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

Structural dependability. Theory and practice

Dolgopolov B.A., Zayko Yu.G., Mikhaylov V.A. A method of identifying the durability indicator of microcircuitry 3

Ankudinov A.V., Antonov A.V., Chepurko V.A. A research of the characteristics of the Kijima-Sumita processes under an increasing rate function 7

Mikhailov V.S. Plan of tests with addition 12

Functional safety and survivability. Theory and practice

Schäbe H. Autonomous Driving – How to Apply Safety Principles 21

Tararychkin I.A. Progressive damage to structural elements of pipeline systems and efficiency assessment of protection measures 34

Risk management. Theory and practice

Shubinsky I.B., Zamyshliaev A.M., Ignatov A.N., Kibzun A.I., Novozhilov E.O. Method of identification of the ranges of (non)acceptable factor values to reduce the risk of freight car derailment due to broken bogie solebar 40

Dolganov A.I. On the reliability of investment risk assessments 47

Gnedenko Forum 53

Original article
Dependability, vol. 19 no. 3, 2019 DOI: 10.21683/1729-2646-2019-19-3-3-6

A method of identifying the durability indicator of microcircuitry

Boris. A. Dolgopolov, *RC Module, Russian Federation, Moscow*
Yuri G. Zayko, *RC Module, Russian Federation, Moscow*
Viktor A. Mikhaylov, *RC Module, Russian Federation, Moscow*

Boris. A. Dolgopolov

Yuri G. Zayko

Viktor A. Mikhaylov

Abstract. *The Aim of this paper is to ensure the compliance of the requirements for the durability of long-life space technology with the fact that regulatory documents for microcircuitry do not contain durability indicators. Thus, in accordance with OST V 11 0998-99, the dependability requirements only contain indicators of reliability and storability. On the other hand, along with the requirements for reliability and storability, the dependability specifications for space technology feature requirements for durability in operation that are usually equal to the gamma-percentile life $T_{l.r}$ = 100 000 h and more if r = 99.9%. Therefore, for such long-life systems one must define durability indicators that are now absent in the technical conditions or other delivery documents. The definition of such indicators by means of durability testing is costly and time-consuming. Thus, an analytical method was proposed, according to which the lower estimate boundary for the gamma-percentile life $T_{l.r}$ of microcircuitry can be obtained by equalizing the probability of no-failure of the microcircuit over time $T_{l.r}$ to the probability of non-occurrence of life failures that put the microcircuit into the limit state, upon which its operation shall be terminated. In this case, in order to obtain $T_{l.r\ =\ 99.9\%}$ = 100 000 h, a non-redundant microcircuit or another product must have the failure rate of 10^{-8} 1/h. In the case of more complex microcircuits, it does not appear to be possible to obtain the required value of $T_{l.r=99.9\%}$ = 100 000 h. The paper suggests extending the use of the proposed method of durability indicator identification taking into consideration the fact that in the systems under consideration the failure of any one product is not allowed and, in this view, various ways of ensuring equipment redundancy are used. Hot standby is understood as a redundancy with one or several backup modules that operate similarly to the main module. Warm standby is understood as a redundancy with one or several modules that operate at a lower rate that the main module until they start functioning as the main module. The paper considers a number of redundancy architectures of a complex microcircuit that enable the specified high durability indicators. The formula was obtained for calculation of the durability indicator for more general cases, when the microcircuit is part of a module backed-up by another identical module. In this case, if the second module is in warm standby, a high durability indicator can be ensured for the microcircuit. If the second module is in hot standby, the specified durability indicator of the microcircuit is not ensured. The considered method of durability indicator identification can be used for other redundancy architectures of modules in a system.*

Keywords: *durability, gamma-percentile life, redundancy, hot standby, warm standby.*

For citation: *Dolgopolov BA, Zayko YuG, Mikhaylov VA. A method of identifying the durability indicator of microcircuitry. Dependability 2019; 3: 3-6 p. DOI: 10.21683/1729-2646-2019-19-3-3-6*

Introduction

In accordance with GOST 27.006-2015 [1], durability is a property of an item, which consists in its ability to perform the required functions in the specified modes and conditions of use, maintenance and repair until the limit state is reached, in which its further operation is unacceptable or impractical, or its recovery is impossible or impractical.

One of the durability indicators of electric components (EC) is the operating life, defined as the total operating time of EC from the beginning of its operation or its resumption after repair until the limit state is reached. The life during which the EC does not reach the limit state with probability r, expressed as a percentage, is called the gamma-percentile life $T_{l.r}$.

In technical specifications, the durability indicator of EC has the form of minimum operating time $T_{o.min}$, which according to OST 4.012.013-84 [2] equals to the corresponding gamma-percentile indicator $T_{l.r}$ if r = 99.9%

$T_{o.min} = T_{l.r}$ if r = 99.9%.

However, in accordance with OST V 11 0998-99 [3], the dependability requirements do not contain indicators of durability. Therefore, there is usually no data on durability in the specifications for newly developed microcircuitry. It should be noted that there is also no durability characteristics in the technical documentation for EC of foreign manufacture [4]. In many practical cases the $T_{l.r}$ estimation of EC must be obtained if the $T_{o.min}$ or $T_{l.r}$ are absent in the corresponding technical documentation or specifications.

Estimation of operating life $T_{l.r}$

The failures of EC used in modern radio electronic equipment usually form the simplest failure flow. For such EC, operation life failures that put EC into the limit state are more typical than degradation failures that are caused by the natural process of aging, wear, corrosion, and fatigue, provided that the operation process is stabilized (the causes of all structural, manufacturing, and operational failures have been eliminated).

EC life failure shall imply the EC failure during time $T_{l.r}$ from the start of operation, the probability $R_{l.f}(t = T_{l.r})$ of which does not exceed a given value (1–γ/100). Then, the time $T_{l.r}$ is defined by the formula

$$R_{l.f}\left(t = T_{l.\gamma}\right) = 1 - e^{-\lambda_o \cdot T_{l.\gamma}} \le \frac{\gamma}{100},$$

or, using the probability of no failure (PNF) of EC, by the formula

$$R_n\left(t = T_{l.\gamma}\right) = 1 - e^{-\lambda_o \cdot T_{l.\gamma}} \ge \frac{\gamma}{100}, \quad (1)$$

where $R_n(t = T_{l.r})$ is the PNF of a non-redundant EC within time t;

λ_o is the operational failure rate (FR) for EC, defined in the handbook [5] or provided by the supplier/manufacturer;

γ is the probability of non-occurrence of life failure.

$T_{l.r}$ for a non-redundant EC derived from the formula (1) is

$$T_{l.\gamma} \ge \frac{-\ln\frac{\gamma}{100}}{\lambda_o}. \quad (2)$$

Experience has shown, that even when using all possible ways to improve reliability, the FR of modern complex digital microcircuitry often exceeds $\lambda_o > 0.03 \cdot 10^{-6}$ 1/h, which, in accordance with formula (2), means the value of the durability index $T_{l.r} < 33333$ h if γ = 99.9%.

However, modern space systems often require the values of $T_{r.r} \ge 100000$ h. In order to ensure such high durability indicators when using modern complex microcircuitry in systems, various redundancy methods have to be considered.

Taking into account the microcircuitry redundancy options

Hot standby is understood as a redundancy with one or several backup modules that operate similarly to the main module. Warm standby is understood as a redundancy with one or several modules that operate at a lower rate than the main module until they start functioning as the main module. Thus, when warm standby is used as a redundancy for microcircuitry, PNF is defined by formula [6]

$$R_{red(w)}(t) = e^{-\lambda_o \cdot t}\left[1 + \frac{1}{\alpha}\left(1 - e^{-\alpha\lambda_o t}\right)\right], \quad (3)$$

where λ_o is the FR of a microcircuit in operational mode;

$\alpha = \lambda_o/\lambda_s$ is the storage factor of a microcircuit in warm standby mode, where λ_s is the FR of a microcircuit in warm standby mode.

Then, in order to achieve a given value of $T_{l.r}$, the following relation should be satisfied

$$R_{red}\left(t = T_{l.\gamma}\right) \ge \frac{\gamma}{100}. \quad (4)$$

Consider the following example:

$\lambda_o = 0.3 \cdot 10^{-6}$ 1/h;

$\alpha = 0.012$;

$T_{l.r(req)} = 100000$ h;

γ = 99.9%.

Then, out the relation (3) at $t = T_{l.r(req)} = 100000$ h we obtain

$R_{red(w)}(t = 100000\text{ h}) = 0.9996 \ge 0.999$,

which corresponds to inequation (4).

When hot standby is used as a redundancy for microcircuitry, PNF is defined by the formula

$$R_{red(n)}(t) = 1 - \left(1 - e^{-\lambda_o \cdot t}\right)^2. \quad (5)$$

Using the example in question, from this formula we obtain

$R_{red(h)}(t = 100000\text{ h}) = 0.9991 \ge 0.999$,

which also corresponds to inequation (4).

Table 1. Calculated values of the PNF of a redundant integrated circuit

$T_{l.r}$, h	100000	110000	120000	130000	140000	150000	160000
$R_{red(w)}(T_{l.r})$	0.9996	0.9995	0.9994	0.9993	0.9991	0.9990	0.9989
$R_{red(h)}(T_{l.r})$	0.9991	0.99895	0.9988	0.9985	0.9983	0.9981	0.9978

Thus, in this example, a redundant microcircuit will ensure the required value of $T_{l.r(req)}$ = 100000 h at γ = 99.9%.

The explicit value of $T_{l.r}$ can be obtained by inserting increasing values of t in increments of $+0.1T_{l.r(req)}$ into formulas (3) and (5) as long as inequation (4) is satisfied. Table 1 shows the obtained values of the PNF of a microcircuit at the given values of $T_{l.r.}$

Thus, in this case, the integrated circuit enables the required durability indicator:

– when warm standby is used: $T_{l.r}$ = 150000 h at r = 99.9%,

– when hot standby is used: $T_{l.r}$ = 100000 h at r = 99.9%.

Taking into account the module redundancy options

In practice, individual integrated circuits are part of modules that are made redundant within a system. Let us assume that a microcircuit, along with other EC, is part of module M_A that is backed-up by module M_B in warm standby. Let us find the PNF of such microcircuit.

An integrated circuit operates without failures during time t in two cases:

1) Module M_A has operated without failure for time t, i.e. a microcircuit in it did not fail

$$R_1(t) = e^{-\lambda_{o(M\_A)} \cdot t}, \qquad (6)$$

where $\lambda_{o(M\_A)}$ is the FR of module M_A in operational mode.

2) The following sequence of events took place:

- module M_A failed at the moment τ ($0 < \tau \le t$) (microcircuit or other EC has failed);
- module M_B did not fail until moment τ;
- at moment τ module M_A turned off and module M_B started to operate as the main module;
- within the remaining time interval $(t - \tau)$ the microcircuit did not fail.

The PNF for this case is the following [7]

$$R_2(t) = \int_0^t a_{M\_A}(\tau) \cdot R_{M\_B}(\tau) \cdot R_{MC}(t-\tau)\, dt, \qquad (7)$$

where $a_{M\_A}(\tau)$ is the probability distribution function of module M_A failure time, or, which is the same, failure rate of module M_A within time τ, which equals $a_{M\_A}(\tau) = \lambda_{o(M\_A)} \cdot e^{-\lambda_{o(M\_A)} \cdot \tau}$;

$R_{M\_B}(\tau)$ is the PNF of module M_B within time τ;

$R_{MC}(t - \tau)$ is the PNF of microcircuit within time $(t - \tau)$.

Combining formulas (6) and (7) and substituting the values of the variables into formula (7), we obtain

$$R_{red(w)}(t) = e^{-\lambda_{o(M\_A)} \cdot t} + \int_0^t \lambda_{o(M\_A)} \cdot e^{-\lambda_{o(M\_A)} \cdot \tau} \cdot e^{-\lambda_{o(M\_B)} \cdot \tau} \cdot e^{-\lambda_{o(MC)} \cdot (t-\tau)} dt =$$

$$= e^{-\lambda_{o(M\_A)} \cdot t} + \frac{\lambda_{o(M\_A)}}{\lambda_{o(M\_A)} + \lambda_{s(M\_B)} - \lambda_{o(MC)}} \cdot e^{-\lambda_{o(MC)} \cdot t} \cdot \left(1 - e^{-\left(\lambda_{o(M\_A)} + \lambda_{s(M\_B)} - \lambda_{o(MC)}\right) t}\right). \qquad (8)$$

Here $\lambda_{o(M\_A)}$ is the FR of module M_A in operational mode;

$\lambda_{s(M\_B)}$ is the FR of module M_B in warm standby mode when off;

$\lambda_{o(MC)}$ is the FR of microcircuit in operational mode.

Substituting the obtained value of $R_{red(w)}(t)$ at $t = T_{l.r}$ from formula (8) into inequation (4), we obtain the condition for the microcircuit to achieve a durability index equal to $T_{l.r}$.

Let us illustrate the case considered with a real-life example [8], in which the following data were used:

$\lambda_{o(M\_A)} = 0.4522 \cdot 10^{-6}$ 1/h;

$\lambda_{s(M\_B)} = 0.016 \cdot 10^{-6}$ 1/h;

$\lambda_{o(MC)} = 30.340 \cdot 10^{-9}$ 1/h;

$T_{l.r}$ = 100000 h;

γ = 99.9 %.

Substituting these data into formula (8), we obtain

$$R_{red(w)}(T_{l.\gamma}) = e^{-0,4522 \cdot 10^{-6} \cdot 10^5} + \frac{0,4522 \cdot 10^{-6}}{0,4522 \cdot 10^{-6} + 0,016 \cdot 10^{-6} - 30,340 \cdot 10^{-9}} \cdot e^{-30,340 \cdot 10^{-9} \cdot 10^5} \times \cdot \left(1 - e^{-\left(0,4522 \cdot 10^{-6} + 0,016 \cdot 10^{-6} - 30,340 \cdot 10^{-9}\right) 10^5}\right) = 0,999897.$$

In this case

$R_{MC(life)}(T_{l.r}) = 0.999897 \ge 0.999$,

i.e. the microcircuit enables the specified durability indicator $T_{l.r}$ = 100 000 h at γ = 99.9%.

When hot standby is used for modules M_A and M_B, the corresponding formula for the PNF of the microcircuit takes the form

$$R_{red(n)}(t) = e^{-\lambda_{o(M\_A)} \cdot t} + \frac{\lambda_{o(M\_A)}}{2 \cdot \lambda_{o(M\_A)} - \lambda_{o(MC)}} \cdot e^{-\lambda_{o(MC)} \cdot t} \cdot \left(1 - e^{-\left(2 \cdot \lambda_{o(M\_A)} - \lambda_{o(MC)}\right) \cdot t}\right). \qquad (9)$$

Then, substituting the example data into formula (9), we obtain

$$R_{red(n)}(T_{l.\gamma}) = e^{-0,4522 \cdot 10^{-6} \cdot 10^5} + \frac{0,4522 \cdot 10^{-6}}{2 \cdot 0,4522 \cdot 10^{-6} - 30,340 \cdot 10^{-9}} \cdot e^{-30,340 \cdot 10^{-9} \cdot 10^5} \times \cdot \left(1 - e^{-\left(2 \cdot 0,4522 \cdot 10^{-6} - 30,340 \cdot 10^{-9}\right) 10^5}\right) = 0,998956.$$

In this case, inequation (4) in not satisfied, i.e. the microcircuit does not ensure the specified durability indicator $T_{l.r}$ = 100 000 h.

The considered method of durability indicator identification can be used for other redundancy architectures of modules in a system [9].

Conclusion

If the durability indicators (for example, the gamma-percentile life $T_{l.r}$) are not specified in the technical specifications or other documents for the delivery of microcircuitry or other EC, the probability that the microcircuit will not reach the limit state, upon which its further operation is unacceptable, over time $T_{l.r}$ can be equalized to the PNF of the microcircuit over time $t = T_{l.r}$.

A non-redundant microcircuit will have a given gamma-percentile life $T_{l.r}$ defined by relation (2). If the FR of the microcircuit does not satisfy relation (2), then in order to achieve a given durability indicator, various redundancy options can be used.

A redundant microcircuit will ensure the given indicator $T_{l.r}$ if the PNF of the microcircuit satisfies relation (4).

Formulas were obtained for estimating the PNF of a microcircuit, when the microcircuit is part of a backed-up module.

The proposed method can be used to evaluate a given durability indicator of a microcircuit or other EC if the initial data on durability is absent.

References

[1] GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016 [in Russian].

[2] OST 4.012.013-84. Electronic equipment. Definition of durability indicators [in Russian].

[3] OST V 11 0998-99. Integrated circuits. General technical conditions [in Russian].

[4] Netes VA. New international standard for dependability. Dependability 2016;3:54-58.

[5] Dependability of Electronic Products Handbook. Moscow; 22-nd Central Research, Design and Test Institute of the Ministry of Defense of Russia; 2006 [in Russian].

[6] Zayko YuG, Smirnov MB. Otsenka nadezhnosti sistem so smeshannym rezervirovaniem [Dependability assessment of systems with combined redundancy]. Dependability 2004;4(11):40-45 [in Russian].

[7] Polovko AM. Osnovy teorii nadiozhnosty [Fundamentals of the dependability theory]. Moscow: Nauka; 1964 [in Russian].

[8] Borisov YuI. O vybore arkhitektury otkazoustoychivykh vychislitelnykh kompleksov dlya kosmicheskikh apparatov [On the selection of the architecture of fail-safe computer systems for spacecraft]. Dependability 2004;2(9):46-51 [in Russian].

[9] Zayko YuG, Iskandarova LN, Trakhtomirov AV. Simulation model to calculate the indices of reliability of redundant radio electronic systems. Dependability 2016;16(3):8-17.

About the authors

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

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

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

Received on: 16.05.2019

A research of the characteristics of the Kijima-Sumita processes under an increasing rate function

Alexander V. Ankudinov, *IATE MEPhI, Russian Federation, Obninsk*
Alexander V. Antonov, *Rosatom Technical Academy, Russian Federation, Obninsk*
Valery A. Chepurko, *JSC RASU, Russian Federation, Moscow*

Alexander V. Ankudinov

Alexander V. Antonov

Valery A. Chepurko

Abstract. Aim. *The paper is dedicated to the research of the models of Kijima-Sumita incomplete restoration processes [1-7]. These models are relatively new and poorly studied. As the case of incomplete restoration is more typical for the operation of today's technical systems, the study of the Kijima-Sumita models appears to be most relevant. In those models, the degree of incompleteness of restoration is defined by the value of coefficient q. The paper cites findings that elaborate upon [5] and [6]. In [5], the restoration function was evaluated in the form of a finite sum with the use of statistical tests. In [6], an integral equation was derived for the restoration function and failure flow parameter. The effect of the restoration factor on those indicators was analyzed as well.This paper aims to derive a density equation of time between failures for the Kijima-Sumita model and such dependability indicators as the average values of the overshoot, undershoot and cycle duration, as well as to analyze the effect of restoration factor q on those indicators. The findings are presented in graph form, with the assumption that the time to first failure adheres to the Weibull distribution law that is at the core of the dependability theory. This paper considers the case of the increasing rate function.* **Methods.** *The required calculations were conducted in the R free programming environment that is specially designed for statistical computing and graphics. The mathematical tools used in this work were the numerical integration methods, such as the method of trapezoids and method of rectangles modified for taking double integrals.* **Conclusions.** *For the Kijima-Sumita process, the paper derives equations and constructs graphs for the densities of time between failures, as well as average values of the overshoot, undershoot and cycle duration. The restoration equation for the Kijima incomplete restoration processes was deduced. The effect of the restoration factor on the above dependability indicators was analyzed for the case of increasing rate function showing that if parameter q increases, the average values of overshoot, undershoot and cycle duration decrease.*

Keywords: *overshoot, undershoot, cycle duration, restoration process, failure flow parameter, rate function, virtual age, restoration factor, complete restoration, minimal restoration.*

For citation: *Ankudinov AV,Antonov AV, Chepurko VA.A research of the characteristics of the Kijima-Sumita processes under an increasing rate function. Dependability 2019; 3: 7-11 p. DOI: 10.21683/1729-2646-2019-19-3-7-11*

Introduction

Let there be some renewable technical system that starts operating at the moment of time t = 0. Let us denote the instants of system failure by τ_1, τ_2, …, and times between failures (repairs) by Δ_1, Δ_2, …. Thus, the instants of failure form the restoration process shown in Figure 1, while expression $\tau_k = \sum_{i=1}^{k} \Delta_i$ shows the actual age of the system at the moment of the k-th failure. In order to simplify the model, we will ignore the repair time of a failed system.

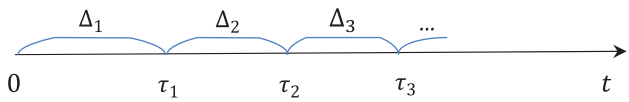


Figure 1. Restoration process

For models described in [3], value q that represents the restoration factor, and some function $V(\{\Delta\},q)$ that defines the so-called virtual age of the system are introduced. Then, V_{i-1} is the virtual age of the system at the moment of the (i–1)-th restoration, while Δ_i, the operation time between the i-th and (i-1)-th failures, has the following conditional distribution function [4,5]:

$$F_i\left(x|V_{i-1}\right)=\frac{F\left(x+V_{i-1}\right)-F\left(V_{i-1}\right)}{1-F\left(V_{i-1}\right)}, \qquad (1)$$

where $F(x)$ is the distribution function of time to first failure.

In [7], two models of the general renewal process are presented: GRP-1 and GRP-2. The GRP-1 model is distinctive in that the n-th restoration affects only the damage sustained by a system between the (n-1)-th and the n-th failures reducing the system's virtual age increment from Δ_i to $q\Delta_i$. A system's virtual age after the n-th restoration is written as follows:

$$V_n = V_{n-1} + q\Delta_n = q\sum_{i=1}^{n}\Delta_i = q\tau_n;\ V_0 = 0.$$

According to the GRP-2 model, each restoration affects the total damage, thus reducing the total virtual age:

$$V_n = qV_{n-1} + q\Delta_n = q\left(q^{n-1}\Delta_1 + q^{n-2}\Delta_2 + \ldots + \Delta_n\right);\ V_0 = 0.$$

This paper will examine the GRP-1 model.

Thus, the types of restoration of elements and systems subject to the Kijima-Sumita processes can be classified as follows:

- complete restoration (q=0, homogenous process);
- minimal restoration (q=1);
- incomplete restoration or "worse than new, but better than before the failure" (0<q<1);
- "worse than before the failure" (q>1).

Let us consider the definitions of undershoot, overshoot and cycle duration. The equation for those indicators will be derived based on the information on the failure flow parameter, for which the expression was obtained in the previous paper [6].

Let us fix a certain moment of time t (see Figure 2). *Forward residual time (overshoot)* is the time remaining to the instant of next failure (restoration) τ_{k+1}. The overshoot is determined from formula [3, 4]:

$$\nu_t = \tau_{k+1} - t,\quad t \geq 0,\quad \left[\tau_k, \tau_{k+1}\right] \ni t. \qquad (2)$$

Reverse residual time (undershoot) is the time elapsed from the latest restoration τ_k to the current instant t. The undershoot is determined from formula [3, 4]:

$$\rho_t = t - \tau_k,\ t \geq 0,\ \left[\tau_k, \tau_{k+1}\right] \ni t. \qquad (3)$$

Cycle duration is the sum of the overshoot and undershoot [3, 4]:

$$\delta_t = \Delta_{k+1} = \nu_t + \rho_t = \tau_{k+1} - \tau_k,\ t \geq 0, \left[\tau_k, \tau_{k+1}\right] \ni t. \qquad (4)$$

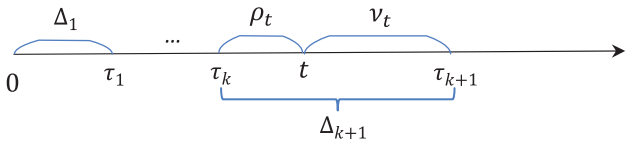


Figure 2. Overshoot and undershoot

Derivation of density equation of time between failures

Knowing the conditional function (1) and conditional density $f_{\Delta_n}\left(x \mid V_{n-1} = y\right) = \frac{f\left(x+y\right)}{1-F\left(y\right)}$, as well as the distribution of the first operation time $F_{\Delta_1}\left(x\right) = F\left(x\right)$, $f_{\Delta_1}\left(x\right) = f\left(x\right)$, the distribution of the second operation time can be found:

$$f_{\Delta_2}\left(x|V_1=y\right) = f_{\Delta_2}\left(x|\tau_1=qy\right) = f_{\Delta_2}\left(x|\Delta_1=qy\right) = \frac{f_{\Delta_1,\Delta_2}(qy,x)}{f_{\Delta_1}(qy)}.$$

Out of which follows:

$$f_{\Delta_1,\Delta_2}\left(qy,x\right) = f_{\Delta_1}\left(qy\right) f_{\Delta_2}\left(x \mid \Delta_1 = qy\right) = f_{\Delta_1}\left(qy\right)\frac{f\left(x+y\right)}{1-F\left(y\right)}.$$

Let us multiply both parts by q(q≠0) and integrate with respect to y between 0 and infinity, thus obtaining the distribution density of the second operation time:

$$f_{\Delta_2}(x) = \int_0^{\infty} f_{\Delta_1,\Delta_2}(qy,x)\,d\left(qy\right) = \int_0^{\infty} f\left(v\right)\frac{f\left(x+v/q\right)}{P\left(v/q\right)}dv.$$

Similarly, the distribution of the third operation time is obtained:

$$f_{\Delta_3}(x) = \int_0^{\infty} f_{\tau_2,\Delta_3}(qy,x)\,d\left(qy\right) = \int_0^{\infty} f_{\tau_2}\left(v\right)\frac{f\left(x+v/q\right)}{P\left(v/q\right)}dv.$$

Using the rule of mathematical induction, we obtain the general expression for the density of random time between failures:

$$f_{\Delta_{k+1}}(x)=\int_0^{\infty} f_{\tau_k}(v)\frac{f\left(x+v/q\right)}{P\left(v/q\right)}dv=\int_0^{\infty} f_{\tau_k}(v)K_f\left(x,v/q\right)dv, \quad (5)$$

where the distribution of the k-th instant of failure is found using a recurrence formula deduced in [6]:

$$f_{\tau_k}(x)=\int_0^{x} f_{\tau_{k-1}}(u)K_f(x-u,qu)du. \quad (6)$$

It is known, that the formula for the rate function of the Weibull distribution is defined by the value of shape variable a. The rate increases if $a > 1$, remains unchanged if a = 1 and decreases if $a\in(0,1)$. This paper, as stated in the abstract above, considers the case of the increasing rate function. Figures 3 and 4 show distribution densities of instants (6) and operation times (5) respectively. Here, the restoration factor is equal to one, while the first operation time is distributed according to the Weibull law with shape parameter $f(x)=\frac{a}{b}\left(\frac{x}{b}\right)^{a-1}e^{-\left(\frac{x}{b}\right)^a}$, where the values of parameters are taken as a=4, b=2.

