen}	+0.3082	moderate	$P \geq 0.95$	significant
r	S_{LSE}	+0.4196	moderate	$P \geq 0.99$	highly significant
A_{Gen}	β_{Ac}	-0.4425	moderate	$P \geq 0.99$	highly significant

• Eysenck's Personality Inventory for temperament appraisal (E – extraversion, n – neuroticism) [14];

• the Prognoz questionnaire for neuropsychic stability (NPS) evaluation (N_{NPS} – NPS score, E_{NPS} – evaluation of NPS) [18];

• Buss-Durkee Hostility Inventory for identifying inclinations to various forms of aggressive behaviour (A_{Gen}, A_A, A_I, A_{Ir}, A_N, A_R, A_S, A_V, A_G) [14];

• level of subjective control identification test for evaluating general and specific aspects of internality (I_{Gen}, General internality; I_A, Achievement; I_F, Failure; I_{FR}, Family relations; I_P, Working relations; I_I, Interpersonal relationships; I_H, Relation to health and disease) [14];

• MMYa-1 general mode test (α_S, self-orientation; α_P, people-orientation; α_T, task-orientation; r, distance from the "ideal" point on the grid μ_2 [8]);

• K. Thomas' conflict mode questionnaire (β_{Com}, Competing; β_{Col}, Collaborating; β_{Compr}, Compromising; β_{Av}, Avoiding; β_{Ac}, Accommodating) [14];

• MM-1 socionic test [19] for determining the components of a person's socionic model S_{IEI}, S_{ESE}, S_{SEE}, S_{ESI}, S_{SEI}, S_{LSE}, S_{SLE}, S_{LSI}, S_{SLI}, S_{LII}, S_{EII}, S_{LIE}, S_{ILE}, S_{EIE}, S_{ILI}, S_{IEE}), the specific dichotomies characteristics ($S_{E/I}$, $S_{L/E}$, $S_{S/I}$, $S_{R/I}$) and integral fitness indicator by socionic criteria (ξ);

• H.J. Eysenck's intelligence test [20] (IQ – intelligence quotient).

Clear correlations (Table 2) were obtained for neuropsychic stability (N_{NPS}, neuropsychic stability in scores, the more the score the worse is the NPS evaluation (E_{NPS})). The lower the neuroticism (n), which characterizes the balance of the nervous system, the better is the NPS. The better is the NPS evaluation, the higher the internality of any kind, especially general internality (I_{Gen}) and internality for failure (I_F). People with good neuropsychic stability are inclined to show higher social responsibility. People with good NPS are also less inclined to aggressive behaviour, both in general (A_{Gen}), and especially self-aggression (A_G, guilt, remorse). This is quite important, since, having made a mistake in the work, it is necessary to think urgently about ways to correct it, and not to engage in self-reflection, which can only lead to additional errors.

As expected, subjects with high levels of general internality turned out to be positively not inclined to such type of behaviour in conflict as "avoidance" (β_{Av}) that is the quintessence of irresponsibility. Also, people with high internality turned out to be not inclined to aggressive behaviour. The highest general internality (I_{Gen}) was discovered in people with a relative predominance in their socionic model of such sociotype as logical intuitive extrovert (S_{LSE}), these people also had the highest self-orientation (α_S).

The most unfit mode of behaviour in terms of the integral indicator (r) was typical for people with a relative predominance in their socionic model of such sociotype as logical sensory extrovert (S_{LSE}).

Individuals with high extraversion (E) were more inclined to such behaviour in conflict as "competing" (β_{Com}). People with higher general aggression (A_{Gen}) were less inclined to such behaviour in conflict as "accommodating" (β_{Ac}).

Due to the fact that the results of the computer exercise in this experiment correlate with the results of psychodiagnostics rather insignificantly, the question was raised whether there is a reliable difference in a number of characteristics between the individual groups of participants.

Table 3. Distribution of psychodiagnostics results by gender

Distribution of NPS evaluations(E_{NPS}) by gender										
E_{NPS}	1	2	3	4	5	6	7	8	9	10
Females	0	0	1	3	3	5	4	3	1	1
Males	0	0	0	3	3	8	8	3	1	1

Distribution of intelligencequotient(IQ) by gender					
IQ	very low < 70	low 70-100	medium 101-110	high 111-130	very high > 130
Females	0	1	3	9	8
Males	0	5	11	6	5

Distribution oftemperament types and neuroticism (n) by gender				
Females	sanguine	phlegmatic	choleric	melancholic
	8	3	8.5	1.5
	n < 12		n > 12	
	11		10	
Males	sanguine	phlegmatic	choleric	melancholic
	18	3.5	5	0.5
	n < 12		n > 12	
	21.5		5.5	

Table 4. Comparisonofexperimentalfindingswithrespecttocriterionχ^2

Distribution of positive and negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z) by gender										
	$R_Z < 0$					$R_Z > 0$				
Females	12					9				
Males	10					17				
Distribution of the sum of sums of squared deviations from the ideal time spent by the gaze in each area in each session (Σ_Σ)by gender										
	$\Sigma_\Sigma < 10.4$		$10.4 \le \Sigma_\Sigma < 19.1$			$19.1 \le \Sigma_\Sigma < 30$			$\Sigma_\Sigma \ge 30$	
Females	4		6			5			6	
Males	8		6			7			6	
Distribution of the sum of sums of squared deviations from the ideal time spent by the gaze in each area in each session (Σ_Σ) by positive or negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z)										
	$\Sigma_\Sigma < 10.4$		$10.4 \le \Sigma_\Sigma < 19.1$			$19.1 \le \Sigma_\Sigma < 30$			$\Sigma_\Sigma \ge 30$	
$R_Z < 0$	4		5			6			7	
$R_Z > 0$	8		7			6			6	
Distribution of neuropsychic stability evaluations (E_{NPS}) by positive or negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z)										
E_{NPS}	1	2	3	4	5	6	7	8	9	10
$R_Z < 0$	0	0	1	1	3	5	8	2	1	1
$R_Z > 0$	0	0	0	5	3	8	4	4	1	1

First of all, since the sample group had almost equal number of male and female participants (27 males and 21 females), a significant difference between gender groups test was conducted. Table 3 shows the distribution of NPS evaluations (E_{NPS}), intelligence quotient (IQ) and temperament among male and female participants.

In general, all participants have NPS not lower than satisfactory, however the dispersion is quite significant, from 3 to 10. According to the SPBGU GA data the typical dispersion is from 4 to 8, large deviations are rare. 3 points is low enough. It is the minimal score that still allows the prognosis for operator activity to be favorable. There is no significant difference in NPS evaluations (E_{NPS}) of males and females by the Pearson's chi-squared test [21] ($\chi^2 = 0.7385 < \chi^2_{crit.0.95} = 5.991$ for $\nu = 2$ [21]).

The distribution of IQ it the group is quite unusual. 13 people had very high IQ. The dispersion is striking compared to the data in [22]. IQ varies from 87 (70 is considered to be the boundary for mental retardation) to 171 (A. Einstein's IQ was 160-180 (although measured indirectly, he did not actually take the test) [23]). There was significant difference in IQ level between the groups of males and females by the Pearson's chi-squared test [21] ($\chi^2_{crit.0.99} = 9.210 > \chi^2 = 7.8652 > \chi^2_{crit.0.95} = 5.991$ for $\nu = 2$ [21]). Females clearly had higher IQ than males. These results on male and female dispatchers are congruent with the data from [22, 24].

According to the SPBGU GA data the findings regarding temperament are unusual as well. The number of sanguine people is typically large, 25. However there are many choleric people as well, 12 participants (25%), which is a lot for groups of flight personnel and dispatchers. There are only 6 phlegmatic participants (12.5%), usually this percentage is a little higher. There is even one melancholic person, that is, a person with a weak type of nervous system. This type of temperament is very rare among flight personnel and dispatchers. 4 people have mixed temperaments, i.e. not one distinct type. In Table 3, mixed types were included as 0.5 of a person added to each of the 4 main types. There is a significant difference in neuroticism (n) between males and females by the Pearson's chi-squared test [21] ($\chi^2_{crit.0.99} = 3.841 > \chi^2 = 4.0114 > \chi^2_{crit.0.95} = 6.635$ for $\nu = 1$ [21]). Females clearly have higher neuroticism (larger portion of melancholic and choleric types of temperament), in other words, their nervous system is less balanced.

Another considered factor is the fact that respondents had positive (26 people) and negative (22 people) differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z). As mentioned above, it was assumed, that the characteristics of attention distribution and switching in the second session would be worse than in the first. However, a significant number of participants (22 people) performed a more difficult task better. The results of these and some other distributions are given in Table 4.

The data from Table 4 shows that although there is a significant difference in some psychodiagnostic results between the two genders, there is no such difference in the experiment results.

There is no significant difference in distribution of positive and negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z) between male and female participants (Table 4) by the Pearson's chi-squared test [21] ($\chi^2 = 2.025 < \chi^2_{crit.0.95} = 3.841$ for $\nu = 1$ [21]).

There is no significant difference in distribution of the sum of sums of squared deviations from the ideal time spend by the gaze in each area in both sessions (Σ_Σ) between male and female participants (Table 4) by the Pearson's chi-squared test [21] ($\chi^2 = 0.9312 < \chi^2_{crit.0,95} = 7,815$ for $\nu = 3$ [21]).

There is no significant difference in distribution of the sum of sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (Σ_Σ) between the groups of subjects with positive and negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z) (Table 4) by the Pearson's chi-squared test [21] ($\chi^2 = 1.6783 < \chi^2_{crit.0.95} = 7.815$ for $\nu = 3$ [21]).

There is no significant difference in neuropsychic stability evaluations (E_{NPS}) between the groups of subjects with positive and negative differences between the sums of squared deviations from the ideal time spent by the gaze in each area in both sessions (R_Z) (Table 4) by the Pearson's chi-squared test [21] ($\chi^2 = 1.2417 < \chi^2_{crit.0.95} = 5.991$ for $\nu = 2$ [21]).

Conclusions. It is well known that "the impact of psychological factors on the reliability of the operator's work is determined by such indicators as safety, timeliness, restorability, availability and psychophysiological stress" [25]. Since "safety is the ability of the operator to maintain performance for a certain time before making a mistake" [25], and the operator's restorability depends on the strength of the nervous system, i.e. on such characteristic as temperament, this experiment covered in one way or another all aspects that determine the reliability of the operator (in this case, the ATC dispatcher). All the findings are of certain interest. Despite the obtained results being somewhat contradictory, this experiment proved to be quite useful, since it also highlighted some shortcomings in the experiment organization. This allowed making corrections to the plan of further research based on the use of the Tobii REX eye tracker and aimed at improving the reliability of professional psychological selection.

