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

Original article
DOI: 10.21683/1729-2646-2017-17-4-3-9

Dependability of objects with non-stationary failure rate

Leonid A. Baranov, *Emperor Nicolas II Moscow State University of Railway Engineering (MIIT), Moscow, Russia*
Yuri A. Yermolin, *Emperor Nicolas II Moscow State University of Railway Engineering (MIIT), Moscow, Russia*

Leonid A. Baranov

Yuri A. Yermolin

Abstract. *Among the diversity and various degrees of significance of the factors that affect an object's failure flow, there is one, i.e. its "ageing," that causes changes in the number of failures per time unit that makes it non-stationary (in terms of dependability). In this context, the elaboration of service procedures is of high importance, especially with regards to long life-cycle objects.* **Methods** *of identifying dependability indicators of stationary objects are known and widely used in practice. Nevertheless, as regards non-stationary objects there are practically no generally accepted approaches to the identification of their dependability indicators that would be convenient for engineering calculations. Meanwhile, the analysis of publications dedicated to this subject given in this paper shows the relevance and potential demand for such methods in various technical matters.* **The aim** *of this paper is in the development of an analytical model of evaluation of dependability indicators of non-stationary objects. The main concept of the proposed approach consists in substituting the real non-stationary object with a virtual analogue, of which the failure flow is stationary, i.e. a formal stationarization (in terms of dependability) of the object occurs, which legitimizes the use of well-developed methods of solving stationary tasks by extending them to the cases of non-stationary objects. The approach is rough. The main problem is identifying the value of the constant failure flow rate of the fake object expressed through the time-dependent parameters of the "ageing" characteristic of the real (non-stationary) object that in this paper is deemed to be known. In order to increase the generality of consideration, the definition of equivalent failure rate (or associated mean time to failure) in this paper is given for three cases: 1) The real object "ages", i.e. its failure rate is an increasing function of time. Two approaches are suggested to the identification of the equivalent failure rate: a) based on the condition of equality of the mean times to failure of both objects (real and fake); b) based on the condition of equality of the dependability functions of the objects to the predefined prediction time. For some laws of "ageing" the task has been solved analytically in closed form. Using the numerical example, the comparative accuracy of the approaches has been evaluated. 2) The object is characterized by a piecewise constant failure rate that is typical to systems and devices that operate in "open" environments (with seasonal changes in failure rate). Both exact and approximate (in linear approximation) expressions for the dependability function and mean time to failure for such object have been obtained. 3) The object's failure rate dependance is a piecewise constant non-periodical time function. Such model is sufficiently universal as after time discretization and piecewise constant approximation with a given accuracy many analytical time dependencies of failure rate can be reduced to it. Method-wise, the task is solved similarly to item 2), i.e. the non-periodic process is treated as a periodic one with an infinitely long period. Under the condition of reasonable practicality of object operation (e.g. for economic reasons) defined in this paper, expressions for the dependability function and mean time to failure have been obtained. The findings of the paper may be useful in solving the dependability-related tasks for non-stationary technical objects.*

Keywords: *dependability; failure flow; non-stationarity; periodicity of object states.*

For citation*: Baranov LA, Yermolin YuA. Dependability of objects with non-stationary failure rate. Dependability 2017;4: 3-9. DOI: 10.21683/1729-2646-2017-17-4-3-9*

Dependability indicators, i.e. probability of no-failure over a given time period $p(t)$ and mean time to failure $\overline{t}$ are a significant criterion of a system's (object's) operation [1]. The failure rate $\lambda(t)$ is the input information for the identification of those indicators. Thus, if $\lambda(t)$ is known

$$p(t) = \exp\left[-\int_0^t \lambda(t)dt\right] \quad (1)$$

and

$$\overline{t} = \int_0^\infty p(t)dt. \quad (2)$$

Most existing engineering methods of calculating an object's dependability indicators are based on the hypothesis of its stationarity [1-4], i.e. assume that the rate of failure flow $\lambda(t)$ does not change in time ($\lambda(t)=\lambda_0=const$). In this case formulas (1) and (2) transform as follows:

$$p(t) = \exp(-\lambda_0 t); \quad (3)$$

$$\overline{t} = 1/\lambda_0. \quad (4)$$

Among the diversity and various degrees of significance of the factors that affect an object's failure flow there is one, i.e. its "ageing", that causes an increase of the number of failures per unit time. This circumstance cannot be ignored in cases of long-term operation of an object: λ stops being constant and becomes an increasing function of time $\lambda(t)$, while the object essentially passes into the non-stationary ("ageing") class. In this context, the elaboration of service procedures is of utmost importance, especially with regards to long lifecycle objects. That is supported by the publications that appeared over the past few years and that contain dependability evaluations of such socially significant facilities as water resource utilization systems of major cities [5], nuclear power plants [6], structures made of composite materials [7], etc.

A number of systems (facilities) operate in periodically changing conditions. In particular, waste water channel systems typically display a dependance between the failure rate and the operating season; for power supply systems the load is a function of different periods of the day. Therefore, in this case the failure rate changes during the day. Rolling stock of various transportation systems, main underground pipelines operate in periodically changing conditions.

In principle, the solution of any dependability-related task for a non-stationary object is algorithmically identical to a similar task for stationary objects. The difficulties though consist in the fact that calculations involve certain mathematical operations (e.g. integration) that cannot be performed in primitive functions. In such cases the applied dependability theory has to allow some simplifying assumptions in order to achieve the desired result. Those assumptions allow obtaining a solution in a rough analytical form that is convenient for subsequent analysis. Such assumptions can be conventionally grouped into several types. Judging by the latest publications [8-11], we can acknowledge the existence of a distinct type of assumptions that involves substituting the failure flow of a real non-stationary object with a fake one that in some respect is equivalent to the initial one and is convenient for solving the specific task at hand.

This paper sets forth the methods of dependability indicators calculation for objects with non-stationary failure flow. It examines "ageing" objects, of which the rate of failure flow λ increases in time, objects with periodic piecewise constant failure rate, objects, of which the failure rate can be represented with a non-periodic piecewise constant function. The last case is sufficiently general, as initially the results of statistical failure data processing is conveniently represented in the above form. Additionally, analytically, after discretization, the given function $\lambda(t)$ can always be represented with a given accuracy with a piecewise constant function of time.

For ageing objects, of which the failure rate increases in time, the main concept of the method consists in substituting the real non-stationary object with a virtual fake analogue, of which the failure flow is stationary and is characterized by a certain constant rate λ_c. Thus, a formal stationarization of the object occurs, which legitimizes the use of well-developed methods of solving stationary dependability-related tasks by extending them to the cases of non-stationary objects. The value λ_c must be "associated" with the parameters of the "law of ageing" of the real object $\lambda(t)$ and be defined by certain additional considerations.

Let us examine two possible approaches to the definition of λ_c for ageing objects.

Approach 1. In accordance with this approach it is suggested to find λ_c out of condition $\overline{t}_c = \overline{t}$, where $\overline{t}_c$ is the mean time to failure of the equivalent ageing object, while $\overline{t}$ is the one of the real ageing object. If $\overline{t}$ is expressed through parameters λ_0, α, β… of the ageing characteristic, then subject to (4) out of this equation we immediately obtain:

$$\lambda_c = \frac{1}{\overline{t}(\lambda_0, \alpha, \beta...)}. \quad (5)$$

In order to demonstrate the use of this approach let us examine a non-stationary object, of which the failure rate changes in time according to law:

$$\lambda(t) = \lambda_0 + \alpha t, \quad (6)$$

where λ_0 is the initial failure rate; α is the object's ageing factor ($\alpha>0$).

For this case in [12], the accurate value of mean time to failure $\overline{t}$ is obtained that is expressed through the parameters of the law of ageing (6):

$$\overline{t}(\lambda_0, \alpha) = \sqrt{\frac{2}{\alpha}} \cdot e^{\frac{\lambda_0^2}{2\alpha}} \cdot \frac{\sqrt{\pi}}{2} \cdot \left[1 - \Phi\left(\frac{\lambda_0}{\sqrt{2\alpha}}\right)\right], \quad (7)$$

where $\Phi(\ )$ is the probability integral.

By substituting this expression into (5), for the failure rate of the fake stationary object λ_c we obtain:

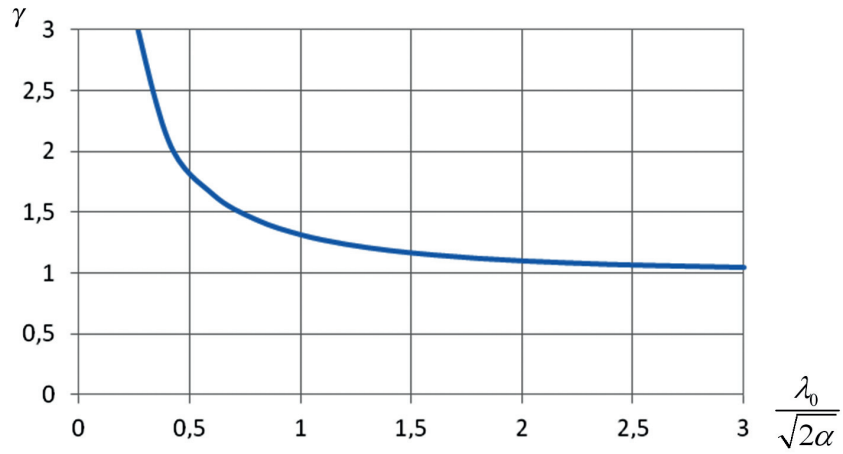


Figure 1. Dependence $\gamma = \gamma\left(\frac{\lambda}{\sqrt{2\alpha}}\right)$

$$\lambda_c = \frac{\sqrt{\frac{2\alpha}{\pi}} \cdot e^{-\frac{\lambda_0^2}{2\alpha}}}{1 - \Phi\left(\frac{\lambda_0}{\sqrt{2\alpha}}\right)}. \quad (8)$$

As we can see in (8), the numeric value λ_c is associated with λ_0 and α by means of a quite complex dependence that is difficult to interpret in physical terms. In order to "feel" the characteristic features of this dependence let us find the coefficient:

$$\gamma = \frac{\overline{t}_0}{\overline{t}(\lambda_0, \alpha)}, \quad (9)$$

where $\overline{t}(\lambda_0, \alpha)$ is calculated in accordance with (7), $\overline{t}_0 = 1/\lambda_0$ is the average life of the object that "ages" according to the law (6), but under the condition α=0 (i.e. essentially a stationary object with the failure rate λ_0). Now the physical meaning of γ becomes clear, i.e. this coefficient shows how many times the mean time to failure decreases in the ageing object compared to the time to failure of a stationary object with an identical initial failure rate. By