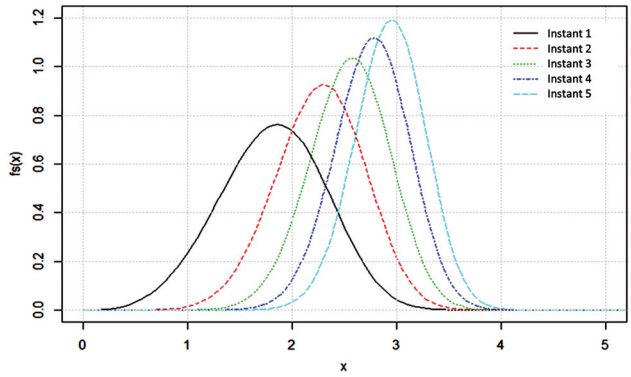


Figure 3. Distribution density of failure instants

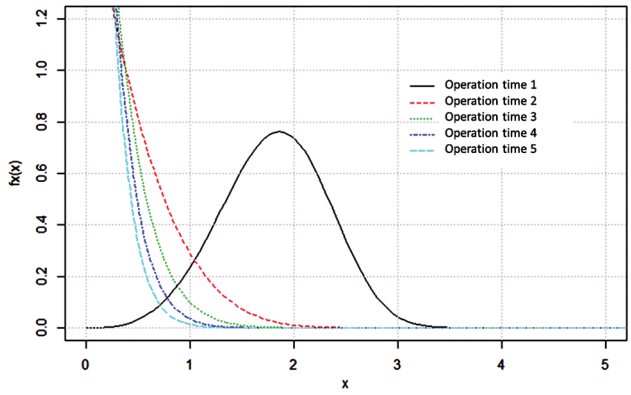


Figure 4. Distribution density of times between failures

Analyzing Figure 3, it can be noted that, as compared to the homogenous restoration, the failure flow of the Kijima model condenses. That is expressed in the fact that the average time between failures reduces, because, as the number of failure increases, the distribution densities of the instants of failure shift to the left at a progressively lower rate. Additionally, unlike a homogenous flow, under which dispersion linearly increases with the growing number of failures, in the Kijima flow the corresponding dispersion slowly decreases. The fact that each next operation time is lower than the previous one can be clearly observed in Figure 4. Obviously, this situation is explained by the incomplete restoration.

Research of undershoot, overshoot and cycle duration

Let us find the undershoot distribution ρ_t (3):

$$P_{\rho_t}(x)=Pr(\rho_t>x)=\sum_{k=0}^{\infty}Pr(\tau_k<t-x;\tau_{k+1}>t)=$$

$$=\int_{-\infty}^{t-x}\int_{t-u}^{\infty}K_f(v,qu)\omega_0(u)dvdu,$$

where $K_f(a,b)=\frac{f(a+b)}{1-F(b)}$.

Having calculated the inner integral, we obtain:

$$P_{\rho_t}(x)=\int_{-\infty}^{t-x}K_P(t-u,qu)\omega_0(u)du, \quad (7)$$

where $K_P(a,b)=\frac{P(a+b)}{P(b)}$.

Let us take the integral of the obtained expression and find the *average undershoot*:

$$R(t)=\int_0^{\infty}P_{\rho_t}(x)dx=\int_0^{t}(t-x)\frac{P(t-x+qx)}{P(qx)}\omega_0(x)dx,$$

where $\omega_0(x)=\sum_{k=0}^{n}f_{\tau_k}(x)=\delta(x)+\sum_{k=1}^{n}f_{\tau_k}(x)=\delta(x)+\omega(x)$,

$\delta(x)$ is the Dirac delta function, therefore:

$$R(t)=tP(t)+\int_0^{t}(t-x)\frac{P(t-x+qx)}{P(qx)}\omega(x)dx. \quad (8)$$

Similarly, let us find the overshoot distribution v_t (2):

$$P_{v_t}(x)=Pr(v_t>x)=\sum_{k=0}^{\infty}Pr(\tau_{k+1}>t+x;\tau_k<t)=$$

$$=\int_{-\infty}^{t}\int_{t+x-u}^{\infty}K_f(v,qu)\omega_0(u)dvdu,$$

where $K_f(a,b)=\frac{f(a+b)}{1-F(b)}$.

Having taken the inner integral, we obtain:

$$P_{v_t}(x) = \int_{-\infty}^{t} K_P(t+x-u, qu)\,\omega_0(u)\,du, \qquad (9)$$

where $K_P(a,b) = \dfrac{P(a+b)}{P(b)}$.

Then we find the *average overshoot* by integrating (9):

$$V(t) = \int_0^{\infty} P_{v_t}(x)\,dx = \int_0^{\infty} P(t+x)\,dx + \int_0^{\infty}\int_0^{t} \frac{P(t+x-u+qu)}{P(qu)}\,\omega(u)\,du\,dx. \qquad (10)$$

Let us proceed to the cycle duration distribution δ_t (4)

$$P_{\delta_t}(x) = Pr(\delta_t > x) = \sum_{k=0}^{\infty} Pr(\Delta_{k+1} > x; \tau_k < t < \tau_k + \Delta_{k+1}) = \int_{-\infty}^{t}\int_{x\vee(t-u)}^{\infty} K_f(v, qu)\,\omega_0(u)\,dv\,du,$$

where $K_f(a,b) = \dfrac{f(a+b)}{1-F(b)}$, $x \vee (t-u) = \max(x, t-u)$.

Let us take the inner integral and find the cycle duration distribution:

$$P_{\delta_t}(x) = \int_0^{t} K_P(x \vee (t-u), qu)\,\omega_0(u)\,du, \qquad (11)$$

where $K_P(a,b) = \dfrac{P(a+b)}{P(b)}$.

Thus, we obtain the *average cycle duration*:

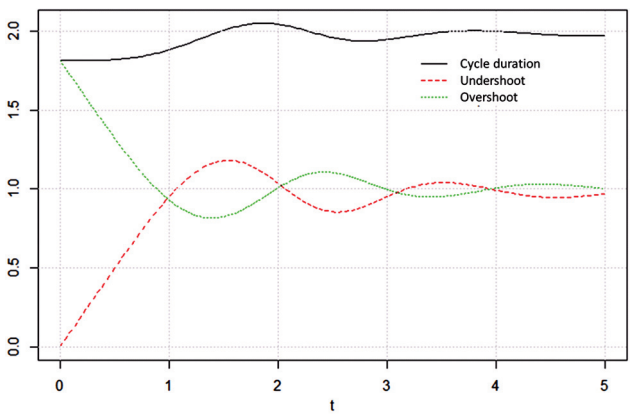


Figure 5. Average cycle duration, undershoot and overshoot for a homogenous flow

Figure 5 shows the graphs of average cycle durations, undershoot and overshoot for a homogenous failure flow. The restoration factor q=0, while the operation times are distributed according to the Weibull law with shape parameter a=4 and scale parameter b=2. At the beginning of the time, the overshoot declines, while the undershoot grows, which is quite logical, as the point of failure approaches. Further, we can observe that over time the oscillations of the overshoot and undershoot graphs, as well as their convergence to asymptotic constant rapidly decrease, wherein the local extremums of such indicators are practically the same.

The graphs in Figures 6 to 8 show how such indicators are affected by the value of the restoration factor q. The higher is parameter q the worse is restoration of the technical system in question. Subsequently, it is obvious that for the selected moment in time, under the increasing restoration factor, we can observe the reduction of the time after the latest restoration (Fig. 6), time remaining to the next failure (Fig. 7) and, respectively, time between failures, observed at the moment of inspection t (Fig. 8).

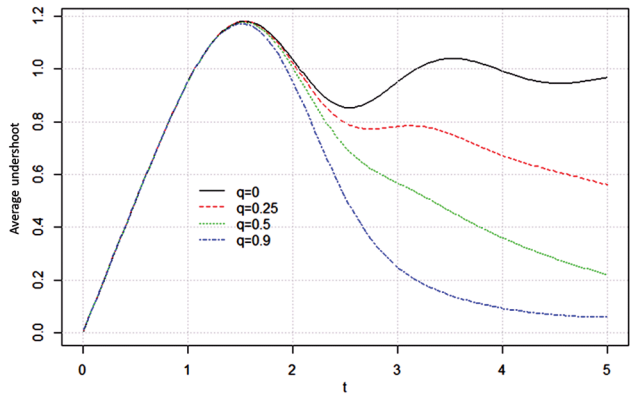


Figure 6. Average undershoot

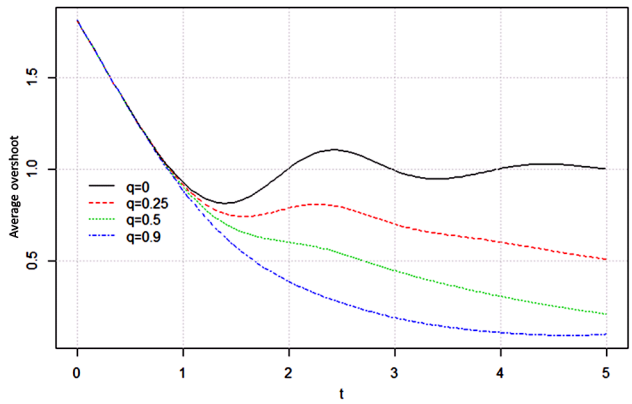


Figure 7. Average overshoot

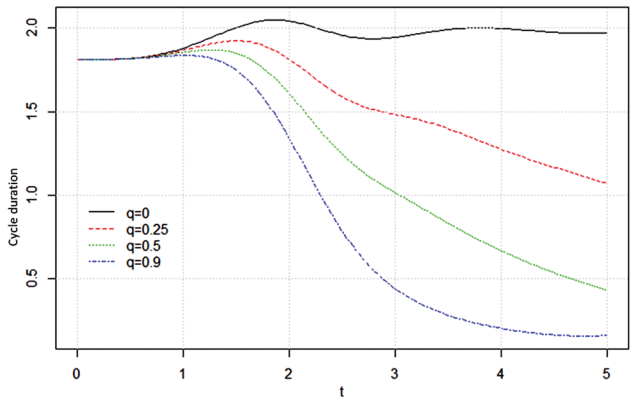


Figure 8. Average cycle duration

In subsequent papers the same dependability indicators are to be examined under the decreasing rate function. Additionally, of interest are the asymptotics of the dependability indicator under $t \to \infty$. It is obvious that the indicators of overshoot, undershoot and cycle duration in the Kijima model asymptotically tend to zero, not to the nonzero constant as it is the case under the homogenous failure flow model.

Conclusion

The paper continued the assessment of the dependability indicators and research of some of the properties of the restoration processes for the Kijima-Sumita models. Currently, the application of such models is of special relevance, as they allow taking into consideration not only complete, but partial restoration of elements and technical systems. The paper derives an equation for the density of arbitrary time between failures, as well as integral equations for the mathematical expectations of the overshoot, undershoot and cycle duration. Research was also conducted that allows concluding that, in case of increasing rate function, as the restoration coefficient grows the reduction of such dependability indicators can be observed.

References

[1] Antonov A.V., Nikulin M.S., Chepurko V.A. Teoriya nadezhnosti. Statisticheskie modeli [Dependability theory. Statistical models]. Moscow: INFrA-M; 2015 [in Russian].

[2] Finkelstein M. Failure rate modelling for reliability and risk. Verlag. London Limited: Springer; 2008.

[3] Daley D.J., Vere-Jones D. An introduction to the theory of point processes: Volume 1: Elementary theory and methods. Verlag New York – Berlin – Heidelberg: Springer; 2003.

[4] Chepurko S.V., Chepurko V.A. Modeli neodnorodnykh potokov v teorii vosstanovlenia. Monografia [Non-uniform streams models in the restoration theory. A monograph]. Obninsk: IATE; 2012 [in Russian].

[5] Chumakov I.A., Antonov A.V., Chepurko V.A. On some properties of Kijima incomplete restoration models. Dependability 2015;3(54):10-15.

[6] Ankudinov A.V., Antonov A.V., Chepurko V.A. Renewal equation for Kijima-Sumita processes. Dependability 2018;18(2):3-9.

[7] Kijima M., Sumita M. A useful generalization of renewal theory: Counting process governed by non-negative markovian increments. Journal of Applied Probability 1986;23:71-88.

[8] Kaminsky M., Krivtsov V. Primenenie metoda Monte-Karlo k otsenke obobshchennogo protsessa vosstanovleniya pri analize dannykh ob otkazakh v period deystviya garantiynykh obyazatelstv [Use of the Monte Carlo method in the evaluation of the extended restoration process as part of failure data analysis during the warranty period]. Reliability: Theory & Applications 2006;1:32-34 [in Russian].

[9] Wibowo W. On approaches for repairable system analysis: Renewal Process, Nonhomogenous Poisson Process, General Renewal Process. Indonesia, Jurnal Industri 2010;9(1):60-66.

[10] Antonov A.V. Otsenka pokazateley nadezhnosti sistem stareyushchego tipa na primere sistem yaderno-energeticheskoy otrasli [Estimation of dependability indicators of ageing systems using the example of nuclear energy systems]. Dependability 2010;1(33):18-29 [in Russian].

About the authors

Alexander V. Ankudinov, post-graduate student, Intelligent Cybernetic Systems Division, Obninsk Institute for Nuclear Power Engineering (IATE MEPhI), Russian Federation, Obninsk, e-mail: anck93@yandex.ru

Alexander V. Antonov, Doctor of Engineering, Professor, Chief Expert of the International Training Center, Rosatom Technical Academy, Russian Federation, Obninsk, e-mail: AVAntonov@rosatomtech.ru.

Valery A. Chepurko, Candidate of Physics and Mathematics, Associate Professor, Chief Specialist of Division for Justifying Calculations of Design Solutions, JSC RASU. Russian Federation, Moscow, e-mail: v.a.chepurko@mail.ru, VAChepurko@rasu.ru

Received on: 06.02.2019

Plan of tests with addition

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

Viktor S. Mikhailov

Abstract. *It is common practice to estimate the values of dependability indicators (point estimation). Normally, the probability of no-failure (PNF) is used as the dependability indicator. Due to economic reasons, determinative dependability tests of highly dependable and costly products involve minimal numbers of products, expecting failure-free testing (acceptance number Q = 0) or testing with one failure (Q = 1), thus minimizing the number of tested products. The latter case is most interesting. By selecting specific values of the acceptance number and number of tested products, the tester performs a preliminary estimation of the planned PNF, while selecting Q = 1 the tester minimizes the risks caused by an unlikely random failure. However, as the value Q grows, the number of tested products does so as well, which makes the testing costly. That is why the reduction of the number of products tested for dependability is of paramount importance.* **Preparation of the plan of tests with addition.** *We will consider binomial tests (original sample) with addition of one product (oversampling) to testing in case of failure of any of the initially submitted products. Testing ends when all submitted products have been tested with any outcome (original sampling and oversampling). Hereinafter it is understood that the testing time is identical for all products. Testing with the acceptance number of failures greater than zero (Q > 0) conducted with addition allows reducing the number of tested products through successful testing of the original sample. The* **Aim** *of the paper consists in preparing and examining PNF estimates for the plan of tests with addition.* **Methods of research of dependability indicator estimates.** *Efficient estimation is based on the integral approach formulated in [6, 8-10]. The integrative approach is based on the formulation of the rule of efficient estimate selection specified on the vertical sum of absolute (or relative) biases of estimates selected out of a certain set based on the distribution law parameter, where, in our case, n is the number of products initially submitted to testing.* **Criterion of selection of efficient estimation for PNF.** *The criterion of selection of an efficient estimate of the probability of failure (or PNF) at a set of estimates is based on the total square of absolute (or relative) bias of the mathematical expectation of estimates* $E\hat{\theta}(n,k,m)$ *from probability of failure p for all possible values of p, n.* **Conclusions.** *PNF estimates for the plan of tests with addition was prepared and examined. For the case n > 3, the PNF estimate* $\hat{P}(n,k,m) = 1-\hat{p}(n,k,m) = 1-(k+m)/(n+k)$ *in comparison with the implicit estimate* $\hat{V}(n,k,m) = 1-\hat{v}(n,k,m)$ *is bias efficient. Testing with the acceptance number of failures greater than zero (Q > 0) conducted with addition allows reducing the number of tested products through successful testing of the original sample. Estimates* $\hat{p}_2$, $\hat{w}_2$ *and* $\hat{w}_3$ *are unbiassed and, as a consequence, bias efficient for the cases n = 2 and n = 3 respectively.*

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

For citation: *Mikhailov VS. Plan of tests with addition. Dependability 2019; 3: 12-20 p. DOI: 10.21683/1729-2646-2019-19-3-12-20*

Introduction

It is common practice to estimate the values of dependability indicators (point estimation). Normally, the probability of no-failure (PNF) is used as the dependability indicator. Due to economic considerations, determinative dependability tests of highly dependable and costly products involve minimal numbers of products, expecting failure-free testing (acceptance number Q=0) or testing with one failure (Q=1), thus minimizing the number of tested products. The latter case is most interesting. By selecting specific values of the acceptance number Q and number of tested products, the tester performs a preliminary estimation of the planned PNF, while selecting Q=1 the tester minimizes the risks caused by an unlikely random failure. However, as the value Q grows, the number of tested products does so as well, which makes the testing costly. That is why the reduction of the number of products tested for dependability is of paramount importance.

Preparation of the plan of tests with addition

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

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

The Aim of the paper

The aim of the paper consists in preparing and examining PNF estimates for the plan of tests with addition.

Preparation and examination of PNF estimates for the plan of tests with addition

Let n be the number of tested products of the same type initially submitted to testing, and let $R = r$ be the number of failed products that includes k failures from n products initially submitted to testing and m failures from k products repeatedly submitted to testing, i.e. $r=k+m$. Then, the number of tested products will be $N=n+k$. Let failures be independent events, then the probability of r failures during tests (hereinafter, $P_n(R=r)$) is easily expressed with a generating function. Let us apply properties of the generating function [3].

The generating function (hereinafter, $\psi_R(z)$) is a mathematical expectation of an exponential function of type z^R, i.e. for the test plan with addition [3]: $\psi_R(z) = Ez^R = \sum_{i=0}^{2n} z^i P_n(R=i)$.

For the case when the original sample consists of one product, the generating function will be [3]:

$$\psi_R(z) = Ez^R = \sum_{i=0}^{2n} z^i P_n(R=i) = q + qpz + p^2z^2.$$

Then, for the case when original sample consists of n products, the generating function will be [3]:

$$\psi_{n;R}(z) = \left(q + qpz + p^2z^2\right)^n.$$

The probability of zero failures during testing of the original sample with volume n [3]:

$$P_n(R=0) = \psi_{n;R}(z) = \left(q + qpz + p^2z^2\right)^n \Big|_{z=0} = q^n.$$

The mathematical expectation of the random value R can be calculated through the expression [3]: $ER = \psi^{(1)}_{n;R}(z=1)$ is the first derivative.

And the probability of getting exactly r failures can be calculated through the expression [3]:

$$P_n(R=r) = \psi^{(r)}_{n;R}(z=0)/r!.$$

Let us construct the derivative of the generating function:

$$\psi^{(1)}_{n;R}(z) = n\left(q + qpz + p^2z^2\right)^{n-1}\left(2p^2z + pq\right),$$

out of which follows that the average number of failures during tests will be

$$ER = \psi^{(1)}_{n;R}(z=1) = n\left(q+qp+p^2\right)^{n-1}\left(2p^2+pq\right) = np(1+p).$$

Then, the probability of one failure during tests can be calculated by the formula:

$$P_n(R=1) = \psi^{(1)}_{n;R}(z=0) = nq^{n-1}pq = npq^n$$

The construction of derivatives of the higher orders is very complicated, and therefore it is not demonstrated in this paper.

The obtained results are not the best option for calculations, therefore, let us construct a more convenient formula for the probability of exactly r failures during tests that is obtained from the following construction procedure ($n \ge k \ge m; r = k + m \le 2n$):

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

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

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

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

$$P_n(r=0) = P_n(k=0, m=0) = q^n;$$

$$P_n(r=1) = P_n(k=1, m=0);$$

$$P_n(r=2;r\le n)=P_n(k=1,m=1)+P_n(k=2,m=0);$$

$$P_n(r=3;r\le n)=P_n(k=2,m=1)+P_n(k=3,m=0);$$

$$P_n(r=4;r\le n)=P_n(k=2,m=2)+$$
$$+P_n(k=3,m=1)+P_n(k=4,m=0);$$

$$P_n(r=5;r\le n)=P_n(k=3,m=2)+$$
$$+P_n(k=4,m=1)+P_n(k=5,m=0);$$

$$P_n(r=6;r\le n)=P_n(k=3,m=3)+P_n(k=4,m=2)+$$
$$+P_n(k=5,m=1)+P_n(k=6,m=0);$$

$$P_n(r=7;r\le n)=P_n(k=4,m=3)+P_n(k=5,m=2)+$$
$$+P_n(k=6,m=1)+P_n(k=7,m=0);$$

…

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

…

$$P_n(r=2n)=P_n(k=n,m=n)=p^{2n}.$$

From the construction logic we obtain the required formula for the probability of exactly r failures:

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

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

Through the calculation of probability $P_n(k=x,m=y)=P_n(k=x)P_n(m=y)$, where $x, y = 0, 1, 2, ..., n$ and $P_n(R=r)$ it is easy to obtain the probability function of the plan of tests with addition:

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

which on the entire set of events $r=k+m=0,1,2,\ldots, 2n$ should be equal to one. Let us verify this fact.

The probability function on the entire set of events can be represented as the sum of the products of each component of the primary polynomial by polynomial, where polynomials have binominal coefficients:

$$P_{n\sum}(n,n)=\sum_{r=0}^{2n}P_n(r)=\sum_{k+m=0}^{2n}P_n(k)P_k(m)=$$
$$=\sum_{k+m=0}^{2n}C_n^k p^k q^{n-k}C_k^m p^m q^{k-m}=q^n+C_n^1 p^1 q^{n-1}\sum_{m=0}^{1}C_1^m p^m q^{1-m}+\ldots+$$
$$+C_n^k p^k q^{n-k}\sum_{m=0}^{k}C_k^m p^m q^{k-m}+\ldots+p^n\sum_{m=0}^{n}C_n^m p^m q^{n-m}=$$
$$=\sum_{k=0}^{n}C_n^k p^k q^{n-k}=1,$$

or:

$$P_{n\sum}(n,n)=\sum_{k=0}^{n}P_n(k)=\sum_{k=0}^{n}C_n^k p^k q^{n-k}=1.$$

An expression for *ER* can also be found in a simpler way. The average number of tested products during tests with addition consists of the number of products that were originally submitted to testing and the average number of failed products that were originally submitted to testing, i.e. $N=n+np$. Then, the average number of failed products during tests with addition will be:

$$E(R,n)=Np=E(k,n)+E(m,n)=$$
$$=np+np*p=(n+np)p=np(1+p).$$

Let us note that the probability $P_n(k,m)$ defines the test results (k,m), therefore, as an estimate of parameter p it is recommended to choose an estimate that defines the maximum probability $P_n(k,m)$.

Let us solve the classical problem of identification of function maximum

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

with respect to p. For that, let us take the logarithm for the function $b(r,p,k,n)$, let us take the derivative with respect to the variable p, set the result to zero and solve an equation with respect to variable p. The resulting estimate $\hat{p}=r/(n+k)=r/(n+r-m)$ determines the maximum of function $b(r,p,k,n)$. Let us consider the properties of the resulting estimate $\hat{p}=r/(n+k)$ and the PNF estimate, as a consequence

$$\hat{P}=1-\hat{p}=1-r/(n+k)=(n-m)/(n+k).$$

Let $k+m=r>1$, then for various $k_1>k_2$, $m_1<m_2$ the following inequality will be true

$$\hat{p}(k_1,m_1)=\frac{r}{n+k_1}<\hat{p}(k_2,m_2)=\frac{r}{n+k_2}, \quad (2)$$

i.e. the dependability of the controlled batch of products (PNF: $\hat{P}(k_1,m_1)=1-\hat{p}(k_1,m_1)$) according to the test of a sample, in which the number of products failed during test k_1 was greater than in the sample of a comparable batch k_2 with the same number r of failures will always be higher $\hat{P}(k_1,m_1)>\hat{P}(k_2,m_2)$ than in a comparable batch of products. In other words, when comparing the results of two finally formed samples (with equal numbers of failures), the priority in dependability is given to the products, whose failures were primarily within the original sample, and not oversampling. In this case, oversampling enables remediation after unsuccessful initial tests. This is the advantage of the test plan with addition.

Unbiassed estimate calculation

Let us determinate the mathematical expectation of the estimate $\hat{p}(n;k,m) = r/(n+k)$:

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

It can be proved that estimate $E(\hat{p}(n;k,m))$ in general is biased. To prove that, a particular case will suffice.