References

1. Air transportation system, <http://avia.pro/blog/aviacionnaya-transportnaya-sistema>; [accessed 27.10.2017].

2. Near collision in India, <http://aviasafety.ru/10346/> [accessed 27.10.2017].

3. Analiz sostoyaniya bezopasnosti poletov v grazhdanskoy aviatsii Rossiyskoy Federatsii v 2015 godu [Analysis of the civilian air safety in the Russian Federation in 2015]. Moscow: FAVT; 2016 [in Russian].

4. Analiz sostoyaniya bezopasnosti poletov v grazhdanskoy aviatsii Rossiyskoy Federatsii v pervom polugodii 2016 goda [Analysis of the civilian air safety in the Russian Federation in the first half of 2016]. Moscow: FAVT; 2016 [in Russian].

5. Sostoyanie bezopasnosti poletov v grazhdanskoy aviatsii gosudarstv-uchastnikov soglasheniya o grazhdanskoy aviatsii i ob ispolzovanii vozdushnogo prostranstva v 2015 godu [Civilian air safety in the member nations of the agreement on civilian aviation and airspace management in 2015]. Moscow: IAC, 2016 [in Russian].

6. Arinicheva OV, Kovalenko GV, Malishevsky AV, Mikhalchevsky YuYu. Vzaimodeystvie ekipazha vozdushnogo sudna so sluzhboy upravleniya vozdushnym dvizheniem: sotsionicheskiy aspekt problemy [Interaction between the flight crew and the air traffic control service: the socionic aspect of the subject]. Herald of the Saint Petersburg State University of Civil Aviation 2016;4(13):5-16 [in Russian].

7. Malishevsky AV, Vlasov EV, Kaymakova EM. Vozmozhnye puti resheniya problemy snizheniya negativnogo vliyaniya chelovecheskogo faktora v chrezvychaynykh situatsiyakh na transporte [Possible ways of reducing the negative effect of the human factor in transportation emergencies]. Biomedical and psychosocial aspects of safety in emergency situations 2015;1:108-114 [in Russian].

8. Malishevsky AV, Arinicheva OV, Vlasov EV. Vozmozhnye puti resheniya problemy snizheniya negativnogo vliyaniya chelovecheskogo faktora na bezopasnost poliotov [Possible ways of reducing the negative effect of the human factor on flight safety]. Transport: science, equipment, management 2016;2:12-20 [in Russian].

9. Arinicheva OV, Kovalenko GV, Malishevsky AV, Mikhalchevsky YuYu. Analiz dinamicheskoy vozdushnoy obstanovki [Analysis of dynamic air environment]. Problemy liotnoy ekspluatatsii i bezopasnost poliotov [Matters of flight operation and air safety] 2016;10:85-119 [in Russian].

10. Maklakov AG. Professionalny psikhologicheskiy otbor personala [Professional psychological selection of personnel]. Teoria i praktika: ouchebnik dlia vuzov [Theory and practice: textbook for higher educational institutions]. Saint-Petersburg: Piter; 2008 [in Russian].

11. Rukovodstvo po psikhologicheskomu obespecheniyu otbora, podgotovki i professionalnoy deyatelnosti letnogo i dispetcherskogo sostava grazhdanskoy aviatsii Rossiyskoy Federatsii [Guidelines for psychological support of selection, training and professional activity of flying and control personnel of civilian aviation of the Russian Federation]. Moscow: Vozdushny transport; 2001 [in Russian].

12. Arinicheva OV, Malishevsky AV. Nedostatki sushchestvuyushchego professionalnogo otbora pilotov i problema ego sovershenstvovaniya [Disadvantages of the existing professional selection of pilots and matters of its improvement]. Transport: science, equipment, management 2016;6:41-51 [in Russian].

13. Mikhailik NF, Malishevsky AV. Kontseptsiya natsionalnoy sistemy spetsialnoy psikhologicheskoy podgotovki

letnogo sostava [Concept of a national system of special psychological training of flying personnel]. Prikladnaya psikhologia [Applied psychology] 1999;4:30-44 [in Russian].

14. Burlachuk LF. Slovar-spravochnik po psikhodiagnostike [Dictionary and handbook of psychodiagnostics]. Saint-Petersburg: Piter; 2008 [in Russian].

15. Arinicheva OV, Gerasimenkova AE, Chepik MG. Vliyanie gendernykh razlichiy v khode eksperimenta s ispolzovaniem oborudovaniya Eye Tracker Tobii REX [The effect of gender differences during an experiment involving Eye Tracker Tobii REX]. Problemy liotnoy ekspluatatsii i bezopasnost poliotov [Matters of flight operation and air safety] 2017;11:137-146 [in Russian].

16. Arinicheva OV, Gerasimenkova AE, Malishevsky AV, Mikhalchevsky YuYu, Chepik MG. Issledovanie professionalno vazhnykh kachestv dispetchera po OVD s ispolzovaniem oborudovaniya Eye Tracker Tobii REX [Research of professionally significant qualities of air traffic controllers using Eye Tracker Tobii REX]. Problemy liotnoy ekspluatatsii i bezopasnost poliotov [Matters of flight operation and air safety] 2017;11:113-120 [in Russian].

17. Gerasimenkova AE, Girenko IYu, Dibrova AA, Lysanova EYu, Chepik MG. Issledovanie professionalno vazhnykh kachestv dispetchera po OVD s ispolzovaniem psikhodiagnostiki [Research of professionally significant qualities of air traffic controllers using psychopdiagnostics]. Problemy liotnoy ekspluatatsii i bezopasnost poliotov [Matters of flight operation and air safety] 2017;11:155-163 [in Russian].

18. Prokhorov AO, editor. Praktikum po psikhologii sostoyaniy: oucheb. posob. [Tutorial on the psychology of states: a study guide]. Saint-Petersburg: Rech; 2004 [in Russian].

19. Malishevsky AV. Nekotorye voprosy sovershenstvovaniya sotsionicheskoy psikhodiagnostiki aviatsionnogo personala [Some matters regarding the improvement of socionic psychodiagnostics of aeronautical personnel]. Transport: science, equipment, management 2017;2:23-30 [in Russian].

20. Eysenck HJ. Check Your Own I.Q. Moscow: EKSMO-Press; 2003.

21. Sidorenko EV. Metody matematicheskoy obrabotki v psikhologii [Methods of mathematical processing in psychology]. Saint-Petersburg: Rech; 2007 [in Russian].

22. Arinicheva OV. Analiz diagnostiki intellektualnykh sposobnostey budushchikh aviatsionnykh spetsialistov [Analysis of intellectual abilities diagnostics of future aeronautic personnel]. Transport: science, equipment, management 2017;2:15-22 [in Russian].

23. Kakoy IQ u Alberta Eynshteyna? [What is Albert Einstein's IQ?], <http://www.bolshoyvopros.ru/questions/2092639-kakoj-iq-u-alberta-enshtejna.html>; [accessed 27.10.2017].

24. Arinicheva OV. Issledovanie intellektualnykh sposobnostey studentov universiteta grazhdanskoy aviatsii [Research of the intellectual abilities of the civilian aviation university students]. Herald of the Saint Petersburg State University of Civil Aviation 2016;4(13):38-57 [in Russian].

25. Danilov DV. Bezopasnost politov [Air safety]. Electronic study guide. Samara: Samara State Aerospace University; 2012 [in Russian].

About the authors

Olga V. Arinicheva, Candidate of Engineering, Senior Lecturer in Flight Operation and Safety in Civilian Aviation, Saint Petersburg State University of Civil Aviation, Russia, Saint Petersburg, e-mail: 2067535@mail.ru, phone: +7 905 206 75 35.

Alexey V. Malishevsky, Candidate of Engineering, Associate Professor, Senior Lecturer in Flight Operation and Safety in Civilian Aviation, Saint Petersburg State University of Civil Aviation, Russia, Saint Petersburg, e-mail: 9909395@bk.ru

Alina E. Gerasimenkova, fifth year student, Faculty of Flight Operation, Saint Petersburg State University of Civil Aviation, major in Organization of Airspace Management, Russia, Saint Petersburg, e-mail: uthfcbvtyrjdf@mail.ru

Mikhail G. Chepik, fifth year student, Faculty of Flight Operation, Saint Petersburg State University of Civil Aviation, major in Organization of Airspace Management, Russia, Saint Petersburg, e-mail: Mixagtr@gmail.com

Received on 10.11.2017

Original article
Dependability, vol. 18 no.1, 2018 DOI: 10.21683/1729-2646-2018-18-1-46-52

Design of a system with a higher safety integrity level out of components with an insufficient safety integrity level

Schäbe Hendrik, *T V Rheinland InterTraffic, Cologne, Germany*

Schäbe Hendrik

Abstract. Aim. *Technical systems are becoming more and more complex. An increasing number of technical systems contains electronic equipment and software, thus their functional safety is of utmost importance. The safety integrity level is defined by a discrete number that characterizes the set of measures against random and systematic failures depending on the specified risk reduction requirements. The concept of safety integrity levels (SIL) was developed as part of various systems of standards. While the safety architecture of a system is considered, the main question arises: how systems with higher SIL are made out of components and subsystems with low SIL. The answer to that question will allow using existing and certified components in the development of systems with specified safety integrity levels, probably with higher SIL than the SIL of the components.* **Methods.** *The paper analyzes and compares the existing rules of system combination with safety integrity levels set forth in various functional safety standards, e.g. EN 50126/8/9, ISO 26262, IEC 61508, DEF-STAN-00-56, SIRF and the Yellow Book. Beside the tolerable failure rates, the system design requirements must make provisions for combining low SIL subsystems to make higher SIL systems. The widest set of methods is defined for SIL 4 compliance. However, this set of methods cannot be reworked for all possible systems into a simple rule for the combination of systems with lower SIL into systems with higher SIL. In general, the combination of systems into a serial structure will make a system with the safety integrity level equivalent to the lowest subsystem safety integrity level. Tentatively, we can assume that by combining two subsystems with the same safety integrity level we can create a system with a safety integrity level one step higher.* **Results.** *It is shown that the general SIL allocation rule established in the DEF-STAN-00-56, the Yellow Book or the SIRF standards cannot be recommended for all countries and any situations. Failure rate and/or observation intervals must be taken into consideration. Its is proven that general rules can only be given for subsystems connected in parallel and some SIL combinations (see e.g. the Yellow Book, SIRF). In each case common failures must be taken into consideration. The general rule may be as follows: in order to achieve system SIL one level higher than the initial level, two component subsystems with the SIL one level lower must be connected in parallel. Other system architectures must be thoroughly studied.*

Keywords: *safety integrity level, combination of subsystems, allowable failure rate.*

For citation: *Sch be H. Design of a system with a higher safety integrity level out of components with an insufficient safety integrity level. Dependability 2018; 18(1): 46-52. DOI: 10.21683/1729-2646-2018-18-1-46-52*

1. Introduction

Technical systems are becoming more and more complex. An increasing number of technical systems contains electronic equipment and software, thus their functional safety is of utmost importance. The safety integrity level is defined by a discrete number that characterizes the set of measures against random and systematic failures depending on the specified risk reduction requirements. The concept of safety integrity levels (SIL) was developed as part of various systems of standards. While the safety architecture of a system is considered, the main question arises: how systems with higher SIL are made out of components and subsystems with low SIL. The answer to that question will allow using existing and certified components in the development of systems with specified safety integrity levels, probably with higher SIL than the SIL of components.