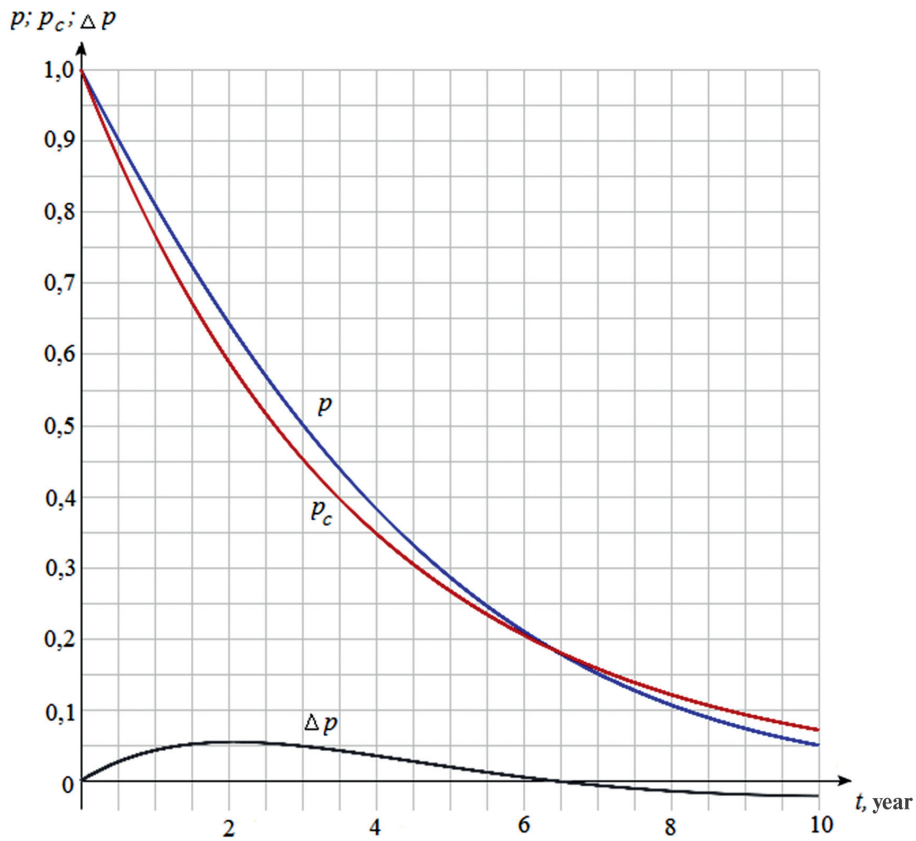


Figure 2. Dependability function of real and fake objects and difference between them

substituting this expression into (9) after some simple transformation we obtain:

$$\gamma = \frac{1}{\sqrt{\pi}} \cdot \frac{e^{\frac{\lambda_0^2}{2\alpha}}}{\frac{\lambda_0}{\sqrt{2\alpha}} \cdot \left[1 - \Phi\left(\frac{\lambda_0}{\sqrt{2\alpha}}\right)\right]}. \quad (10)$$

As we can see, γ is the function of only the dimensionless variable $\frac{\lambda_0}{\sqrt{2\alpha}}$, which makes it possible to represent this dependence with one graph (Fig. 1).

The graph shows that as the value of the argument grows the curve tends to one, which is totally explainable: the higher is the value of failure rate λ_0, the lower is the influence (other things equal) of the object's ageing factor on its mean time to failure.

Figure 2 gives a certain idea of the concept of stationarization. It is designed for the case of a linearly ageing object with the values of parameters $\lambda_0 = 0.2$ [1/year] and $\alpha = 0.02$ [1/year^2].

Fig. 2 shows the graphs of the dependability functions of a real (ageing) object $p(t)$ constructed using expression (1) subject to (6):

$$p(t) = \exp\left[-\int_0^t (\lambda + \alpha t)dt\right] = \exp\left[-\left(\lambda_0 t + \frac{\alpha}{2}t^2\right)\right], \quad (11)$$

and fake stationary $p_c(t)$:

$$p_c(t) = \exp(-\lambda_c t), \quad (12)$$

where λ_c is calculated using (8).

The graphs given in Fig. 2 – in terms of physics – can be commented in the following way. If an object's mean time to failure is interpreted as a certain technical resource, then Fig. 2 shows that during the stationarization there is a kind of a formal redistribution of the probabilities of "spending" of its parts in the course of the object's operation. The dependence graph $\Delta p(t)=p(t)-p_c(t)$ in the same figure gives an idea of how this redistribution occurs.

Even given its logical justifiability this approach cannot be used universally. The fact is that the linearly ageing object under consideration is a rare example, for which the mean time to failure can be expressed with the parameters of the characteristic of its ageing in the analytical form. Therefore it suggested to further use another approach to the definition of λ_c that is not associated with such difficulties.

Approach 2. The value of failure rate λ_c is identified based on the formula:

$$p(t_{gv}) = p_c(t_{gv}), \quad (13)$$

i.e. out of the condition of equality of the probabilities of no-failure of the real ("ageing") and fake (stationary) object at the given moment in time t_{gv}.

Normally, an object's dependability is evaluated not generally, but for a certain interval T_{frc}, i.e. the time of forecast with regard to the current moment. Then, in view of (1) and (10) the correlation (13) becomes as follows:

$$\int_0^{T_{frc}} \lambda(t)dt = \lambda_c T_{frc}, \quad (14)$$

out of which we deduce the following:

$$\lambda_c = \frac{1}{T_{frc}} \int_0^{T_{frc}} \lambda(t)dt, \quad (15)$$

i.e. the failure rate of the fake object is defined as the mean value $\lambda(t)$ over the time of forecast.

By way of example let us find out how the formula for λ_c will look under the two laws of object ageing: 1) in the form of an *n*-power parabola and 2) in the form of a rising exponential curve.

Case 1. The failure rate of a non-stationary object is as follows:

$$\lambda(t) = \lambda_0 + \alpha t^n. \quad (16)$$

By substituting this dependence into (15) we have:

$$\lambda_c = \lambda_0 + \frac{\alpha T_{frc}}{n+1} \quad (17)$$

In particular, if $n = 1$ (object considered in approach 1) expression (17) becomes as follows;

$$\lambda_c = \lambda_0 + \frac{\alpha}{2} T_{frc}. \quad (18)$$

*Case 2.*The object "ages" according to law:

$$\lambda(t) = \lambda_0 e^{\alpha t}. \quad (19)$$

Then out of (15) follows:

$$\lambda_c = \frac{\lambda_0}{\alpha T_{frc}}\left(e^{\alpha T_{frc}} - 1\right). \quad (20)$$

Expressions (17), (18) and (20) show that under this approach λ_c depends not only on the parameters of the object's ageing characteristic, but also on the time of forecast T_{frc}.

The evaluation of the mean time to failure of a fake stationary object $\bar{t}_c$, as it follows from (5), now also becomes a function of T_{frc} and is:

for case 1:

$$\bar{t}_c = \frac{n+1}{(n+1)\lambda_0 + \alpha T_{frc}}; \quad (21)$$

for case 2:

$$\bar{t}_c = \frac{\alpha T_{frc}}{\lambda_0\left(e^{\alpha T_{frc}} - 1\right)}. \quad (22)$$

Let us evaluate the allowable error of identification of the mean time to failure $\bar{t}$ of the real object for the case of linearly ageing object, for which $\bar{t}$ is defined by formula (7) [12]. We will evaluate the degree of proximity of $\bar{t}_c$ to the real value of $\bar{t}$ with the relative reduced error δT that is calculated according to formula:

$$\delta\bar{t} = \left(\frac{\bar{t}-\bar{t}_c}{\bar{t}}\right)\cdot 100\% = \left(1-\frac{\bar{t}_c}{\bar{t}}\right)\cdot 100\%, \qquad (23)$$

where $\bar{t}_c$ is calculated according to (21) (given that n= 1).

Under the conditions of the above numerical illustration (λ_0= 0.2 [1/year];α= 0.02 [1/year^2]) as per (7) we deduce $\bar{t}$ = 3.79 years. The estimate for $\bar{t}_c$ under these parameters (as per (21) $\bar{t}_c = \frac{2}{0.4+0.02\cdot T_{frc}}$. By substituting these values into (23) we have:

$$\delta\bar{t} = \left[1-\frac{2}{3.79(0.4+0.02T_{frc})}\right]\cdot 100\%. \qquad (24)$$

As we can see, the relative reduced error depends on the time of forecast T_{frc}. The values of this error are given in the Table 1.

Table 1

T_{frc}, годы	1	2	3	4	5	6	7	8	9
$\delta\bar{t}$, %	-25,64	-19,93	-14,72	-9,94	-5,54	-1,48	2,28	5,76	9,02

The data in the Table show that as the time of forecast grows the relative reduced error in the identification of the mean time to failure reverses sign and can reach fairly high values.

Now let us consider the dependability function and mean time to failure of an object with a periodic piecewise constant failure rate.

Let T be the period of changes in the failure rate that consists of l generally different time intervals (see Fig. 3, where l = 3), τ_i be the time period between the beginning of the n-th period and the end of the i-th interval of this period.

For convenience, it is assumed that $\tau_0 = 0$, τ_i=T, i= 0, 1, …, l. In this case λ_i is the failure rate, τ_i–τ_{i-1} is the duration of the i-th interval in the n-th period. In the authors' paper [13] under this change model of failure rate expressions for the dependability function $p(t)$ and mean time $\bar{t}$ to failure were obtained:

$$p(t) = e^{-\left[(n-1)A+B_{i-1}+\lambda_{i-1}\{t-[(n-1)T+\tau_{i-1}]\}\right]} \text{ if}$$

$$(n-1)T+\tau_{i-1} < t \le (n-1)T+\tau_i, \qquad (25)$$

where

$$A = \sum_{j=1}^{j=l}\lambda_j(\tau_j-\tau_{j-1});$$

$$B_{i-1} = \begin{cases} 0; \ if \ i=1 \\ \sum\limits_{j=1}^{j=i-1}\lambda_j(\tau_j-\tau_{j-1}); \ if \ i>1 \end{cases}$$

$$\bar{t} = \frac{1}{1-e^{-A}}\sum_{j=1}^{j=l}\frac{1}{\lambda_j}\left[1-e^{-\lambda_j(\tau_j-\tau_{j-1})}\right]. \qquad (26)$$

Under the practically justified assumption λT<<1 after the Maclaurin expansion of the exponential curves under linear approximation we deduce:

$$p(t) = 1-\left\{(n-1)A+B_{i-1}+\lambda_{i-1}[t-[(n-1)T+\tau_{i-1}]\right\} \text{ if}$$

$$(n-1)T+\tau_{i-1} < t \le (n-1)T+\tau_i; \qquad (27)$$

$$\bar{t} = \frac{1}{1-\left[1-\sum\limits_{j=1}^{j=l}\lambda_j(\tau_j-\tau_{j-1})\right]}\sum_{j=1}^{j=l}\frac{1}{\lambda_j}\left\{1-[1-\lambda_j(\tau_j-\tau_{j-1})]\right\} = \frac{1}{\bar{\lambda}}, \qquad (28)$$

where $\bar{\lambda} = \sum\limits_{j=1}^{l}\lambda_j\frac{\tau_j-\tau_{j-1}}{T}$ is the mean failure rate over the period T.