Let us determine the mathematical expectation of estimate $\hat{p}(n=1) = r/(1+k)$:

$$n=1: E(\hat{p}(n=1))= \sum_{r=0}^{2} \frac{r}{1+k} P_1(r)= 0*P_1(k=0,m=0)+$$
$$+\frac{1}{2}P_1(k=1,m=0)+1*P_1(k=1,m=1)=$$
$$=\frac{1}{2}pq+p^2=0,5(p+p^2).$$

Therefore, estimate $\hat{p}(n=1) = r/(1+k)$ is biased. Estimate $\hat{p}(n=1)$ can be presented in the following form:

$$\hat{p}\left(n=1\right)= \frac{r}{1+k} \equiv \begin{cases} 0\ , r=0,k=0,m=0; \\ \dfrac{1}{2}, r=1,k=1,m=0; \\ 1\ , r=2,k=1,m=1. \end{cases}$$

By equating the mathematical expectation of unknown estimate $\hat{w}_1(n=1;k,m)$ to parameter p, it is easy to obtain an unbiased estimate of probability of failure $\hat{w}_1$ for the case $n=1; p_0, p_1, p_2$ are unknown probabilities:

$$E\left(\hat{w}_1\right)= \sum_{r=0}^{2} \frac{r}{1+k} \hat{w}_1 P_1(r)= p_0(1-p)+p_1\left(p-p^2\right)+p_2p^2=p;$$

$$p^0: p_0\, p^0 = p_0 *1 = 0 \Rightarrow p_0 = 0; p^1: p_1 p^1 = p \Rightarrow p_1 = 1;$$

$$p^2: -p^2 p_1 + p^2 p_2 = 0 \Rightarrow p_2 = p_1 = 1;$$

$$\hat{w}_1 \equiv \begin{cases} 0 & , r=0,k=0,m=0; \\ 1 & , r=1,k=1,m=0; \\ 1 & , r=2,k=1,m=1. \end{cases}$$

An unbiased estimate is an indicator function, i.e. in case of failures estimate $\hat{w}_1$ is equal to one, if otherwise, this estimate is equal to zero. The option when n=1 is practically not interesting, because it coincides with the binominal plan, therefore, it will not be considered in this paper.

Let us determine the mathematical expectation for $\hat{p}(n=2) = r/(2+k)$

$$n=2: E(\hat{p}(n=2))= \sum_{r=0}^{4} \frac{r}{2+k} P_2(r) = 0*P_2\ (k=0,m=0)+$$
$$+(1/3)P_2(k=1,m=0)+(2/3)P_2(k=1,m=1)+$$
$$+(1/2)P_2(k=2,m=0)+(3/4)P_2(k=2,m=1)+1*$$
$$*P_2(k=2,m=2)=0*q^2+(1/3)2p^1q^2+(2/3)2p^2q+$$
$$+(1/2)p^2q^2+(3/4)2q^3q+1*p^4=2p\,(1-p)(1/3-(1/3)p+$$
$$+(2/3)p+(1/4)p-(1/4)p^2)+(3/2)p^3-(3/2)p^4+p^4=$$
$$=2p(1-p)(1/3+(7/12)p-(1/4)p^2)+(3/2)p^3-$$
$$-(3/2)p^4+p^4=\left(\frac{2}{3}\right)p+\left(\frac{7}{6}\right)p^2-\left(\frac{1}{2}\right)p^3-\left(\frac{2}{3}\right)p^2-\left(\frac{7}{6}\right)p^3+$$
$$+\left(\frac{1}{2}\right)p^4+\left(\frac{3}{2}\right)p^3-\left(\frac{3}{2}\right)p^4+p^4=\left(\frac{2}{3}\right)p+\left(\frac{1}{2}\right)p^2-\left(\frac{1}{6}\right)p^3\ ;$$

$$p=0,5: E(\hat{p}(n=2))=1/3+1/8-1/(6*8)=21/48\ .$$

Therefore, estimate $\hat{p}(n=2) = r/(2+k)$ is biased. Estimate $\hat{p}$(n=2) can be presented as:

$$\hat{p}(n=2)\equiv \begin{cases} 0, & r=0,k=0,m=0; \\ 1/3, r=1,k=1,m=0; \\ 2/3, r=2,k=1,m=1; \\ 1/2, r=2,k=2,m=0; \\ 3/4, r=3,k=2,m=1; \\ 1, & r=4,k=2,m=2. \end{cases}$$

Let us note that for the results $\hat{p}(r=2,k=1,m=1) = 2/3$ and $\hat{p}(r=2,k=2,m=0) = 1/2$ the dependability of the controlled batch of products, in which some products in the sample failed during initial test, is higher than in the products whose failures occurred during repeated test and with the same number of failures. That corresponds to the property of estimate $\hat{p} = r/(n+k)$, expressed by formula (2).

It is easy to obtain an unbiased estimate $\hat{s}_2$ for parameter p:

$$\hat{s}_2 \equiv \begin{cases} 0, & r=0,k=0,m=0; \\ 1/2, r=1,k=1,m=0; \\ 5/8, r=2,k=1,m=1; \\ 6/8, r=2,k=2,m=0; \\ 7/8, r=3,k=2,m=1; \\ 1, & r=4,k=2,m=2. \end{cases}$$

For this purpose the mathematical expectation of the supposed unbiased estimate with unknown probabilities p_{ik} must be equated to parameter p and necessary transformations must be carried out:

$$E(\hat{p}(n=2)=\sum_{r=0}^{4}\hat{p}(n=2)P_2(r)=[p_{00}=0;p_{22}=1]=p_{00}q^2+$$
$$+p_{10}2pq^2+p_{11}2p^2q+p_{20}p^2q^2+p_{21}2p^3q+p^4=2p_{10}p-$$
$$-2p_{10}2p^2+2p_{10}p^3+2p_{11}p^2-2p_{11}p^3+p_{20}p^2-2p_{20}p^3+$$
$$+p_{20}p^4+p_{21}2p^3-p_{21}2p^4+p_{22}p^4=2p_{10}p-4p_{10}p^2+$$
$$+2p_{11}p^2+p_{20}p^2+2p_{10}p^3-2p_{11}p^3-2p_{20}p^3+p_{21}2p^3+$$
$$+p_{20}p^4-p_{21}2p^4+p_{22}p^4=p.$$

For this equation to be true, the coefficients with different degrees of parameter p must be equal to zero, with the exception of the first degree where the coefficient must be equal to one:

$$p^1:2p_{10}p^1=p\Rightarrow p_{10}=1/2;$$
$$p^2:-4p_{10}p^2+2p_{11}p^2+p_{20}p^2=0\Rightarrow 2p_{11}+p_{20}=2\Rightarrow$$
$$\Rightarrow 2p_{11}=2-p_{20};$$
$$p^3:2p_{10}p^3-2p_{11}p^3-2p_{20}p^3+2p_{21}p^3=0\Rightarrow 2p_{11}+2p_{20}-2p_{21}=$$
$$=1\Rightarrow 2-p_{20}+2p_{20}-p_{20}-1=1\Rightarrow p_{20}=6/8\Rightarrow p_{11}=5/8;$$
$$p^4:p_{20}p^4-p_{21}2p^4+p_{22}p\,\hat{}\,4=0\Rightarrow[p_{22}=1]:2p_{21}-p_{20}=$$
$$=p_{22}\Rightarrow 2p_{21}=p_{20}+1\Rightarrow p_{21}=7/8.$$

This heterogeneous system of linear equations is always resolvable and has an infinite set of similar solutions (the number of variables is greater than the number of equations):

$$p_{00}=0;p_{10}=1/2;p_{11}=5/8;p_{20}=6/8;p_{21}=7/8;p_{22}=1.$$

Let us note that the failure probabilities must satisfy the slack inequality $0\le p_{ij}\le 1$. Let us also point out that, in practice, for two controlled batches of products with the same number of failures in the generated samples for the results $p_{20}=6/8$ and $p_{11}=5/8$ the dependability of the first controlled batch of products $1-p_{20}=1-6/8=2/8$, for which some products in the original sample and oversampling failed only during initial tests k=2, m=0, is lower than for products of the second controlled batch $1-p_{11}=1-5/8=3/8$, where failures occurred during repeated tests in oversampling as well. This result contradicts the property (see formula (2)) of the biased estimate $\hat{p}(r=k+m,k,m)=r/(n+k)$) and makes it difficult to choose an efficient estimate.

Further, in order to avoid contradictions when looking for new estimates of the failure probability, it is necessary to take into account that the values of estimates for the same number of failures do not depend on the fact, in which sample (original or additional) the failures occurred. Therefore, this principle of looking for new estimates of the failure probability $\hat{w}(n;k,m)$ can be presented as follows:

$$\hat{w}(k\_1+m\_1=r,k\_1,m\_1)=$$
$$=\hat{w}(k\_2+m\_2=r,k\_2,m\_2),\qquad(3)$$

i.e. we reject the property estimate $\hat{p}$ expressed by formula (2).

Similarly to the above reasoning, let us demonstrate the method of finding new estimates:

$$\hat{w}_2(0):=p_0;\ \hat{w}_2(1):=p_1;\ \hat{w}_2(2):=p_2;\ \hat{w}_2(3):=p_3;\ \hat{w}_2(4):=p_4$$

$$E(\hat{w}_2)=\sum_{r=0}^{4}\hat{w}_2(r)P_2(r)=p=p_0q^2+p_1 2pq^2+p_2 2p^2q+$$
$$+p_2p^2q^2+p_3 2p^3q+p_4p^4=2p_1p-2p_1 2p^2+2p_1p^3+$$
$$+2p_2p^2-2p_2p^3+p_2p^2-2p_2p^3+p_2p^4+p_3 2p^3-p_3 2p^4+$$
$$+p_4p^4\,2p_1p-4p_1p^2+2p_2p^2+p_2p^2+2p_1p^3-2p_2p^3-$$
$$-2p_2p^3+p_3 2p^3+p_2p^4-p_3 2p^4+p_4p^4.$$

In order for this equality to be true, the coefficients with different degrees should be equal to zero, with the exception of the first degree, where the coefficient should be equal to one:

$$p^0:p_0p^0=p_0*1=0\Rightarrow p_0=0;$$

$$p^1:2p_1=1\Rightarrow p_1=1/2;$$

$$p^2:-4p_1p^2+2p_2p^2+p_2p^2=0\Rightarrow -2+3p_2=0\Rightarrow p_2=2/3;$$

$$p^3:2p_1p^3-2p_2p^3-2p_2p^3+p_3 2p^3=$$
$$=0\Rightarrow 1-8/3+2p_3=0\Rightarrow p_3=5/6;$$

$$p^4:p_2p^4-p_3 2p^4+p_4p^4=$$
$$=0\Rightarrow 2/3-10/6+p_4=0\Rightarrow p_4=1;$$

$$p_0=0;p_1=1/2;p_2=2/3;p_3=5/6;p_4=1.$$

This heterogeneous system of linear equations is always solvable and has only one solution (the number of variables 2**n* is equal to the rank (number of linearly independent equations) [5]), which will be estimate $\hat{w}_2$!

Similarly to the previous example (case n=2), let us determine the mathematical expectation of estimate $\hat{p}(n=3)=r/(3+k)$:

$$n=3:\ E(\hat{p}(n=3))=\sum_{r=0}^{6}\frac{r}{3+k}P_3(r).$$

After all the required manipulations (they are not presented due to complicated expressions) the following result will be obtained: estimate $\hat{p}(n=3)=\sum_{r=0}^{6}\frac{r}{3+k}$ is biased. Estimate $\hat{p}(n=3)=\sum_{r=0}^{6}\frac{r}{3+k}$ is presented as follows:

$$\hat{p}(n=3)=\sum_{r=0}^{6}\frac{r}{3+k}\equiv\begin{cases}0,r=0,k=0,m=0;\\1/4,r=1,k=1,m=0;\\1/2,r=2,k=1,m=1;\\2/5,r=2,k=2,m=0;\\3/5,r=3,k=2,m=1;\\4/5,r=4,k=2,m=2;\\1/2,r=3,k=3,m=0;\\2/3,r=4,k=3,m=1;\\5/6,r=5,k=3,m=2;\\1,r=6,k=3,m=3.\end{cases}$$

Let us determine an unbiased estimate of failure probability for the case n=3 ($\hat{w}_3(r)$), using the principle expressed by the formula (3). The probability values of this estimate are determined through its mathematical expectation that should be equal to the estimated parameter p:

$$\hat{w}_3(0):=p_0;\hat{w}_3(1):=p_1;\hat{w}_3(0):=p_2;\hat{w}_3(3):=p_3;$$
$$\hat{w}_3(4):=p_4;\hat{w}_3(5):=p_5;\hat{w}_3(6):=p_6;$$

$$E(\hat{w}_3(r))=p=p_0q^3+p_1 3pq^3+3p_2(p^2q^2+p^2q^3)+$$
$$+p_3(6p^3q^2+p^3q^3)+p_4(3p^4q+3p^4q^2)+p_5 3p^5q+$$
$$+p_6p^6=3p_1(p-3p^2+3p^3-p^4)+3p_2(p^2-2p^3+p^4)+$$
$$+3p_2(p^2-3p^3+3p^4-p^5)+6p_3(p^3-2p^4+p^5)+$$
$$+p_3(p^3-3p^4+3p^5-p^6)+3p_4(p^4-p^5)+$$
$$+3p_4(p^4-2p^5+p^6)+3p_5(p^5-p^6)+p_6p^6$$

$$p^0:p_0p^0=p_0*1=0;p_0=0;$$

$$p^1:3p_1=1;p_1=1/3;$$

$$p^2:-9p_1+3p_2+3p_2=0\Rightarrow 6p_2=3\Rightarrow p_2=1/2;$$

$$p^3:9p_1-6p_2-9p_2+6p_3+p_3=0\Rightarrow 6p_2+$$
$$9p_2-6p_3-p_3=3\Rightarrow p_3=9/14;$$

$$p^4:-3p_1+3p_2+9p_2-12p_3-3p_3+3p_4+3p_4=$$
$$=0\Rightarrow 12p_2-15p_3+6p_4=1\Rightarrow p_4=65/84;$$

$$p^5:-3p_2+6p_3+3p_3-3p_4-6p_4+3p_5=0\Rightarrow p_5=75/84;$$

$$p^6:-p_3+3p_4-3p_5+p_6=0\Rightarrow p_6=1;$$

$$\hat{w}_3(r)\equiv\begin{cases}0,r=0;\\1/3,r=1;\\1/2,r=2;\\9/14,r=3;\\65/84,r=4;\\75/84,r=5;\\1,r=6.\end{cases}$$

A similar search for unbiased estimates for cases n=4 and n=5 was unsuccessful, because the obtained results of the probability values exceeded 1, which is not acceptable. Therefore, for n>3 the construction of an unbiased estimate according to the rule $\hat{p}(k_1+m_1=r,k_1,m_1)=\hat{p}(k_2+m_2=r,k_2,m_2)$ is problematic!

Let us introduce a new term: let the estimate of failure probability (hereinafter, $\hat{v}$) center the probability function $P_{n\sum}$ relative to the limits of its values. This means that intervals $[0;\hat{v}]$ and $[\hat{v};1]$ of values of such estimates with the probability 0.5 cover the estimated parameter p. Such estimates will be called centered. Let us note that for some test plans centered estimates are close to efficient estimates [6, 8]. In this case, the centered estimate v is calculated from the following expression (replacing p with v in the formula (1)):

$$P_{n\sum}(k\le x,m\le y,\hat{v})=\sum_{k=0}^{x}\sum_{m:m+k\le x+y,m\le k,m\le y}P_n(k,m,\hat{v})=0,5.$$

For the solution for this equation to exist be unique, it is necessary to verify the monotonicity of $P_{n\sum}$ with respect to variable p [1, 7]. It should be reminded that $P_n(k,m):=C_n^k C_k^m p^{k+m}q^{n-m}, r=k+m.$

Taking thee derivative of $P_{n\sum}$ to the parameter p, the results will be the following:

$$(P_{n\sum}(k\le x,m\le y,p))'_p=$$
$$=\sum_{k=0}^{x}\sum_{m:m+k\le x+y,m\le k,m\le y}C_n^kC_k^{r-k}(rp^{r-1}q^{n-r+k}-(n-r+k)p^rq^{n-r+k-1})$$

Due to the complexity of the obtained expression, it is not possible to prove or dispose of the monotonicity of $P_{n\sum}$. However, it is possible for the most interesting cases as r=0, r=1 и r=2. Let us consider these cases:

$$r=0:\ (P_{n\sum}(n,p,k=0,m=0))'_p=$$
$$=C_n^0C_0^{0-0}\ [(0+0)p^{-1}q^n-np^0q^{n-1}\ ]=-nq^{n-1}<0;$$

$$r=1:\ (P_{n\sum}(n,p,k=1,m=0))'_p=$$
$$=C_n^1C_1^0\left[(1+0)p^0q^n-npq^{n-1}\right]-C_n^0C_0^0nq^{n-1}=$$
$$=nq^n-n^2pq^{n-1}-nq^{n-1}=nq^{n-1}(1-p-np-1)=$$
$$=-pn(n+1)q^{n-1}<0;$$
$$r=2:\ (P_{n\sum}(n,p,k=1,m=1))'_p=C_n^1C_1^1[(1+1)pq^{n-1}-$$
$$-(n-1)p^2q^{n-2}\ ]+C_n^1C_1^0[(1+0)p^0q^n--npq^{n-1}]-$$
$$-C_n^0C_0^0nq^{n-1}=2npq^{n-1}-n(n-1)p^2q^{n-2}+nq^n-n^2pq^{n-1}-$$
$$-nq^{n-1}=npq^{n-2}(2(1-p)-(n-1)p)-pn(n+1)q^{n-1}=$$
$$=npq^{n-2}(2-p-np)-pn(n+1)q^{n-1}=npq^{n-2}(2-n-1)\le 0$$

Table 1. The values of LCB of parameter *p* for different scopes of tests (in horizontal direction) and failure events (in vertical direction) if γ=0,8

	n	1	2	3	4	5	6	7	8
k=0	*m*=0	0.199	0.105	0.071	0.054	0.043	0.036	0.031	0.027
k=1	*m*=0	0.445	0.287	0.212	0.168	0.139	0.119	0.104	0.092
k=1	*m*=1	1	0.445	0.287	0.212	0.168	0.139	0.119	0.104

Table 2. The values of UCB of parameter *p* for different scopes of tests (in horizontal direction) and failure events (in vertical direction) if *α*=0,2

	n	1	2	3	4	5	6	7	8
k=0	*m*=0	0.800	0.552	0.415	0.331	0.275	0.235	0.205	0.182
k=1	*m*=0	0.894	0.710	0.582	0.488	0.422	0.370	0.330	0.297
k=1	*m*=1	1	0.894	0.710	0.582	0.488	0.422	0.370	0.330

Table 3. The values of the centered estimate $\hat{v}$ for different scopes of tests (in horizontal direction) and failure events (in vertical direction)

	n	1	2	3	4	5	6	7	8
k=0	*m*=0	0.292	0.206	0.159	0.129	0.108	0.094	0.082	0.074
k=1	*m*=0	0.707	0.5	0.384	0.313	0.264	0.226	0.201	0.179
k=1	*m*=1	1	0.707	0.5	0.384	0.313	0.264	0.226	0.201

$$r=2:\ (P_{n\sum}(n,p,k=2,m=0))'_p = C_n^2 C_2^0[(2+0)pq^n -$$
$$-np^2q^{n-1}\ ]+C_n^1C_1^0[(1+0)p^0q^n - np^1q^{n-1}\ ]-C_n^0C_0^0nq^{n-1} =$$
$$= n(n-1)pq^n - 0,5n^2(n-1)p^2q^{n-1}+nq^n - n^2pqq^{n-1} -$$
$$-nq^{n-1} = n(n-1)pq^{n-1}(1-p-0,5np)-pn(n+1)q^{n-1} =$$
$$= npq^{n-2}(0,5np-n)\le 0.$$

Therefore, for cases when *r*=0, *r*=1, *r*=2 probability function $P_{n\sum}$ monotonically decreases with the increasing parameter *p* and, therefore, the centered estimate $\hat{v}$ of parameter *p* for the test plan with addition is unique.

The centered estimate defines the lower (upper) confidence boundary (hereinafter referred to as LCB (UCB)) of the interval of the unknown parameter *p* with the confidence probability γ=0,5 or significance level α=1–γ=0,5. On the other hand, any estimate of LCB (UCB) of the interval of unknown parameter *p* can be interpreted as a point estimate of parameter *p* with a strong bias (downward bias is for LCB and upward bias is for UCB). Unidirectional LCB (hereinafter referred to as $\hat{p}_L$) and UCB (hereinafter referred to as $\hat{p}_U$) of the interval with unknown parameter *p* with confidence probability γ=1–α are calculated in accordance with the following formulas:

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

The boundaries of the central confidence interval are calculated in accordance with the following formulas [4]:

$$P_{n\sum}(x,y,\hat{p}_L)=1-\alpha/2,\ P_{n\sum}(x,y,\hat{p}_U)=\alpha/2\ .$$

Tables 1, 2 and 3 show the values of LCB, UCB of parameter *p* and values of the centered estimate $\hat{v}$ for the most realistic scopes of tests and failure events.

Let us formulate a criterion for choosing an efficient estimate of failure probability (or PNF) and construct – on the basis of the formulated criterion – an improved (and biased) estimate of failure probability (and, therefore, the estimate of the PNF) for the test plan with addition for *n*>3 and choose the efficient one among the proposed estimates.

Research methods for estimating dependability indicators

The search for efficient estimates is based on the integral approach described in [6, 8-10]. The integral approach is based on construction of the rule for choosing an efficient estimate $\hat{\theta}_0(n;k,m)$ specified on the sum of the absolute (or relative) bias of estimates of $\hat{\theta}_0(n;k,m)$, selected from a certain set, from the parameter of the distribution law, where in this case *n* is the number of products initially put up for testing.

Criterion for choosing and efficient estimate for PNF

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

In order to select an efficient estimate of the probability of failure (or PNF) the concept of an absolutely efficient estimate by bias and parameter *p* variation within $0\le p\le 1$

are required. In order to obtain the final result, the functional (hereinafter referred to as $L(\hat{\theta}(n;k,m))$ on the limited set $n_1 \le n_i \le n_j$, $i = 1,\ldots,j$ is constructed [6, 8–10] as a criterion for efficient estimate $\hat{\theta}(n;k,m)$:

$$L(\hat{\theta}(n;k,m)) = \frac{1}{j} \sum_{n_1 \le n_i \le n_j} \int_0^1 (E\hat{\theta}(n_i;k,m) - p)^2 dp \quad (4)$$

Estimate $\hat{\theta}_0(n;k,m)$ that minimizes the functional $L(\hat{\theta}(n;k,m))$ on a given set of estimates is an efficient bias estimate on a given set of biased estimates. Among estimates that similarly minimize functional $L(\hat{\theta}(n;k,m))$, an estimate that has the minimal mean-square deviation (classical definition of an efficient estimate [1]) is to be selected. We will call this estimate more efficient in comparison with the selected ones.

Selecting estimates with minimal deviation involves constructing a functional (hereinafter referred to as $D(\hat{\theta}(n;k,m)$) by summarizing mathematical expectations of squares of relative deviations of estimates of $\hat{\theta}(n;k,m)$ from parameter p for all possible values p, n [6, 8-10]:

$$D(\hat{\theta}(n;k,m)) = \frac{1}{j} \sum_{n_1 \le n_i \le n_j} \int_0^1 E(\hat{\theta}(n_i;k,m) - p)^2 dp \quad (5)$$

An estimate that provides zero to functional $L(\hat{\theta}(n;k,m)$)=0 (unbiased estimate) and minimizes functional $D($ $\hat{\theta}(n;k,m))$ will be called absolutely biased.

Let us limit the scope tests as $0 \le n \le 10$, which is the cost limit for highly reliable and complicated products. Then, formula (4) will be as follows:

$$L(\hat{\theta}(n;k,m)) = \frac{1}{10} \sum_{1 \le i \le 10} \int_0^1 (E\hat{\theta}(n_i;k,m) - p)^2 dp.$$

And formula (5) will be presented as:

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

Table 4 shows the results of the substitution into functional $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$ in accordance with formulas (4) and (5) of the following estimates of failure probability $\hat{\theta}$: $\hat{p}, \hat{p}_2, \hat{w}_2, \hat{w}_3, \hat{v}$. The calculations were carried out with the step of $dp = 10^{-3}$.

Table 4 shows that for options $n>3$ estimate $\hat{p}$ has a minimal bias compared to estimate $\hat{v}$. $\hat{p}_2$, $\hat{w}_2$ and $\hat{w}_3$ estimates are unbiased and, as a result, are efficient for options n=2 and n=3 respectively.

Table 4 shows that estimate $\hat{v}$ has a slight advantage over estimate $\hat{p}$ as regards minimal deviation of its values from parameter p. Therefore, the estimate $\hat{p} = (k+m)/(n+k)$ can be taken as a desired efficient bias estimate among the proposed ones.

Let us note that the variation of the step of summation changes the functional result, but does not change the result of estimates comparison.