The concept of safety integrity levels is defined and used in a number of standards, such as IEC 61508 [6], DEF-STAN 0056 [1], EN 50126 [2], EN 50128 [3], EN 50129 [4] and many others (see, for example, [5, 7, 8]). In those standards are commonly defined four different safety integrity levels.

A safety integrity level is defined by the following two primary aspects:

a) Successfully managing random failures requires that the maximum tolerable hazardous failure rate of all the systems' safety functions must not be exceeded.

b) A set of measures must be in place to protect the system against systematic failures.

It should be noted that for software only systematic failures are of relevance and the identification of failure rate values is not foreseen. That is due to the fact that normal software is not supposed to have random failures.

2. Safety integrity levels

Table 1 shows four safety integrity levels and tolerable hazard rate (THR) levels as per standards [1], [4] and [6].

The tolerable hazard rate of a system is the maximum tolerable level of hazardous failures of component equipment that is defined by the safety integrity level specified for such equipment. Here we note that SIL values are identical for [4] and [6] and different for [1]. Thus, their SILs are not comparable. Even despite the fact that the THR values for [4] and [6] are identical, the provided measures of systematic failure protection are different, their SILs are not identical.

Standards [2] and [3] do not set forth any target values of hazardous failure rate. Standard [2] only requires the presence of safety integrity levels, while standard [3] is dedicated to software and describes SIL without numerical THR values. Standard [1] specifies target values of hazardous failures implicitly in the form of verbal equivalents only.

3. Combination of safety integrity levels

In this section we will describe the rules of combination of safety integrity levels (SIL) as they are used in various standards.

3.1. DEF-STAN-00-56 standard

In standard [1], the rules are given in item 7.4.4, table 8. The reader should not confuse these rules of SIL combination ([1]) with the SIL of [4], as they are different characteristics.

These rules come down to the following:

The combination of two SIL 3 devices connected in parallel results in a SIL 4 system;

The combination of two SIL 2 devices connected in parallel results in a SIL 3 system;

The combination of two SIL 1 devices connected in parallel results in a SIL 2 system;

The combination of two SIL x and SIL y devices connected in parallel results in a SIL $\max(x; y)$ system;

Note that "combination of devices connected in parallel" means that two devices or functions are combined in such a ways as only the hazardous failure of both components (or their functions) can cause a hazardous failure of the system. Out of these rules we see that the combination of two devices will at best lead to a SIL that is only one level higher than the component SILs. Additionally, a system with a certain SIL cannot be built by combining devices or functions without a SIL, at least with no application of these general SIL combination rules.

3.2. The Yellow Book

Another interesting source is the Yellow Book [10]. The Yellow Book is a British national regulation that became obsolete when common safety methods appeared. Nevertheless, it contains interesting information. In [10] SIL is defined the same way as in [4], yet the rules are quite different from those set forth in standard [1].

Table 1. Four values for different SILs and standards

SIL	IEC 61508 / EN 50129	DEF-STAN-00-56
1	10^{-6} 1/h ≤ THR < 10^{-5} 1/h	Frequent ≈ 10^{-2} 1/h
2	10^{-7} 1/h ≤ THR < 10^{-6} 1/h	Probable ≈ 10^{-4} 1/h
3	10^{-8} 1/h ≤ THR < 10^{-7} 1/h	Occasional ≈ 10^{-6} 1/h
4	10^{-9} 1/h ≤ THR < 10^{-8} 1/h	Remote ≈ 10^{-8} 1/h

Table 2. Combination of SIL rules in the Yellow Book (Table 17-2)

Upper SIL level	Lower level function SIL		Combinator (if required)
	Main	Other	
SIL 4	SIL 4 SIL 4 SIL 3	no SIL 2 SIL 3	no SIL 4 SIL 4
SIL 3	SIL 3 SIL 3 SIL 2	no SIL 1 SIL 2	no SIL 3 SIL 3
SIL 2	SIL 2 SIL 1	no SIL 1	no SIL 2
SIL 1	SIL 1	no	no

3.3. GOST R IEC 61508

Standard [6] does not have a good rule of SIL combination as in the previously mentioned ones. Nevertheless, this standard enables the improvement of the safety integrity level through the combination of lower SILs of subsystems. The general rule is as follows (see IEC 61508-2, item 7.4.4.2.4): "Selecting the channel with the highest safety integrity level that has been achieved and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of elements". Here *N* is the number of allowable hazardous faults for the system of elements combined in parallel, i.e. the number of hazardous faults that allowed for the system. It should be noted that in order to achieve a certain system safety integrity level by means of component combination, the requirements for the number of allowed hazardous faults and proportion of right-side failures of elements must be met in accordance with the table of IEC 61508-2. Type A/B elements/systems should be distinguished (IEC 61508-2, item, 7.4.4.1.2).

An element can be regarded as type A if for the components required to achieve the safety function the following conditions are fulfilled:

a) the failure modes of all constituent components are well defined;

b) the behaviour of the element under fault conditions can be completely determined;

c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

Other elements/systems are type B. The rules for achieving required SILs for systems of type A and type B per IEC 615008-2-2 are given in Tables 3 and 4 respectively.

Tables 3 and 4 clearly show that standard [6] does not provide a simple rule for SIL combination. Not only the subsystem combination solutions and the number of allowed hazardous faults define a system's safety integrity level, but the proportion of right-side failures as well. However it can be observed that as the number of allowable hazardous faults and the proportion of right-side failures of an element is maintained in cases when same type (A

Table 3. Rules for achieving required SIL in type A systems

Percentage of an element's right-side failures	Number of hazardous faults allowed for a system		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% -< 90%	SIL 2	SIL 3	SIL 4
90% -< 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Table 4. Rules for achieving required SIL in type B systems

Percentage of an element's right-side failures	Number of hazardous faults allowed for a system		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% -< 90%	SIL 1	SIL 2	SIL 3
90% -< 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

or B) subsystems are used, the SIL increases by one. That means that if there are two same-SIL subsystems with the same proportion of right-side failures of an element, their combination will increase the SIL by one level. A combination of subsystems with different types and/or different proportions of right-side failures of an element may yield different results and in such cases additional analysis may be required.

3.4. SIRF 400

The SIRF standard [9] is the German standard of the methods of railway rolling stock safety jointly developed by the German railway industry, Deutsche Bahn, German railway operators society and German federal railway administration. This document can be referenced in Germany, while outside of Germany this standard my not be recognized.

The document describes the following principles. If two subsystems are connected in series (e.g. with an IF gate in the fault tree) the lowest SIL will also be the resultant SIL of such system.

00	01
10	11

Figure 1. Allowable combinations for SIL 1 (per standard [9])

00	01	02
10	11	12
20	21	22

Figure 2. Allowable combinations for SIL 2 (per standard [9])

00	01	02	03
10	11	12	13
20	21	22	23
30	31	32	33

Figure 3. Allowable combinations for SIL 3 (per standard [9])

00	01	02	03	04
10	11	12	13	14
20	21	22	23	24
30	31	32	33	34
40	41	42	43	44

Figure 4. Allowable combinations for SIL 4 (per standard [9])

For combinations of parallel systems the following rules are set forth:

a) systems with SIL > 0 must not be made out of elements with SIL 0;

b) SIL can be decreased only by one level for the AND gate in the fault tree;

c) exception out of (b): one branch assumes all the safety functions;

d) exception out of (b): common failure analysis is performed;

e) in case of (d) the appropriate method (FMEA, HAZOP, etc.) must be used down to the lowest level of the fault tree in order to show that common failures are impossible.

Note that the SIRF standard uses the term "SAS" that is generally equivalent to SIL, but is not completely identical. Figures 1 to 4 show the allowed and forbidden combinations. The green color shows allowed combinations, the red shows the forbidden combinations, while the yellow means that subsystem independence is to be established only based on deep analysis. Figures 1 to 4 show the SIL combinations allowed per [9].

While neglecting the combination of two independent SIL 2 subsystems for achieving a SIL 4 system, we can see that primarily the combination of two same-SIL subsystems will result in a system with the SIL one level higher.

3.5. Numerical approach

In this section we will perform calculations using only hazard rates, i.e. tolerable hazard rates that are to be ensured by means of combination of homogeneous subsystems. Possible measures of prevention of systematic failures are not taken into consideration.

The analysis is based on the following assumptions:

1) a comparator is not required;

2) T is the test interval. During the inspection all failures and defects are identified and eliminated that will make a subsystem as good as new;

3) the system consists of two subsystems that are connected in parallel and have identical SILs;

4) it is required to create a subsystem with a SIL one level higher than that of the component subsystems.

The hazard rate of the combined system is roughly identified as follows

$$\lambda=\lambda_1\cdot\lambda_2\cdot T,$$

where λ_1 is failure rate of the first system, 1/h;

$\lambda_2$is failure rate of the second system, 1/h;

T is the observation period, h.

Table 5. SIL and tolerable hazard rates of subsystems and whole system for the observation period of 10000 hours

System		Subsystems		
SIL	**Rate value**	**Required rate value**	**SIL**	**Rate value**
4	10^{-8} 1/h	10^{-10} 1/h	3	10^{-7} 1/h
3	10^{-7} 1/h	10^{-8} 1/h	2	10^{-6} 1/h
2	10^{-6} 1/h	10^{-6} 1/h	1	10^{-5} 1/h

Table 5 below contains the results for the time period T = 10000 h, i.e. about a year.

We can see that for all three cases (SIL 2...4 for systems) the subsystems will comply with the requirements (target level) if the subsystems have the SIL one step lower that the target SIL of the system. However, this calculation must be complimented with the common failure analysis. To that effect, we will use [6]. Despite the fact that [4] shows another approach in 3.2, we will use [6] due to the simple fact that it provides numerical values. In the worst case, beta, i.e. common failure ratio, will be 10%. That is the part of the failure rate that is to be used for describing common failures. Later, in the process of identification of hazardous failure rate of the combined system, common failures will dominate. If now each subsystem has the SIL n, the hazardous fault rate of the combined system will be 10% of $10^{-(n+4)}$1/h, i.e. will be equal to $10^{-(n+5)}$1/h.