After several transformations, formulas (25) and (27) can be brought to the following form:

$$p(t) = e^{-\left\{(n-1)\bar{\lambda}T+\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i\{t-[(b-1)T+\tau_{i-1}]\}\right\}}; \qquad (29)$$

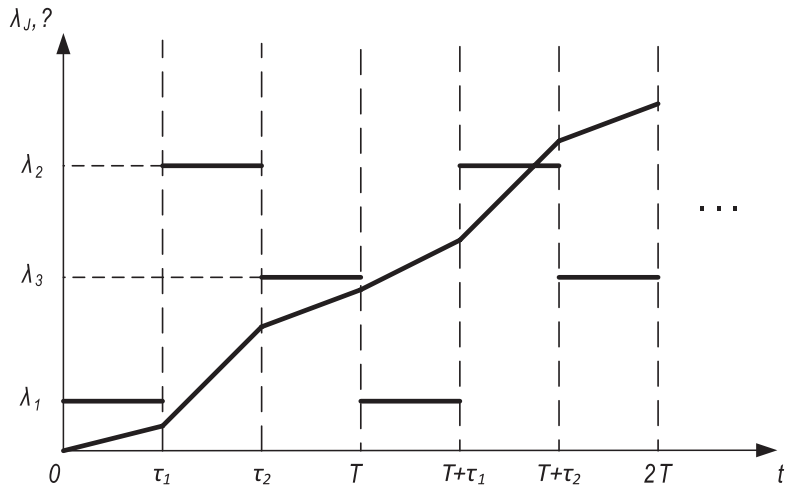


Figure 3. Failure rate model

$$p(t)=1-\{(n-1)\bar{\lambda}T+\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i[t-[(n-1)T+\tau_{i-1}]]\},(30)$$

where $\bar{\lambda}_{i-1}$ is the mean failure rate over the time equal to the (i-1)-th interval (unlike $\bar{\lambda}$, the mean failure rate for the period T).

The formulas for the dependability function $(n-1)T+\tau_{i-1}< t\le(n-1)T+\tau_i$ the summand $\bar{\lambda}_{i-1}\tau_{i-1}$ is not zero only if $i>1$.

For the purpose of calculating the probability of no failure over the fixed time $t=T_f$ using this formula, the value T_f is reported in terms of:

$$t=T=(n-1)T+\tau_{i-1}+\Delta t, \qquad (31)$$

where $0\le\Delta t\le\tau_i-\tau_{i-1}$

Thus, for a particular case when T is divided into two intervals (in the first of which the failure rate λ_1, in the second of which λ_2) and $\frac{\lambda_2}{\lambda_1}=\alpha$, $\frac{\tau_1}{T}=\beta$, the mean time to failure is defined by the formula:

$$\bar{t}=\frac{1}{\lambda_2(\alpha\beta+1-\beta)}.$$

If this expression is obtained from (28), it is assumed that $\lambda_{\max}T<<1$, where $\max\limits_j=\lambda_j$.

The results of calculation of $\bar{t}=f(\beta)$ under fixed λ_2 are given in Fig. 4. If α=1, a stationary failure flow takes place.

Let us proceed to the general case, when dependence $\lambda(t)$ is defined by a piecewise constant non-periodical function. As it was mentioned above the failure rate model is sufficiently universal.

As a non-periodical process can be considered as a periodical one with an infinitely long period, we obtain the dependability function for this case out of (29) under $n=1$. Indeed, the value T can be chosen to be quite large and equal to the time of forecast T_{frc}, during which, as it was stated above, the value of the dependability function is of interest. The value $p(t=T_{frc})$ is so small that the use of the object under $t>T_{frc}$ is of no practical interest. Under these conditions

$$p(t)=e^{-\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i(t-\tau_{i-1})} \text{ if } \tau_{i-1}<t\le\tau_i=T_{frc}. \qquad (32)$$

It remains an open question under what $\tau_{i-1}<t\le\tau_i$ the practical usefulness of the calculations is lost. Let $p(T_{frc})=p_k$ be the probability of no-failure, under which the operation of a non-maintainable object end or a repairable object it is submitted to repairs. Then the duration of the predicted time period T_{frc} subject to (28) is found using equation:

$$p_k=e^{-[\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i(T_{frc}-\tau_{i-1})]}. \qquad (33)$$

From which

$$\ln p_k=-[\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i(T_{frc}-\tau_{i-1})]$$

and

$$T_{frc}=\frac{1}{\lambda_i}\left(-\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i\tau_{i-1}-\ln p_k\right) \qquad (34)$$

Therefore, within the time interval from the beginning of object operation to $t=T_{frc}$ the dependability function is defined by formula (33). If it is required to calculate the probability of no-failure over the fixed time $T_f<T_{frc}$, the value

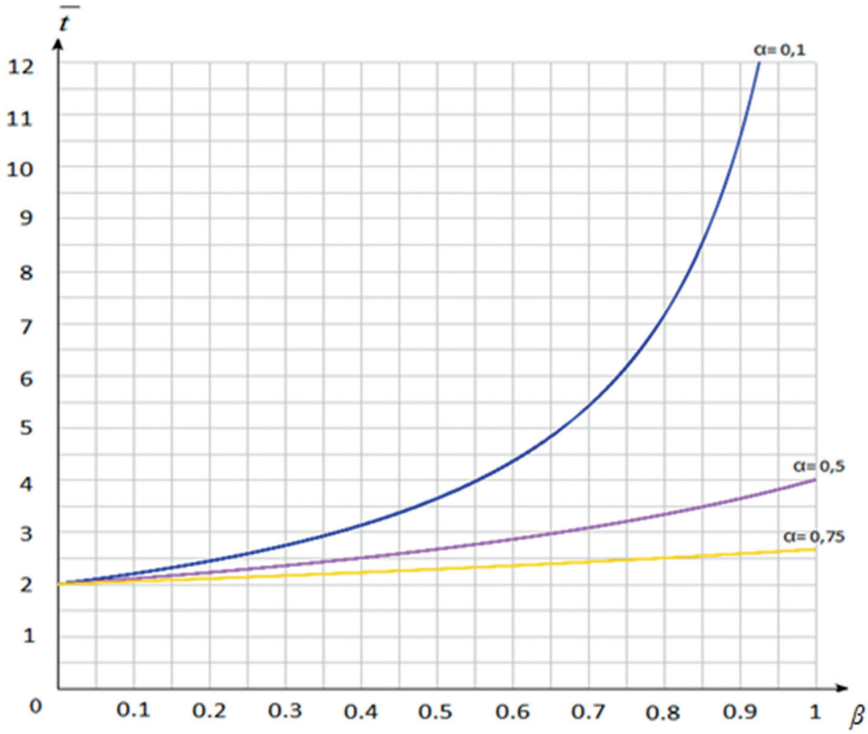


Figure 4. Dependence $\bar{t}=f(\beta)$ under different values of α

T_f has the form $t=\tau_{i-1}+\Delta t$, where $0\le\Delta t<T_{frc}-\tau_{i-1}$.

The linear approximation of $p(t)$ if $\lambda_{\max}T_f<<1$, where $\lambda_{\max}=\max_i \lambda_i$ is as follows:

$$p(t)=1-[\bar{\lambda}_{i-1}\tau_{i-1}+\lambda_i(t-\tau_{i-1})].$$

The mean time to failure in this case is defined by formula

$$\bar{t}=\frac{1}{\bar{\lambda}},$$

where $\bar{\lambda}$ is the mean failure rate of the time T_{frc}.

If linear approximation is not used, the expression of the mean time to failure $\bar{t}$ is calculated using formula (26), in which l is equal to the number of intervals of constant failure rate over time T_{frc}.

Conclusion

1. Solutions are shown for the tasks of identifying the mean time to failure and dependability function for various non-stationary failure flows.

2. Models of "ageing" objects are described, of which the failure rate is defined by a temporally increasing function, models of objects with periodic piecewise constant failure rate, models of objects with non-periodic piecewise constant failure rate. The solutions of tasks for various non-stationary failure flows come down to the last model after time discretization and piecewise constant approximation of the failure rate time dependence performed with the specified accuracy.

3. The shown solution results can be conveniently used in calculation of technical objects dependability.

References

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

2. Shubinsky IB. Strukturnaya nadiozhnost informatsionnykh system. Metody analiza [Structural dependability of information systems. Analysis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2012 [in Russian].

3. Zhao X, Al-Khalifa KN, Nakagawa T. Approximate methods for optimal replacement, maintenance, and inspection policies. Journal of Reliability Engineering & System Safety 2015;144: 68-73.

4. Ke H, Yao K. Block replacement policy with uncertain lifetimes. Journal of Reliability Engineering & System Safety 2016;148:119-124.

5. Ermolin Yu A. Reliability estimation of urban wastewater disposal networks. In: Hayworth GI, editor. Reliability Engineering Advances. New York (USA): Nova Science Publishers, Inc.; 2009.

6. Kancev D, Giorgiev B, Volkanovski A, Gepin M. Time-dependent unavailability of equipment in an ageing NPP: sensitivity study of a developed mode. Journal of Reliability Engineering & System Safety 2016;149:107-120.

7. Chiachio J, Chiachio M, Sankararaman S, Saxena A, Goebel K. Condition-based prediction of time-dependent reliability in composites. Journal of Reliability Engineering & System Safety 2015;142:134-137.

8. Alekseev MI, Yermolin YuA. Nadiozhnost setei i soorouzheniy sistem vodootvedenia [Dependability of networks and structures of water disposal systems]. Moscow: Izdatelstvo ASV; 2015 [in Russian].

9. Yermolin YuA, Alekseev MI. Ouchiot "starenia" obiekta pri otsenke yego nadiozhnosti [Consideration of "aging" of an object in the evaluation of its dependability]. Vodosnabzhenie i sanitarnaya tekhika 2016;5:68-71 [in Russian].

10. Wang Z, Chen W. Time-variant reliability assessment through equivalent stochastic process transformation. Journal of Reliability Engineering & System Safety 2016;152:166-175.

11. Eryilmaz S. A reliability model for a three-state degraded system having random degradation rates. Journal of Reliability Engineering & System Safety 2016;156:59-63.

12. Baranov LA, Ermolin YA. Estimation of reliability indices of a "linearly ageing" object. Dependability 2015;4:61-64.

13. Baranov LA, Yermolin YuA. Nadiozhnost sistem s periodicheskoy kousochno-postoyannoy intesivnostiu otkazov [Dependability of systems with periodic piecewise constant failure rate]. Elektrotekhnika (in print) [in Russian].