Example. Products are part of a redundant piece of equipment. It is required to make a point estimate of PNF products according to the binominal reliability tests. While planning determinative dependability tests, the tester, when calculating sample volume (n=6), took into account only one failure (Q=1), minimizing the risk of the improbable unpredictable failure. In this case, the predicted PNF value was $\hat{P} = 1 - 1/n = 5/6 = 0,83$ that corresponds to the requirements of the technical specifications (PNF should be at least 0.83) for the product. Given that during tests the failure of product is unlikely, it was decided to carry out the dependability tests with addition to reduce the costs. During the test two outcomes are possible: no failure and one failure (as planned). In case of no failure there is no need for oversampling. Let us consider these options:

1) No-failure tests. No-failure tests with addition:

$$\hat{P} = 1 - \hat{p}(n = 5, k = 0, m = 0) =$$
$$= 1 - r/(n+k) = 1 - 0/(5+0) = 1;$$

$$\hat{V} = 1 - \hat{v}(n = 5, k = 0, m = 0) = 1 - 0,108 = 0,892.$$

One-sided LCB of PNF as $n=5, \gamma = 1-\alpha = 1-0,2 = 0,8$ was (see Table 2)

$$\hat{P}_n(n = 5, r = 0) = 1 - \hat{p}_e(n = 5, k = 0, m = 0) =$$
$$= 1 - 0,275 = 0,725.$$

Binominal tests with one failure:

$$\hat{P}(n = 6, r = 0) = 1 - r/n = 1 - 0/6 = 1.$$

One-sided LCB of PNF as $n = 6, r = 0, \gamma = 0,8$ (calculated according to the Clopper-Pearson equation [2]) was $\hat{P}_L(n = 6, r = 0) = (1-\gamma)^{\overline{6}} = 0.764.$

2) Tests with one failure. Tests with addition and with one failure:

$$\hat{P} = 1 - \hat{p}(n = 5, k = 1, m = 0) =$$
$$= 1 - r/(n+k) = 1 - 1/(5+1) = 0,83;$$

Table 4. Results of substitution of the proposed estimates of failure probability into functionals $L(\hat{\theta}(n;k,m))$ and $D(\hat{\theta}(n;k,m))$

Functional	$\hat{p}_2(n=2)$	$\hat{w}_2(n=2)$	$\hat{w}_3(n=3)$	$\hat{p}\ (n>3)$	$\hat{v}(n>3)$
$L(\hat{\theta}(n;k,m))$	$2.6 \cdot 10^{-33}$	$2.6 \cdot 10^{-33}$	$5.1 \cdot 10^{-33}$	$2 \cdot 10^{-4}$	$1.51 \cdot 10^{-3}$
$D(\hat{\theta}(n;k,m))$	0.0687	0.0418	0.0418	0.0187	0.0164

$$\hat{V} = 1 - \hat{v}\left(n = 5, k = 1, m = 0\right) = 1 - 0,264 = 0,736.$$

One-sided LCB of PNF as $n=5$, $\gamma=1-\alpha=1-0,2=0,8$ was (see Table 2)

$$\hat{P}_L\left(n = 5, r = 1\right) = 1 - \hat{p}_U\left(n = 5, k = 1, m = 0\right) = \\ = 1 - 0.422 = 0.588.$$

Binominal tests with one failure: $\hat{P} = 1 - r / n = 1 - 1 / 6 = 0,83.$

One-sided LCB of PNF as $n = 6, r = 1, \gamma = 0,8$ (calculated according to the Clopper-Pearson equation [2]) was $\hat{P}_L\left(n = 6, r = 1\right) = 0.578.$

Conclusions

PNF estimates for the plan of tests with addition was prepared and examined. For the case of $n>3$, the PNF estimate $\hat{P}(n,k,m) = 1 - \hat{p}(n,k,m) = 1 - (k+m)/(n+k)$ in comparison with the implicit estimate $\hat{V}(n,k,m) = 1 - \hat{v}(n,k,m)$ is bias efficient.

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

Estimates $\hat{p}_2, \hat{w}_2, \hat{w}_3$ are unbiased and, as a consequence, bias efficient for the cases $n=2$ and $n=3$ respectively.

References

[1] Borovkov A.A. Matematicheskaya statistika [Mathematical statistics]. Novosibirsk: Nauka; 1997 [in Russian].

[2] Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. Matematicheskie metody v teorii nadezhnosti [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965 [in Russian].

[3] Krupkina T.V. Teoriya veroyatnostey i matematicheskaya statistika. Chast 2. Elektronnyy kurs lektsiy [Probability theory and mathematical statistics. Part 2. Electronic series of lectures]. Krasnoyarsk: Siberian Federal University; 2011 [in Russian].

[4] Shulenin V.P. Matematicheskaya statistika. Chast 1. Parametricheskaya statistika: ouchebnik [Mathematical statistics. Part 1. Parametric statistics: a textbook]. Tomsk: Izdatelstvo NTL; 2012 [in Russian].

[5] Kostrikin A.I. Vvedenie v algebru. Chast I. Osnovy algebry: uchebnik dlya vuzov [Introduction to algebra. Part 1. Basic algebra: textbook for higher educational institutions. Moscow: MCCME; 2004 [in Russian].

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

[7] Fikhtengolts G.M. Kurs differentsialnogo i integralnogo ischisleniya. Tom 1 [Course of differential and integral calculus. Volume 1]. Moscow: Nauka; 1969 [in Russian].

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

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

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

About the author

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

Received on: 14.04.2019

Autonomous Driving – How to Apply Safety Principles

Hendrik Schäbe, TÜV Rheinland InterTraffic GmbH, Köln, Germany

Hendrik Schäbe

Abstract: *We discuss safety principles of autonomous driving road vehicles. First, we provide a comparison between principles and experience of autonomous or automatic systems on rails and on the road. An automatic metro operates in a controlled and well-defined environment, passengers and third persons are separated from driving trains by fences, tunnels, etc. A road vehicle operates in a much more complex environment. Further, we discuss safety principles. The application of safety principles (e.g. fail-safe or safe-life) is used to design and implement a safe system that eventually fulfils the requirements of the functional safety standards. The different responsibility of human driver and technical driving system in different automation levels for autonomous driving vehicles require the application of safety principles. We consider, which safety principles have to be applied using general safety principles and analysing the relevant SAE level based on the experience from projects for the five levels of automated driving as defined by the SAE. Depending on the level of automation, the technical systems are implemented as fail-silent, fails-safe or as safe-life.*

Keywords: *safety architecture, autonomous driving, road vehicles*

For citation: *Schäbe H. Autonomous Driving – How to Apply Safety Principles. Dependability 2019; 3: 21-33 p. DOI: 10.21683/1729-2646-2019-19-3-21-33*

1. Introduction

Autonomous driving on the street [2] has become more and more popular and the first demonstrator systems are operational [4,10,21]. On the other hand, automatic metros and people movers are already successfully working for many years.

In this paper, we compare the different levels of automation as defined by UITP [23] and SAE [22] and their meaning for the system. In addition, manual fallback modes are considered.

For road vehicles, currently a large number of assistance system is available that are able to handle specific situations. This leads to the impression that these vehicles move autonomously.

In general, the situation for a road vehicle is much more complex than that of a train.

We describe differences regarding approval for automated metros, road vehicles and so called automated guided vehicles (AGV). Legal requirements for homologation of road vehicles according to the convention on road traffic are discussed and the implication for the system and the behavior of the driver.

Autonomous driving has become a very important subject of research and first pilot projects. In safety technology, the application of safety principles as e.g. fail-safe or safe-life is a very important tool to design and implement a safe system that eventually fulfils the requirements of the standards for functional safety. Safety principles have already been described and applied to guided transport systems, including system with immaterial guidance principles.

In earlier papers, safety principles have been described and later applied to guided driving.

In the present paper, we systematically consider which safety principles have to be applied for which SAE level of autonomously driving systems und we show how an autonomous system could be built. This is partially done with the help of general safety principles, partially by analysing the relevant SAE level based on the experience from several projects.

According to UN resolution [24] or SAE [22], autonomous driving on the road knows five different levels:

- 0 No automation
- 1 Driver assistance
- 2 Partial automation
- 3 Conditional automation
- 4 High automation
- 5 Full automation

For the levels 0-2, the driver is fully responsible for driving, starting from level 3 the automated driving equipment monitors the vehicle.

This different responsibility of human driver and technical driving system requires the application of safety principles. In the present paper, we systematically consider which safety principles have to be applied for which level und we show how such a system could be built.

This is partially done with the help of general safety principles, partially by analysing the relevant level.

We start with a very simple and abstract model of the system and show that there exist different possibilities to implement autonomous driving. An important result is that an arbiter needs to be installed that gives the human driver the possibility to override the decisions of the autonomous system to fulfil legal requirements.

For the five levels of automated driving as defined by the SAE [22], safety principles are derived. For the levels 0-2, the driver is fully responsible for driving, whereas starting from level 3, the automated driving equipment monitors the vehicle. To give the driver the possibility to intervene, means that this must be implemented according to the relevant safety integrity level and that the driver must have enough time to take over control. The latter strongly depends on the level of automation and the speed and the environment in which the vehicle moves.

Depending on the level of automation, the technical system are implemented as fail-silent or as safe-life. There are also exclusions, when the technical systems can be implanted as fail safe, when the vehicle always can be brought to a safe stop, e.g. when driving with low speed and on a controlled territory.

We consider the two main functions of guidance and braking / acceleration and their role for autonomous driving. Moreover, detection and reaction with regard to fixed and moving obstacles is discussed.

Two basic requirements for autonomous systems are that they need to be developed according to the relevant standards of functional safety fulfilling an ASIL (or SIL) level and that the capability of the autonomous driving system must at least on the same level as that of a human driver.

We note that Wachenfeld[26] has proposed a stochastic approach to show that an autonomous system fulfils a certain level of performance or safety. This, however, can only be seen additional evidence, the main evidence for a safe system is an appropriate safety architecture implemented according to the rules of functional safety, see ISO 26262 [18].

We sketch the current technical possibilities for automated driving and the existing technical solutions. Especially, we discuss the possibilities and restrictions of artificial intelligence. We briefly describe a roadmap of possible next steps.

2. The status with metros, people movers and road vehicles

2.1. Metros and people movers

In many cities in the meanwhile automated metros and automated people movers are working

Examples are

- On the New York City Subway, the BMT Canarsie Line.

• On the London Underground, the Central, Northern, Jubilee, and Victoria lines run with ATO.

• On the Nuremberg U-Bahn, existing U2 and new U3 lines converted to ATO.

• On the Barcelona Metro, the L9 (as the Europe's longest driverless line), L10 and L11 runs with ATO.

• The Rio Tinto Group has the iron ore railway driverless go-ahead.

• The Tren Urbano, has an Siemens ATC system that allows for fully automatic operation.

• The Vancouver SkyTrain.

• Frankfurt Airport Skyline.

• Copenhagen Metro.

• On the Milan Metro, the M1 Red Line runs with ATO.

On the Mass Rapid Transit (Singapore), all lines operating currently run with ATO since 1987.

For metros and people movers, a principle of separation has been applied: The automated trains are separated from all other traffic, running in the tunnels, open track is separated by fences, platform screen doors are used to separate the trains from passengers. This simplified the exploitation conditions significantly.

The automated train protection system (ATP) is used to prevent collision and derailment. This allows also manually operated trains to use the same network.

The normal safety requirement for the ATP is a safety integrity level SIL 4. Nevertheless, manually operated fallback modes exist. Partially stewards are present to assist the passengers, especially in case in case of evacuation.

For metros and people movers, the UITP [24] has established 5 levels of automation. That means, the picture is not black and white, knowing either manual or automated driving. Automation is a stepwise process. The following five levels are established, UITP [24]:

GoA 0 is on-sight train operation, similar to a tram running in street traffic.(No automation at all)

GoA 1 is manual train operation where a train driver controls starting and stopping, operation of doors and handling of emergencies or sudden diversions.

GoA 2 is semi-automatic train operation (STO) where starting and stopping is automated, but a driver operates the doors, drives the train if needed and handles emergencies. Many ATO systems are GoA 2.

GoA 3 is driverless train operation (DTO) where starting and stopping are automated but a train attendant operates the doors and drives the train in case of emergencies.

GoA 4 is unattended train operation (UTO) where starting and stopping, operation of doors and handling of emergencies are fully automated without any on-train staff.

As a conclusion, automatic metros and automatic people movers can be seen as established systems. However, one needs to note that they operate in a controlled and simplified environment.

2.2. Road vehicles

We need to distinguish two situations:

a) driving on an open road and

b) driving on private territory

Without going into details we must be aware of the fact that for driving on an open road, the Convention requires a driver to be always present which is implemented in the national law of almost all countries. For driving on private territory, the traffic law is not applicable – the car would be a moving machine. Nevertheless, also here, safety requirements have to be obeyed. This type of vehicles is known as Automated Guided Vehicles (AGVs) and is becoming more and more popular.

The general impression on how autonomous driving works is mainly dominated by vehicles as the Google[14] vehicle or the Tesla[9] and other systems that have shown up in the meanwhile. Simpler systems are those for automated parking, which is carried out using the mobile phone, the driver being outside. Studies for autonomous driving have been carried out with a driver on board for testing purposes or for demonstration. Automated Guided Vehicle on closed areas or transport systems in workshops are also applied. The latter systems are strictly speaking not road vehicles but moving machines.

As an example, just consider the Google vehicle [14]. This is a Smart-like vehicle with two seats and one can read that it drives autonomously, with no driver action being necessary.

Alas, an accident has been reported and Google said it bears "some responsibility" after the car struck the municipal bus in Mountain View, Google [14]. That means that the Google vehicle caused a crash. In that case, the car would be responsible, i.e. finally its manufacturer. However, also the driver and his responsibility need to be discussed.

Another example is a Tesla vehicle [9] that crashed into a trailer. The driver did not react since he relied on automated driving and died as a consequence of the crash. In fact, the technical driving system of the Tesla was not able to detect the trailer. Then the question arises on the responsibility for the accident. Surely, the automatic systems needed permanent supervision by the driver and the question arises whether the driver was sufficiently instructed. Also, it needs to be discussed whether the driver had the possibility to stop the vehicle or take over the steer. This includes reaction time as well as features of the technical systems.

By the SAE [22] and the UN [24] the following levels have been defined.

• 0 No automation
• 1 Driver assistance
• 2 Partial automation
• 3 Conditional automation
• 4 High automation
• 5 Full automation

Table 1. Overview of automation levels [22]

SAE level	Name	Narrative definition	Execution of Steering and Acceleration / Deceleration	Monitoring of Diving Equipment	Fallback Performance of Dynamic Driving Task	System capability (Driving Modes)
Human driver monitors the driving environment						
0	No automation	The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver assistance	The driving-mode specific execution by a driver assistance system of either steering or acceleration / deceleration using information about the driving environment and with expectation that the human driver performs all remaining aspects of the dynamic driving task	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial automation	The driving mode-specific execution by one or more driver assistance systems of both steering and acceleration / deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task	System	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving equipment						
3	Conditional automation	The driving mode-specific execution by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene	System	System	Human driver	Some driving modes
4	High automation	The driving mode-specific execution by an automated driving system of all aspects of the dynamic driving task, even if the human driver does not respond appropriately to a request to intervene	System	System	System	Some driving modes
5	Full automation	The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.	System	System	System	All driving modes

Detailed information on the levels is shown on the following table 1.

The currently present systems are mainly systems for assisted driving. The assistant helps in simple situations, however, the driver has always full responsibility. Examples are

- Distance assistant,
- Platooning,
- Lane assistant,
- Highway pilot for trucks.

A short glance on the approval systems shows the differences:

- Automated metros are assessed according to EN 50126 [6], EN 50128 [7], EN 50129 [8] and approved based on local laws on metros, that differ per country,
- Road vehicles are approved by a European approval based on ECE rules. In Germany this institution for approval is the KBA, in Netherlands this is the RDW,
- AGVs are not road vehicle and not a train, they are considered as automated machines and approval is according to Machine directive [19] and IEC 61508 [16].

A new law for homologation of road vehicles in Germany allows automated driving in specific cases – note that this is not assisted driving – but driver must be able to overrule the technical system.

This is in line with Convention on Road Traffic [3], which says:

- article 8, 1: "Every moving vehicle or combination of vehicles shall have a driver",
- article 8, 3: „ Every driver shall possess the necessary physical and mental ability and be in a fit physical and mental condition to drive.",
- article 8, 5. "Every driver shall at all times be able to control his vehicle or to guide his animals."

Currently, these principles are implemented in the laws of the countries.

From this discussion we can conclude that experience and also safety principles from automatic metros cannot be directly used for road vehicles. First, the legal situation is different, second, there are differences regarding the applicable standards and third, the environment is different. An automatic metro is located in a controlled and well-defined environment that makes automatic driving possible. Passengers are separated from moving systems, e.g. by using platform screen doors that allow access only directly into the train. This does not hold in the general situation for a road vehicle.

3. General Safety principles and safety integrity levels

In this chapter we will briefly remember the main safety principles, see Gülker & Schäbe [15] and Gayen & Schäbe [11,12] and Gräfling & Schäbe [13] and give a short review on safety integrity levels.

Fail safe: If the system has a safe stopping state, i.e. a safe state in which it is not operational and this state is stable which can be reached fast enough, then the fail safe principle can be applied. It means that a system is brought into this sate if a failure occurs which cannot be tolerated. This principle can be implemented as inherent fail-safety, reactive fail-safety or composite fail-safety.

Safe life (fail operational): If the system does not have a safe stopping state which can reached fast enough, then the safety function has to be ensured. This is mainly done by using redundancies.

Fail silent: The fail silent principle is applied to a function the loss of which is tolerable since it is either an assistance function or the function is implemented in several instances. Then, failure of the function must be such that there is no repercussion on the safe functioning of the system. That means, that a fail-silent system must detect its failures and possible dangerous states and switch itself off without influencing other systems in a dangerous way.

Whenever a function might lead to harm, i.e. injury of fatalities to persons, material damage, damage to the environment, functional safety has to be applied. That means that the risk arising from a possible functional failure must be reduced to an acceptable level.

For this sake, safety integrity levels are defined. According to ISO 26262 [17] this can be QM, ASIL A to ASIL D with ASIL D being the most severe. IEC 61508 [16], which knows the safety integrity levels 1 to 4. is applicable for moving machines.

In practice this means, that for all driving functions and all driving sub-systems, the necessary safety level (ASIL or SIL) has to be determined using a risk analysis.

A safe life system is a system, in contrast to a fail-safe system, does not switch itself off in case of a failure, but where the safety function is ensured even in case of one (or sometimes several) failures.

The safety integrity levels (SIL / ASIL) are defined in standards for functional safety. IEC 61508 and EN 50129 define SIL 1 to SIL 4. ISO 26262 [17] defines the automotive SIL (ASIL) A to D.

The SIL / ASIL consists of two essential requirements:

- Maximum tolerable rate of dangerous failure which cannot be exceeded
- Measures against systematic failures (verification, traceability of requirement, specific techniques)

4. Abstract Model of the System

Lotz [18] proposed an architecture consisting of three levels: a navigational level, a manoeuvring level and a controller level. We will try to discuss a model that is as simple as possible.

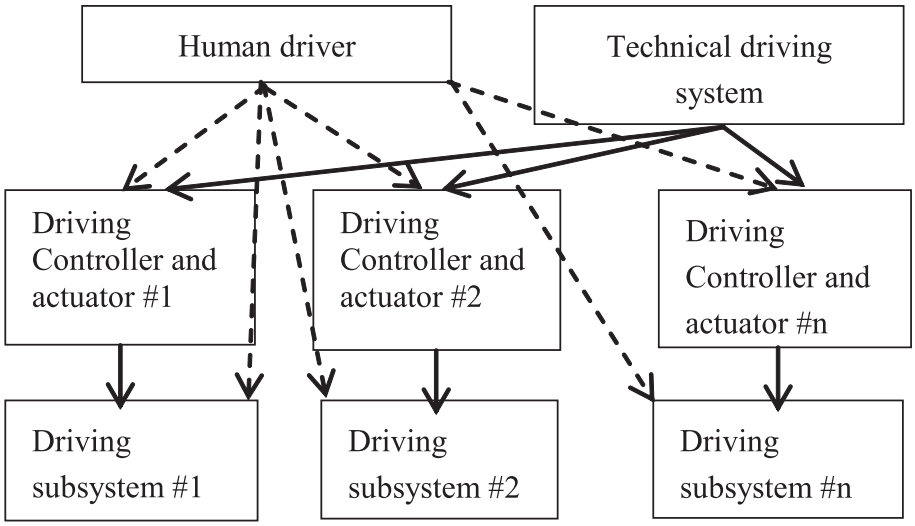


Figure 1. Scheme of a vehicle with automatic driving capabilities

For systems that drive automatically, partially automatically or autonomously, we will use the following very simple structure for the system. In fact, this system must be equipped not only with a human driver, but also with a technical driving system, that carries out the driving.

The vehicle consists of driving sub-systems as steering, braking, acceleration systems etc. in a very abstract manner. These sub-systems could be even very simple systems as pure mechanical steering system, pneumatic brake systems etc. The driving is carried out by the human driver using these driving sub-systems directly.

The manoeuvring and navigational level according to Lotz [18] have here been combined in one system (human driver / technical driving system).

If a vehicle shall be operated by a technical system which does the driving in place of the human driver or supports the human driver, then this system must have access to the driving sub-systems. This is possible only using a driving controller and actuator. That means that these types of systems must be present in the vehicle to allow for driving by a technical system.

Then, this allows also the human driver to access the driving sub-systems via the driving controllers.

Hence, there are different possibilities to operate these subsystems.

a. The driver can directly access the driving sub-systems, e.g. the steering wheel is mechanically connected to the steered axle.

b. The driver accesses the driving sub-system via a controller and an actuator which operate the sub-system electronically. A typical example for such a system is an electric parking brake.

c. The technical driving system accesses the driving subsystem via a controller and actuator

Discussing figure 1 it becomes clear that arbitration between the commands of the human driver and the technical driving system must take place.

There are different levels on which arbitration can take place:

a) driving subsystems

In this case the force applied by the driving controller and actuator must be so small that the driver can always overrule without a problem. However, he would be either required to switch off the driving controller an actuator manually, or those system need to have an in-built function to detect the interference of the driver and switch themselves off.

b) driving controller and actuator

Here, the driving controller has two inputs with different priority. The high priority input is used by the driver, the low priority input by the technical driving system. The arbitration is done by the driving controller which detects overruling by the human driver and switches off the input from the technical driving system. Many controllers in modern cars (brake controller, steering controller etc.) have an additional input for assistance systems which just fulfils this requirement. This approach assumes that the human driver himself controls the vehicle via x-by-wire via the relevant controllers.

c) technical driving system

Arbitration is between the human driver and the technical driving system. If the human driver overrules the technical driving system the latter does not generate its own control signals but simply transfers the signals of the human driver to the driving controllers.

The choice on one of the approaches is a choice of the manufacturer of the vehicle. However, this choice influences the suppliers of the driving controllers and actuators. They need to implement different architectures in their controllers.

In case a) they need to detect intervention of the man driver and deactivate the actuator.

In case b) they need to have two inputs with different priority and need to carry out arbitration

In case c) only one input is necessary and no arbitration is necessary.

We see that x-by-wire is a necessary precondition for solutions b) and c).

We will guide ourselves by the requirements for a fully autonomous driving vehicle with a possibility for the human driver to take over responsibility at any time.

5. Level analysis

5.1. Levels 0 and 1

In this section we will analyse the levels (SAE [22]) of automatisation and draw conclusions for the safety architecture of a vehicle.

In levels 0-1 execution of steering and acceleration and deceleration is in the responsibility of the human driver, the driver is responsible for monitoring and the technical system is able to support some driving modes (level 1).

That means, the human driver is doing the driving and the technical driving system can only add some supporting functionality as warn the driver or react in cases, when he is not able to react (emergency brake assistant). This means that the technical driving system must be fail silent, i.e. upon failure of this system the driving behaviour of the vehicle must not be influenced or only influenced in such a manner that safe driving is still possible. The driver should be warned, if such an assistance system fails to work.

5.2. Level 2

In automation level 2, the system takes responsibility in some driving modes. The human driver monitors the technical driving system and he is the fall back solution. That means, that all technical systems are pure assistance systems and that

R1) The driver must have the technical possibility to interfere, i.e. to override the technical systems. That means, that each controller for acceleration, braking and steering that receives signals from the human driver and from the technical driving system must have a voter which always gives priority to the driver. In fact this means that an electronic control system needs to be present for these function that has an ASIL that coincides with the function, mainly this would be ASIL D. This control system then must have a priority input for the driver and another non-priority input for the technical driving system. The relevant driving controller must detect, when the driver wants to override the technical driving system and has to carry out the required reaction.

R2) The driver must have enough time to detect wrong or faulty behaviour of the technical driving system and react and be able to bring the vehicle back to a safe driving state. That means, that the controllers have to limit the influence of the technical driving system, e.g. limit the level of acceleration, deceleration and the steering angles or angular speed and angular acceleration and jerks so that the driver always has the time to react.

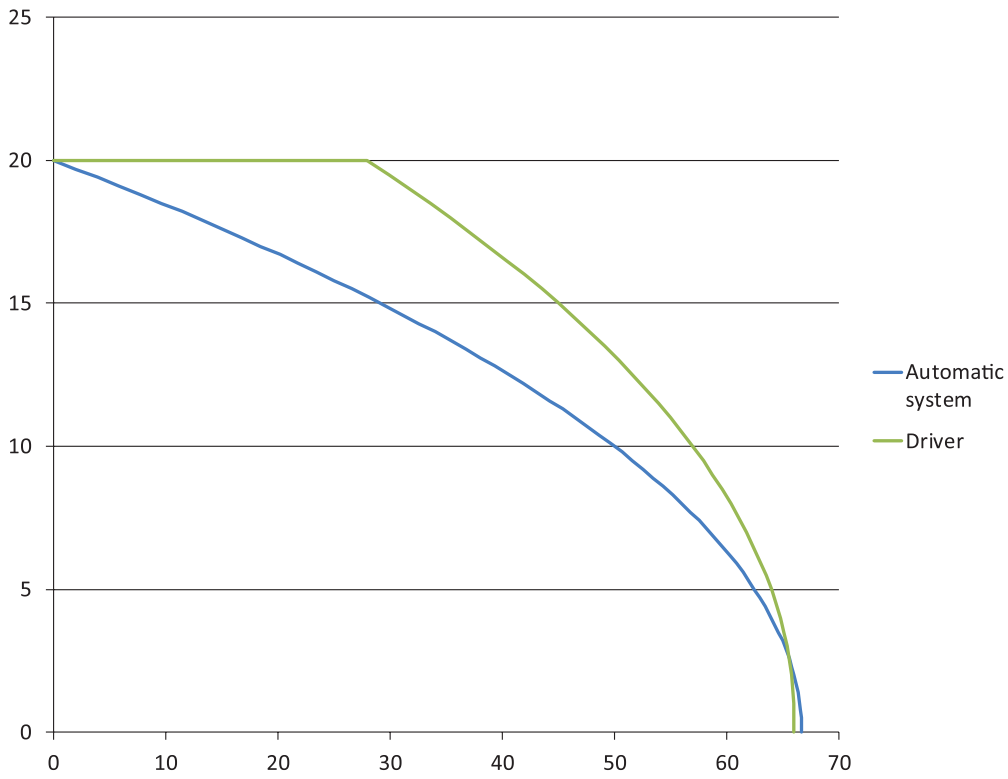


Figure 2. Example for a brake curve.