Thus, the combined system can have the SIL of (n+1) at best. It should be concluded that without special assumptions on common failures the system's safety can be increased by one level by combining two subsystems with the same SIL.

3.6. Brief summary of SIL combination methods

Beside the tolerable failure rates, the system design requirements must make provisions for combining low SIL subsystems to make higher SIL systems. Standard [1], in its item 7.3.3 states: "Design rules and techniques appropriate to each Safety Integrity Level... shall be determined prior to implementation...". There are no specific rules.

Standards [6] (part 2, annex A3, annex B) and [4] (annex E) set forth different methods for different SILs. The widest set of methods is defined for SIL 4 compliance. However, this set of methods cannot be reworked for all possible systems into a simple rule for combining systems with lower SIL into systems with higher SIL. However, the general rule seems to be that a system's SIL can be improved one level by combining two subsystems with a lower SIL.

4. Examples

Example 1

The system consists of two subsystems and does not contain software. A comparator is not required. Each subsystem verifies the differences between itself and the other subsystem and disables the other subsystem in case of discrepancies. That means that a shutdown of the whole system is a safe situation. Figure 5 shows the block diagram of the system of example 1.

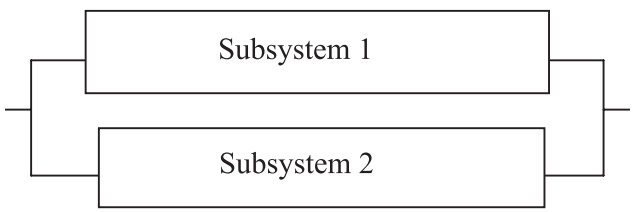


Figure 5. Block diagram of the system of example 1

If the safety integrity level of both subsystems is SIL 3 and they are independent, they can be combined into a SIL 4 system. The design rules for SIL 3 and SIL 4 systems differ insignificantly. If a system is to be SIL 2, it suffices to combine two SIL 1 subsystems. If both subsystems are SIL 2 and the system is to be SIL 3, the system is to be studied more thoroughly. The design rules for a SIL 3 system differ from those used for SIL 2 systems.

Example 2

The system is largely identical to that of example 1, yet both subsystems are managed by common software (see figure 6).

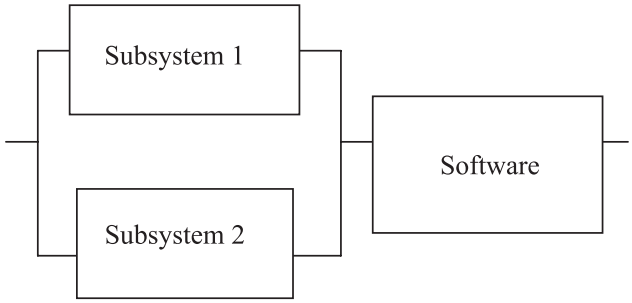


Figure 6. Block diagram of the system of example 2

If a system is to be SIL 4, the software is to be SIL 4 as well. (The SIL of the software must be at least as high as the system's). SIL 2 systems can be made of two parallel SIL 1 systems with SIL 2 software. If a system is to be SIL 3, the software is to be SIL 3 as well. If the hardware is SIL 2, in order to achieve the system's SIL 3 additional considerations must be given, as in example 1.

Example 3

This system is similar to the system of example 1, yet it contains diverse software. Figure 7 shows the block diagram of the system of example 3.

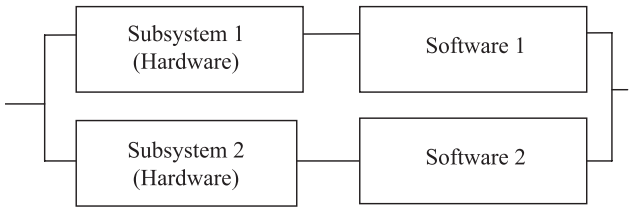


Figure 7. Block diagram of the system of example 3

Both subsystems use diverse software. SIL distribution follows the same considerations as in example 1. A system's SIL 4 can be ensured by two SIL 3 subsystems each with SIL 3 software. SIL 2 systems can be made of

two SIL 1 subsystems. In order to make a SIL 3 system out of two SIL 2 subsystems, additional considerations must be given.

Example 4

The system consists of one hardware channel, but the software is redundant (Figure 8). The software "redundancy" can be created using two different software packages or redundant programming methods (diverse software). In any case software diversity must be ensured.

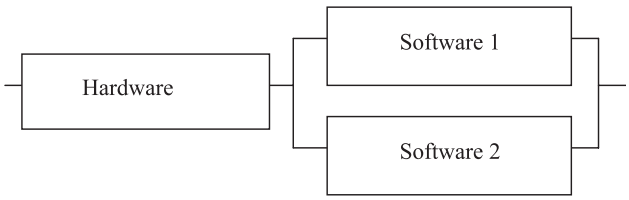


Figure 8. Block diagram of the system of example 4

Let us assume the system must be SIL 4. In this case, the hardware must also have SIL 4, while both versions of software must be designed at least per SIL 3. Additionally, it must be proven that each hardware failure is detected by software, i.e. at least two versions of software have been designed and that facilities are in place to initiate system safe state. If a system is to be SIL 2, the hardware must be SIL 2 and two versions of software each designed at least per SIL 1. A system's SIL 3 can be ensured if the hardware is SIL 3 and each version of the software is SIL 2. However, the feasibility must be thoroughly examined. The matter of independence of software versions operating within the same hardware is not trivial. In any case software must be diverse.

Example 5

In this example we are considering an electronic subsystem consisting of hardware, software and other system equipment operating in parallel (hardware bypass) (Figure 9).

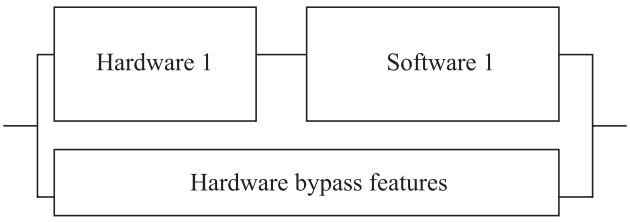


Figure 9. Block diagram of the system of example 5

If the hardware bypass facilities have the SIL required for the system, no SIL requirements should be imposed on hardware 1 and software 1. Additionally, the same logic as in example 1 can be used: SIL 4 of a system can be achieved through the SIL 3 of the subsystems (hardware 1 and software 1 on one side and SIL 3 of the hardware bypass features on the other side). Software 1 must have the SIL not lower that the SIL of hardware 1.

5. Conclusion

The general SIL allocation rule established in the DEF-STAN-00-56, the Yellow Book or the SIRF standards cannot be recommended for all countries and any situations. Failure rate and/or observation intervals must be taken into consideration. General rules can only be given for subsystems connected in parallel and some SIL combinations (see e.g. the Yellow Book, SIRF). In each case common failures must be taken into consideration. The general rule may be as follows: in order to achieve system SIL one level higher than the initial level, two component subsystems with the SIL one level lower must be connected in parallel. Other system architectures must be thoroughly studied. A good indicator of the compliance of the chosen system architecture with the target SIL is the fulfillment of the condition that the required system's failure rate per the SIL does not exceed the failure rate value calculated based on the failure rate of the component subsystems. Normally, combining subsystems into series a system is created that has the safety integrity level equivalent to the lowest SIL of the component subsystems.

6. References

1. DEF-STAN 0056 (1996) Safety management requirements for defence systems. Part 1: General requirements. Part 2: Guidelines. Issue 2, 13.2.1996.

2. EN 50126 – GOST R IEC 62278 Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS); 2008.

3. EN 50128 – STB IEC 62279 Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems; 2011.

4. EN 50129 – STB IEC 62425 Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling; 2011.

5. Gräfling S, Schäbe H. The agri-motive safety performance integrity level – Or how do you call it? In: proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012. Helsinki (Finland): Curran Associates, Inc.; 2012. p. 6091-6100.

6. IEC 61508 (2010) Functional safety of electrical, electronic, programmable electronic safety-related systems. Parts 1-7; 2010.

7. Schäbe H. Definition of Safety Integrity Levels and the Influence Assumptions, Methods and Principles Used. In: Spitzer C, Schmocker U, Dang VN, editors. Proceedings of the International Conference on Probabilistic Safety Assessment and Management PSAM 7 / ESREL 2004. Berlin (Germany): Springer-Verlag London Ltd; 2004. p. 1020-1025.

8. Schäbe H, Jansen H. Computer architectures and safety integrity level apportionment. In: Sciutto G, editor. Safety and Security in Railway Engineering. WIT Press; 2010. p. 19-28.

9. SIRF (2011), Vehicle safety policy, version 1,1.6.2011.

10. Engineering Safety Management (The Yellow Book), Volumes 1 and 2. Fundamentals and Guidance, issue 4. 2007.

Note: the Yellow Book has been replaced with the CS-MREA application guide.