About the authors

Leonid Avramovich Baranov, Doctor of Engineering, Professor, Head of Control and Information Security Department, Emperor Nicolas II Moscow State University of Railway Engineering (MIIT), Moscow, Russia, e-mail: baranov.miit@gmail.com

Yuri Alexandrovich Yermolin, Doctor of Engineering, Professor of Control and Information Security, Emperor Nicolas II Moscow State University of Railway Engineering (MIIT), Moscow, Russia, e-mail: ermolin.y@yandex.ru

Received on 21.07.2017

Original article
DOI: 10.21683/1729-2646-2017-17-4-10-15

An example of calculation of a fault tree with logic loops

Yevgeny P. Sorokoletov, *Bi Petron, Saint Petersburg, Russia*

Yevgeny P. Sorokoletov

Aim. *In the course of fault tolerance analysis of complex technical systems using the method of fault tree-based methods, logic loops may occur when, from the point of view of fault tree structure, the system sustains itself. The recursion in the fault tree structure disrupts the logical equation and does not allow performing the calculation and associated analysis. A complex system is understood as one performing a multitude of functions, fault tolerant through a number of redundancy techniques, having intersystem communications and high level of integration of hardware and software components. This paper looks into a particular case of solving the problem of logical recurrence of a fault tree that occurred during an aircraft's power supply system analysis for compliance with airworthiness requirements and aviation regulations.* **Method.** *The paper reviews known ways of solving the set task (both manual and automatic), describes the advantages and disadvantages, applicability and ultimately provides a comparative evaluation based on the results of calculation of occurrence probability of certain aircraft power supply system failures. The method of solving the problem of fault tree recurrence presented in this paper is based on identifying recursive elements in the tree's structure with subsequent reduction of the cyclic connections to a converging spiral by modelling the initial state of the analyzed system.* **Results.** *The calculation of the fault tree under consideration is performed both by means of the method presented in this paper, and the most applicable in the particular case known methods of resolving recurrence. Additionally, comparative results of calculation of other special situations are shown. They are not considered in this paper but demonstrate the distinctive features of different methods. The calculations show that the methods yield the most diverging results in cases when the system is redundant and has feedbacks.* **Conclusions.** *The method presented in the paper has been tested as part of an aircraft's power supply system fault tolerance analysis. The developed method in some cases enables manual resolution of the logic loop problem in the fault tree without a significant increase of computational resources while preserving the analytical solution (minimum fault tree cross sections). On the other hand, this solution may cause a fast growth of the fault tree size in cross-system analysis. In special cases, antithetical events like «operability» and «failure» may become mixed-up in the fault tree structure, which will entail the requirement to use complementary operator inversion and subsequently a manifold increase of the computation time. Another limitation of the method may stem from situations when it is impossible to identify the «initial» and «normal» states of the system under analysis. Given the above, the author classifies the presented method as an engineering method of limited applicability.*

Keywords: *fault tree analysis, logic loops, recursive references, fault tolerance analysis, power supply system.*

For citation: *Sorokoletov EP. An example of calculation of a fault tree with logic loops. Dependability 2017;4: 10-15. DOI: 10.21683/1729-2646-2017-17-4-10-15*

Introduction

Fault tree analysis (FTA) of complex technical systems may involve recursive references. That is typical for cases when fault tolerant systems are analyzed, in which context, from the FTA logic and structure point of view, the system sustains itself. This problem is covered in a number of publications [1,2,3]. In the engineering practice the problem of logic loops is most frequently encountered when evaluating the safety of civil aviation and nuclear industry systems as, firstly, such facilities have to comply with high requirements in terms of dependability and fault tolerance and, secondly, in the above industries FTA is one of the basic safety case methods [4,5]. Logic loops mainly occur during the analysis of distributed redundant systems with many intersystem connections, such as power supply systems (PSS), hydraulic supply systems (HSS), air conditioning and ventilation systems (ACVS), etc. Recursive references can also occur during the analysis of highly integrated systems and feedback systems. The highest probability of logic loop occurrence is observed in cases of intersystem analysis (Figure 1).

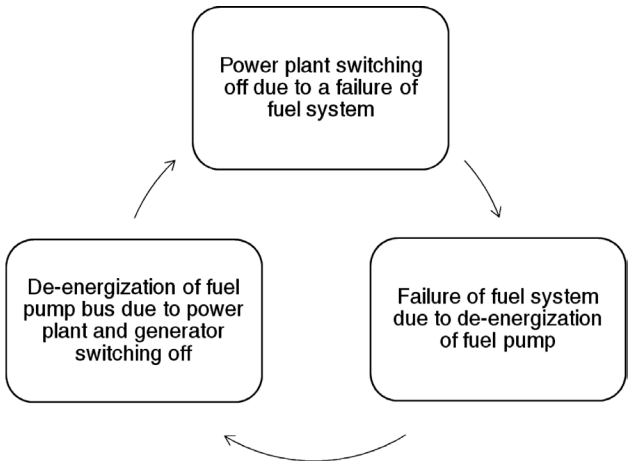


Figure 1. Example of logic loop at intersystem level

Initial data and problem definition

Let us consider a simplified example of the fault tolerance analysis of an aircraft power supply system, as a result of which the problem of logical recurrence of the fault tree structure was solved.

The fault tolerance analysis of aircraft system [5, 6], in general terms, is to determine possible functional failure (FF) of systems, to estimate the hazard level of FF (on the basis of which requirements and budgets of probability are prepared), to analyze possible causes and calculate the probability of FF occurrence. Depending on the situation, a table method, a logic scheme method, a Markov analysis or fault tree analysis can be used as methods of calculation. The last several methods are most widespread due to well-defined structure and powerful analytical capabilities.

The object of analysis is the aircraft power supply system. This system, from a functional point of view, belongs to the class of standard two-channel power supply systems. In this case it is possible to use open sources to describe system operation [7]. The primary alternating current (AC) PSS consists of two generation channels (according to the number of main engines), which can operate separately or in parallel as well as redundant generation channel from the airborne auxiliary power (AAP). Secondary direct current (DC) PSS also consists of two channels and includes rectifiers (Rec) that transform alternating current into direct current, accumulator batteries (ABs) used as a source of emergency power supply, as well as DC-to-AC converter for emergency power supply of alternating current consumers from AB. Each channel of alternating and direct current system consists of a generation subsystem and system of distribution of alternating and direct current accordingly. The distribution system consists of central bus (CB) connected to the corresponding generation channels and several buses (Bus) that supply consumers.

Under normal conditions the power supply is provided by two main generation channels of alternating and direct current. The integration of buses of CB, descent of the aircraft to the start altitude of AAP and switch on of the corresponding generation channel of AAP are carried out in case of failure of one or two main generation channels. The start of AAP is carried out from the bus of accumulator batteries powered by the secondary PSS with direct current under normal conditions, and in case of emergency power supply from accumulator batteries.

Given the above, in the field of fault tolerance analysis of PSS the estimation of probability of de-energization of alternating and direct current consumers is carried out, that at the system level is expressed in de-energization of the corresponding buses of distribution devices. Let us consider

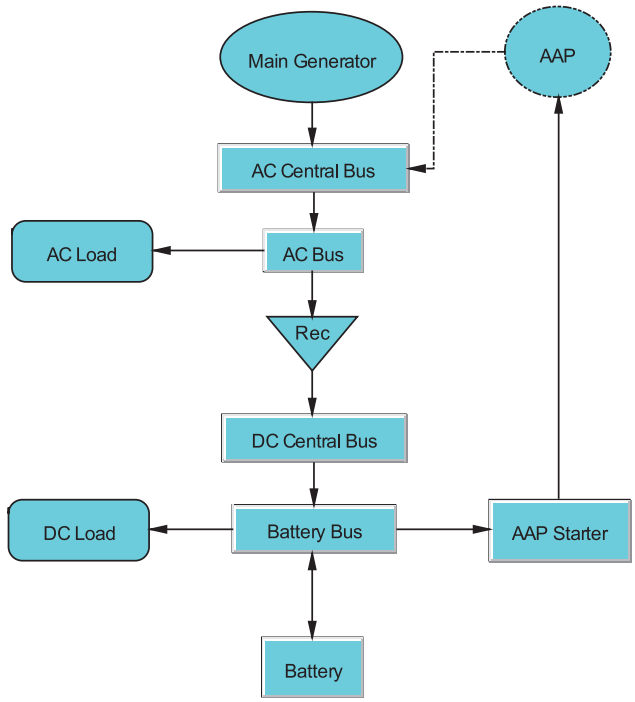


Figure 2. Simplified diagram of the one generation channel of PSS of the aircraft

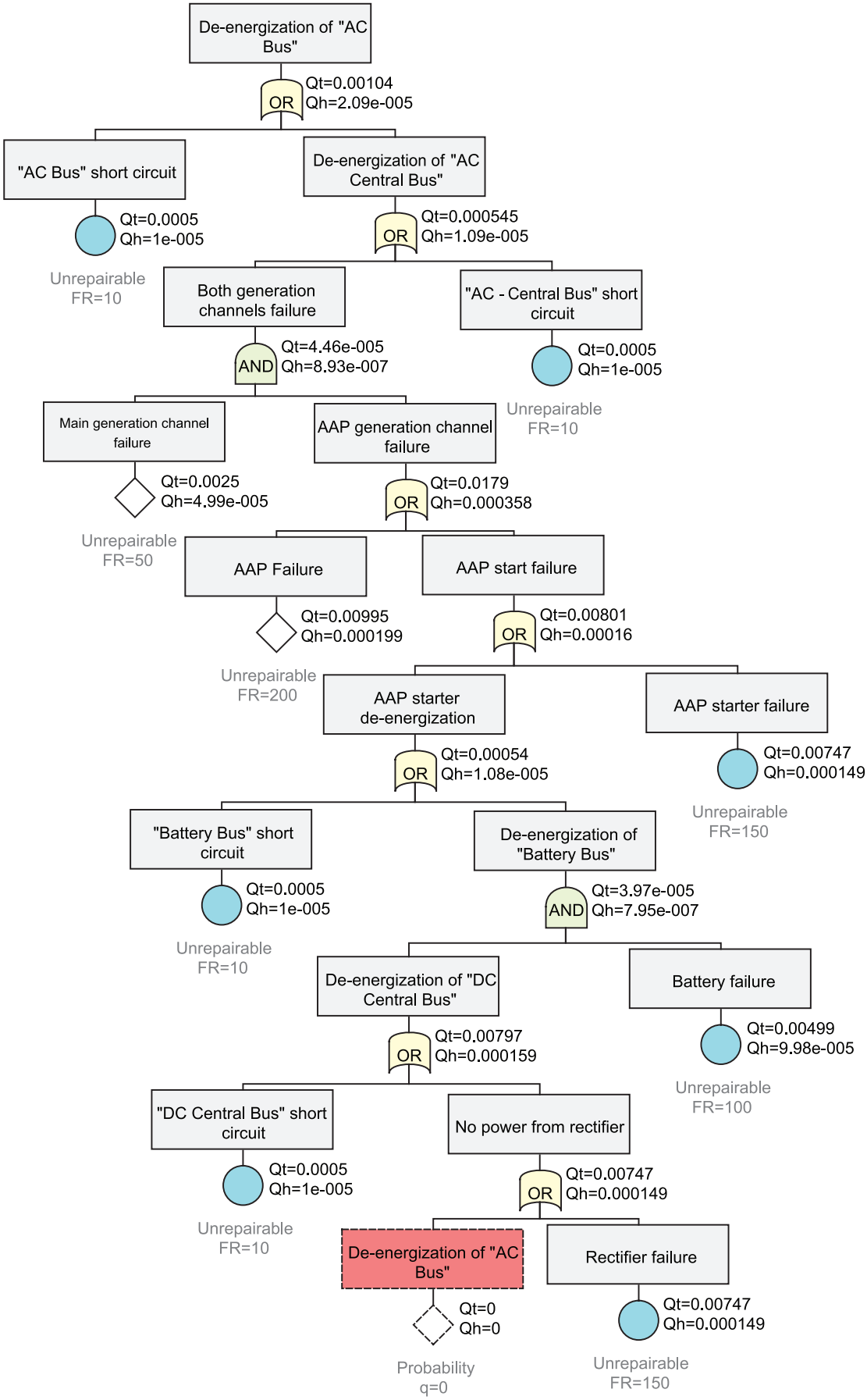


Figure 3. Fault tree «De-energization of Bus-AC bus»

the simplified scheme of PSS from the one main generation channel (actuator-generator), the redundant channel of AAP (Figure 2) and the mechanism of the logic loop generation during deductive analysis.