Moreover, the driver must be trained for this function or the controllers must be designed in such a manner that they give enough time for reaction for any driver.

Requirement R2 leads to the following requirements for automatic driving.

• Braking: braking by automatic systems must be with a smaller acceleration than the driver could apply, the difference in accelerations (vehicle, driver) must still allow for a reaction time of the driver (braking curves),

• Steering: the distance from dangerous objects (other vehicles, border of the lane etc.) must be large enough to allow for drivers reaction, together with a limit of the steering angle. This might lead to speed restrictions.

• Perhaps the driver needs special training.

Figure 2 shows an example of a brake curve. Speed (m/s) versus distance is shown. There are two curves, one for automatic braking (deceleration 3 m/s^2) versus braking by driver (5 m/s^2), where a reaction time of 1.3 s has been taken into account for the driver. The initial speed is 20 m/s.

In this example, the driver is still able to come to a standstill in time, if he detects that the automatic system fails to brake. Of course, the driver must react and be able to react with 1.3 s.

For steering, similar requirements must be taken into account: Driver must have necessary reaction time. This reaction time depends on the distance to shoulder or adjacent lane, the speed and the reaction of the system. The latter includes maximal angular velocities and accelerations with which the system might show a faulty reaction.

The current technical solutions are supported by the following existing equipment:

• Different controllers or safe computers are available that are qualified according to up to ASIL D / SIL 4,

• Sometimes even „intelligent sensors“ with a SIL available.

• Different, diverse sensors (no SIL), which are cross-validated by the safe computer. Examples of such sensors are cameras, lasers, radar, infrared, ultrasonic etc.

• Multiple, diverse actors; safety relays as electric actors, the use of proven mechanical systems is also possible.

5.3. Level 3

Level 3 differs from level 2 in just one point. The technical driving system is responsible for monitoring of the driving equipment. That means that the system must diagnose itself and the environment in order to decide whether it can go on with driving or whether the human driver must act as a fall back solution. The following questions are important

R3) A clear handshake must be defined between human driver and technical driving system. Either the technical driving system must go on with functioning until the human driver has accepted to take over control or

R4) A certain time of e.g. one second is foreseen for the human driver to take over control at any time, if the technical driving system asks him to do so.

In the first case, the technical driving must be safe life, in the second case the latency time for the human driver to take over must be ensured by technical systems – either by the safe life property or just by the driving situations and speed. Timing considerations can be found in Vogelpohl et al. [25].

5.4. Levels 4 and 5

Levels 4 and 5 are even more advanced. The difference between levels 4 and 5 is relatively small, since the distribution of responsibilities is the same, only in level 4 some driving modes are excluded, which allows the technical driving system to have limited capabilities. However, when this system is active, it must be able to take full responsibility.

As a consequence, the technical driving system must always ensure safe driving and would need to be safe life.

The relevant requirements are derived the so called GAMÈ principle, which can be found e.g. in EN 50126 [6] “All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system“. Here we apply the phrase on guided transport system just to an autonomously driving vehicle. We compare the classical vehicle with a human driver with an autonomously driving vehicle. Then, there are two aspects to be considered:

a) Performance and

b) The technical system (vehicle and technical driving system) are sufficiently free from dangerous failures.

Both aspects are considered separately. For performance, the technical driving system must be at least as good as a human driver in the relevant driving situations, see Mazzega et al. [20]. If this cannot be ensured for all driving situations, the set of relevant driving situations must be limited and the human driver must handle the most complex ones.

The second, the safety aspect, can be handled as for any technical system by defining an appropriate safety level (ASIL or SIL). This leads to

R5) The performance of the technical driving system as reaction time, detection and handling of traffic situations etc. with an un-failed system must be at least as good as that of a human driver.

R6) The technical driving system must be developed according to a reasonable SIL / ASIL.

For level 4, a clear handshake must be defined how to pass over responsibility between technical driving system and human driver. Especially, the driving modes must be defined, where the technical driving system must not be used for reasons of e.g. insufficient performance. Handshake must be carried out either during standstill or the technical driving system must early enough inform the driver that it wants to pass control to

the driver and the driver must take responsibility. If the driver does not take over, the technical driving system must still have the possibility to stop the vehicles as long as it is in a driving mode, where automatic driving is allowed and possible.

If the driver passes responsibility to the technical driving system he must have responsibility until the technical driving system informs him that it has taken over responsibility.

When driving on an open road, the driver must be in full responsibility of the driving behavior of the vehicle, see the Convention [3]. Then, even if the technical driving system is able to perform up to SAE level 5 with the necessary safety integrity, the driver must have the possibility to intervene. So, the requirements under a) and b) mentioned for SAE level 2 hold if driving on an open road.

Autonomous driving, i.e. driving without intervention of a human driver is in fact only realized in SAE level 4 (partially) or 5 (completely). This holds even if the laws require a driver to be present.

6. Implementation of safety principles

6.1. Assistance systems

It is clear that for technical driving systems in levels up to 2 the systems must and can be fail silent and R1 and R2 must be fulfilled to ensure that the driver has the possibility to take over control.

6.2. Application of the fail-safe principle

First of all, we need to determine whether there exists a safe stopping state that can be reached sufficiently quick. Assume the velocity of the vehicle is limited to a value v, the braking deceleration is a and the reaction time t then the vehicle will stop within a distance of

$$s = v \cdot t + v/(2a).$$

Assuming that the steering has no limitation, stopping the vehicle will be a safe action if there is no obstacle within a distance of s from the outer boundaries of the. This area can be made even smaller taking into account that

- actual direction of steering and the (physical) limitations of changes of the steering angle and
- physical limitations for changing the driving direction.

In such case, the technical driving system and the driving controllers could be a complete fail safe system, stopping the vehicle in case that a failure is detected.

Depending on the free space around, the vehicle speed is determined. Obviously, the less free space available, the slower the vehicle must drive. Driving controllers need to be developed and implemented according to an adequate SIL / ASIL, which depends on the speed of the system.

6.3. Application of the safe life principle

If the vehicle is intended to move faster, the technical driving system and the driving controllers must be safe life, at least as long as the vehicle is in motion.

Driving controllers need to be developed and implemented according to an adequate SIL. This is for the brake (ABS / ESP) mainly ASIL D, for the steering ASIL B…ASIL D, depending on the function of this controller. With such a choice most of the vehicles can perform with velocities up to 250 km/h.

The implementation using safety principles differs whether we are talking on a road vehicle or a moving machine. In the first case the environment cannot be assumed to be under control, in the second case this can be ensured since the technical driving system acts on private territory. In this latter case it is much easier to ensure enough free space.

From this consideration it becomes also clear, that not all functions must be always implemented with the highest SIL / ASIL. This depends very much on the speed and the environment. If speed is limited by physical or other means, then also a lower SIL or ASIL can be used. In any case this needs to be shown by the risk analysis that has to be accrued out based on ISO 26262 [17] or IEC 61508 [16].

The following functions are the main functions to be considered:

- Guidance

How to implement such a function including the steering is described in Bouwman, Schäbe & Vis [1]. Mostly the steering of the axles needs to be safe life and a safe computer has to be used in the technical driving system to determine the steering angles. Another important function is determination of the location, where differential GPS, maps together with ultrasonic sensors, radar or lasers or cameras or different types of marking placed physical on the lane of the vehicle can be used. The safe computer will determine the real location and compare this with the assumed location as a result of its steering activities and correct or stop he vehicle.

- Braking and acceleration

Assuming that the vehicle moves along the desired trajectory, the vehicle needs to start, move and stop. So the vehicle needs to react to these commands. It is important to limit the speed e.g. in curves or at narrow places and to be able to perform an emergency stop, if parts of the system fail. In order to perform this function, the system needs to know the location.

Solely with these two functions the vehicle would move without taking into account the environment. Any change in the environment could lead to a collision or the vehicle leaving its track.

- Reaction to unforeseen events (obstacle)

The vehicle must be able to detect obstacles. By an obstacle we denote any object that is in the (planned) or near the (planned) trajectory of the vehicle. We need

to distinguish fixed obstacles and moving obstacles. In the beginning we consider as only strategy of the vehicle to stop in front of the obstacle. Moving around the obstacle will be considered later together with moving obstacles

a) Stationery obstacle: To detect the technical driving system needs to have a blueprint of the environment and needs to compare the real environment with that blueprint and detect differences. This would require certain algorithms for detection and classification of objects. Note that "detection" and "blueprint" does not mean that the technical driving system uses optical means. It can be optical means, but also others or in combination.

In a first step the obstacle as such needs to be detected. This is possible only at a certain distance and takes a certain time. This performance of the system might limit the speed, since the vehicle must always come to a standstill in front of the object.

In a second step the technical driving system can classify the obstacles as small. Note that this classification can be present implicitly if the technical driving system will not detect obstacles of small size. Such a classification is always present due to limitations of the system.

If the obstacle is small enough and not tall, the vehicle might decide to go on with driving.

b) Moving obstacles: Moving obstacles must be traced and its motion must be predicted using the actual position and speed. It must also be taken into account whether the object can accelerate or decelerate or change its motion direction. The latter factors strongly depend on the nature of the object. E.g. a motorbike can reach other acceleration values as a pedestrian. In order to provide a good prediction, the technical driving system must cluster moving objects according to their capability of motion. Consequently, for each object of the different clusters future positions must be predicted and the technical driving system must define the motion of the vehicle in such a manner that collisions are avoided. This might lead to the decision to stop or to keep the present fixed position.

Depending on the performance of the clustering and prediction algorithms, the technical driving system would behave more or less conservatively. With better algorithms the technical driving system would stop less frequently. We remind that the performance of these algorithms together with the stopping process in case of doubts about the future trajectory of the obstacle must be as least as good as that of a human driver. This includes of course strategies to drive around an obstacle.

c) Stationery obstacles that could start moving are in fact a combination of cases a) and b) discussed above. This means, that the technical driving system must not only trace moving obstacles but must also be able to classify stationery obstacles and provide a judgement on whether they might move and with which velocity and in which direction. A most safe strategy would surely be to stop at a safe distance of any unknown object.

If a proper reaction of the vehicle cannot be ensured for all driving situations, the set of relevant driving situations must be limited and the human driver must handle the more complex ones. This would lead to an SAE level 4 situation. An example would be a strategy, where the technical driving system takes over control on a motorway and the human driver in the city.

7. Problems

In connection with autonomous driving some problems appear. We will, discuss only some of them and try to describe possible technical solutions.

a) Assume an autonomous vehicle cannot prevent an accident and needs to make a choice, e.g. between material damage, environmental damage and injury or – even worse – injuring or even killing either an older or younger person, another driver, the own passengers etc., see e.g. EK [5] (Ethic commission)

This type of discussions automatically comes up when the responsibility for driving is carried over from the human driver to a technical driving system. The ethic problem that is behind this discussion cannot be solved in this paragraph. It is obvious that a technical solution to this problem would require to distinguish between persons and objects or animals, to discriminate between different persons etc. This would require rather complex algorithms, if it is feasible at all.

The simplest solution to the problem is to apply the principle of driving on sight. That means the rule for the autonomous vehicle would be to drive only with such a velocity that it can stop before each obstacle that appears on the road. This requirement covers:

- Detection of any obstacle above a certain size,
- Prediction of movement of objects (which is the most complicated part),
- Reducing speed if necessary to come to a standstill before such an obstacle.

Based on such a "safety first" approach, later on objects of certain (small) size can be neglected to ensure performance and avoid the vehicle stopping in front of a leaf or a plastic bag.

b) Additional information

A vehicle might optionally use additional information provided by the infrastructure, which might lead to better performance regarding safety.

Let us consider the following example. The vehicle uses information from cameras mounted on the street and has the possibility to "look around the corner". Then, it could e.g. detect a suddenly appearing child running out of the house, what a human driver could not.

c) Safety targets

Since the target of autonomous driving behaviour would always be the performance of a human driver, the technical driving system would have to fulfil this important requirement. However, assume that autonomous systems will set a new target in the future – then the question

will arise: Does the driver have the right to switch the automatic system off and decrease the achieved level of safety? It would be somehow equivalent to a train driver switching off automatic train protection, e.g. to use some speed margins. This simple example shows that the way to autonomous driving would be a one-way street, with no return to manual driving at the end.

8. Possible next steps

Based on the current status one can imagine the following future steps for road vehicle.

• Safe guidance (lane keeping) could be implemented, e.g. using differential GPS together with good update service of precise maps. All work on the road and all temporarily blocked roads need to be present on these maps.

• Stopping before traffic lights enforced by a wireless transmission of information between traffic lights and vehicles. Nevertheless, the driver needs to watch out for violators, e.g. cyclists even if he has a green lights.

• Speed limit enforcement, e.g. the speed limit is transmitted in a wireless manner form a sign broadcasting the speed limit or the sign is read by a camera, alternatively a map is used as source.

• Handling of simple traffic situations as e.g. on motorways following the lane, without overtaking manoeuvres.

• Vehicles on separated areas and on separated road networks.

Further development might lead to a following scenario, which include:

• The road or lane might be separated by two fences forming a controlled environment and on this environment a vehicle can run automatically, with steering, braking, driving implemented according to ASIL D.

• Vehicles drive with very short distances using platooning.

• At certain places entry and exit to this network of roads is allowed. There, the driver takes over the automatic vehicle and drives it manually to the destination.

• The necessary information as maps, position, speed limits, communication with other automated vehicles would be implemented on the vehicle, rather than on the road.

• The infrastructure would be rather cheap, consisting of the road and fences. Comparing this with a railway, the infrastructure is more flexible, no signals, no switches, no ballast and sleepers are necessary.

In all these cases, the relevant technical systems would need to be safe life systems with a safety level up to ASIL D / SIL 4.

Regarding future development, also possible problems need to be considered, that an automatic or autonomous vehicle driving on the road need to face to become comparable with a human driver. First of all, such a system needs to distinguish objects as persons or animals from unmoving objects. Another example would be to distinguish vehicles on high wheel from bridges etc. Another problem is that sometimes intentions of a person or animal need to be guessed: does the person or the animal intend to cross the road and step on the road? A typical example would be a child with a ball standing on the sidewalk, having dropped the ball and this has moved on the street. There are a lot of such tasks would require intelligence and one would tend to use artificial intelligence for such a task.

Assume now that artificial intelligence should be implemented for autonomous driving. Then requirements for SIL 4 / ASIL D would need to be implemented in full rigor in the software and the hardware. On the other hand, the algorithms for artificial intelligence are voluminous and complex. If then e.g. traceability needs to be shown from a requirement as e.g. “The algorithm must distinguish human beings from other objects” one might imagine the complexity of such a task. This would only be one requirement. The entire complex of requirements to the software would have to take into account a lot of driving situations, in the environment etc. If the algorithm is a self learning algorithm, one needs to ensure that it has learned in a certain time enough and this must be proven in the light of the standards IEC 61508 [16] and / or ISO 26262 [17]. Another possibility would be to use a proven in use argument and accumulated $3\ 10^9$ hours in service, see IEC 61508 [16] part 7 annex D. With 600 hours of driving per year that would mean to have 5 000 000 vehicles driving an entire year under controlled circumstances, i.e. with trained drivers that can override the system and that would also register all events – or the vehicle has to do this. One can decrease the number of vehicles by increasing the number of driving hours per year, e.g. up to 6,000, which would mean driving in shifts. Nevertheless, still 500,000 vehicles would be necessary. In addition, each change of the software would require to repeat this approval process

The conclusions is that solutions for the safety relevant software must be simpler, without guessing intentions etc. in order to overcome these problems. Artificial intelligence would be good for assistance systems.

9. Conclusions

In this paper we have provided some considerations on automatic (or autonomous) driving for rail and road vehicles. It turns out that for road vehicles, the environment is much more complex than for rail vehicles. Therefore, the experience from e.g. automatic metros cannot be directly used.

In this paper we have presented some ideas on possible safety architecture for autonomous driving, deduced from known safety principles and from general requirements. We have analysed the SAE levels and the implication for the safety architecture per level.

Possible implementation principles have been described and specific problems of autonomous driving have been discussed. So, it is recommended to follow the design principles as described in chapter 6 for the implementation of autonomous driving systems. It is important to understand the safety architecture of the vehicle and to find out, whether it is a pure assistance system (fail-silent), whether the fail-safe principle is applied or the safe-life principle need to be applied. The guidance of this principles should be used for safety assessment of autonomously driving vehicles.

Most of the existing systems are either pure assistance systems or they are dedicated to simplified traffic situations

It has to be expected that the first safe solutions for autonomous driving would come for situations with a simplified environment, especially where the environment is controlled or even adapted to the task of autonomous driving. Here, a special solutions are AGV (automatic guided vehicles) that are just moving in an environment fully adapted to them, but not on an open road.

References

[1] Bouwman, R., Schäbe, H., Vis, H. (2009), Application of safety principles for a guidance system in public transport, *ESREL 2009, Proceedings Reliability, Risk and Safety*, vol. 3, p. 2275-2278.

[2] Breitinger M. (2016), Kabinett erlaubt teilautomatisiertes Fahren, http://www.zeit.de/mobilitaet/2016-04/autonomes-fahren-gesetzentwurf-verkehrsrecht-alexander-dobrindt, published 13.4.2016, retrieved on 19.10.2017

[3] Convention (1973), *Convention on Road Traffic*, 8.11.1968, European Additional Treaty from 1.5.1071 and Protocol 1.3.1973.

[4] Daimler 2017 The Mercedes-Benz Future Bus The future of mobility, *https://www.daimler.com/innovation/autonomous-driving/future-bus.html*, retrieved on 19.10.2017

[5] EK 2017, *ETHIK-KOMMISSION AUTOMATISIERTES UND VERNETZTES FAHRE*N (Ethics Commission for automated and networked driving, in German), Bericht, Juni 2017, WWW.BMVDI.DE

[6] EN 50126 *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety* (RAMS) (EN 50126), 1999

[7] EN 50128 Railway applications — Communication, signaling and processing systems — Software for railway control and protection systems, 2011, correction 2014.

[8] EN 50129 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, 2003

[9] Focus (2016) Todesfall im selbstfahrenden E-AutoUS-Verkehrsaufsicht prüft Teslas "Autopilot", *http://www.focus.de/auto/elektroauto/todesfall-im-selbstfahrenden-auto-us-verkehrsaufsicht-prueft-teslas-autopilot_id_5687341.html*, 1.7.2016

[10] Frog 2017, Website, www.frog.nl, retrieved on 19.10.2017

[11] Gayen, J.-T., Schäbe, H. (Miss-) Konzeptionen von Sicherheitsprinzipien, *Signal und Draht*, 100 Nr. 7+8 (2008) pp. 11-18.

[12] Gayen, J.-T. , Schäbe, H. (Mis-) conceptions of safety principles, *ESREL 2008, Proceedings Safety, Reliability and Risk analysis*, vol. 2, pp. 1283-1291

[13] Gräfling, S., Schäbe, H., The agri-motive safety performance integrity level – or how do you call it?, *ESREL 2012 / PSAM 11*, paper 26 Fr2_1, 10 p..

[14] Google car (2016) Google self-driving car hits public bus near Mountain View headquarters *http://www.mercurynews.com/2016/02/29/google-self-driving-car-hits-public-bus-near-mountain-view-headquarters/*, retrieved on 19.10.2017.

[15] Gülker, J., Schäbe, H., 2006, Physical Principles of Safety, *Safety and Reliability for Managing Risk, Proc. of ESREL 2006*, pp. 1045-1050.

[16] IEC 61508 *Functional safety of electrical / electronic / programmable electronic safety-related systems*, 2010, parts 1-7,

[17] ISO 26262 Road vehicles — Functional safety, 2018, parts 1-10,

[18] Lotz, G.O. 2017, *Eine Referenzarchitektur für die assistierte und automatisierte Fahrzeugführung mit Fahrereinbindung*, Dissertation Technical University Darmstadt, 2017 (A reference architecture for assisted and automatic driving with driver intervention),

[19] Machine Directive (2006) DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

[20] Mazzega, J., Köster, F., Lemmer, K.,. Form, T., *Absicherung hochautomatisierter Fahrfunktionen*, Automobiltechnische Zeitschrift, 118 (2016), no. 10, 48-52 (Safe Implementation of Highly automated Driving Functions)

[21] Nahverkehrspraxis (2017), Weltpremiere: Daimler Buses präsentiert autonom fahrenden Stadtbus", *http://www.nahverkehrs-praxis.de/news/nahverkehr-spraxis-top-news/article/weltpremiere-daimler-buses-praesentiert-autonom-fahrenden-stadtbus/*, retrieved on 19.10.2017

[22] SAE (2016) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, *SAE J3016*, September 2016.

[23] UITP 2017, *International Association of Public Transport*. "A global bid for automation: UITP Observatory of Automated Metros confirms sustained growth rates for the coming years". *Belgium*, retrieved 19.10.2017

[24] UN (2017) *Economic Commission for Europe, Inland Transport Committee, World Forum for Harmonization of Vehicle Regulations, Consolidated Resolu-*

tion on the Construction of Vehicles, (R.E.3), Revision 6, 11.7.2017

[25] Vogelpohl, T., Vollrath, M., Kühn, M. Hummel, T. Gehlert, T., (2016), *Übergabe von hochautomatisiertem Fahren zu manueller Steuerung*, Forschungsbericht Nr. 39, Unfallforschung der Versicherer GDV, August 2016, ISBN 978-3-939163-67-1

[26] Short English Version:

[27] Vogelpohl, T., Vollrath, M. (2016) UDV (Unfallforschung der Versicherer) *Takeover times in highly automated driving Compact accident research*, Nr.57, 07/2016

[28] Wachenfeld, H. K. (2016), *How Stochastic can Help to Introduce Automated Driving*, Dissertation, Technical University Darmstadt, 19.10.2016

About the author

Hendrik Schäbe, Dr. rer. nat. habil., Chief Expert on Reliability, Operational Availability, Maintainability and Safety, TÜV Rheinland InterTraffic, Cologne, Germany, e-mail: schaebe@de.tuv.com

Received on: 18.03.2019

Original article
Dependability, vol. 19 no. 3, 2019 DOI: 10.21683/1729-2646-2019-19-3-34-39

Progressive damage to structural elements of pipeline systems and efficiency assessment of protection measures

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

Igor A. Tararychkin

Abstract. *The* **Aim** *of this paper is to evaluate the effect of transportation node protection on the resilience of pipeline systems to the development of damage by the mechanism of progressive blocking of nodes as well as the efficiency analysis of the employed protection measures. Damage to a point element of a system due to simultaneous transition into the down state of all the pipelines converging into it is called blocking. The process of progressive blocking of a transportation system's nodes in a random order is considered to be progressive damage of a network structure. Progressive damage is a hazardous emergency development scenario that is associated with the disconnection of first some, then all end product consumers from the source. A system's ability to resist progressive damage is estimated by the resilience indicator, the average share of the damaged nodes whose blocking in a random order causes the disconnection of all end product consumers from the source.* **Methods of research.** *A system's indicator of resilience to progressive blocking of nodes was defined using computer simulation. The resilience indicator can only be used in comparative analysis of network structure properties if the analyzed systems are comparable. The condition of comparability of systems with protected point elements is the presence of equal numbers of disconnectable consumer nodes and damageable nodes. If the analyzed systems include protective peripheral clusters that represent interconnected sets of point elements, the following must be equal to enable the comparability of such systems:*
– number of peripheral clusters with two and more consumer nodes on condition of equal number of such nodes within each system;
– most probable order of disconnection from the source of both individual consumers and peripheral clusters with equal numbers of end product consumers.
Results. *A system's resilience to progressive blocking can be improved by means of managerial and technical measures of transportation node protection. It has been established that the highest efficiency of protection of individual point elements is achieved in case of protection of a consumer node located at the shortest possible distance from the source of the end product. It is demonstrated that the peripheral cluster for protection of a transportation system should be synthesized by including consumers situated at the minimal possible distance from the source node.*
Conclusions. *The development of emergency situations by the mechanism of progressive blocking of nodes is a hazardous scenario of pipeline system damage. The resilience of a network structure to damage can be improved by means of measures of transportation system nodes protection. The highest efficiency of protection of individual point elements is achieved in case of protection of a consumer node located at the shortest possible distance from the source of the end product. The peripheral cluster for protection of a transportation system from progressive damage should be synthesized by including consumers situated at the minimal possible distance from the source node.*

Keywords: *system, pipeline, node, damage, protection, resilience.*

For citation: *Tararychkin IA. Progressive damage to structural elements of pipeline systems and efficiency assessment of protection measures. Dependability 2019; 3: 34-39 p. DOI: 10.21683/1729-2646-2019-19-3-34-39*

Pipeline transportation systems are used in various industries for the purpose of delivering fuel, raw materials and end products to consumers. Such complex engineering facilities may include larger numbers of structural elements that interact among each other and ensure the reproduction of the functional effect even in the presence of damaging factors [1-3]. The operation of such potentially hazardous technical systems is associated with the possibility of failure of individual structural elements both due to the effects of internal processes, and as the result of interaction with the environment [4-7].

Due to the presence of excessive connections within a network the transition of one or more structural elements into the down state can be usually compensated by immediate redistribution of traffic.