About the author:

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

Received on 28.11.2017

Original article
Dependability, vol. 18 no.1, 2018 DOI: 10.21683/1729-2646-2018-18-1-53-60

Functional dependency between the number of wagons derailed due to wagon or track defects and the traffic factors[1]

Aleksey M. Zamyshliaev, *JSC NIIAS, Moscow, Russia*
Aleksey N. Ignatov, *Moscow Aviation Institute, Moscow, Russia*
Andrey I. Kibzun, *Moscow Aviation Institute, Moscow, Russia*
Evgeni O. Novozhilov, *JSC NIIAS, Moscow, Russia*


Aleksey M. Zamyshliaev


Aleksey N. Ignatov


Andrey I. Kibzun


Evgeni O. Novozhilov

Aim. *Rolling stock derailment is one of the most hazardous transportation incidents. Depending on the gravity of the consequences they may also be classified as accidents or train wrecks. The consequences of a derailment may vary from routine maintenance of the track and one or two wagons to an overhaul of the track and depot repairs of three or more wagons, as well as loss of cargo and long interruption of service. It must be noted that beside the damage to infrastructure and rolling stock caused by derailments there is a risk of environmental disaster. The Russian Federation along with the US, China and India has some of the world's longest rail networks that in places border with environmentally sensitive areas, e.g. national reserves and parks. Therefore, if a train carries hazardous cargo, e.g. gasoline or toxic gases and some of its wagons derailed, the harm related to the repair or decommissioning of rolling stock, track and possible loss of cargo may be aggravated by the damage caused by an environmental disaster that would cause great material losses to JSC RZD. In this context it appears to be of relevance to evaluate the functional dependency between the potential number of cars derailed and various factors, e.g. speed or amount of cargo carried by the train, for subsequent preparation of recommendations for the reduction of the potential number of derailed cars and, subsequently, reduction of possible harm.* **Methods.** *Probability theory and mathematical statistics methods were used, i.e. maximum likelihood method, negative binomial regression.* **Results.***For various groups of incidents, i.e. derailment as the result of wagon or locomotive unit malfunction out of switch, derailment as the result of rail malfunction out of switch, derailment at a switch not caused by previous derailment, specific functions of the average number of derailed wagons are identified. The paper shows a formula that allows – under a defined set of various factors, e.g. train speed, plan and profile of track, length and mass of the train – identifying the distribution series of the number of derailed wagons.* **Conclusions.** *The preliminary analysis of available Russian freight train derailment records it was shown that for various groups of transportation incidents the descriptive statistics of respective samples significantly differ, which is also the case for the US records. The construction of a functional dependence between the average number of derailed wagons and various traffic factors due to malfunction of wagons or locomotive units out of switches, it was identified that the available records do not suffice to forecast the number of derailed wagons in tangents. Mathematical models with a low superdispersion parameter were constructed for derailments due to track malfunction out of switches and derailments at switches.*

Keywords: *derailment, train wreck, traffic factors, maximum likelihood method, negative binomial regression.*

For citation*: Zamyshliaev AM, Ignatov AN, Kibzun AI, Novozhilov EO.Functional dependency between the number of wagons derailed due to wagon or track defects and the traffic factors. Dependability 2018;18(1): 53-60. DOI: 10.21683/1729-2646-2018-18-1-53-60*

[1] The deliverables were obtained as part of the performance of public assignment of the Ministry of Education of Russia no. 2.2461.2017/PCh and with the support of the Russian Foundation for Basic Research and JSC RZD within the framework of research project no. 17-20-03050 ofi_m_RZD

1. Introduction

The analysis of the factors that cause the most severe consequences of wagon derailments in train operations is based on the research of transportation incident records. For the period between 2013 and 2016 there are 262 records of derailment of freight wagons and passenger cars that occurred in the Russian Federation, not counting the records of transportation incidents classified as train wrecks. In the context of the railways of the US and India mentioned above out of [1, 2] follows that 2493 derailments occurred in the US in 2015 and 2016, while in India during the 2010-2011 and 2014-2015 periods 293 derailment took place, data for China is classified. It appears to be logical to use US records for the purpose of analysis, as it was done, for example, in the evaluation of damage caused by transportation incidents in [3], or Indian records. However, while the records of transportation incidents in the US and Russia are practically identical, differences exist. Russian records contain information on the presence or absence of switch at the location of derailment, plan and profile of track. We believe those factors bear upon not only the derailment itself, but the gravity of the consequences as well. There is no publicly available detailed information on the transportation incidents in India. Therefore American or Indian records cannot be used and the analysis will be based on Russian data only.

While researching the numbers of derailed wagons a confidence interval can be constructed for the potential number of derailed wagons of the distribution law of the number of derailed wagons can be deduced. However, those characteristics will be insufficient, as they will be identical for trains of both 3 wagons and 63 wagons. Therefore, the functional dependence between the number of derailed wagons and various factors must be identified. In [4], among the factors that have an effect on the consequences of derailments, the following ones are set forth: speed at the moment of derailment, remaining length (total number of wagons starting from the first derailed one), presence of additional locomotives in the middle/tail, proportion of loaded wagons. However, information of the curve radius and presence of gradient at the location of derailment was not taken into consideration. In [5] the level of derailment (level of hazard) was evaluated that depends on the class of track, tonnage handled, presence of signalling systems (e.g. train detection). The resulting dependence is integral in its nature and does not enable the reduction of the risk of derailment for individual trains. In [6] a similar task was researched that was related to finding the functional dependence between the probability of derailment and length of the train, number of kilometers travelled and class of track. However, the track geometry was not taken into consideration either. In this context the dependences proposed in [4-6] must be specified and clarified subject to the task under consideration in order to enable the development of practical recommendations.

The examination of Russian wagon derailment records has shown that some of them are not completely filled, i.e. there is the problem of missed data. Some values are missed both for the speed at the moment of derailment and the number of wagons in the trainset. As it is very difficult to recover those parameters, these observations were excluded from further analysis. Besides that, some derailments occurred not due to technical causes (track condition, bogie condition), but rather weather conditions or human factor that cannot be expressed in the nominal scale, hence such observations were not considered either. Consequently, various functional dependences in this paper were constructed based on 172 observations. Samples with and without missed data were compared as well.

2. Preliminary data analysis

First, let us construct a frequency diagram and find the descriptive statistics of the number of derailed cars.

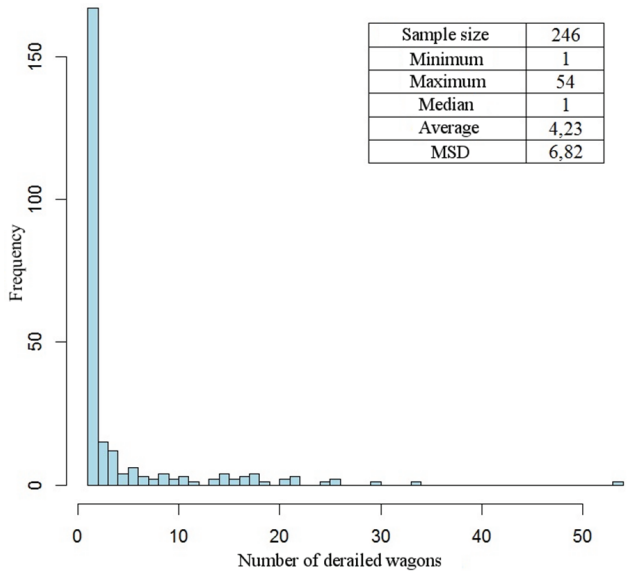


Figure 1. Frequency diagram and descriptive statistics of the number of derailed cars in case of freight train derailments and crashes

As we can see in figure 1, in most cases one wagon derails, while the average number of derailed wagons is about 4, while MSD is about 1.5 of the sample average. Therefore, it is important to find the functional dependence between the number of derailed wagons and the values of associated factors in order to reduce the severity of the consequences of derailments.

The descriptive statistics of the number of derailed wagons differ depending on the cause of derailment and the presence or absence of switch at the location of derailment.

So further analysis will be made for the three groups of accidents individually: derailment as the result of wagon or locomotive unit malfunction out of switch, derailment as the result of rail malfunction out of switch, derailment on a switch not caused by previous derailment due to track

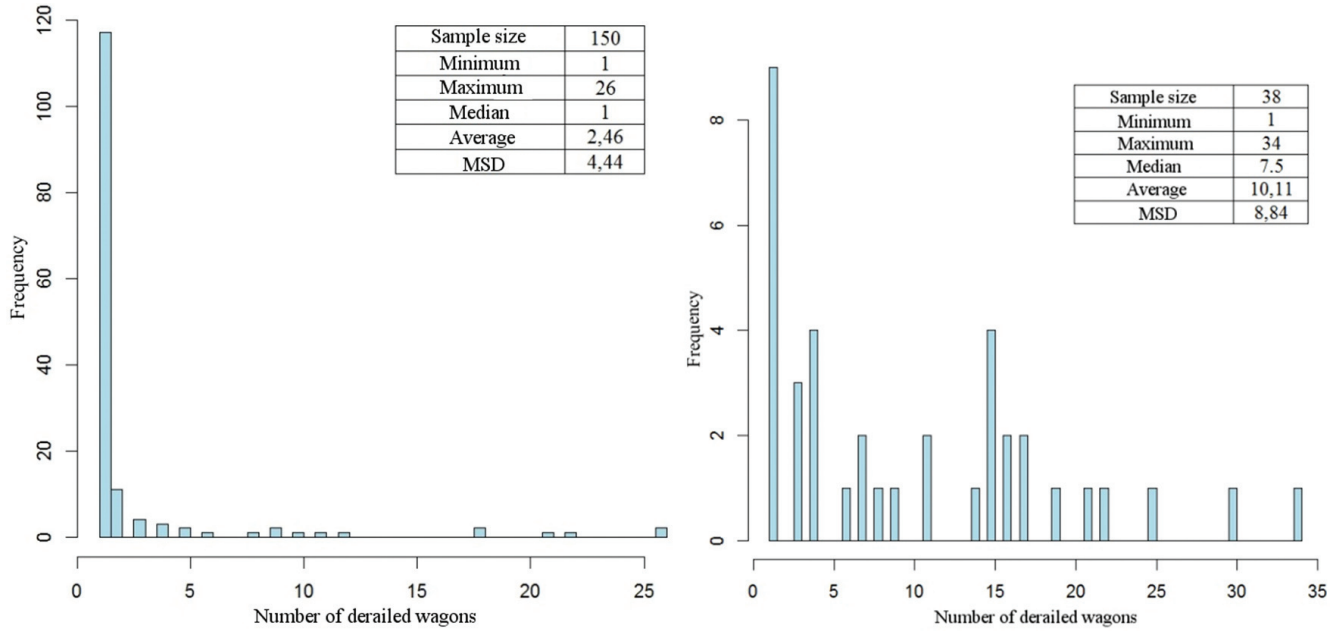


Figure 2. Frequency diagram and descriptive statistics of the number of derailed wagons in case of freight train derailments out of switches caused by wagon or locomotive unit (*left*) malfunction and track malfunction (*right*)

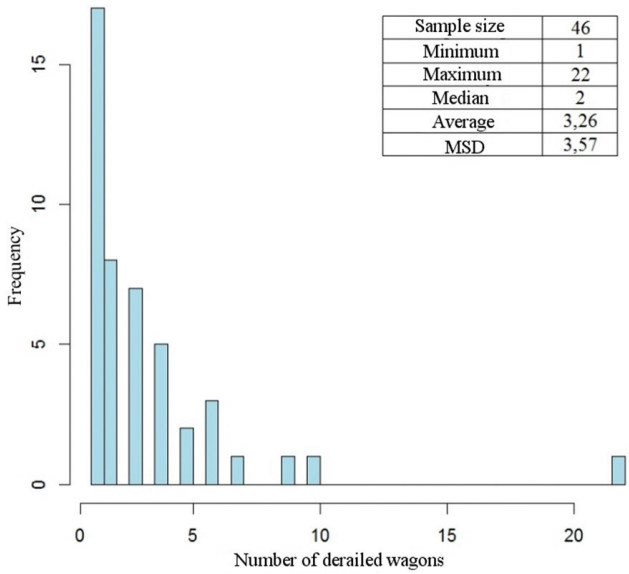


Figure 3. Frequency diagram and descriptive statistics of the number of derailed cars in case of freight train derailments at switches not caused by previous derailments, due to track or wagons/locomotive units malfunction

or wagon/locomotive unit malfunction. Note that within the time period under consideration 4 derailments occurred on switches as the result of a derailed wagon caused other wagons to derail after hitting the switch. These cases are classified separately, because derailed units do not always cause further derailments due to contact with s switch.