For example, let us examine the causes of de-energization of alternating current (AC) consumers and, accordingly, of the Bus-AC bus (Figure 3). As the Figure of PSS and fault tree shows the generation channel of APP is cold standby, among other reliable operation of which depends on the state of elements under redundancy themselves. Thus, when considering the dependability of elements under redundancy, the recursive reference on its node appears in the root of the fault tree (marked). Designations, main logical operators and corresponding formulas of the fault tree are defined in accordance with [8].

Basic elements of the fault tree are unrepairable as the calculation is performed on time interval of one flight of the aircraft. Each basic element has the corresponding constant failure rate (FR, λ) with the dimension 10^{-6} (1/h). For the fault tree, the two indicators are calculated in the following way: failure probability (non-availability) Q_t and failure probability for 1 flight hour Q_h.

$$Q_t = 1 - (1 - q) \times e^{-\lambda t};$$

$$Q_h = Q_t / t.$$

Review of the method of calculation of fault trees with logic loops

Manual and automatic solution methods are suggested by different calculation methods of FTA with logic loops [2, 3, 9, 10, 11, 12, 13, 14, 15, 16]. The simplest models involve breaking cyclic connections through the removal of the recursive element. In [2] it is proposed to carry out the analysis of intersystem communication and break relatively weak connection that allows obtaining independent fault trees. Weak connection implies that the system contribution to the probability of occurrence of the event under consideration is negligible. At the place of this communication a zero or an absolute event is created. The analyst's task is to calculate and compare the strength of communication and determine the broke section of the logic loop to substitute, respectively, with a "0" or a "1". The similar algorithm with automatic tools is offered in [16], but in this algorithm the whole logical expression AND/OR is substituted; this algorithm includes the specific event.

Simply removing elements of the logic loop allows quickly solving the problem, but this action negatively affects the accuracy of calculation and the possibility of a deeper research, for example, through the common cause failure analysis [5, 6]. It should be noted that in contrast with the previous example, in a real system the second main generation channel connected via buses of CB exists, thus we cut all redundant sources for intermediate levels of the fault tree, removing the recursive reference.

Another method used to solve problems with cycles is based, in one form or another, on the simulation of "initial" state of the system [13] as well as on heavy regulation of the realization procedure of failures and corresponding consequences [10]. The last is achieved via adding to the fault tree structure the dynamic logical element "Sequence gate", which would specify the required sequence and the subsequent calculation by means of Monte-Carlo simulation. In this research this method wasn't used due to the strict requirements for the computing resources, non-valid results of simulation for short time intervals corresponding to the time of one flight as well as the impossibility to obtain the analytical solution for the purpose of the following common cause failure analysis (this is the requirement of certification authority).

Method and description of the solution

To solve the above situation in the aviation an informal method was assumed which consists in dividing failure sets of PSS into the groups "Before AAP start" and "After AAP start". However, in this sense, there are difficulties with accuracy of taking into account the event of possible no-start of AAP, the probability of which was being multiplied to the corresponding failures of PSS, as if these are two independent events. Absolutely, this event could be classified as "optimistic". To obtain more exact result, another method should be used which allows taking into account a variety of common causes of failures without violation of the analysis logic.

The meaning of the proposed solution of the fault tree with logic loops is to reduce cyclic communication to the spiral form. To obtain such result it is needed to simulate "normal" system state and put this model into the place of the recursive element. After this action the new fault tree is formed taking into account both the recursive element and the initial tree of the first cycle. Thus, the spiral of calculation

Table 1. Comparison of FTA logic loop solution methods

Special situation	Methods of substituting the recursive element		
	"0"	"1"	Initial state modelling
CB1 power failure	$Qt=1.06\times10^{-7}$	$Qt=0.99\times10^{-7}$	$Qt=1\times10^{-7}$
CB1 and CB2 power failure. Emergency power supply to AC power consumers	$Qt=4.91\times10^{-8}$	$Qt=8.85\times10^{-7}$	$Qt=1.52\times10^{-11}$
Rec1 bus power failure	$Qt=3.89\times10^{-8}$	$Qt=3.89\times10^{-8}$	$Qt=3.89\times10^{-8}$
Rec1 and Rec2 bus power failure Initiation of emergency power supply to DC power consumers	$Qt=6.81\times10^{-9}$	$Qt=1.94\times10^{-8}$	$Qt=1.68\times10^{-9}$

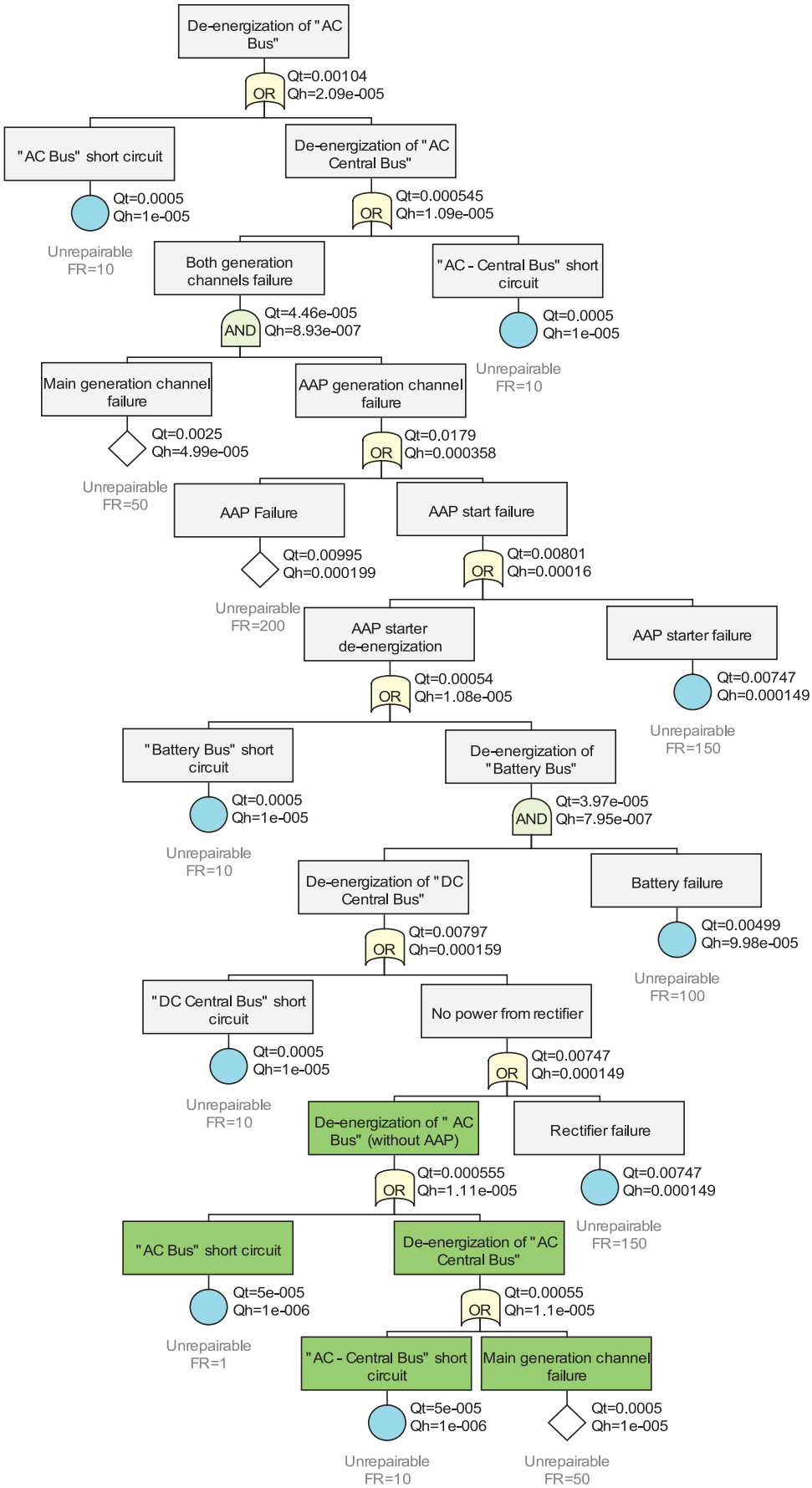


Figure 4. Marking of the “normal” system state and putting it into the place of the recursive element

is formed in the cycle's place. Coming back to the considered system, the normal state consists in the successful operation of the main generation channel when the AAP channel is disabled (Figure 4). The boundary of FTA configuration in accordance with the criteria "Taking into account AAP" and "Without taking into account AAP" (marked part of fault tree) is marked for logical separation.

Conclusion

Let us present some of the calculation results of exceptions of an aircraft's dual-channel PSS using various methods of solving the recurrence problem in FTA.

AS we can see from Table 1, the calculation results under one or another logic loop resolution method depend not so much from the method of substitution as from the complexity of the analyzed event. Thus, the largest discrepancy is observed when analyzing compatible failures of the buses of two generation channels at once. As noted above, in such cases the substitution of the recursive element with a "1" or "0" among other things cuts off all possible redundant sources.

The presented method in some cases enables manual resolution of the logic loop problem in the FTA without a significant increase of computational resources while preserving the analytical solution.

Though it should be noted that the presented method has been developed and tested as part of a private PSS analysis and is not applicable in cases when it is impossible to identify the "initial" and "normal" states of the system under analysis. In other words, the method should be classified as an engineering one.

The method in some cases has a disadvantage caused by possible confusion in the FTA structure of the states of "operability" and "failure". Correcting this effect may require an inversion of the event with logical operator NOT which causes a manifold increase of computation time and the requirements for clear formulation of the events under consideration.

The method also causes an increase in the fault tree size, which may limit its applicability at the intersystem level.

References

1. ASME Standard for probabilistic risk assessment for nuclear power plant application. New York: The American Society of Mechanical Engineers; 2002.

2. Coles GA, Powers TB. Breaking the logical loop to complete the probabilistic risk assessment. In: Proceeding of PSA 89: International Topical Meeting Probability, Reliability, and Safety Assessment. Pennsylvania (USA); 1989. p. 1155–1160.

3. Demichela M, Piccinini N, Ciarambino I, Contini S. How to avoid the generation of logic loops in the construction of fault tree. Reliability Engineering and System Safety 2004;84:197–207.

4. NUREG-0492 Fault tree hand-book. US Nuclear Regulatory Commission. Washington, D.C. (USA); 1981.

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

6. SAE ARP4754A Guidelines for Development of Civil Aircraft and Systems. Pennsylvania: SAE International; 2010.

7. GOST 24898-81. Electrical power systems of aircraft and helicopters. Reliability factor design procedure. Introduction. 1983-01-01. Moscow: Izdatelstvo standartov; 1982 [in Russian].

8. GOST R 27.302-2009. Dependability in technics. Fault tree analysis. Introduction. 15-12-2009. Moscow: Standartinform; 2011 [in Russian].

9. Ciarambino I, Contini S, Demichela M, Piccinini N. How to avoid the generation of loops in the construction of fault tree Proceedings on RAMS. Seattle (USA); 2002.