If, as an emergency unfolds, the network damage process continues, that will cause first some, then all end product consumers to be disconnected.

In this context, within a short period of time, some number of linear and point elements may transition into the down state [8-11]. Damage to a linear element (pipeline) means its inability to further handle traffic. If a structure's point element is damaged, any traffic through such node will also be terminated.

Then, the blocking of an individual node of a system may be considered as the result of simultaneous transition into the down state of all the pipelines converging into it.

If the damage to a network structure occurs in the form of progressive blocking of individual system nodes in a random order, such scenario of emergency development is called progressive blocking.

Progressive blocking is accompanied by a rapid degradation of the transportation capacity of the system and may cause the disconnection from the source of all end product consumers.

A system's resilience to progressive blocking can be improved by protecting individual point elements. Protection of a transportation node is understood as a set of measures to ensure guaranteed non-transition into the down state of all pipelines that converge into it.

It is obvious that node protection is an efficient tool of improving a whole system's resilience to the development of progressive blocking, however, literary sources do not provide recommendations regarding the implementation of protection measures and selection of optimal protection architectures.

The *Aim of this paper* is to evaluate the effect of transportation node protection on the resilience of pipeline systems to the development of damage by the mechanism of progressive blocking of nodes, as well as to analyze the efficiency of the employed protection measures.

The effect of protection of individual system nodes on its resilience to the development of progressive damage

Let us examine the structure diagram of a pipeline system shown in Fig. 1. It has the source node A, as well as consumers B, C, D, E, F.

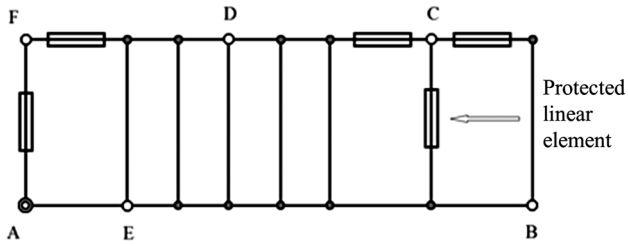


Figure 1. Structure diagram of a pipeline system with protected transportation nodes

Consumer nodes C and F are protected, as only protected linear elements converge into them. Node F is connected to the source that is protected by transportation connection AF, cannot be disconnected from it and thus is not disconnectable. Protected node C is considered disconnectable despite being protected, as in case of progressive blocking it can be disconnected from the source.

The following designations are used in the research of the process of progressive blocking:

U_0, the total number of product consumers that may be disconnected from the source in case of progressive blocking development;

Q_0, the share of the total number of disconnectable consumers that were disconnected from the source of product at the given instant of system time;

R_y, the total number of damageable, i.e. unprotected transportation nodes that can be blocked;

r_x, the current number of blocked nodes in the process of progressive damage;

Y, the degree of damage of the unprotected part of a network structure observed at the given instant of system time ($Y = r_x / R_y$).

Dependence $Q_0(Y)$ is the damage diagram of the structure and has the form of a staircase function. Thus, for the network entity shown in Fig. 1 the damage diagram is shown in Fig. 2.

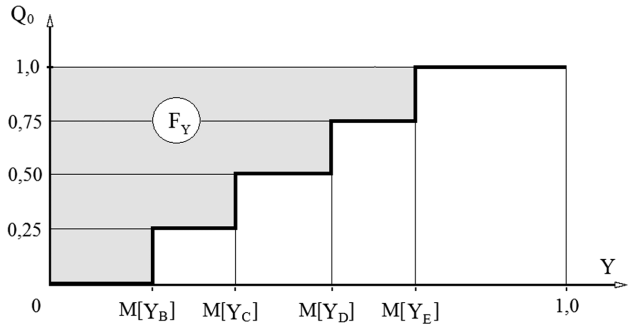


Figure 2. Damage diagram of a network structure

Values $M[Y_B]$, … $M[Y_E]$ are the mathematical expectations of the scopes of damage that trigger progressive disconnection of consumers B, … E from the source [12].

A system's indicator of resilience to the development of progressive blocking of nodes is the area F_Y of the staircase figure shown in Fig. 2:

$$F_Y = \{M[Y_B] + M[Y_C] + M[Y_D] + M[Y_E]\} / U_0.$$

Thus, the resilience indicator represents the average share of a system's damageable nodes whose blocking in a random order causes the disconnection of all disconnectable end product consumers from the source.

As pipeline transportation systems may differ in complexity and include various numbers of structural elements, the correct comparison of the values of their durability indicators is only possible if the corresponding dependences $Q_0(Y)$ are similar to each other.

Matching of damage diagrams of systems with protected point elements is, in principle, only possible under certain conditions. Let us assume that the analyzed network structures have identical numbers of:

- consumer nodes that may be disconnected from the source in case of blocking process development;
- damageable nodes, i.e. nodes that may transition into the down state due to the lack of appropriate protection.

In this case, the considered systems are comparable, while the comparison of the values of their resilience indicators proves to be correct.

If the set of protected system nodes is interconnected, such network fragment is considered to be a protection cluster [13]. A cluster is called central if it contains a source node. Otherwise it is called peripheral.

The presence of protection clusters has a significant effect on the development of progressive blocking. For instance, if a peripheral cluster has several consumers, at a certain instant of system time they will be disconnected from the source of product simultaneously.

For that reason, besides the above list of comparability conditions, sufficient conditions must be specified, whose fulfilment enables correct comparability of expected values of F_γ in cases when the system has protection clusters.

So, if there are peripheral clusters, the network structures are comparable if they comply with the additional list of conditions and have the following features:

– identical numbers of peripheral clusters with two and more consumer nodes and identical number of such nodes within each;

– identical orders of disconnection from the source of both individual consumers and peripheral clusters with equal numbers of product consumers.

Thus, the above primary and additional sufficient conditions of comparability of network structure properties allow identifying the feasibility of comparison of their resilience indicator values.

The efficiency analysis of the protection measures taken as regards individual nodes of a transportation system took into account the results of computer simulation [14]. The resilience of a system was estimated both subject to the remoteness of the protected transportation node from the source, and its functionality.

In the general case, a transportation system can include the following types of point elements:

– source of the end product node;
– consumer nodes;
– hubs.

The above elements have different functionalities, and it can be assumed that their protection affects the resilience of systems to progressive damage to different extents. Additionally, the resilience of a network entity to damage also depends on the distance between the protected node and the source of the end product. The remoteness from the source is defined as the minimal number of transitions that must be made along the existing network in order to match the analyzed node with the active source.

The effects of the above factors on the development of progressive blocking of nodes were studied using a system whose structure diagram is shown in Fig. 3.

The choice of the above diagram is due to the following structural features:

– network nodes left and right of the source of product are symmetrical;

– each consumer node on the left can be associated with a hub on the right that is at the same distance from the source of product;

– all consumer nodes are at various distances from the source of the end product.

In the process of progressive damage simulation each calculation model included only one protected node. For

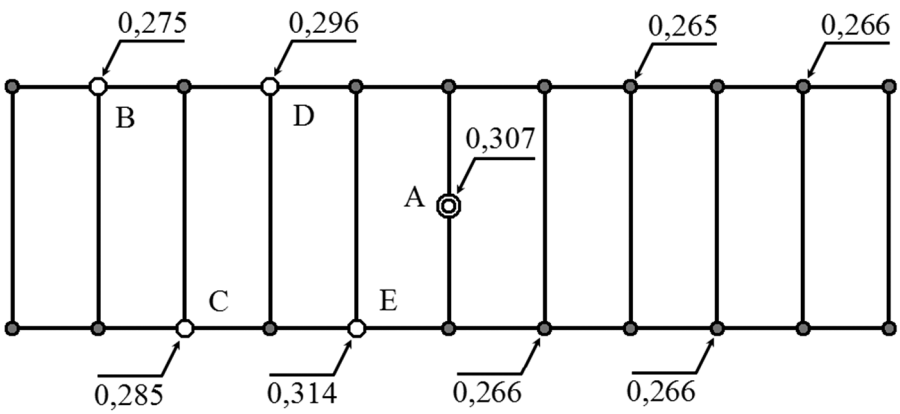


Fig. 3. Structure diagram used for the estimation of the effect of protection of individual nodes of a transportation system on its resilience to progressive blocking

that reason, during each calculation procedure the number of damageable nodes in the system was 22, while the number of disconnectable consumers was 4.

The expected values of F_Y in such conditions are comparable and allow evaluating not only the effect of the type of a protected node, but also its remoteness from the source on the resilience of the network entity to progressive damage.

For clarity, the established values of F_Y are shown in Fig. 3 next to arrows that indicate the protected point element of the system. The analysis of the obtained results allows concluding the following:

– the most pronounced positive effect is achieved by protecting consumer nodes located at the minimal distance from the source of product;

– as the distance between the protected consumer and the source increases, the efficiency of the protection measures steadily declines;

– the efficiency of protection of hubs is lower as compared to that of the consumer nodes situated at the same distance from the source of product;

– protecting remote hubs practically does not change the values of the resilience indicator.

Thus, while evaluating the protection of individual point elements of a transportation system, it must be noted that the preferable solution consists in protecting a consumer node located at the shortest possible distance from the source of the end product.

As the distance between the protected consumer and the source increases, the efficiency of the protection measures decreases, which should be taken into consideration in the development of design solutions. Additionally, the protection of the source node should be recommended as an efficient measure, if such procedure is possible.

Protective peripheral cluster and its effect on the resilience of network structures to damage

The presence of a peripheral cluster within a transportation system has a significant effect on its resilience to the development of progressive blocking of nodes. In this context, of interest is the search for such cluster configuration that enables the maximum positive effect subject to the existing resource restrictions. In the most general terms, we can assume that the costs associated with the protection of transportation nodes are proportional to the number of protected linear elements. Then, the synthesis of the protection cluster should be considered as an optimization procedure associated with the search for the solutions that would enable the required level of protection under the minimal number of protected linear elements [15].

The complexity of the task at hand consists in the fact that obtaining reliable information on the properties of network entities with various configurations of the peripheral cluster requires a preliminary estimation of the comparability of such structures' properties.

First of all, the compared entities must have the same number of disconnectable consumers, as well as the same number of damageable nodes. Additionally, the systems' peripheral clusters must include identical numbers of end product consumers.

The above conditions are indispensable for correct comparison of the properties of network structures. The condition of sufficiency is associated with the attainment of similarity of damage diagrams of comparable entities. For that purpose, the compared structures must have the same highest-probability consumer disconnection sequence.

The above sufficient condition, provided that the system has peripheral clusters of various configurations, usually is not achieved. In this case, instead of searching for specific values of F_Y, attention should be focused on the analysis of the general patterns and dynamics of damage development in cases when the system has a protection cluster with several end product consumers. Let us note that if a peripheral cluster has several consumers, all of them are disconnected from the source of product simultaneously.

Let a system with 6 disconnectable consumers have a peripheral cluster that includes 3 consumers. Depending on the adopted configuration of the protection cluster the damage diagrams may differ. Let us assume that the cluster is situated not far from the source, and a simultaneous disconnection of its 3 consumers happens last. The damage diagram of such system will be as shown in Fig. 4a. If the cluster with three consumers disconnects first, the corresponding damage diagram is as shown in Fig. 4b.

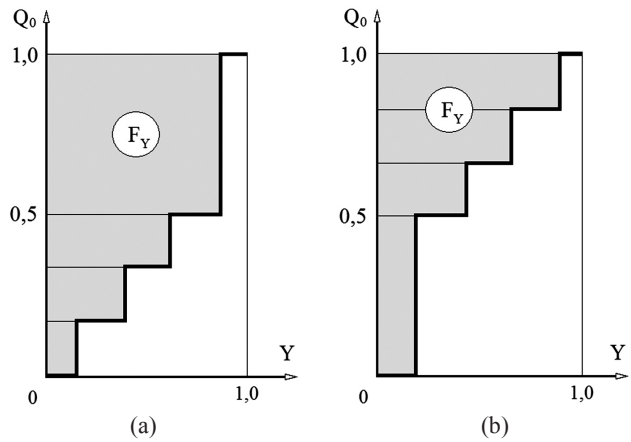


Fig. 4. Damage diagram of network structures with simultaneous disconnection from the source of the consumers that make the peripheral cluster last (a) and first (b)

As F_Y is the area of a staircase figure on the damage diagram, it should be assumed that damage in the form shown in Fig. 4a proves to be the most preferable. In this case the conditions are objectively beneficial for the maximum possible value of F_Y.

That means that it should be recommended to design the peripheral cluster in such a way as to primarily include consumers that are least remote from the source of the end product.

Let us verify that provision using a specific example. Let us examine the structure diagram of a pipeline system shown in Fig. 5a. Protection cluster C1 includes 4 consumers, that, in case of progressive blocking of nodes, will be disconnected from the source together and before all others.

The damage diagram for this case is shown in Fig. 6a. If 4 less remote consumers are included in the peripheral cluster (Fig. 5b), the damage diagram of such system will be as shown in Fig. 6b.

The obligatory requirements of compatibility of structures SIT1 and SIT2 are met in this case. The specified values of F_Y can be compared subject to the reservation of impossibility of completely matching corresponding damage diagrams.

The defined resilience characteristics of structures designated SIT1 and SIT2 are shown in Table 1.

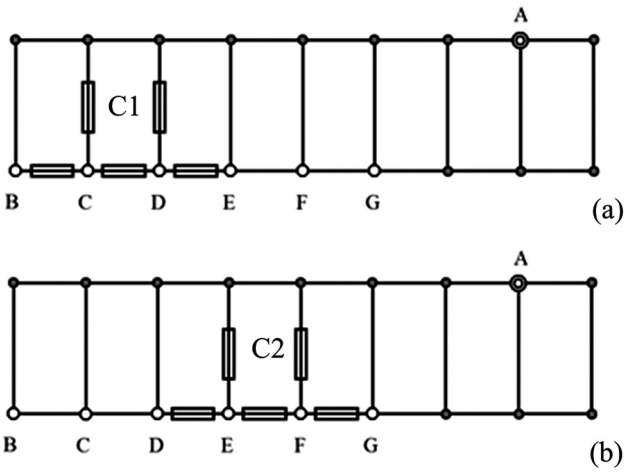


Figure 5. Structure diagrams of SIT1 (a) and SIT2 (b) with a peripheral cluster situated more or less far from the source of the end product A

As it can be seen, the previously made assumption regarding the expected properties of items is completely confirmed. That means that design solution associated with the formation of the peripheral cluster should provide for the inclusion of consumers that are least remote from the source of the end product.

The matter of the practicality of inclusion of hubs into the peripheral cluster is of applied significance and must be examined in depth. Figure 7 shows structure diagrams of SIT3 (a) and SIT4 (b) that include clusters C3 and C4 that are different from cluster C2 of system SIT2 in the presence of additional hubs. Increasing the number of nodes in clusters C3 and C4 requires the inclusion of new damaged point elements in order to ensure the observance of the comparability requirements.

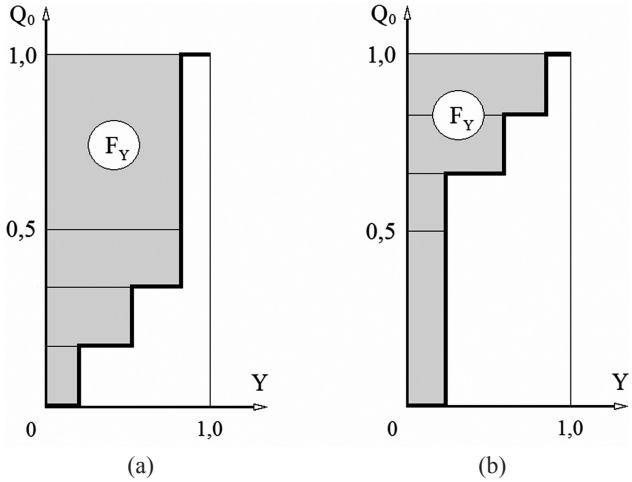


Figure 6. Appearance of the damage diagram of network structures SIT1 (a) and SIT2 (b)

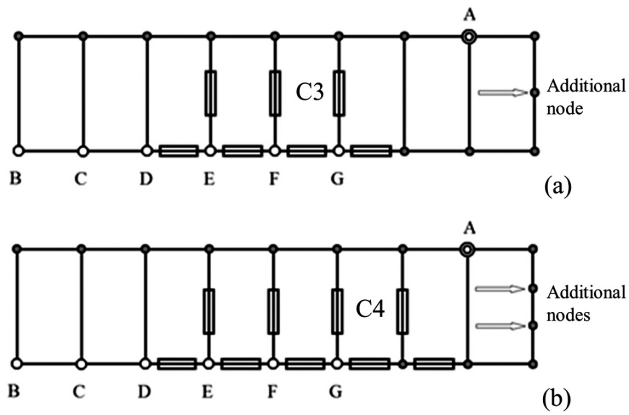


Figure 7. Structure diagrams SIT3 (a) and SIT4 (b) with additional distributed nodes and protection clusters C3 and C4

Due to that the total number of point elements in SIT3 is 19 (Fig. 7a), while SIT4 has 20 such elements (Fig. 7b).

The defined values of F_Y for the above network entities are shown in Table 1 and allow concluding that the inclusion of additional point elements into the peripheral cluster is only justified in case of decreasing distance to the source of the end product.

Conclusions

1. The development of emergency situations by the mechanism of progressive blocking of nodes is a hazardous scenario of pipeline system damage. The resilience of a network structure to damage can be improved by means of measures of transportation system nodes protection. The highest efficiency

Table 1. Characteristics of the network structures that comply with the comparability requirements

Network structure designation	Number of damageable nodes	Number of disconnectable consumer nodes		Expected value F_Y
		of the system	of the peripheral cluster	
SIT1	16	6	4	0.265
SIT2	16	6	4	0.296
SIT3	16	6	4	0.342
SIT4	16	6	4	0.401

of protection of individual point elements is achieved in case of protection of a consumer node located at the shortest possible distance from the source of the end product.

2. The peripheral cluster for protection of a transportation system from progressive damage should be synthesized by including consumers situated at the minimal possible distance from the source node.

References

[1] Cherkesov G.N., Nedosekin A.O., Vinogradov V.V. Functional survivability analysis of structurally complex technical systems. Dependability 2018;18(2):17-24.

[2] Cherkesov G.N., Nedosekin A.O. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. Dependability 2016;16(2):3-15.

[3] Cherkesov G.N., Nedosekin A.O. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. Dependability 2016;16(2):3-15.

[4] Menon S.E. Pipeline Planning and Construction Field Manual. Gulf Professional Publishing, USA; 2011.

[5] Winston R., editor. Oil and Gas Pipelines. Integrity and Safety Handbook. John Wiley & Sons, Inc.; 2015.

[6] Silowash B. Piping Systems Manual. The McGraw-Hill Companies, Inc.; 2010.

[7] Escoe K.A. Piping and Pipeline Assessment Guide. Elsevier Inc.; 2006.

[8] Sabet S.A., Reza Nayyeri S.M. Seismic Behavior of Buried Pipelines Subjected to Normal Fault Motion. Advances in Science and Technology Research Journal 2016;10(30):84-88.

[9] Vazouras P., Karamanson S. Finite element analysis of buried steel pipelines under strike-slip fault displacement. Journal of Soil Dynamics and Earth-quake Engineering 2010;30(11):1361-1376.

[10] Lele S.P., Hamilton J.M., Panico M., Arslan H. Advanced continuum modeling to determine pipeline strain demand due to ice-gouging. Journal of International Society of Offshore and Polar Engineers 2013;23(1):22-28.

[11] Ramesh S. Pipeline Integrity Handbook Risk Management and Evaluation. Elsevier Inc.; 2014.

[12] Gmurman V.E. Teoriya veroyatnostey i matematicheskaya statistika: Ucheb. posobie dlya vuzov [Probability theory and mathematical statistics: Textbook for higher educational institutions]. Moscow: Vysshaya shkola; 2004 [in Russian].

[13] Snarsky A.A., Lande D.V. Modelirovanie slozhnykh setey: Ucheb. Posobie [Simulation of complex networks: Textbook]. Kiev: Inzhiniring; 2015 [in Russian].

[14] Tararychkin I.A., Blinov S.P. Osobennosti povrezhdeniya setevykh struktur i razvitiya avariynykh situatsiy na obiektakh truboprovodnogo transporta [The distinctive features of damage to network structures and development of accidents in pipeline transportation facilities]. Bezopasnost truda v promyshlennosti 2018;3:35-39 [in Russian].

[15] Tararychkin I.A. Strategii zashchity obektov truboprovodnogo transporta ot strukturnykh povrezhdeniy pri razvitii avariynykh situatsiy [Strategies to protect pipeline transportation facilities from structural damage in emergency situations]. Bezopasnost truda v promyshlennosti 2018;2:52-57 [in Russian].

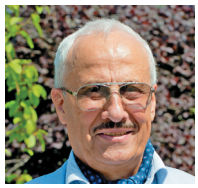
About the author

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

Original article
Dependability, vol. 19 no. 3, 2019 DOI: 10.21683/1729-2646-2019-19-3-40-46

Method of identification of the ranges of (non)acceptable factor values to reduce the risk of freight car derailment due to broken bogie solebar[1]

Igor B. Shubinsky, *JSC NIIAS, Russian Federation, Moscow*
Alexey M. Zamyshliaev, *JSC NIIAS, Russian Federation, Moscow*
Alexey N. Ignatov, *Moscow Aviation Institute, Russian Federation, Moscow*
Andrey I. Kibzun, *Moscow Aviation Institute, Russian Federation, Moscow*
Evgeny O. Novozhilov, *JSC NIIAS, Russian Federation, Moscow*



Igor B. Shubinsky

Alexey M. Zamyshliaev

Alexey N. Ignatov

Andrey I. Kibzun

Evgeny O. Novozhilov

Abstract. Aim. *According to the Russian freight car crash/derailment investigation records for the period between 2013 and 2016., derailments and crashes during train operations were mostly caused by rolling stock malfunctions, while about a third of such derailments were due to bogie solebar fracture. The average number of derailed units of rolling stock is 4.16 in case of derailment due to solebar fracture against 1.73 in case of derailments due to other rolling stock malfunctions. Previously, a method was developed that allows making decisions to discard a batch of solebars. On the other hand, solebars from batches exempt from discarding can be subject to fractures over time. In this context, it appears to be of relevance to develop a method that would enable timely uncoupling of a car for its submission to depot/full repairs in order to avoid solebar fracture. For this purpose, factor models of fracture hazard estimation should be considered. Such factors may include the number of kilometers travelled from the last maintenance depot (MD), as well as the number of kilometers and days until the next scheduled full/depot repairs. The probability of solebar fracture can be used as the quantitative characteristic of the hazard of solebar fracture. However, probability estimation in the form of, for instance, the frequency of solebar fracture is only possible when observation data is available on when fracture or critical defect of solebar did not occur, yet such data is not collected. Therefore, the hazard index of solebar fracture should be developed. As it is difficult to manage the frequency of car submission to MD, the hazard index must depend only on the number of days and kilometers to repairs. Using the constructed index, the ranges of (non) acceptable factor values must be defined in order to enable decision-making regarding car uncoupling and submission to repairs, should the MD car inspector have doubts regarding the necessity of uncoupling.* **Methods.** *Methods of mathematical programming were used in this paper*. **Results. Conclusions.** *An impact index was built that characterizes the probability of freight car solebar fracture depending on the number of days and kilometers until the next scheduled repairs of such car. Based on that index, two methods of definition of ranges of (non)acceptable factor values were proposed. The first method was based on the values of the impact index. The second one was based on the identification of some parameters of ranges of (non)acceptable factor values and selection – out of all ranges – of the best ones in terms the lowest hazard of solebar fracture. Such selection was made by solving problems of mixed integer programming with quadratic constraint.*

Keywords: *risk, derailment, solebar fracture, impact index, hazard index*

For citation: *Shubinsky IB, Zamyshliaev AM, Ignatov AN, Kibzun AI, Novozhilov EO. Method of identification of the ranges of (non)acceptable factor values to reduce the risk of freight car derailment due to broken bogie solebar. Dependability 2019; 3: 40-46 p. DOI: 10.21683/1729-2646-2019-19-3-40-46*

[1] The deliverables were obtained 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

Introduction

Operation of freight trains is associated with the risk of various adverse events: locomotive fires, uncoupling of cars in transit, collisions involving automotive vehicles and trains in rail crossings, train derailments. According to [1], the risk of the above and other transportation accidents is the functional of probability and damage. Decision-making aimed at maintaining an acceptable level of risk involves building a risk matrix according to the principles described in [2].

Out of the above and other transportation accidents both in Russia, and in the Western countries, derailments are the most common object of research. This type of incidents is characterized by grave consequences and occurs relatively frequently. In [3], the number of derailed cars was estimated using the maximum likelihood method and quantile regression. In [4], the research focused on the estimation of the number of derailed cars depending on the number of the first (counting from the front end of the train) derailed unit of rolling stock. In [5], the effect of switches and particular track geometry on the number of derailed unit of rolling stock was researched. Let us note that an examination of incident records is sufficient for damage estimation, while probability estimation also requires examining the cases when transportation incidents did not occur. For that reason, it is extremely difficult to build factor models that associate the probability of a transportation accident with the values of various factors. In this context, simplified models are normally considered that take into consideration, for instance, the track geometry at the location of derailment: in [6] the probability of derailment depended on the class of track, length of the consist and the number of travelled kilometers, [7] examined the average number of transportation incidents that depends on the number of kilometers travelled by trains and cars. An alternative solution to the above described integral estimation of probability for the purpose of reducing the frequency of derailments is the construction of impact indexes [8] that are based on the frequency of factor manifestation in cases of transportation incidents.