3. Primary designations

In the j-th group of incidents out of n_j transportation incident records involving freight train wagons derailment during train operation let us examine a certain i-th record. Let

c_{ij} be the total number of derailed units of rolling stock (locomotive sections and wagons);

k_{ij} bethe counting number of the unit (from the head of the train) that was the first to derail;

v_{ij} be the speed of the train at the moment of derailment, km/h;

l_{ij} be the number of wagons in the train;

l_{ij}^L be the total number of locomotive units in the train;

w_{ij} be the weight of the train, t;

$æ_{ij}$ be the rate of curve (value inversely proportional to the curve radius) at the place of derailment (for tangents the rate of curve is taken to be equal to zero);

γ_{ij} be the track profile at the place of derailment measured in promille having the minus sign if the gradient is downward and plus sign if the gradient is upward.

Let us also introduce an auxiliary variable $c^{\max}=l^L+l-k+1$, that is the realization of certain random value $C^{\max}=l^L+l-K+1$, where K is the random value that characterizes the number of the first derailed unit. Further, we will call random value $C^{\max}$ the remaining length of the train. Note that there is a statistical relation between the number of the derailed wagons and the remaining length of the train [4, 7-8]. Let us introduce another auxiliary variable (function) $\tilde{\mu}(w,l)$ that characterizes the loading factor (per [4]) of the train that depends on the train weight w and the number l of the transported wagons that is calculated using formula

$$\tilde{\mu}(w,l) \stackrel{def}{=} \pi_1 \frac{w}{l} + \pi_2, \qquad (1)$$

where π_1 and π_2 are unknown parameters. Consequently, the closer the function $\tilde{\mu}(w,l)$ is to zero, the higher is the number of empty wagons in the trainset. And vice versa, the closer the function $\tilde{\mu}(w,l)$ is to one, the lower is the number of empty and higher is the number of loaded

wagons in the trainset. As the tare of a four-axle wagon is about 23 tons and the carrying capacity is around 69 tons, the coefficients π_1 and π_2 can be found by solving a system of linear equations

$$\begin{cases} 23\pi_1 + \pi_2 = 0, \\ (23+69)\pi_1 + \pi_2 = 1. \end{cases} \quad (2)$$

By solving system (2) we obtain π_1=1/69, π_2=–1/3. By substituting the obtained π_1 and π_2 into (1) we obtain

$$\tilde{\mu}(w,l) = \frac{w}{69l} - \frac{1}{3},$$

By setting $\tilde{\mu}_{ij} \overset{\text{def}}{=} \tilde{\mu}(w_{ij}, l_{ij})$ we will obtain the train's weight ratio at the *i*-th derailment in the *j*-th group of incidents. Note that in the US incident records the number of loaded wagons is given explicitly, while in the Russian records there is not such characteristic, hence the ratio of loaded-to-total number of wagons has to be estimated.

In some records one or another characteristic may be missing or given inexplicitly which causes the problem of missed data. The missed values are often averaged out of the available ones, but in the context of the task at hand this approach cannot be used, as each transportation incident is unique and their number is not large. For that reason for each group of incidents we will further compare samples with missed values and complete sets of required characteristics.

4. Problem definition and method of solution

Let us examine the *j*-th group of transportation incidents, the total number of which within the period under consideration is n_j. Let C_j be a random value that characterizes the number of wagons and locomotive units that will derail as part of a group of incidents. As a derailment will inevitably involve not less than one unit of rolling stock, the following equality has place

$$C_j = 1 + \tilde{C}_j,$$

where $\tilde{C}_j$ is an auxiliary non-negative random value, of which the distribution law we will estimate later that has values in the set Z_+. Note that the distribution series of random values C_j and $\tilde{C}_j$ depend on the set of parameters $w, l, \tilde{\mu}(w,l), æ, \gamma$ and the realization $c^{\max}$ of random value $C^{\max}$, while the realizations $\tilde{c}_{ij}$ of random value $\tilde{C}_j$ can be obtained from formula $\tilde{c}_{ij} = c_{ij} - 1$.

As random value $\tilde{C}_j$ is discrete, we cannot use the linear regression tools in the evaluation of the functional dependence between this random value and parameters $c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma$. Ordinal regression is partially similar to linear regression for an integral-valued dependent variable, yet in our case it cannot be used either, as not for all numbers out of the range of sample realization values there are derailments with identical numbers of derailed wagons.

Quantile regression [9] is another method of finding the desired dependence. However, due to the small number of observations at the level of dependability of, for example, α=0,999 and with 40 observations quantile regression does not appear to be usable. For that reason we will use the maximum likelihood method and negative binomial regression, namely we will assume conditional distribution $\tilde{C}_j$ to be common-negative binomial distribution with parameters r_j and p_j.

Let us recall the formulas for negative binomial regression for the case under consideration [10-11]

$$\begin{cases} P\{\tilde{C}_j = \tilde{c} \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma\} = \\ \quad = \dfrac{\Gamma(\tilde{c} + r_j)}{\Gamma(\tilde{c}+1)\Gamma(r)} p_j^{\tilde{c}} (1-p_j)^{r_j}, \\ \mathbf{M}[\tilde{C}_j \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma] = \dfrac{p_j r_j}{1-p_j}, \\ \mathbf{D}[\tilde{C}_j \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma] = \dfrac{p_j r_j}{(1-p_j)^2}. \end{cases} \quad (3)$$

Let

$$\mathbf{M}[\tilde{C}_j \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma] = \\ = f_j(a_{1j}, a_{2j}, \ldots, a_{m_j j}, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma), \quad (4)$$

$$\mathbf{D}[\tilde{C}_j \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma] = \\ = f_j(a_{1j}, a_{2j}, \ldots, a_{m_j j}, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma)(1 + \\ + \theta_j f_j(a_{1j}, a_{2j}, \ldots, a_{m_j j}, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma)). \quad (5)$$

where $f_j(a_{1j}, a_{2j}, \ldots, a_{m_j j}, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma)$ is a function that is normally the exponential transformation of the linear function based on the parameters of function $a_{1j}, a_{2j}, \ldots, a_{m_j j}$ to be defined; parameter $\theta_j > 0$ characterizes the superdispersion and is also to be defined.

By substituting (4) – (5) into (3) and introducing for convenience the additional designation $a_j \overset{\text{def}}{=} (a_{1j}, a_{2j}, \ldots, a_{m_j j})^{\mathrm{T}}$, we obtain

$$p_j = \frac{\theta_j f_j(a_j, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma)}{1 + \theta_j f_j(a_j, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma)}, \; r_j = \frac{1}{\theta_j}.$$

Thus

$$P\{\tilde{C}_j = \tilde{c}_{ij} \mid C^{\max} = c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma\} = \\ = \frac{\Gamma(\tilde{c}_{ij} + 1/\theta_j)}{\Gamma(\tilde{c}_{ij}+1)\Gamma(1/\theta_j)} (\theta_j f_j(a_j, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma))^{\tilde{c}_{ij}} \times \\ \times (1 + \theta_j f_j(a_j, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma))^{-(\tilde{c}_{ij} + 1/\theta_j)}.$$

Let us construct the log-likelihood function

$$\overline{L}_j(a_j,\theta_j,\tilde{c}_{ij},c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij},i=\overline{1,n_j}) =$$
$$= \ln\left(\prod_{i=1}^{n_j} P\{\tilde{C}_j=\tilde{c}_{ij}\mid c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij}\}\right) =$$
$$= -n_j\ln(\Gamma(1/\theta_j)) + \sum_{i=1}^{n_j}(\ln(\Gamma(\tilde{c}_{ij}+1/\theta_j)) +$$
$$+\tilde{c}_{ij}\ln(\theta_j f_j(a_j,c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij})) -$$
$$-(\tilde{c}_{ij}+1/\theta_j)\ln(1+\theta_j f_j(a_j,c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij})) -$$
$$-\ln(\Gamma(\tilde{c}_{ij}+1))).$$

Let us set the problem of finding the unknown vector a_j and parameter θ_j

$$(\theta_j^*,a_j^*)^{\mathrm{T}} =$$
$$= \arg\max_{a_j\in R^{m_j},\theta>0} \overline{L}_j(a_j,\theta_j,\tilde{c}_{ij},c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij},i=\overline{1,n_j}). \quad (6)$$

Note that the quality of the constructed model (selection of function $f_j(\cdot)$) is characterized by not only the optimal value of the log-likelihood function $\overline{L}_j(a_j^*,\theta_j^*,\tilde{c}_{ij},c_{ij}^{\max},w_{ij},l_{ij},\tilde{\mu}_{ij},æ_{ij},\gamma_{ij},i=\overline{1,n_j})$, but the value of parameter θ_j^* as well. The closerparameter θ_j^* is to zero, the better is the constructed model, as the dispersion of random value $\tilde{C}_j$ is linear in parameter θ.

5. Solution of the problem

First, let us describe the general principles of selection of functions $f_j(\cdot)$. According to [9] functions should be selected with exponentials of a certain function linear in the evaluated regression parameter. According to [4] the selected factors that accompany a transportation incident are the logarithms of movement speed and remaining train length, loading factor, as well as their various combinations. Now let us consider each group of transportation incident individually.

5.1. Derailment due to wagon or locomotive unit malfunction out of switch

For this group of traffic incidents let us select function $f_1(\cdot)$ as follows

$$f_1(a_1,c^{\max},w,l,\tilde{\mu}(w,l),æ,\gamma) = f_1(a_1,c^{\max},\tilde{\mu}(w,l),æ,\gamma) =$$
$$= \chi_{æ\neq 0}\exp\{a_{11}+a_{21}æ\ln(v)+a_{31}(1-\tilde{\mu})\ln(c^{\max})\ln(v)\cdot$$
$$\cdot\min(0,\gamma)+a_{41}(1-\tilde{\mu})\ln(c^{\max})+a_{51}(1-\tilde{\mu})^2\ln(c^{\max})\ln(v)\cdot$$
$$\cdot\min(0,\gamma)+a_{61}\tilde{\mu}+a_{71}\chi_{\gamma>0}\tilde{\mu}\ln(c^{\max})\ln(v)\}+$$
$$+\chi_{æ=0}\exp\{a_{81}+a_{91}\chi_{\gamma<0}\ln(c^{\max})\ln(v)+a_{101}\chi_{\gamma>0}\tilde{\mu}\ln(v)\ln^2(c^{\max})\},$$

where χ_A is the characteristic (indicator) function of a certain event A i.e.

$$\chi_A \overset{\text{def}}{=} \begin{cases} 0, & x\notin A,\\ 1, & x\in A.\end{cases}$$

Let us comment the choice of function $f_1(\cdot)$. The function splits into two summands: the first one characterizes the gravity of consequences of derailment in curves ($\chi_{æ\neq 0}$), while the second characterizes the gravity of consequences of derailment in tangents ($\chi_{æ=0}$).