10. Han SH, Lim H. Top event probability evaluation of a fault tree having circular logics by using Monte Carlo method. Nuclear Engineering and Design 2012;243:336–340.

11. Jung WS, Han SH. Development of an analytical method to break logical loops at the system level. Reliability Engineering and System Safety 2005;90:37–44.

12. Lim HG, Jang SC. An analytic solution for a fault tree with CLs in which the systems are linearly interrelated. Reliability Engineering and System Safety 2007;92:804–807.

13. Lim HG, Jang SC. Systematic treatment of circular logics in a fault tree analysis. Nuclear Engineering and Design 2012;245:172-179.

14. Matsuoka T. An exact method for solving logical loops in reliability analysis. Reliability Engineering and System Safety 2009;94:1282–1288.

15. Vaurio J. A recursive method for breaking complex logic loops in Boolean system models. Reliability Engineering and System Safety 2007;92:1473–1475.

16. Yang JE, Han SH, Park JH, Jin YH. Analytic method to break logical loops automatically in PSA. Reliability Engineering and System Safety 1997;56:101–105.

About the author

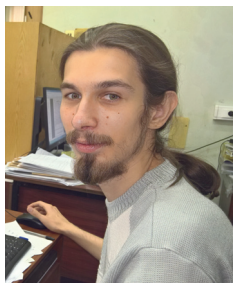
Yevgeny P. Sorokoletov, Head of Fault Tolerance Engineering, Bi Petron, post-graduate student, Engineering Department, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint Petersburg, Russia, E-mail: sorokoletov.john@gmail.com.

Received on 25.05.2017

Original article
Dependability, vol. 17 no.4, 2017 DOI: 10.21683/1729-2646-2017-17-4-16-22

The mechanism of constructing an analytical solution for calculating the probability of no-failure of a cold standby system with heterogeneous elements

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



Dmitry M. Krivopalov

Evgeny V. Yurkevich

Abstract. *The task related to the calculation of the probability of no-failure (PNF) of spacecraft onboard equipment is due to the fact that with the growth of the number of types and quantity of involved elements the process of dependability calculation becomes more complex and time-consuming. In the context of design for dependability, when the process of recalculation is performed repeatedly, this drawback is critical. In order to simplify the calculations, assumptions are made. For instance, in redundant systems heterogeneous elements are used. This approach does not allow evaluating the dependability of a system that features essentially different elements. In order to reduce the time of dependability calculation of the system under consideration, as well as to increase the accuracy of the results, the paper suggests a method of analytical solution for PNF calculation. It is suggested to use the system dependability time dependence function as the main dependability indicator, while for individual elements the respective failure rate is proposed. The authors look at the problem of consideration of the complexity of such function's construction for the cases of functional dependability calculation, when the elements of the system under consideration may not be homogeneous. For a system that includes any number of essentially different elements with cold redundancy, a method was developed and mathematically justified that allows representing in matrix form an analytic expression for calculation of probability of no-failure (PNF). The importance of considering the performance of the facilities that ensure redundancy of functional units is demonstrated in the context of design for dependability of spacecraft. A special attention is given to systems that include a random number of essentially different elements with cold redundancy. As one of the ways of solving the above problem, the paper shows that in this case a numeric evaluation of dependability is possible using rough computation with integration and differentiation. It is proposed to evaluate the degree of approximation of such calculations as both the accuracy of the computer itself and the complexity of the system under consideration. For that purpose, serial representation of the function of probability of no-failure is used for a system after the initiation of each next element under redundancy. The resulting function is formed by grouping of summands in particular order. The potential of replacing the differentiation and integration operations is shown. Under known matrix coefficients the application of the suggested algorithm will significantly improve the accuracy and speed of PNF computation. The practical details of the task related to ensuring spacecraft operational stability under environmental effects are characterized by the importance of the factor of prompt decision-making regarding the generation of control signal aimed at ensuring homoeostasis of the onboard systems performance. The analytic expression for calculation of PNF of a system comprised of a random number of elements can be used for mapping data in computer memory as part of decision support.*

Keywords: *design for dependability, technical systems, essentially different system components, cold redundancy, probability of no-failure, analytical expression, computation speedup, dependability estimation accuracy improvement, computer memory.*

For citation*: Krivopalov DM, Yurkevich EV. The mechanism of constructing an analytical solution in calculating the probability of no-failure of a cold standby system with heterogeneous elements. Dependability 2017;4: 16-22. DOI: 10.21683/1729-2646-2017-17-4-16-22*

Introduction

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

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

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

In [4] it was shown that analytic solutions could be represented in matrix form, which is very convenient in terms of computer memory placement. In order to fully automate the PNF calculation it is required to develop a mechanism for matrix coefficient definition. For that purpose it is required to consider their changes under differentiation and integration according to the main calculation formulas.

Change of coefficients under differentiation

Let us examine a random system out of four elements.

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

The functions $A(t)$, $B(t)$, $C(t)$, $D(t)$ are polynomials in powers of t, of which the number of summands is defined by the number of respective identical system elements.

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

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

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

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

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

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

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

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

In that case, the PNF calculation formula – if the fifth element is initiated – will be as follows:

$$P_5(T) = P_4(T) + \int_0^T p_5(\tau,T)\cdot f_4(\tau)d\tau,$$

$P_4(T)$ is the PNF of a system out of four elements over time T;

$p_5(\tau,T)$ is the PNF of the fifth (initiated) element within the time period from τ to T;

$f_4(\tau)$ is the failure density distribution of the system out of four elements for the moment in time τ.

In the calculation formula the distribution density must be defined.

$$f_4(t) = -\frac{P_4(t)}{dt} =$$

$$= -\left(A(t)\cdot e^{-\lambda_1 t} + B(t)\cdot e^{-\lambda_2 t} + C(t)\cdot e^{-\lambda_3 t} + D(t)\cdot e^{-\lambda_4 t}\right)\frac{1}{dt} =$$

$$= \left(-A(t)\cdot e^{-\lambda_1 t}\right)\frac{1}{dt} + \left(-B(t)\cdot e^{-\lambda_2 t}\right)\frac{1}{dt} +$$

$$+\left(-C(t)\cdot e^{-\lambda_3 t}\right)\frac{1}{dt} + \left(-D(t)\cdot e^{-\lambda_4 t}\right)\frac{1}{dt}.$$

Let us consider the summand individually.

$$\left(-A(t)\cdot e^{-\lambda_1 t}\right)\frac{1}{dt} = \left(-\left(a_0 + a_1 t + a_2 t^2 + a_3 t^3\right)\cdot e^{-\lambda_1 t}\right)\frac{1}{dt} =$$

$$= \left(\left(\lambda_1 a_0 - a_1\right) + \left(\lambda_1 a_1 - 2a_2\right)t + \left(\lambda_1 a_2 - 3a_3\right)t^2 + \left(\lambda_1 a_3\right)t^3\right)\cdot e^{-\lambda_1 t}.$$

The other summands are differentiated similarly.

As previously, we will present the result of differentiation as a matrix.

	λ_1	λ_2	λ_3	λ_4
t^0	$\lambda_1 a_0 - a_1$	$\lambda_2 b_0 - b_1$	$\lambda_3 c_0 - c_1$	$\lambda_4 d_0 - d_1$
t^1	$\lambda_1 a_1 - 2a_2$	$\lambda_2 b_1 - 2b_2$	$\lambda_3 c_1 - 2c_2$	$\lambda_4 d_1 - 2d_2$
t^2	$\lambda_1 a_2 - 3a_3$	$\lambda_2 b_2 - 3b_3$	$\lambda_3 c_2 - 3c_3$	$\lambda_4 d_2 - 3d_3$
t^3	$\lambda_1 a_3$	$\lambda_2 b_3$	$\lambda_3 c_3$	$\lambda_4 d_3$

Let us represent the distribution densities of probability B as a coefficient matrix.

$$B = \begin{pmatrix} \lambda_1 a_0 - a_1 & \lambda_2 b_0 - b_1 & \lambda_3 c_0 - c_1 & \lambda_4 d_0 - d_1 \\ \lambda_1 a_1 - 2a_2 & \lambda_2 b_1 - 2b_2 & \lambda_3 c_1 - 2c_2 & \lambda_4 d_1 - 2d_2 \\ \lambda_1 a_2 - 3a_3 & \lambda_2 b_2 - 3b_3 & \lambda_3 c_2 - 3c_3 & \lambda_4 d_2 - 3d_3 \\ \lambda_1 a_3 & \lambda_2 b_3 & \lambda_3 c_3 & \lambda_4 d_3 \end{pmatrix}.$$

As the calculations will be performed using a computer, a common formula must be defined that can be used to cal-

culate any element of the matrix B depending on its line and column index. For that purpose, let us complement matrix A with an extra line of zeroes.

$$A=\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} \Rightarrow \begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}.$$

Then, the calculation of matrix B will be transformed.

$$B=\begin{pmatrix} \lambda_1 a_0 - a_1 & \lambda_2 b_0 - b_1 & \lambda_3 c_0 - c_1 & \lambda_4 d_0 - d_1 \\ \lambda_1 a_1 - 2a_2 & \lambda_2 b_1 - 2b_2 & \lambda_3 c_1 - 2c_2 & \lambda_4 d_1 - 2d_2 \\ \lambda_1 a_2 - 3a_3 & \lambda_2 b_2 - 3b_3 & \lambda_3 c_2 - 3c_3 & \lambda_4 d_2 - 3d_3 \\ \lambda_1 a_3 - 4\cdot 0 & \lambda_2 b_3 - 4\cdot 0 & \lambda_3 c_3 - 4\cdot 0 & \lambda_4 d_3 - 4\cdot 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda_1 a_0 - 1a_1 & \lambda_2 b_0 - 1b_1 & \lambda_3 c_0 - 1c_1 & \lambda_4 d_0 - 1d_1 \\ \lambda_1 a_1 - 2a_2 & \lambda_2 b_1 - 2b_2 & \lambda_3 c_1 - 2c_2 & \lambda_4 d_1 - 2d_2 \\ \lambda_1 a_2 - 3a_3 & \lambda_2 b_2 - 3b_3 & \lambda_3 c_2 - 3c_3 & \lambda_4 d_2 - 3d_3 \\ \lambda_1 a_3 - 4a_4 & \lambda_2 b_3 - 4b_4 & \lambda_3 c_3 - 4c_4 & \lambda_4 d_3 - 4d_4 \end{pmatrix};$$

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

Note. A similar result is obtained if coefficients a_4, b_4, c_4, d_4 are present in the respective polynomials $A(t)$, $B(t)$, $C(t)$, $D(t)$.

Thus, the differentiation process takes the following form:

$$f_4(t)=-\frac{P_4(t)}{dt}=-\frac{A^{\mathrm{T}}\cdot T\cdot F(\Lambda,t)^T}{dt}=B^{\mathrm{T}}\cdot T\cdot F(\Lambda,t)^T;$$

$$A=\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} \Rightarrow B=\begin{pmatrix} a_0' & b_0' & c_0' & d_0' \\ a_1' & b_1' & c_1' & d_1' \\ a_2' & b_2' & c_2' & d_2' \\ a_3' & b_3' & c_3' & d_3' \end{pmatrix}.$$

The differentiation is substituted with the calculation of the coefficients of matrix B out of matrix A and matrix elements, which is a much simpler operation from the machine computation point of view. The common formula for calculation of the elements of matrix B is:

$$B_{i,j}=\Lambda_j\cdot A_{i,j}-i\cdot A_{i+1,j},\ i=1..N,\ j=1..N,$$

i is the line index in the respective matrix;
j is the column index in the respective matrix;
N is the number of elements in the initial system.