Out of all causes of freight car derailments/crashes due to technical rolling stock malfunctions, the solebar fractures entail the most significant damage. Research of the problem of solebar fracture normally involves the examination of the specific design solutions of such solebar and their effect on the fracture [9-11]. At the same time, we must note [12], that suggested boundaries of allowed frequency of solebar fracture and occurrence of defects that require repairs. However, that method aims to identify batches of solebars to be rejected, not to prevent the fracture of a specific solebar, which is the subject of this paper. As it is impossible to completely eliminate the probability of solebar fracture, the number of such fractures is to be minimized. In this context, it appears to be logical to estimate the probability of solebar fracture of a specific car of a specific train. However, it is impossible to build an estimate of the probability of solebar fracture using, for instance, logistic or probit regression, as there are no available statistics regarding the non-occurrence of solebar fractures. At the same time, similarly to [5], the hazard index of solebar fracture can be built using only data on the occurrence of fractures.

The construction of the hazard index involves identifying the factors that affect the frequency of the transportation incident under examination that can be managed. Three factors can be identified, i.e. the number of kilometers travelled by the train from the last maintenance depot (MD) operation, the number of kilometers a car can travel until the next depot/full repairs, number of days a car can travel until the next depot/full repairs. It is obvious that as the distance from the latest MD operation increases and the number of days and kilometers until the next scheduled repairs decreases, the probability of a defect occurring within a solebar grows. However, the frequency of MD operations is unlikely to change. At the same time, during MD operations, there is always a probability of a car being submitted to unscheduled repairs. For that reason, further on in this paper only the number of kilometers a car can travel until the next depot/full repairs, number of days a car can travel until the next depot/full repairs are considered as factors.

Given the above, the paper builds a hazard index of solebar fracture that depends on the number of kilometers travelled by train from the last MD operation and number of days from the last depot repairs/car manufacture. Based on that index, a risk matrix is constructed for the purpose of preventing solebar fracture.

Construction of the hazard index of solebar fracture

Let there be M records of depot repairs with the indication of required solebar repairs that contain the following information:

d_i, number of kilometers travelled by the train after the latest MD repairs, km;

s_i, number of kilometers travelled by the train from the latest depot/full repairs/car construction, km;

t_i, number of days from the latest depot/full repairs/car construction;

y_i, year of solebar manufacture.

As the quality of casting delivered by the same solebar manufacturer may vary from year to year, let us – out of all available records – choose those that pertain to solebars of a single manufacturer and same year of manufacture and further number and examine them. Let their total number be m. As it is difficult to manage the number of kilometers until the next MD repairs, this factor will not be further considered. As in cars of different types with solebars by the same manufacturer the number of kilometers until the next repairs may differ, we will consider the new value $\hat{s} = f(s)$ that characterizes the remaining number of kilometers until

scheduled repairs and is calculated according to [13]. Similarly, we will introduce the value $\hat{t} = g(t)$ that characterizes the remaining number of days until scheduled repairs and is also calculated according to [13].

An accurate assessment of the risk of occurrence of a defect with subsequent solebar fracture requires estimating $P(\hat{s},\hat{t})$, i.e. the probability of a solebar requiring repairs when the number of days until repairs is $\hat{t}$ and kilometers until repairs is $\hat{s}$. Assessing function $P(\hat{s},\hat{t})$ requires the availability of observations data on the absence of defects in a solebar, i.e. it must be known, when exactly a defect occurred in a solebar. However, no such observations are made. In this context, the classical probability estimation in the form of a frequency, logistic or probit regression is impossible. The authors of [8] encountered a similar problem, when they proposed using impact indexes that allow identifying the factors that cause transportation incidents and are based only on transportation incident records. Similarly to [8], let us build a heuristic function

$$I(\hat{s},\hat{t}) \overset{\text{def}}{=} \frac{\sum_{i=1}^{m} \chi_{[\hat{s},+\infty]\times[0,+\infty]\cup[0,+\infty]\times[\hat{t},+\infty]}(s_i,t_i)}{N}, \qquad (1)$$

where

$$\chi_A(z) = \begin{cases} 1, z \in A, \\ 0, z \notin A, \end{cases}$$

while N is the total number of solebars of a certain year of manufacture by a certain manufacturer that had been in operation for a year, that replaces function $P(\hat{s},\hat{t})$ that serves the analysis and reduction of the risk of solebar fracture. Function $I(\hat{s},\hat{t})$ characterizes the hazard of defect occurrence and, as a consequence, fracture of a specific solebar of a specific car and depends on the number of kilometers $\hat{s}$ and days $\hat{t}$ until the next repairs of such car. Function $I(\hat{s},\hat{t})$ is calculated as the relation of the number of cases when defects were identified in solebars with the number of days until repairs less than $\hat{t}$ or the number of kilometers until repairs less than $\hat{s}$ to the total number of solebars of a certain year of manufacture by a certain manufacturer that had been in operation for a year. Such choice of this function $I(\hat{s},\hat{t})$ is due to the fact that if, in the past, many failures/solebar fractures with the number of days until repairs less than $\hat{t}$ or number of kilometers until repairs less that $\hat{s}$ were identified, the hazard of solebar fracture is high.

Let us describe the properties of function $I(\hat{s},\hat{t})$:

(i) function $I(\hat{s},\hat{t})$ does not monotonically increase with respect to each of its parameters;

(ii) $I(+\infty,+\infty) = 0$;

(iii) $\forall \hat{s} \geq 0 \;\; \forall \hat{t} \geq 0 \;\; I(\hat{s},0) = I(0,\hat{t}) = \max\limits_{\hat{s}\geq 0,\hat{t}\geq 0} I(\hat{s},\hat{t}) = m/N.$

Let us comment the above properties. Property (i) guarantees that as the number of days or kilometers until repairs decreases, the hazard of occurrence of defects does not decrease. Let us note that function $P(\hat{s},\hat{t})$ also does not monotonously increase with respect to each of its parameters, as the physical properties of a solebar do not improve with travelled kilometers. Property (ii) guaranties that after repairs the hazard will be equal to zero (it is assumed that repairs completely eliminate defects). Property (iii) guarantees that the maximum value of the hazard index is achieved at the maximum possible distance or maximum possible number of days without repairs.

Finding the ranges of (non)acceptable factor values

According to [1], a risk matrix is a tool that allows ranking and representing risks by identifying their frequencies and severity of consequences. Essentially, a risk matrix is a function that is defined over a space composed of the probability of a transportation incident and damage that enables executive decision-making aiming to reduce the risk of such transportation incident. Such function has four values and thus divides the probability space into four connected domains: range of negligible risk, range of acceptable risk, range of undesirable risk, range of critical risk. Each of those ranges characterizes the requirements for measures aimed at reducing the risk of incident. The boundaries of such ranges can be smooth [1] or nonsmooth [14]. Normally, such matrix is used in strategic planning and management, while day-to-day management requires more than the frequency of incidents and specific yearly damage. In this context, of relevance is the construction of ranges of (non)acceptable factor values that affect the frequency and damage caused by transportation incidents, as it was done in [14]. Let us introduce the following designations:

D_1 is the range of negligible risk;

D_2 is the range of acceptable risk;

D_3 is the range of undesirable risk;

D_4 is the range of critical risk.

First, let us construct such ranges based only on the hazard index (1):

$D_1 = \{(\hat{s},\hat{t}) : 0 \leq I(\hat{s},\hat{t}) < i_1\}$;

$D_2 = \{(\hat{s},\hat{t}) : i_1 \leq I(\hat{s},\hat{t}) < i_2\}$;

$D_3 = \{(\hat{s},\hat{t}) : i_2 \leq I(\hat{s},\hat{t}) < i_3\}$;

$D_4 = \{(\hat{s},\hat{t}) : i_3 \leq I(\hat{s},\hat{t})\}$,

where $i_1 < i_2 < i_3$ are certain numbers. Such numbers can be defined based on economic considerations. Let c_1 be the average cost of depot/full repairs, c_2 be the average loss caused by car idling during repairs, while c_3 is the average damage caused by car derailment/freight train crash due to solebar fracture. It is obvious that if for a certain point $(\hat{s},\hat{t})$ the risk of solebar fracture exceeds the cost of repairs and damage caused by car idling, such point must fall within the range of undesirable or critical risk. In this context, we can assume that $i_1 = \frac{1}{2}\frac{c_1+c_2}{c_3}$, $i_2 = \frac{c_1+c_2}{c_3}$, $i_3 = \frac{3}{2}\frac{c_1+c_2}{c_3}$.

Let us note that another approach to the definition of ranges of (non)acceptable factor values involves locking certain parameters of ranges (for instance, the area) and searching for the best such ranges in plane $\hat{t}O\hat{s}$. For that purpose, we will build ranges of (non)acceptable factor values as shown in Fig. 1.

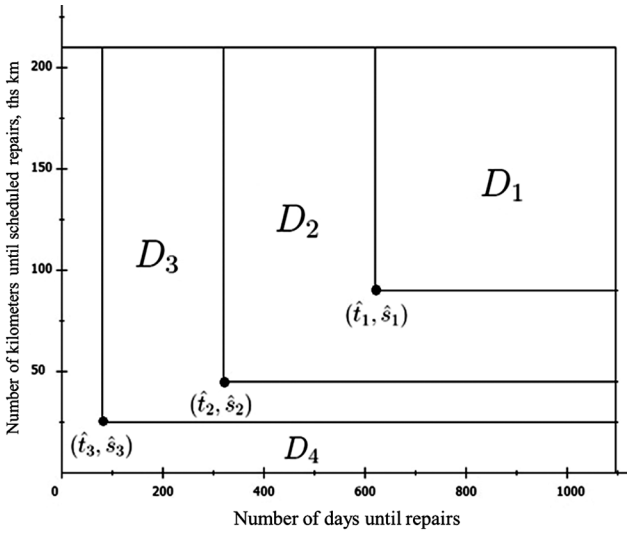


Fig. 1. Special form of the diagram of (non)acceptable factor values

Whereas

$$D_1 = (\hat{s}^1, 210000] \times (\hat{t}^1, 1095],$$
$$D_2 = (\hat{s}^2, 210000] \times (\hat{t}^2, 1095] \cap D_1,$$
$$D_3 = (\hat{s}^3, 210000] \times (\hat{t}^3, 1095] \cap D_1 \cap D_2,$$
$$D_4 = [0, 210000] \times [0, 1095] \cap D_1 \cap D_2 \cap D_3,$$

where values $\hat{s}^1 \geq \hat{s}^2 \geq \hat{s}^3$, $\hat{t}^1 \geq \hat{t}^2 \geq \hat{t}^3$ are to be identified.

In order to identify $\hat{s}^j$, $\hat{t}^j$, or essentially the boundaries of sets D_j, let us note that there is an unlimited number of sets D_j of identical area. Every such set is characterized by a certain value of maximum hazard index within it. Accordingly, we will search for such sets D_j as to

$$S_{D_1} \geq s_1, S_{D_1 \cup D_2} \geq s_2, S_{D_1 \cup D_2 \cup D_3} \geq s_3,$$

where $s_1 < s_2 < s_3$ are certain predefined parameters. Such parameters can be specified, for instance, based on geometric constraints: $s_1 = \frac{1}{4}S$, $s_2 = \frac{2}{4}S$, $s_3 = \frac{3}{4}S$, where $S = S_{D_1 \cup D_2 \cup D_3 \cup D_4}$. On optimal sets D_j the maximum value of the hazard index must be the lowest out of all the remaining sets of the same area. Given the above, the problem of finding parameters $\hat{s}^1$, $\hat{t}^1$ becomes as follows

$$\max_{\hat{s}^1 < \hat{s} \leq 210000, \hat{t}^1 < \hat{t} \leq 1095} I(\hat{s}, \hat{t}) \to \min_{\hat{s}^1 \geq 0, \hat{t}^1 \geq 0}. \quad (2)$$

with constraints

$$(210000 - \hat{s}^1)(1095 - \hat{t}^1) \geq s^1. \quad (3)$$

Problem (2) subject to constraint (3) is a problem of nonlinear programming, which complicates the solution. Let us therefore simplify the task by introducing integer $\delta_i \in \{0,1\}$ variables, $i = \overline{1, M}$. Variable δ_i equals to zero if in the i-th record out of m considered it is stated that $\hat{s}^1 \geq \hat{s}_i$ and $\hat{t}^1 \geq \hat{t}_i$, and to one, if otherwise. Using variables δ_i, we conclude that problem (2) subject to constraint (3) comes down to problem

$$\sum_{i=1}^{m} \delta_i \to \min_{210000 \geq \hat{s}^1 \geq 0, 1095 \geq \hat{t}^1 \geq 0, \delta_i \in \{0,1\}} \quad (4)$$

with constraints

$$(1 - \delta_i)\hat{s}_i \leq \hat{s}^1, i = \overline{1, m}, \quad (5)$$

$$(1 - \delta_i)\hat{t}_i \leq \hat{t}^1, i = \overline{1, m} \quad (6)$$

and constraint (3). Let s_1^* and t_1^* be points that define the boundary of set D_1 obtained out of the solution of problem

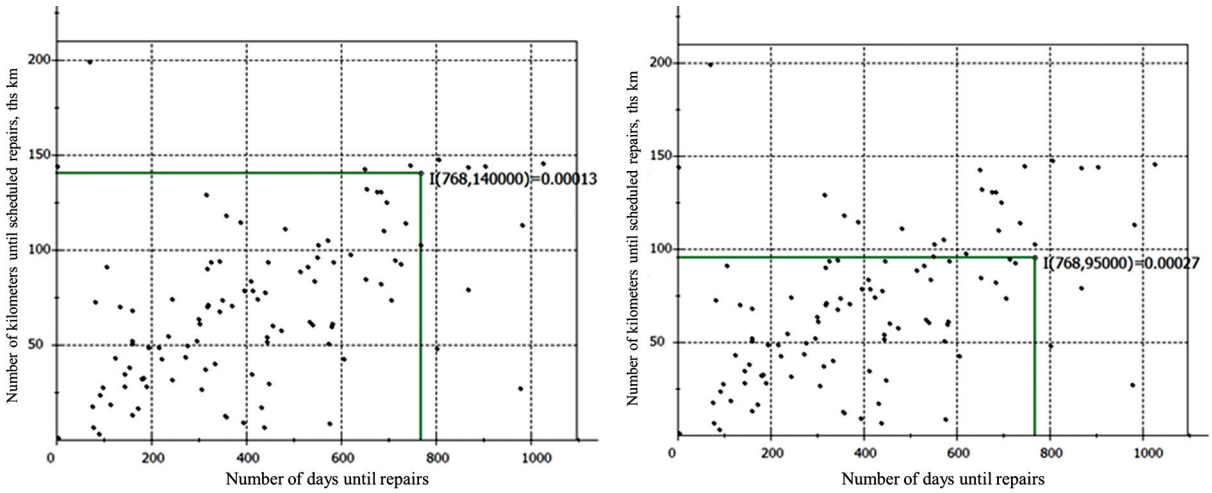


Figure 2. Values of hazard index $I(\hat{s}, \hat{t})$ under N=100000

Table 1. Information on the number of kilometers until repairs

Number of km until repairs	143548	665	198865	17278	6051	72373	2501	23317	27410	90631	18460	42994
Number of days until repairs	2	4	71	77	79	83	90	92	98	106	114	125
Number of km until repairs	69673	34066	27656	37715	50458	67534	12714	51974	16367	31546	32384	27573
Number of days until repairs	135	144	144	154	160	160	161	161	172	180	184	191
Number of km until repairs	48288	48072	42490	54148	31241	73995	43001	49288	51872	63043	60743	26186
Number of days until repairs	195	216	222	236	245	245	272	276	297	300	303	306
Number of km until repairs	36612	128533	69670	89674	70884	93159	93423	39596	93873	67490	73325	12043
Number of days until repairs	314	317	318	318	320	327	327	335	344	345	351	356
Number of km until repairs	117655	11877	70430	114233	8977	78327	83145	34292	78273	73877	16865	6496
Number of days until repairs	358	359	370	389	394	396	410	412	414	425	432	438
Number of km until repairs	77204	51497	53710	93079	29083	59903	57380	110608	88367	90629	61746	60260
Number of days until repairs	441	444	445	447	449	456	475	483	515	530	535	541
Number of km until repairs	83401	95796	102241	104506	50167	8145	59087	60796	93256	42433	97020	142347
Number of days until repairs	545	551	553	573	574	577	581	583	585	606	620	650
Number of km until repairs	84005	131848	130384	81517	130416	109896	124811	73301	94070	92140	113741	144321
Number of days until repairs	652	654	676	684	685	691	697	707	715	726	736	747
Number of km until repairs	102477	47759	147077	78562	143361	143654	26937	112502	145128			
Number of days until repairs	768	803	806	869	869	904	979	983	1026			

(4) subject to constraints (3), (5)–(6). Then, similarly, in order to find the boundaries of set D_2 we must solve problem

$$\sum_{i=1}^{m}\gamma_i \to \min_{s_1^* \geq \hat{s}^2 \geq 0, t_1^* \geq \hat{t}^2 \geq 0, \gamma_i \in \{0,1\}} \quad (7)$$

with constraints

$$(1-\gamma_i)\hat{s}_i \leq \hat{s}^2, i=\overline{1,m}, \quad (8)$$

$$(1-\gamma_i)\hat{t}_i \leq \hat{t}^2, i=\overline{1,m}, \quad (9)$$

$$(210000-\hat{s}^2)(1095-\hat{t}^2) \geq s^2. \quad (10)$$

Let s_2^* and t_2^* be points that define the boundary of set D_2 obtained out of the solution of problem (7) subject to constraints (8)–(10). In order to find the boundaries of set D_3 we must solve problem

$$\sum_{i=1}^{m}æ_i \to \min_{s_2^* \geq \hat{s}^3 \geq 0, t_2^* \geq \hat{t}^3 \geq 0, æ_i \in \{0,1\}} \quad (11)$$

with constraints

$$(1-æ_i)\hat{s}_i \leq \hat{s}^3, i=\overline{1,m}, \quad (12)$$

$$(1-æ_i)\hat{t}_i \leq \hat{t}^3, i=\overline{1,m}, \quad (13)$$

$$(210000-\hat{s}^3)(1095-\hat{t}^3) \geq s^3. \quad (14)$$

Let t_3^*, s_3^* be the solution of problem (11) subject to constraint (12)-(14).

Problem (4) subject to constraints (3), (5)-(6), problem (7) subject to constraints (8)-(10), problem (11) subject to constraints (12)-(14) are problems of mixed integer programming with quadratic constraints and can be solved using Opti Toolbox in Matlab. Let us note that the search

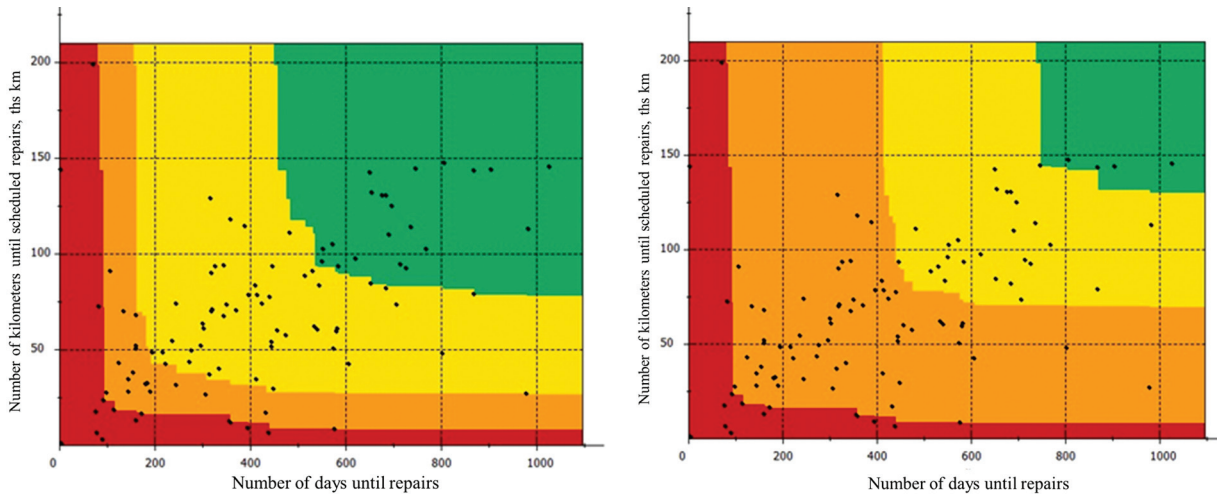


Fig. 3. Diagram of (non)acceptable factor values under i_1=0,0004, i_2=0,0009, i_3=0,001 (left) and i_1=0,0001, i_2=0,0005, i_3=0,001 (right)

for the boundaries of set D_j can be ruled not by the area of the corresponding set, but, for instance, the length of one of the boundaries of such set.

An example

Let there be 105 annual cases when a defect was detected in a solebar, while N=100000. Table 1 shows data on the number of days to scheduled repairs and number of kilometers until scheduled repairs in such cases.

Using the data given in Table 1, let us deduct the value of the hazard index in some points of plane $\hat{t}O\hat{s}$ (Figure 2).

Now, let us construct the ranges of (non)acceptable factor values for various parameters i_1, i_2, i_3 (Fig. 3).

As it follows from Figure 3, changes in the values of parameters i_1, i_2, i_3 significantly affect the ranges of (non)acceptable factor values that contribute to solebar fracture.

By specifying $s_1 = 5 \cdot 10^7$, $s_2 = 1,25 \cdot 10^8$, $s_3 = 1,75 \cdot 10^8$ we obtain $t_1^* = 620,27$, $s_1^* = 104561,9$, $t_2^* = 297$, $s_2^* = 51974$, $t_3^* = 114$, $s_3^* = 27410$ and the next range of (non)acceptable factor values that contribute to solebar fracture (Fig. 4).

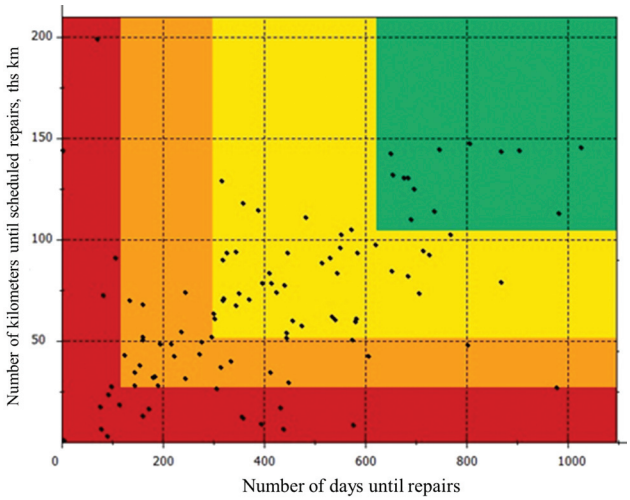


Fig. 4. Diagram of (non)acceptable factor values constructed based on the solution of the optimization problems

Conclusion

The paper examined the problem of identification of the ranges of (non)acceptable factor values contributing to bogie solebar fracture. For that purpose, a hazard index was built that depends on the number of days and kilometers until the next scheduled depot/full repairs. Based on that index, two methods of definition of ranges of (non)acceptable factor values were proposed. The first one was completely based on the values of the hazard index. As the absolute value of the hazard index is not a direct estimation of the probability of solebar fracture, a second method was proposed, that involved identifying the area of a certain range of (non) acceptable values and out of all sets with identical areas such was selected that had the lowest values of maximum hazard index.

References

[1] GOST 33433-2015. Functional safety. Risk management on railway transport. Moscow: Standartinform; 2016 [in Russian].

[2] Novozhilov EO. Guidelines for construction of a risk matrix. Dependability 2015;3:80-86.

[3] 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.

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

[5] 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.

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

[7] Schafer DH. Effect of Train Length on Railroad Accidents and a Quantitative Analysis of Factors Affecting Broken Rails. MS thesis. University of Illinois at Urbana–Champaign; 2006.

[8] Zamyshliaev AM, Kan YuS, Kibzun AI, Shubinsky IB. Statisticheskaya otsenka opasnosti vozniknoveniya proisshestviy na zheleznodorozhnom transporte [Statistical evaluation of accident hazard in railway transportation]. Dependability 2012;2:104-117 [in Russian].

[9] Lukin VV, Belsky AO. Calculation of the side frame and bolster freight car bogie finite element method. The Trans-Siberian Bulletin 2013;1(13):7-12 [in Russian].

[10] Galiev II, Nikolaev VA, Sergeyev BB, Samohvalov EA, Loucks DY. The reasons for violations of traffic safety of freight cars in operation. The Trans-Siberian Bulletin 2013:3(15):133-141 [in Russian].

[11] Kim JS, Shin KB, Yoon HJ, Lee WG. Durability evaluation of a composite bogie frame with bow-shaped side beams. Journal of Mechanical Science and Technology 2012;26(2):531-536.

[12] Method of categorization of freight cars as having reduced operational safety in terms of dependability and safety of cast parts of bogies (solebars). Approved by the Commission for Rail Traffic Safety of the Railway Transportation Council. Proceedings no. 1 of June 6-7, 2013. Approved by the Commission of Authorized Rolling Stock Specialists of Railway Administrations of the Railway Transportation Council. Proceedings no. 55 of February 19-21, 2013.

[13] Regulations on the service and repair system of freight cars cleared for operation in public tracks on inter-

national routes. Approved by the Proceedings of the Fifty-Seventh Meeting of the Railway Transportation Council of the Members of the Commonwealth of Independent States, October 16-17, 2012.

[14] Kibzun AI, Ignatov AN. Metodika organizatsii profilaktiki transportnogo proisshestviya [Method of organization of transportation accident prevention]. In: Proceedings of the Second Science and Engineering Conference Intelligent Control Systems in Railway Transportation ISUZhT 2013; 2013. p. 177-179.