In the part related to the derailments in curves three groups of summands can be identified: the first group contains the summands with parameters a_{11} and a_{21} that are invariant by the train load, the second group contains the summands with parameters a_{31}, a_{41}, a_{51} of which the effect increases with the reduction of train load, the third group contains the summands with parameters a_{61}, a_{71} of which the effect increases with the growth of train load. The severity of the consequences for loaded trains is increased by the presence of upward gradient, while for empty trains it is increased by not only the presence, but also the degree of downward gradient. The common trait of all the groups of summands is the fact that almost every summand there is either a logarithm of movement speed, or a logarithm of maximum number of derailed wagons, or sometimes their product. That is due to the fact that as the speed and maximum number of derailed wagons grows, a higher number of wagons are supposed to derail.

In the part related to derailments in tangents the summand with parameter a_{91} is not zero in case of movement along downward gradients, the summand with parameter a_{101} is not zero in case of movement along upward gradients. Derailments with serious consequences (more than 15 derailed wagons) happened not in steep downward or upward gradients, hence only the presence of a gradient rather than its degree is used.

By solving problem (6) we obtain the following estimates of maximum likelihood a_{11}^*, a_{21}^*, …, a_{101}^*, θ_1^*.

Note that in case of upward gradient in curves all the summands except the constant in function $f_1(\cdot)$ are non-negative under the obtained values of parameters a_{21}^*, …, a_{101}^*. Therefore, any increase of parameters $c^{\max}, v, \tilde{\mu}(w,l), æ$ causes a higher average number of derailed wagons, which corresponds with the physics of derailment. In case of downward gradient in curves there is a non-positive summand with parameter a_{61}^*. That is, among other things, due to the fact that in case of low train load $\tilde{\mu} < 0{,}13587$ the sample average number of derailed trains was 4.54 wagons, while the sample average was 1.38 wagons in case of $\tilde{\mu} \geq 0{,}13587$. This assumption is confirmed by the suggested model as

Table 1. Estimation of maximum likelihood a_{11}^*, a_{21}^*, …, a_{101}^*, θ_1^* based on sample with derailments in curves and tangents

a_{11}^*	a_{21}^*	a_{31}^*	a_{41}^*	a_{51}^*	a_{61}^*	a_{71}^*	a_{81}^*	a_{91}^*	a_{101}^*	θ_1^*
-7.76	315.69	286.88	0.63	-333.03	4.32	0.17	-1.55	0.2	0.04	3.83

Table 2. Estimation of maximum likelihood a^*_{11}, a^*_{21}, …, a^*_{101}, θ^*_1 based on sample with derailments only in curves (65 observations)

a^*_{11}	a^*_{21}	a^*_{31}	a^*_{41}	a^*_{51}	a^*_{61}	a^*_{71}	a^*_{81}	a^*_{91}	a^*_{101}	θ^*_1
-7.25	307.22	284.43	0.54	-329.86	3.85	0.16	–	–	–	1.87

Table 3. Estimation of maximum likelihood a^*_{11}, a^*_{21}, …, a^*_{101}, θ^*_1 based on sample with derailments only in angents (35 observations)

a^*_{11}	a^*_{21}	a^*_{31}	a^*_{41}	a^*_{51}	a^*_{61}	a^*_{71}	a^*_{81}	a^*_{91}	a^*_{101}	θ^*_1
–	–	–	–	–	–	–	-1.52	0.2	0.04	6.05

$$\frac{\partial f_1(a_1^*, c^{\max}, \tilde{\mu}(w,l), æ, \gamma)}{\partial \gamma} =$$

$$= f_1(a_1, c^{\max}, \tilde{\mu}(w,l), æ, \gamma)(a_{31}^*(1-\tilde{\mu})\ln(v)\ln(c^{\max}) +$$

$$+a_{51}^*(1-\tilde{\mu})^2 \ln(v)\ln(c^{\max})) < 0 \Leftrightarrow a_{31}^* + a_{51}^*(1-\tilde{\mu}) < 0 \Leftrightarrow$$

$$\Leftrightarrow 1-\tilde{\mu} < -\frac{a_{31}^*}{a_{51}} \Leftrightarrow \tilde{\mu} > 1+\frac{a_{31}^*}{a_{51}} = 0{,}13587.$$

Note that records regarding derailments in tangents are insufficient, as if we examine the samples on the derailments in tangents and curves separately, the results will be as follows.

By comparing the results in tables 1, 2 and 3 we conclude that joint consideration of derailments in curves and tangents somewhat alters the predicted average number of derailed wagons in curves, while leaving the average number of derailed wagons in tangents practically unchanged. At the same time the dispersion that is characterized by parameter θ^*_1 changes significantly. Therefore, derailments in curves and tangents should be separated from each other.

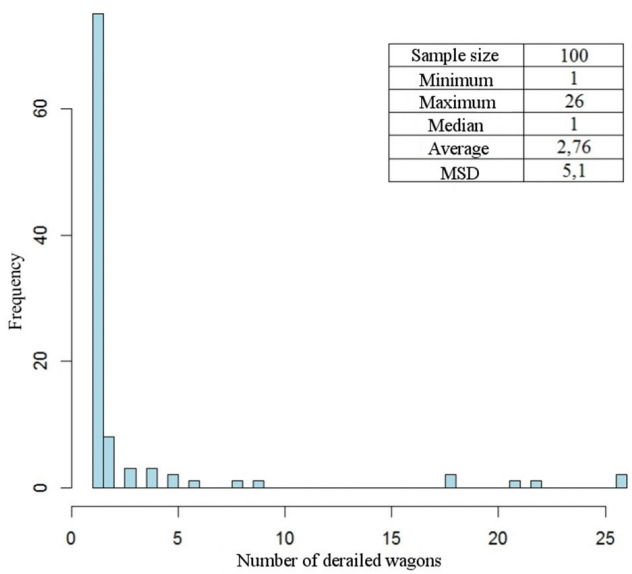


Figure 4. Frequency diagram and descriptive statistics of the number of derailed wagons in case of freight train derailments out of switches caused by wagon or locomotive unit malfunction according to a sample with no missed data

Additionally, during data processing it turned out that the sample average of the number of derailed wagons in tangents is higher than the sample average of the derailed wagons in curves (3.74 versus 2.23 wagons). Therefore, additional research is required both in terms of the depth of research (increased number of considered records) and in terms of the quality of considered records, namely the clarification of information on the causes of the occurred accidents and track characteristics in the location of derailment, especially in tangents.

A detailed example of the resultant formulas is given in [12].

In this section, the analysis was based on a sample with the following characteristics.

5.2. Derailment due to track malfunction out of switch

For this group of traffic incidents let us select function $f_2(\cdot)$ as follows

$$f_2(a_2, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma) = f_2(a_2, c^{\max}, \tilde{\mu}(w,l), æ, \gamma) =$$

$$= \exp\{a_{12} + a_{22}\tilde{\mu} + a_{32}\ln(v) + a_{42}\ln(c^{\max})\}.$$

The principle of function $f_2(\cdot)$ construction is similar to the one of function $f_1(\cdot)$. This function is also similar to the one suggested for the estimation of the average number of derailed wagons due to track malfunction in [4]. Additionally, in function $f_2(\cdot)$ unlike in $f_1(\cdot)$ the is no parameter γ. That is due to the fact that out of 38 incidents caused by track malfunction in 11 cases it was impossible to identify the gradient value. Parameter æ is also absent as it was used in the identification of the model with the best log-likelihood function value.

By solving problem (6) we obtain the following estimates of maximum likelihood a_{12}, a_{22}, a_{32}, a_{42}, θ^*_2.

Table 4. Estimated maximum likelihood a^*_{12}, a^*_{22}, a^*_{32}, a^*_{42}, θ^*_2

a^*_{12}	a^*_{22}	a^*_{32}	a^*_{42}	θ^*_2
-6.4	1.01	0.68	1.48	0.3

All the summands of function $f_2(\cdot)$ turn out to be positive and therefore any increase in the traffic parameters will cause a higher average number of derailed wagons, which is logical.

In this section, the analysis was based on a sample with the following characteristics.

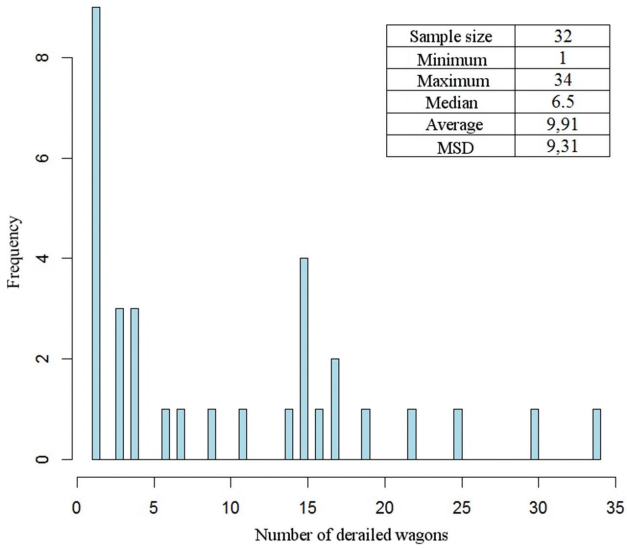


Figure 5. Frequency diagram and descriptive statistics of the number of derailed wagons in case of freight train derailments out of switches caused by track malfunction according to a sample with no missed data

5.3. Derailment at a switch not caused by prior derailment

For this group of traffic incidents let us select function $f_3(\cdot)$ as follows

$$f_3(a_3, c^{\max}, w, l, \tilde{\mu}(w,l), æ, \gamma) = f_3(a_3, c^{\max}, \tilde{\mu}(w,l), æ, \gamma) = \exp\{a_{13} + a_{23}\tilde{\mu}\ln(v) + a_{33}\tilde{\mu}\ln^2(c^{\max}) + a_{43}\ln(v) + a_{53}\ln(v)\ln(c^{\max})\}.$$

Note that in this case function $f_3(\cdot)$ does not contain variables γ and æ, as it is extremely difficult or sometimes even impossible to identify them for incidents that occurred at switches.