Change of coefficients under integration

The next step of calculation is the integration:

$$\int_0^t p_5(\tau,t)\cdot f_4(\tau)d\tau =$$

$$=\int_0^t e^{-\lambda_5(t-\tau)}\cdot\begin{pmatrix} A'(\tau)\cdot e^{-\lambda_1\tau}+B'(\tau)\cdot e^{-\lambda_2\tau}+ \\ +C'(\tau)\cdot e^{-\lambda_3\tau}+D'(\tau)\cdot e^{-\lambda_4\tau} \end{pmatrix}d\tau =$$

$$=e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau+e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau+$$

$$+e^{-\lambda_5 t}\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau+e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau.$$

Two distinctly different cases are possible: λ_5 can either numerically match one of the four failure rates, or not match it. Depending on that, the expression under the integral sign significantly transforms.

Let us consider the case when the failure rates of the initiated element matches the failure rate of one of the elements of the system under consideration, e.g. the first one.

$$\lambda_5=\lambda_1$$

Then the respective integral will be simplified.

$$e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=e^{-\lambda_1 t}\cdot\int_0^t A'(\tau)d\tau=$$

$$=e^{-\lambda_1 t}\cdot\int_0^t a_0'+a_1'\tau+a_2'\tau^2+a_3'\tau^3 d\tau=$$

$$=\left(a_0' t+\frac{a_1'}{2}t^2+\frac{a_2'}{3}t^3+\frac{a_3'}{4}t^4\right)\cdot e^{-\lambda_1 t}.$$

Further, let us examine the remaining integrals.

The PNF of a system out of 5 elements is the combination of the sum of the PNFs of the system out of 4 elements and the result of integration. Let us write how the coefficients will change in the case of matching for one type of element types (λ_1):

$$P_5(t)=P_4(t)+\int_0^t p_5(\tau,t)\cdot f_4(\tau)d\tau =$$

$$=A(t)\cdot e^{-\lambda_1 t}+e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau+$$

$$+B(t)\cdot e^{-\lambda_2 t}+e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau+$$

$$+C(t)\cdot e^{-\lambda_3 t}+e^{-\lambda_5 t}\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau+$$

$$+D(t)\cdot e^{-\lambda_4 t}+e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau =$$

$$=\left(a_0+a_1 t+a_2 t^2+a_3 t^3+a_4 t^4\right)\cdot e^{-\lambda_1 t}+$$

$$+\left(a_0' t+\frac{a_1'}{2}t^2+\frac{a_2'}{3}t^3+\frac{a_3'}{4}t^4\right)\cdot e^{-\lambda_1 t}+$$

$$+B(t)\cdot e^{-\lambda_2 t}+e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau+$$

$$+C(t)\cdot e^{-\lambda_3 t}+e^{-\lambda_5 t}\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau+$$

$$+D(t)\cdot e^{-\lambda_4 t}+e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau=$$

$$=\begin{pmatrix} a_0+(a_1+a_0')t+\left(a_2+\frac{a_1'}{2}\right)t^2+ \\ +\left(a_3+\frac{a_2'}{3}\right)t^3+\left(a_4+\frac{a_3'}{4}\right)t^4 \end{pmatrix}\cdot e^{-\lambda_1 t}+$$

$$+B(t)\cdot e^{-\lambda_2 t}+e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau+$$

$$+C(t)\cdot e^{-\lambda_3 t}+e^{-\lambda_5 t}\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau+$$

$$+D(t)\cdot e^{-\lambda_4 t}+e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau.$$

I.e. the initial matrix A transforms in such a way that some matrix elements are combined with some summands.

$$A=\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}\Rightarrow A=\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1+a_0' & b_1 & c_1 & d_1 \\ a_2+\frac{a_1'}{2} & b_2 & c_2 & d_2 \\ a_3+\frac{a_2'}{3} & b_3 & c_3 & d_3 \\ a_4+\frac{a_3'}{4} & b_4 & c_4 & d_4 \end{pmatrix}.$$

The common formula of coefficients calculation in the matching part is as follows:

$$A_{i+1,j}=A_{i+1,j}+\frac{B_{i,j}}{i},\ \text{if}\ \Lambda_j=\lambda_k,\ i=1..N,\ j=1..N,$$

i is the line index in the respective matrix;
j is the column index in the respective matrix;
k is the index of the initiated element of matrix Λ;
N is the number of elements in the initial system.

Let us consider the case when the failure rate of the initiated element does not match any of the failure rates of the system's elements.

$$\lambda_5\neq\lambda_1,\ \lambda_5\neq\lambda_2,\ \lambda_5\neq\lambda_3,\ \lambda_5\neq\lambda_4.$$

Then, the integration will become more complex:

$$e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=e^{-\lambda_5 t}\cdot\int_0^t a_0'\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau+$$

$$+e^{-\lambda_5 t}\cdot\int_0^t a_1'\tau\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau+$$

$$+e^{-\lambda_5 t}\cdot\int_0^t a_2'\tau^2\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau+e^{-\lambda_5 t}\cdot\int_0^t a_3'\tau^3\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau.$$

Let us take each integral in sum individually:

$$\blacksquare\ e^{-\lambda_5 t}\cdot\int_0^t a_0'\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=a_0'\cdot e^{-\lambda_5 t}\cdot\int_0^t e^{(\lambda_5-\lambda_1)\tau}d\tau=$$

$$=a_0'\cdot e^{-\lambda_5 t}\cdot\left(\frac{1}{\lambda_5-\lambda_1}\cdot e^{(\lambda_5-\lambda_1)t}-\frac{1}{\lambda_5-\lambda_1}\right)=$$

$$=\frac{a_0'}{\lambda_5-\lambda_1}\cdot e^{-\lambda_1 t}-\frac{a_0'}{\lambda_5-\lambda_1}\cdot e^{-\lambda_5 t};$$

$$\blacksquare\ e^{-\lambda_5 t}\cdot\int_0^t a_1'\tau\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=a_1'\cdot e^{-\lambda_5 t}\cdot\int_0^t\tau\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=$$

$$=a_1'\cdot e^{-\lambda_5 t}\cdot\left(\frac{1}{\lambda_5-\lambda_1}\cdot t\cdot e^{(\lambda_5-\lambda_1)t}-\frac{1}{(\lambda_5-\lambda_1)^2}\cdot e^{(\lambda_5-\lambda_1)t}+\frac{1}{(\lambda_5-\lambda_1)^2}\right)=$$

$$=\frac{a_1'}{\lambda_5-\lambda_1}\cdot t\cdot e^{-\lambda_1 t}-\frac{a_1'}{(\lambda_5-\lambda_1)^2}\cdot e^{-\lambda_1 t}+\frac{a_1'}{(\lambda_5-\lambda_1)^2}\cdot e^{-\lambda_5 t};$$

$$\blacksquare\ e^{-\lambda_5 t}\cdot\int_0^t a_2'\tau^2\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=a_2'\cdot e^{-\lambda_5 t}\cdot\int_0^t\tau^2\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=$$

$$=a_2'\cdot e^{-\lambda_5 t}\cdot\begin{pmatrix}\frac{1}{\lambda_5-\lambda_1}\cdot t^2\cdot e^{(\lambda_5-\lambda_1)t}-\frac{2}{(\lambda_5-\lambda_1)^2}\cdot t\cdot e^{(\lambda_5-\lambda_1)t}+ \\ +\frac{2}{(\lambda_5-\lambda_1)^3}\cdot e^{(\lambda_5-\lambda_1)t}-\frac{2}{(\lambda_5-\lambda_1)^3}\end{pmatrix}=$$

$$=\frac{a_2'}{\lambda_5-\lambda_1}\cdot t^2\cdot e^{-\lambda_1 t}-\frac{2a_2'}{(\lambda_5-\lambda_1)^2}\cdot t\cdot e^{-\lambda_1 t}+$$

$$+\frac{2a_2'}{(\lambda_5-\lambda_1)^3}\cdot e^{-\lambda_1 t}-\frac{2a_2'}{(\lambda_5-\lambda_1)^3}\cdot e^{-\lambda_5 t};$$

$$\blacksquare\ e^{-\lambda_5 t}\cdot\int_0^t a_3'\tau^3\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=a_3'\cdot e^{-\lambda_5 t}\cdot\int_0^t\tau^3\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau=$$

$$=a_3'\cdot e^{-\lambda_5 t}\cdot\begin{pmatrix}\frac{1}{\lambda_5-\lambda_1}\cdot t^3\cdot e^{(\lambda_5-\lambda_1)t}-\frac{3}{(\lambda_5-\lambda_1)^2}\cdot t^2\cdot e^{(\lambda_5-\lambda_1)t}+ \\ +\frac{6}{(\lambda_5-\lambda_1)^3}\cdot t\cdot e^{(\lambda_5-\lambda_1)t}-\frac{6}{(\lambda_5-\lambda_1)^4}\cdot e^{(\lambda_5-\lambda_1)t}+\frac{6}{(\lambda_5-\lambda_1)^4}\end{pmatrix}=$$

$$= \frac{a_3'}{\lambda_5-\lambda_1}\cdot t^3\cdot e^{-\lambda_1 t} - \frac{3a_3'}{(\lambda_5-\lambda_1)^2}\cdot t^2\cdot e^{-\lambda_1 t} + \frac{6a_3'}{(\lambda_5-\lambda_1)^3}\cdot t\cdot e^{-\lambda_1 t} -$$

$$- \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\cdot e^{-\lambda_1 t} + \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\cdot e^{-\lambda_5 t}.$$

Let us sum up the results of integration by grouping the summands:

$$e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau =$$

$$= \left(\begin{array}{l}\left(\left(\frac{a_0'}{\lambda_5-\lambda_1} - \frac{a_1'}{(\lambda_5-\lambda_1)^2} + \frac{2a_2'}{(\lambda_5-\lambda_1)^3} - \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right) + \right.\\ + \left(\frac{a_1'}{\lambda_5-\lambda_1} - \frac{2a_2'}{(\lambda_5-\lambda_1)^2} + \frac{6a_3'}{(\lambda_5-\lambda_1)^3}\right)\cdot t + \\ \left. + \left(\frac{a_2'}{\lambda_5-\lambda_1} - \frac{3a_3'}{(\lambda_5-\lambda_1)^2}\right)\cdot t^2 + \frac{a_3'}{\lambda_5-\lambda_1}\cdot t^3\right)\end{array}\right)\cdot e^{-\lambda_1 t} +$$

$$+ \left(-\frac{a_0'}{\lambda_5-\lambda_1} + \frac{a_1'}{(\lambda_5-\lambda_1)^2} - \frac{2a_2'}{(\lambda_5-\lambda_1)^3} + \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right)\cdot e^{-\lambda_5 t}.$$

Integrals with other polynomials are calculated in a similar way.