About the authors

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

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

Alexey N. Ignatov, Candidate of Physics and Mathematics, Moscow Aviation Institute, Moscow, Russian Federation, phone: +7 (906) 059 50 00, alexei.ignatov1@gmail.com

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

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

Поступила: 22.02.2019

On the reliability of investment risk assessments

Andrey I. Dolganov, *Sev. R. Development, Russian Federation, Moscow*

Andrey I. Dolganov

Abstract. *The paper examines the reliability of investment risk estimates based on probabilistic realizations of purpose-designed scenarios. The calculations of the probabilities of scenario realization were based on logical and probabilistic methods. The reliability of risk assessment is understood as the probability of successful completion of a project, fulfillment of all contractual obligations: construction in compliance with the architectural and engineering design and quality requirements, within the contractual period and approved budget. Investment risks were estimated based on eight primary scenarios. The realization of the risks of the main group depended on the realization of the various numbers of risk scenarios of each subgroups in the main group. For instance, the first scenario of the main group consisted in the risk of faulty project ROI analysis and the risk of underestimated construction budget. The second one consisted in the risk of underestimated construction budget and risk associated with the selection of the basic flowsheet and primary process parameters, etc. The risks of each subgroup could be obtained by means of expert estimations or, in case of sufficient statistical data, based on the actual distributions. A mathematical model was developed for the purpose of a computerized solution. The mathematical model also allowed identifying such dependability factors as "weight", "significance" and "contribution" of each risk in the success of an investment project (reliability structure of investment risk estimation). The analysis of calculation data enabled the identification of the probability of successful project completion (reliability), the risks that are the most important, significant and having the largest contribution to the successful implementation of investment projects. Also, the risks were identified that have the least pronounced effect on the successful implementation of an investment project.*

Keywords: *probability, investment, model, dependability, risks, system, scenarios.*

For citation: *Dolganov AI. On the reliability of investment risk assessments. Dependability 2019; 3: 47-52 p. DOI: 10.21683/1729-2646-2019-19-3-47-52*

This paper examines the reliability of the estimates of investment risks based on probabilistic realizations of purpose designed scenarios. The calculations of the probabilities of scenario realization were based on logical and probabilistic methods.

The reliability of risk assessment is understood as the probability of successful completion of a project, fulfillment of all contractual obligations: construction in compliance with the required architectural and engineering design, quality, within the contractual period and approved budget.

In order to solve the problem, let us identify the following risks that make the main group that consists of eight scenarios (Table 8).

1. Q_1, the effect of design errors, including errors in the design and estimate documentation, incomplete detailed documentation;

2. Q_2, the effects of construction errors that define the quality of construction and installation works, possibility of industrial accidents, etc.;

3. Q_3, the effects of investment management errors that define the project execution period, possibility of contracts execution failures, etc.;

4. Q_4, the effects of negative economic fluctuations, including economic sanctions, sudden foreign exchange rate fluctuations, changes in other market indicators;

5. Q_5, the effects of unstable political situation, deterioration of social situation (strikes, environmental events, etc.);

6. Q_6, the effects of cataclysms (earthquakes, floods, etc.);

7. Q_7, the effects of financial risks.

In turn, the realization of the risks in each group depends on the realization of the scenarios of the subgroups of risks in such groups. Thus, the first subgroup of risks that take into consideration the effects of errors in design and estimate documentation, incomplete detailed documentation, includes:

1.1. $Q_{1\text{-}1}$, the risk of ROI analysis errors;

1.2. $Q_{2\text{-}1}$, the risk of underestimation of project budget;

1.3. $Q_{3\text{-}1}$, the risk associated with the selection of the basic flowsheet and primary process parameters;

1.4. $Q_{4\text{-}1}$, the risk caused by architectural solution and design solution errors;

1.5. $Q_{5\text{-}1}$, the risk caused by errors in the inquiry specifications and cost estimates;

Table 1

	$Q_{1\text{-}1}$	$Q_{2\text{-}1}$	$Q_{3\text{-}1}$	$Q_{4\text{-}1}$	$Q_{5\text{-}1}$	$Q_{6\text{-}1}$	$Q_{7\text{-}1}$	$Q_{8\text{-}1}$	$Q_{9\text{-}1}$
$C_{1\text{-}1}$	1	1	0	0	0	0	0	0	0
$C_{2\text{-}1}$	0	1	1	0	0	0	0	0	0
$C_{3\text{-}1}$	0	0	0	1	1	0	0	0	0
$C_{4\text{-}1}$	0	0	0	0	1	1	0	0	0
$C_{5\text{-}1}$	0	0	0	1	0	0	1	0	0
$C_{6\text{-}1}$	0	0	0	1	0	0	0	1	0
$C_{7\text{-}1}$	0	0	0	1	0	0	0	0	1

1.6. $Q_{6\text{-}1}$, the risk caused by delays in engineering documentation development;

1.7. $Q_{7\text{-}1}$, the risk of biased design solutions;

1.8. $Q_{8\text{-}2}$, the risk of the use of unique materials;

1.9. $Q_{9\text{-}1}$, the risk of underestimation of the construction period;

The scenarios for the risks of the first subgroup are shown in Table 1.

Thus, the first scenario consists in the risk of faulty project ROI analysis and the risk of underestimated construction budget. The second one consists in the risk of underestimation of the construction budget and risk associated with the selection of the basic flowsheet and primary process parameters. And so on.

Thus, the probability of the effect of design errors, including errors in the design and estimate documentation, Q_1, is defined by the realization of scenarios $C_{1\text{-}1}$, *or* $C_{2\text{-}1}$, *or* $C_{3\text{-}1}$, *or* $C_{4\text{-}1}$, *or* $C_{5\text{-}1}$, *or* $C_{6\text{-}1}$, *or* $C_{7\text{-}1}$.

The second subgroup of risks that take into consideration the effects of construction errors that define the quality of construction and installation works (CIW), possibility of industrial accidents, etc. includes:

2.1. $Q_{1\text{-}2}$, the risk of non-fulfillment of obligations by contractors and equipment suppliers;

2.2. $Q_{2\text{-}2}$, the risk of violation of CIW process regulations;

2.3. $Q_{3\text{-}2}$, the risk of the use of materials that do not comply with the design solutions;

2.4. $Q_{4\text{-}2}$, the risk of longer construction time by fault of the general contractor;

2.5. $Q_{5\text{-}2}$, the risk of failure to achieve the project's technical indicators;

2.6. $Q_{6\text{-}2}$, the risk of delayed commissioning of the facility;

2.7. $Q_{7\text{-}2}$, the risk of non-receipt of the required authorizations and approvals.

The scenarios for the risks of the second subgroup are shown in Table 2.

Table 2

	$Q_{1\text{-}2}$	$Q_{2\text{-}2}$	$Q_{3\text{-}2}$	$Q_{4\text{-}2}$	$Q_{5\text{-}2}$	$Q_{6\text{-}2}$	$Q_{7\text{-}2}$
$C_{1\text{-}2}$	1	1	0	0	0	0	0
$C_{2\text{-}2}$	0	1	1	0	0	0	0
$C_{3\text{-}2}$	0	1	0	1	0	0	0
$C_{4\text{-}2}$	1	0	0	0	1	0	0
$C_{5\text{-}2}$	0	0	0	0	1	1	0
$C_{6\text{-}2}$	1	1	1	0	0	0	1

The third subgroup of risks that take into consideration the effects of investment management errors that define the project execution period, possibility of contracts execution failures, etc. includes:

3.1. $Q_{1\text{-}3}$, the of risk of selection of a wrong strategy;

3.2. $Q_{2\text{-}3}$, the risk of wrong prediction;

3.3. $Q_{3\text{-}3}$, the risk of managerial errors;

3.4. $Q_{4\text{-}3}$, the risk of supervision and regulation errors.

The scenarios for the risks of the third subgroup are shown in Table 3.

Table 3

	$Q_{1\text{-}3}$	$Q_{2\text{-}3}$	$Q_{3\text{-}3}$	$Q_{4\text{-}3}$
$C_{1\text{-}3}$	1	1	0	0
$C_{2\text{-}3}$	1	0	1	0
$C_{3\text{-}3}$	0	0	1	1

The fourth subgroup of risks that takes into consideration the effects of negative economic fluctuations including economic sanctions, sudden foreign exchange rate fluctuations, changes in other market indicators, includes:

4.1. $Q_{1\text{-}4}$, the risk of international economic sanctions;

4.2. $Q_{2\text{-}4}$, the risk caused by sudden foreign exchange rate fluctuations;

4.3. $Q_{3\text{-}4}$, the risk of incorrect market assessment: increasing competitiveness, etc.;

4.4. $Q_{4\text{-}4}$, the risk of incorrect market capacity evaluation;

4.5. $Q_{5\text{-}4}$, the risk of incorrect market share assessment;

The scenario for the risks of the fourth subgroup are shown in Table 4.

Table 4

	$Q_{1\text{-}4}$	$Q_{2\text{-}4}$	$Q_{3\text{-}4}$	$Q_{4\text{-}4}$	$Q_{5\text{-}4}$
$C_{1\text{-}4}$	1	0	0	0	0
$C_{2\text{-}4}$	0	1	0	0	0
$C_{3\text{-}4}$	0	0	1	0	0
$C_{4\text{-}4}$	0	0	0	1	0
$C_{5\text{-}4}$	0	0	0	0	1

The fifth subgroup of risks that takes into consideration the effects of unstable political situation, deterioration of social situation (strikes, environmental events, etc.) includes:

5.1. $Q_{1\text{-}5}$, the risk of deteriorating social situation;

5.2. $Q_{2\text{-}5}$, the risk of politically motivated strikes;

5.3. $Q_{3\text{-}5}$, the risk of environmental protests;

5.4. $Q_{4\text{-}5}$, the risk of political demonstrations;

The scenarios for the risks of the fifth subgroup are shown in Table 5.

Table 5

	$Q_{1\text{-}5}$	$Q_{2\text{-}5}$	$Q_{3\text{-}5}$	$Q_{4\text{-}5}$
$C_{1\text{-}5}$	1	1	0	0
$C_{2\text{-}5}$	1	0	1	0
$C_{3\text{-}5}$	1	0	0	1

The sixth subgroup of risks that takes into consideration the effects of cataclysms (earthquakes, floods, etc.) includes:

6.1. $Q_{1\text{-}6}$, the risk of off-design earthquakes;

6.2. $Q_{2\text{-}6}$, the risk of insufficiency of adopted design measures in cases of design-basis earthquakes;

6.3. $Q_{3\text{-}6}$, the risk of flooding;

6.4. $Q_{4\text{-}6}$, the risk of landslides caused by background earthquakes or flooding.

The scenarios for the risks of the sixth subgroup are shown in Table 6.

Table 6

	$Q_{1\text{-}6}$	$Q_{2\text{-}6}$	$Q_{3\text{-}6}$	$Q_{4\text{-}6}$
$C_{1\text{-}6}$	1	1	0	0
$C_{2\text{-}6}$	1	0	1	0
$C_{3\text{-}6}$	1	0	0	1

The seventh subgroup of risks that takes into consideration the effects of financial risks includes:

7.1. $Q_{1\text{-}7}$, the risk of non-availability of financial loan;

7.2. $Q_{2\text{-}7}$, the risk of changing interest rate;

7.3. $Q_{3\text{-}7}$, the risk of investor's insufficient own circulating assets;

7.4. $Q_{4\text{-}7}$, the risk of financial losses as the result of changes in the exchange rate that may occur between the conclusion of contract and the settlement;

7.5. $Q_{5\text{-}7}$, the inflation risk, i.e. the possibility of depreciation of capital (in the form of the company's financial assets), as well as the expected income generated by financial operations amidst inflation;

7.6. $Q_{6\text{-}7}$, tax risk that is characterized by the probability of introduction of new taxes and fees for specific business activities, possibility of increased rates of existing taxes and fees, changes in the terms and conditions of individual taxes, probability of cancellation of existing tax exemptions as regards the company's business activities;

7.7. $Q_{7\text{-}7}$, the systemic risk defined by inefficient funding of the company's current expenditures, which causes a high relative share of the standing costs in the overall sum.

The scenarios for the risks of the seventh subgroup are shown in Table 7.

Table 7

	$Q_{1\text{-}7}$	$Q_{2\text{-}7}$	$Q_{3\text{-}7}$	$Q_{4\text{-}7}$	$Q_{5\text{-}7}$	$Q_{6\text{-}7}$	$Q_{7\text{-}7}$
$C_{1\text{-}7}$	1	1	0	0	0	0	0
$C_{2\text{-}7}$	0	1	1	0	0	0	0
$C_{3\text{-}7}$	0	0	1	1	0	0	0
$C_{4\text{-}7}$	0	0	0	1	1	0	0
$C_{5\text{-}7}$	0	0	0	0	1	1	0
$C_{6\text{-}7}$	0	0	0	0	0	1	1

Shown in Tables 1 to 7 are: Q_i, the probability of realization of the i-th risk; C_i, logical conjunction scenarios.

Company's losses ("failed" investment) are associated with the realization of risk scenarios shown in Table 8: *or* (Q_1 *and* Q_3), *or* (Q_1 *and* Q_6), *or* (Q_2 *and* Q_3), *or* (Q_2 *and* Q_5, *and* Q_6), *or* (Q_1 *and* Q_3, *and* Q_4), *or* (Q_1 *and* Q_3, *and* Q_5), *or* (Q_3 *and* Q_4, *and* Q_5, *and* Q_6), *or* (Q_7).

Table 8

	Q_1	Q_2	Q_3	Q_4	Q_5	Q_6	Q_7
C_1	1	0	1	0	0	0	0
C_2	1	0	0	0	0	1	0
C_3	0	1	1	0	0	0	0
C_4	0	1	0	0	1	1	0
C_5	1	0	1	1	0	0	0
C_6	1	0	1	0	1	0	0
C_7	0	0	1	1	1	1	0
C_8	0	0	0	0	0	0	1

The given data for Q_i, i = 1, …, 7 are the probabilities identified based on the scenarios given in Tables 1 to 7.

In Table 9, the following data is given for the example in question. Risks Q_{i-j} (probability of realizations of i risks of the j-th group) in the example in question were obtained by means of expert evaluation. In case of sufficient statistical data, probability Q_{i-j} should be identified based on the actual distributions.

Shown in Table 9 are: Q_i, the probability of realization of the i-th risk; R_i, instead, the probability of non-realization of the i-th risk, i.e. $R_{i-j} = 1 - Q_{i-j}$.

Let us write the probability of successful implementation of an investment project:

$$R_c = 1 - Q_c, \tag{1}$$

Where

$$Q_c = \begin{vmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \\ C_7 \\ C_8 \end{vmatrix} = \begin{vmatrix} Q_1Q_3 \\ Q_1Q_6 \\ Q_2Q_3 \\ Q_2Q_5Q_6 \\ Q_1Q_3Q_4 \\ Q_1Q_3Q_5 \\ Q_3Q_4Q_5Q_6 \\ Q_7 \end{vmatrix}. \tag{1/}$$

Thus, each scenario is a multicriterion value. In order to account for all the risks, the realization of possible "unsuccessful" scenarios should be described, i.e. it must be identified how damage can occur. Table 8 describes the scenarios of model (1/).

A mathematical model was developed for the purpose of a computerized solution of problem (1). The probability of successful project completion subject to the above probabilities is 0.93742. Therefore, the probability of "failure" or losses is 6,258%. The mathematical model allows identifying the "weight" (2), as well as the "significance" (3) and "contribution" (4) of each risk to the success of an investment project. The findings are given in Table 10.

$$g_{Q_i} = \frac{G\{\Delta_{Q_i} y(Q_1,\ldots,Q_n)\}}{2^n} = \sum_{j=1}^{l} 2^{-(r_j-1)} - \sum_{f=1}^{k} 2^{-(r_f-1)}, \tag{2}$$

where f = 1, …, k; j = 1, …, l; r_f, r_j are the ranks of elementary conjunctions; k, l are the number of conjunctions that contain $Q_i^{/}, Q_i$ ($Q_i^{/} = R_i$) and not contain the i-th argument; n is the number of fixed variables of the initial function.

The "weight" of the Boolean difference (2) characterizes the importance of risk Q_i for the reliability of investment. The "weight" of an elements also characterizes the relative number of such critical states, in which the failure of an individual scenario causes the failure of the whole model (and vice versa, the recovery causes the recovery) out of all states of the model with $Q_i = 1$. The criterion of the "weight" of a risk g_{x_i} characterizes the location of such risk Q_i in the model (of the system) (Q_1, …, Q_n).

The "significance" of risk Q_i is a partial derivative of mathematical model Q_c (1/) with respect to the probability of risk Q_i, i.e.

$$\zeta_{Q_i} = \frac{\partial P\{y(Q_1,\ldots,Q_n)=1\}}{\partial P\{Q_i=1\}} = \frac{\partial Q_c}{\partial Q_i}. \tag{3}$$

The criterion of "significance" characterizes the rate of change of the reliability of investment. The "significance" is the conditional probability under condition of realization of risk Q_i. Additionally, the criterion of "significance" allows identifying the risks that enable the highest increase in the reliability of the chosen model.

The "contribution" of element Q_i to system (risk scenarios) $y(Q_1, \ldots, Q_n)$ is the product of risk Q_i and its "significance", i.e.

$$B_{x_i} = Q_i \frac{\partial Q_c}{\partial Q_i} = Q_i \frac{Q_c - Q_{c0}^{(i)}}{Q_i} = Q_c - Q_{c0}^{(i)}. \tag{4}$$

The criterion of "contribution" characterizes the increase of dependability after recovery of scenario with risk Q_i.

The concept of "specific contribution" is a more general characteristic than simply "contribution". The "specific contribution" of risk Q_i to system (scenario) $y(Q_1, \ldots, Q_n)$ is the standardized "contribution" of such risk, i.e.

$$b_{Q_i} = B_{Q_i} / \sum_{i=1}^{n} B_{Q_i}. \tag{5}$$

Table 9

$R_{1\text{-}1}$	$R_{2\text{-}1}$	$R_{3\text{-}1}$	$R_{4\text{-}1}$	$R_{5\text{-}1}$	$R_{6\text{-}1}$	$R_{7\text{-}1}$	$R_{8\text{-}1}$	$R_{9\text{-}1}$
0.850	0.850	0.850	0.800	0.750	0.250	0.900	0.900	0.750
$Q_{1\text{-}1}$	$Q_{2\text{-}1}$	$Q_{3\text{-}1}$	$Q_{4\text{-}1}$	$Q_{5\text{-}1}$	$Q_{6\text{-}1}$	$Q_{7\text{-}1}$	$Q_{8\text{-}1}$	$Q_{9\text{-}1}$
0.150	0.150	0.150	0.200	0.250	0.750	0.100	0.100	0.250
$R_{1\text{-}2}$	$R_{2\text{-}2}$	$R_{3\text{-}2}$	$R_{4\text{-}2}$	$R_{5\text{-}2}$	$R_{6\text{-}2}$	$R_{7\text{-}2}$	–	–
0.900	0.900	0.900	0.850	0.850	0.850	0.990	–	–
$Q_{1\text{-}2}$	$Q_{2\text{-}2}$	$Q_{3\text{-}2}$	$Q_{4\text{-}2}$	$Q_{5\text{-}2}$	$Q_{6\text{-}2}$	$Q_{7\text{-}2}$	–	–
0.100	0.100	0.100	0.150	0.150	0.150	0.010	–	–
$R_{1\text{-}3}$	$R_{2\text{-}3}$	$R_{3\text{-}3}$	$R_{4\text{-}3}$	–	–	–	–	–
0.950	0.900	0.900	0.800	–	–	–	–	–
$Q_{1\text{-}3}$	$Q_{2\text{-}3}$	$Q_{3\text{-}3}$	$Q_{4\text{-}3}$	–	–	–	–	–
0.050	0.100	0.100	0.200	–	–	–	–	–
$R_{1\text{-}4}$	$R_{2\text{-}4}$	$R_{3\text{-}4}$	$R_{4\text{-}4}$	$R_{5\text{-}4}$	–	–	–	–
0.850	0.850	0.950	0.950	0.850	–	–	–	–
$Q_{1\text{-}4}$	$Q_{2\text{-}4}$	$Q_{3\text{-}4}$	$Q_{4\text{-}4}$	$Q_{5\text{-}4}$	–	–	–	–
0.150	0.150	0.050	0.050	0.150	–	–	–	–
$R_{1\text{-}5}$	$R_{2\text{-}5}$	$R_{3\text{-}5}$	$R_{4\text{-}5}$	–	–	–	–	–
0.650	0.750	0.950	0.800	–	–	–	–	–
$Q_{1\text{-}5}$	$Q_{2\text{-}5}$	$Q_{3\text{-}5}$	$Q_{4\text{-}5}$	–	–	–	–	–
0.350	0.250	0.050	0.200	–	–	–	–	–
$R_{1\text{-}6}$	$R_{2\text{-}6}$	$R_{3\text{-}6}$	$R_{4\text{-}6}$	–	–	–	–	–
0.950	0.950	0.990	0.850	–	–	–	–	–
$Q_{1\text{-}6}$	$Q_{2\text{-}6}$	$Q_{3\text{-}6}$	$Q_{4\text{-}6}$	–	–	–	–	–
0.050	0.050	0.010	0.150	–	–	–	–	–
$R_{1\text{-}2}$	$R_{2\text{-}2}$	$R_{3\text{-}2}$	$R_{4\text{-}2}$	$R_{5\text{-}2}$	$R_{6\text{-}2}$	$R_{7\text{-}2}$	–	–
0.950	0.977	0.990	0.750	0.850	0.950	0.900	–	–
$Q_{1\text{-}2}$	$Q_{2\text{-}2}$	$Q_{3\text{-}2}$	$Q_{4\text{-}2}$	$Q_{5\text{-}2}$	$Q_{6\text{-}2}$	$Q_{7\text{-}2}$	–	–
0.050	0.023	0.010	0.250	0.150	0.050	0.100	–	–

Table 10

g_1	g_2	g_3	g_4	g_5	g_6	g_7
0.203	0.141	0.234	0.016	0.047	0.172	0.453
ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7
0.03445	0.02019	0.31606	0.00003	0.00050	0.27474	0.98754
B_1	B_2	B_3	B_4	B_5	B_6	B_7
0.00998	0.00130	0.00901	0.00001	0.00008	0.00276	0.05011
b_1	b_2	b_3	b_4	b_5	b_6	b_7
0.136	0.018	0.123	0.000	0.001	0.038	0.684

Calculation data in the form of differential characteristics of risks $g_{Q_i}, \zeta_{Q_i}, b_{Q_i}$ shown in Table 10 clearly demonstrates the distribution of the role of all primary risks over the given dependability structure in the context of various problems.

Table 11 shows relative values of risk parameter p_i ($i = 1, \ldots, 7$) that were obtained:

$$p_i = p_i / p_{max}. \qquad (6)$$

Table 11

g_1	g_2	g_3	g_4	g_5	g_6	g_7
0.45	0.31	0.52	0.03	0.10	0.38	1.00
ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ξ_6	ξ_7
0.03	0.02	0.32	0.00	0.00	0.28	1.00
b_1	b_2	b_3	b_4	b_5	b_6	b_7
0.20	0.03	0.18	0.00	0.00	0.05	1.00

The analysis of calculation data allows for the following *conclusions*.

The probability of successful project completion (reliability) under the Table 8 scenarios is 93.7%. Therefore, the probability of "failure" is 6.3%.

Q_7 and Q_3, i.e. the effects of the financial and managerial risks are the most important, significant and contributing factors of the investment risks.

Q_4, the effect of negative economic fluctuations, and Q_5, i.e. the effect of political instability in the country, have *the least* effect on the probability of an investment project completion.

References

[1] Dolganov AI. Nadezhnost sterzhnevykh zhelezobetonnykh konstruktsiy [Dependability of framed concrete structures]. Magadan: MAOBTI; 2001 [in Russian].

[2] Dolganov AI. Optimizatsiya mostovykh zhelezobetonnykh balok po kriteriyu nadezhnosti [Optimization of reinforced concrete beams of bridges with respect to dependability]. In: Problemy optimalnogo proektirovaniya sooruzheniy: Sb. dokladov II Vserossiyskogo seminara [Matters of optimal design of structures: Proceedings of the second All-Russian seminar]. Novosibirsk: NSUACE; 1998 [in Russian].

[3] Dolganov AI, Danielov ER. Problemy optimalnogo proektirovaniya sooruzheniy: Sb. dokladov III-go Vseros. seminara: V 2-kh tomakh. T. 1 [Matters of optimal design of structures: Proceedings of the third All-Russian seminar in two volumes. Volume 1]. Novosibirsk: NSUACE; 2000 [in Russian].

[4] Dolganov AI. Optimizatsiya zhelezobetonnykh konstruktsiy s uchetom kriteriev nadezhnosti i minimalnoy stoimosti [Optimization of reinforced concrete structures with respect to the criteria of dependability and minimal cost]. Magadan: Northern International University Publishing; 2002 [in Russian].

[5] Dolganov AI. Otsenka nadezhnosti monolitnykh mnogoetazhnykh zdaniy [Dependability assessment of site-cast multi-floor buildings]. Industrial and civil engineering 2010;8:50-51 [in Russian].

[6] Dolganov AI. O nadezhnosti sooruzheniy massovogo stroitelstva [On the dependability of mass-built structures]. Industrial and civil engineering 2010;11:66-68 [in Russian].

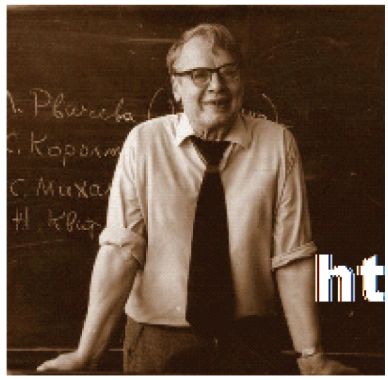
[7] Dolganov AI. Ob obespechennosti ledovoy nagruzki v Finskom zalive [On the assurance of ice loading in the Gulf of Finland]. Proceeding of the 9-th international research and practice conference: RAS Academic Council, Federal Agency for Scientific Organizations, EMERCOM of Russia, Russian Foundation for Basic Research. Moscow: The Peoples' Friendship University of Russia; 2015 [In Russian].

[8] Dolganov AI, Sakharov AV. On the assignment of dependability level. Dependability 2018;18(3):18-21.

About the author

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

Received on: 17.01.2019



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