By solving problem (6) we obtain the following estimates of maximum likelihood a_{13}, a_{23}, …, a_{53}, θ^*_3.

Table 5. Estimated maximum likelihood a^*_{13}, a^*_{23}, …, a^*_{53}, θ^*_3

a^*_{13}	a^*_{23}	a^*_{33}	a^*_{43}	a^*_{53}	θ^*_3
-1.49	0.99	-0.16	-0.91	0.43	0.41

In this section the analysis was based on a sample with the following characteristics.

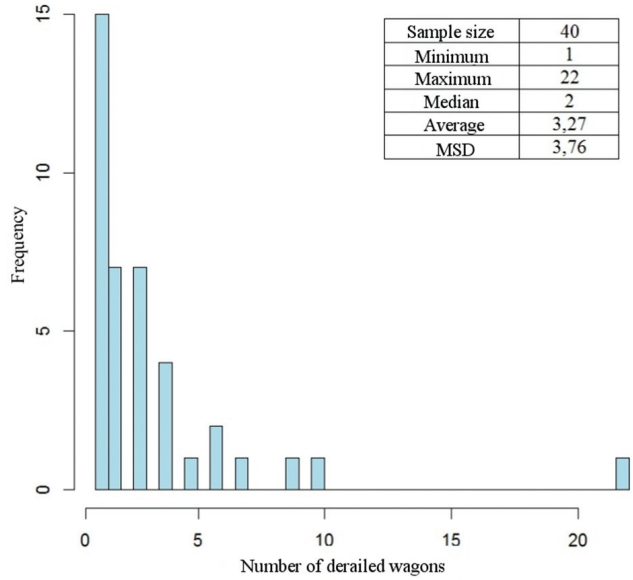


Figure 6. Frequency diagram and descriptive statistics of the number of derailed cars in case of freight train derailments at switches not caused by previous derailments

6. Conclusion

This paper shows a functional dependency between the average number of derailed wagons and various traffic factors: train speed, plan and profile of track, length and mass of the train. Various groups of transportation accidents are defined: derailment as the result of wagon or locomotive unit malfunction out of switch, derailment as the result of rail malfunction out of switch, derailment on a switch not caused by previous derailment. Based on the maximum likelihood method and negative binomial regression, functions of average number of derailed wagons are defined. The paper shows a formula that allows – under a defined set of various factors, e.g. train speed, plan and profile of track, length and mass of the train – identifying the distribution series of the number of derailed wagons. The results of the research can later be used in the evaluation of the risk of freight train derailment throughout the Russian rail network.

References

1. <http://safetydata.fra.dot.gov/>
2. <http://www.indianrailways.gov.in/>
3. Goriainov AV, Zamyshliaev AM, Platonov EN. Analysis of effects of factors on the damage caused by accidents in transportation using regression models. Dependability 2013;2:126-144.
4. Liu X, Saat MR, Qin X, Barkan CPL. Analysis of U.S. freight-train derailment severity using zero-truncated negative binomial regression and quantile regression. Accident Analysis and Prevention 2013;59:87-93.
5. Liu X, RapikSaat M, Barkan CPL. Freight-train derailment rates for railroad safety and risk analysis. Accident Analysis and Prevention 2017;98:1-9.

6. Anderson RT, Barkan CPL. Derailment probability analysis and modeling of mainline freight trains. In: Proceedings of the 8-th International Heavy Haul Conference, Rio de Janeiro (Brazil): International Heavy Haul Association; 2005. p. 491–497.

7. Bagheri M, Saccomanno F, Chenouri S, Fu LP. Reducing the threat ofin-transit derailments involving dangerous goods through effective placement along the train consist. Accident Analysis and Prevention 2011;43:613–620.

8. Saccomanno FF, El-Hage S. Minimizing derailments of railcars carrying dangerous commodities through effective marshaling strategies. Transportation Research Record 1989;1245:34–51.

9. Koenker R, Hallock KF. Quantile Regression. Journal of Economic Perspectives 2001; 15(4):143-156.

10. DeGroot MH, Schervish MJ. Probability and Statistics. 4th ed. Addison-Wesley; 2012.

11. Cameron AC, Trivedi PK. Essentials of Count Data Regression in A Companion to Theoretical Econometrics. Baltagi BH, editor. Blackwell Publishing Ltd; 2003.

12. Zamyshliaev AM, Ignatov AN et al. Ob otsenkekolichestvavagonov v skhodepripoezdnoyrabotenaosnovefaktornykhmodeley [On the evaluation of the number of derailed wagons in operation based on factor models]. In: Proceedings of the Sixth Science and Engineering Conference Intelligent Control Systems in Railway Transportation. Computer and mathematical modeling. ISUZHT 2017. 2017. p. 132-135.

About the authors

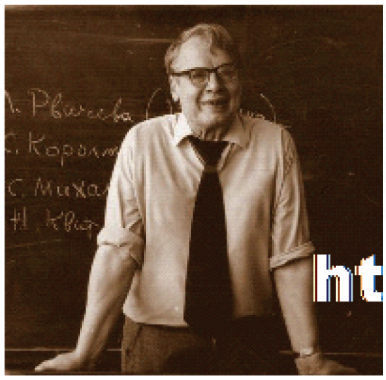
Aleksey M.Zamyshliaev, Doctor of Engineering, Deputy Director General, JSC NIIAS, Moscow, Russia, phone: +7 495 967 77 02, e-mail: A.Zamyshlaev@gismps.ru

Aleksey N. Ignatov, Moscow Aviation Institute, postgraduate student, Moscow, Russia, phone: +7 906 059 50 00, alexei.ignatov1@gmail.com

Andrey I. Kibzun, Doctor of Physics and Mathematics, Professor, Moscow Aviation Institute, Head of Chair, Moscow, Russia, phone: +7 499 158 45 60, e-mail: kibzun@mail.ru

Evgeny O. Novozhilov, Candidate of Engineering, Head of Unit, JSC NIIAS, Moscow, Russia, phone: +7 495 967 77 02, e-mail: eo.novozhilov@vniias.ru.

Received on 16.10.2017



Gnedenko e-Forum

International Group on Reliability

http://Gnedenko-Forum.org/

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc.

Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications".

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.

Join Gnedenko Forum!

Welcome!

More than 500 experts from 44 countries worldwide have already joined us!

To join the Forum, send a photo and a short CV to the following address:

Alexander Bochkov, PhD

a.bochkov@gmail.com

Membership is free.

REQUIREMENTS OF EDITION ON EXECUTION OF PAPERS IN JOURNALS OF PUBLISHING GROUP OF IDT PUBLISHERS

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 109029, Moscow, Str. Nizhegorodskaya, 27, Building 1, office 209, LLC "JOURNAL DEPENDABILITY" or e-mail: E.Patrikeeva@gismps.ru (in scanned form).

The letter should be attached to a paper text containing the summary and keywords, information on authors, bibliographic list, and one complete set of figures. All listed items are to be presented in an electronic form (on CD or via the e-mail address provided above).

Attention! Titles of papers, names of authors, summary and keywords must be presented, in Russian and English languages, according to the requirements of the Higher Attestation Commission. The information on each author should contain the following standard data:

- Surname, name, patronymic;
- Scientific degree, academic status, honorary title;
- Membership of relevant public unions, etc.;
- Place of employment, position;
- The list and numbers of Journals of IDT Publishers in which papers of the author have been previously published;
- Contact information.

Texts should be presented in Word 97-2003 format in a 12-point typeface; the text should not be formatted. Paragraphs should be arranged by pressing the "return" key. The text of the paper should be double-spaced on pages of A4; on the left there should be a margin of 2 cm; pages should be numbered, the «first line indent» is obligatory.

All alphabetical designations represented in figures should be explained in the body text or in a legend.

Inconsistencies between designations in figures and in the text are inadmissible. Numbering should only be applied to those formulas and equations that are referred to in the text.

Simple formulas appearing directly in the text (for example, m^2, n^2t, $c = 1 + DDF - A_2$), and the Greek letters and symbols, for example, β, © may be typed using the Symbol font. When it is not possible to type directly in the text editor, use the "Microsoft Equation" formula editor (available with the complete installation of Microsoft Office) or the "Mathtype" formula-editing program. Representation of formulae in the text in the form of images is not admissible. Photos and figures for papers should be provided in individual files with extension TIF, EPS or JPG with a resolution of not less than 300 dpi. The list of literature referred to in the paper (bibliography) is presented according to order of citation and provided at the end of paper. References to the literature in the text are marked by serial numerals in square brackets.

To authors that are published in journals of "IDT Publishers".

In addition to the journal, information on each author will be presented at the techizdat.ru site in the «Authors» section on the individual web page.

Authors of papers for publication have the opportunity to send an electronic photo and additional material to appear on this individualised Internet-business card. At their own discretion, authors can present more details about themselves, interesting examples and stories of solutions to technical problems, about contemporary problems according to subjects of corresponding journal, etc. This material should not exceed 1000 characters including spaces.

SUBSCRIPTION TO THE JOURNAL «DEPENDABILITY»

It is possible to subscribe to the journal:

- Through the agency «Rospechat»
  – for the first half of the year: an index 81733;

- Under the catalogue "Press of Russia" of the agency «Books-services»:
  – for half a year: an index 11804;

- Through the editorial office:
  – for any time-frame
  tel.: 8-916-105-81-31; e-mail: evgenya.patrikeeva@yandex.ru

SUBSCRIBER APPLICATION FOR DEPENDABILITY JOURNAL

Please subscribe us for 20___
from No. _____ to No._____ number of copies _____

Company name	
Name, job title of company head	
Phone/fax, e-mail of company head	
Mail address (address, postcode, country)	
Legal address (address, postcode, country)	
VAT	
Account	
Bank	
Account number	
S.W.I.F.T.	
Contact person: Name, job title	
Phone/fax, e-mail	

Publisher details: Dependability Journal Ltd.
Address of the editorial office: office 209, bldg 1, 27 Nizhegorodskaya Str., Moscow 109029, Russia Phone/fax: 007 (495) 967-77-02, e-mail: evgenya.patrikeeva@yandex.ru
VAT 7709868505 Account 890-0055-006
Account No. 40702810100430000017
Account No. 30101810100000000787

Address of delivery:

To whom:_____

Where:_____

_____

To subscribe for Dependability journal, please fill in the application form and send it by fax or email.
In case of any questions related to subscription, please contact us.
Cost of year subscription is 4180 rubles, including 18 per cent VAT.
The journal is published four times a year.

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