The PNF of a system out of 5 elements is the combination of the sum of the PNFs of the system out of 4 elements and the result of integration. Let us write how the coefficients will change in the case of no-matching for one of the element types (λ_1):

$$P_5(t) = P_4(t) + \int_0^t p_5(\tau,t)\cdot f_4(\tau)\,d\tau =$$

$$= A(t)\cdot e^{-\lambda_1 t} + e^{-\lambda_5 t}\cdot\int_0^t A'(\tau)\cdot e^{(\lambda_5-\lambda_1)\tau}d\tau + B(t)\cdot e^{-\lambda_2 t} +$$

$$+ e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau + C(t)\cdot e^{-\lambda_3 t} + e^{-\lambda_5 t}\cdot$$

$$\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau + D(t)\cdot e^{-\lambda_4 t} + e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau =$$

$$= \left(a_0 + a_1 t + a_2 t^2 + a_3 t^3\right)\cdot e^{-\lambda_1 t} +$$

$$+ \left(\begin{array}{l}\left(\left(\frac{a_0'}{\lambda_5-\lambda_1} - \frac{a_1'}{(\lambda_5-\lambda_1)^2} + \frac{2a_2'}{(\lambda_5-\lambda_1)^3} - \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right) + \right.\\ + \left(\frac{a_1'}{\lambda_5-\lambda_1} - \frac{2a_2'}{(\lambda_5-\lambda_1)^2} + \frac{6a_3'}{(\lambda_5-\lambda_1)^3}\right)\cdot t + \\ \left. + \left(\frac{a_2'}{\lambda_5-\lambda_1} - \frac{3a_3'}{(\lambda_5-\lambda_1)^2}\right)\cdot t^2 + \frac{a_3'}{\lambda_5-\lambda_1}\cdot t^3\right)\end{array}\right)\cdot e^{-\lambda_1 t} +$$

$$+ \left(-\frac{a_0'}{\lambda_5-\lambda_1} + \frac{a_1'}{(\lambda_5-\lambda_1)^2} - \frac{2a_2'}{(\lambda_5-\lambda_1)^3} + \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right)\cdot e^{-\lambda_5 t} +$$

$$+ B(t)\cdot e^{-\lambda_2 t} + e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau + C(t)\cdot e^{-\lambda_3 t} + e^{-\lambda_5 t}\cdot$$

$$\cdot\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau + D(t)\cdot e^{-\lambda_4 t} + e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau =$$

$$= \left(\begin{array}{l}\left(\left(a_0 + \frac{a_0'}{\lambda_5-\lambda_1} - \frac{a_1'}{(\lambda_5-\lambda_1)^2} + \frac{2a_2'}{(\lambda_5-\lambda_1)^3} - \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right) + \right.\\ + \left(a_1 + \frac{a_1'}{\lambda_5-\lambda_1} - \frac{2a_2'}{(\lambda_5-\lambda_1)^2} + \frac{6a_3'}{(\lambda_5-\lambda_1)^3}\right)\cdot t + \\ \left. + \left(a_2 + \frac{a_2'}{\lambda_5-\lambda_1} - \frac{3a_3'}{(\lambda_5-\lambda_1)^2}\right)\cdot t^2 + \left(a_3 + \frac{a_3'}{\lambda_5-\lambda_1}\right)\cdot t^3\right)\end{array}\right)\cdot e^{-\lambda_1 t} +$$

$$+ \left(-\frac{a_0'}{\lambda_5-\lambda_1} + \frac{a_1'}{(\lambda_5-\lambda_1)^2} - \frac{2a_2'}{(\lambda_5-\lambda_1)^3} + \frac{6a_3'}{(\lambda_5-\lambda_1)^4}\right)\cdot e^{-\lambda_5 t} +$$

$$+ B(t)\cdot e^{-\lambda_2 t} + e^{-\lambda_5 t}\cdot\int_0^t B'(\tau)\cdot e^{(\lambda_5-\lambda_2)\tau}d\tau + C(t)\cdot e^{-\lambda_3 t} + e^{-\lambda_5 t}\cdot$$

$$\int_0^t C'(\tau)\cdot e^{(\lambda_5-\lambda_3)\tau}d\tau + D(t)\cdot e^{-\lambda_4 t} + e^{-\lambda_5 t}\cdot\int_0^t D'(\tau)\cdot e^{(\lambda_5-\lambda_4)\tau}d\tau.$$

As the result of initiation of an additional element with the failure rate of $\lambda_5 \neq \lambda_1$, the coefficients realigned in a certain way according to exponential $-\lambda_1 t$. The degree of polynomial $A(t)$ did not increase. Additionally, the integration created a summand that will be in the sum of the coefficient for the new exponential $-\lambda_5 t$. Let us write the complete result of summation in matrix form:

$$P_5(t) = P_4(t) + \int_0^t p_5(\tau,t)\cdot f_4(\tau)\,d\tau;$$

$$P_5(t) = A^T\cdot T\cdot F(\Lambda,t)^T;$$

$$\Lambda = \begin{pmatrix}\lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5\end{pmatrix};$$

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

$$A = \begin{pmatrix} a_0 + \frac{a_0'}{\lambda_5 - \lambda_1} - \frac{a_1'}{(\lambda_5 - \lambda_1)^2} + \frac{2a_2'}{(\lambda_5 - \lambda_1)^3} - \frac{6a_3'}{(\lambda_5 - \lambda_1)^4} \\ a_1 + \frac{a_1'}{\lambda_5 - \lambda_1} - \frac{2a_2'}{(\lambda_5 - \lambda_1)^2} + \frac{6a_3'}{(\lambda_5 - \lambda_1)^3} \\ a_2 + \frac{a_2'}{\lambda_5 - \lambda_1} - \frac{3a_3'}{(\lambda_5 - \lambda_1)^2} \\ a_3 + \frac{a_3'}{\lambda_5 - \lambda_1} \end{pmatrix}$$

$$b_0 + \frac{b_0'}{\lambda_5 - \lambda_2} - \frac{b_1'}{(\lambda_5 - \lambda_2)^2} + \frac{2b_2'}{(\lambda_5 - \lambda_2)^3} - \frac{6b_3'}{(\lambda_5 - \lambda_2)^4}$$

$$b_1 + \frac{b_1'}{\lambda_5 - \lambda_2} - \frac{2b_2'}{(\lambda_5 - \lambda_2)^2} + \frac{6b_3'}{(\lambda_5 - \lambda_2)^3}$$

$$b_2 + \frac{b_2'}{\lambda_5 - \lambda_2} - \frac{3b_3'}{(\lambda_5 - \lambda_2)^2}$$

$$b_3 + \frac{b_3'}{\lambda_5 - \lambda_2}$$

$$c_0 + \frac{c_0'}{\lambda_5 - \lambda_3} - \frac{c_1'}{(\lambda_5 - \lambda_3)^2} + \frac{2c_2'}{(\lambda_5 - \lambda_3)^3} - \frac{6c_3'}{(\lambda_5 - \lambda_3)^4}$$

$$c_1 + \frac{c_1'}{\lambda_5 - \lambda_3} - \frac{2c_2'}{(\lambda_5 - \lambda_3)^2} + \frac{6c_3'}{(\lambda_5 - \lambda_3)^3}$$

$$c_2 + \frac{c_2'}{\lambda_5 - \lambda_3} - \frac{3c_3'}{(\lambda_5 - \lambda_3)^2}$$

$$c_3 + \frac{c_3'}{\lambda_5 - \lambda_3}$$

$$d_0 + \frac{d_0'}{\lambda_5 - \lambda_4} - \frac{d_1'}{(\lambda_5 - \lambda_4)^2} + \frac{2d_2'}{(\lambda_5 - \lambda_4)^3} - \frac{6d_3'}{(\lambda_5 - \lambda_4)^4}$$

$$d_1 + \frac{d_1'}{\lambda_5 - \lambda_4} - \frac{2d_2'}{(\lambda_5 - \lambda_4)^2} + \frac{6d_3'}{(\lambda_5 - \lambda_4)^3}$$

$$d_2 + \frac{d_2'}{\lambda_5 - \lambda_4} - \frac{3d_3'}{(\lambda_5 - \lambda_4)^2}$$

$$d_3 + \frac{d_3'}{\lambda_5 - \lambda_4}$$

$$\begin{pmatrix} \left(-\frac{a_0'}{\lambda_5 - \lambda_1} + \frac{a_1'}{(\lambda_5 - \lambda_1)^2} - \frac{2a_2'}{(\lambda_5 - \lambda_1)^3} + \frac{6a_3'}{(\lambda_5 - \lambda_1)^4} \right) + \\ + \left(-\frac{b_0'}{\lambda_5 - \lambda_2} + \frac{b_1'}{(\lambda_5 - \lambda_2)^2} - \frac{2b_2'}{(\lambda_5 - \lambda_2)^3} + \frac{6b_3'}{(\lambda_5 - \lambda_2)^4} \right) + \\ + \left(-\frac{c_0'}{\lambda_5 - \lambda_3} + \frac{c_1'}{(\lambda_5 - \lambda_3)^2} - \frac{2c_2'}{(\lambda_5 - \lambda_3)^3} + \frac{6c_3'}{(\lambda_5 - \lambda_3)^4} \right) + \\ + \left(-\frac{d_0'}{\lambda_5 - \lambda_4} + \frac{d_1'}{(\lambda_5 - \lambda_4)^2} - \frac{2d_2'}{(\lambda_5 - \lambda_4)^3} + \frac{6d_3'}{(\lambda_5 - \lambda_4)^4} \right) \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Thus, the integration process in case of initiation of elements can be reduced to the transformation of matrix A: its expansion and associated recalculation of the coefficients. The common formula for calculation of the coefficients for the non-matching part of the matrix is:

$$A_{i,j} = A_{i,j} + \frac{B_{i,j}}{\Lambda_k - \Lambda_j} + \sum_{m=1}^{N-i} \frac{(-1)^m \cdot B_{i+m,j} \cdot (m+i-1)!}{(\Lambda_k - \Lambda_j)^{m+1} \cdot (i-1)!},$$

if $\Lambda_j \neq \lambda_k$, $i = 1..N$, $j = 1..N$,
i is the line index in the respective matrix;
j is the column index in the respective matrix;
k is the index of the initiated element of matrix Λ;
N is the number of elements in the initial system.

A common formula is also required for the summands that will make up a new coefficient for the exponential of the initiated element failure rate, i.e. for the formula:

$$-\frac{a_0'}{\lambda_5 - \lambda_1} + \frac{a_1'}{(\lambda_5 - \lambda_1)^2} - \frac{2a_2'}{(\lambda_5 - \lambda_1)^3} + \frac{6a_3'}{(\lambda_5 - \lambda_1)^4}.$$

$$A_{i,k} = A_{i,k} + \sum_{m=1}^{N} \frac{(-1)^m \cdot B_{m,j} \cdot (m-1)!}{(\Lambda_k - \Lambda_j)^m},$$

if $\Lambda_j \neq \lambda_k$, $i = 1..N$, $j = 1..N$,
i is the line index in the respective matrix;
j is the column index in the respective matrix;
k is the index of the initiated element of matrix Λ;
N is the number of elements in the initial system.

Algorithmic diagram of the analytic solution

By combining the obtained formulas for the cases when the initiated element matches or does not match one of the types of the elements in the initial system, an analytic solution for this iteration can be obtained using the diagram shown below.

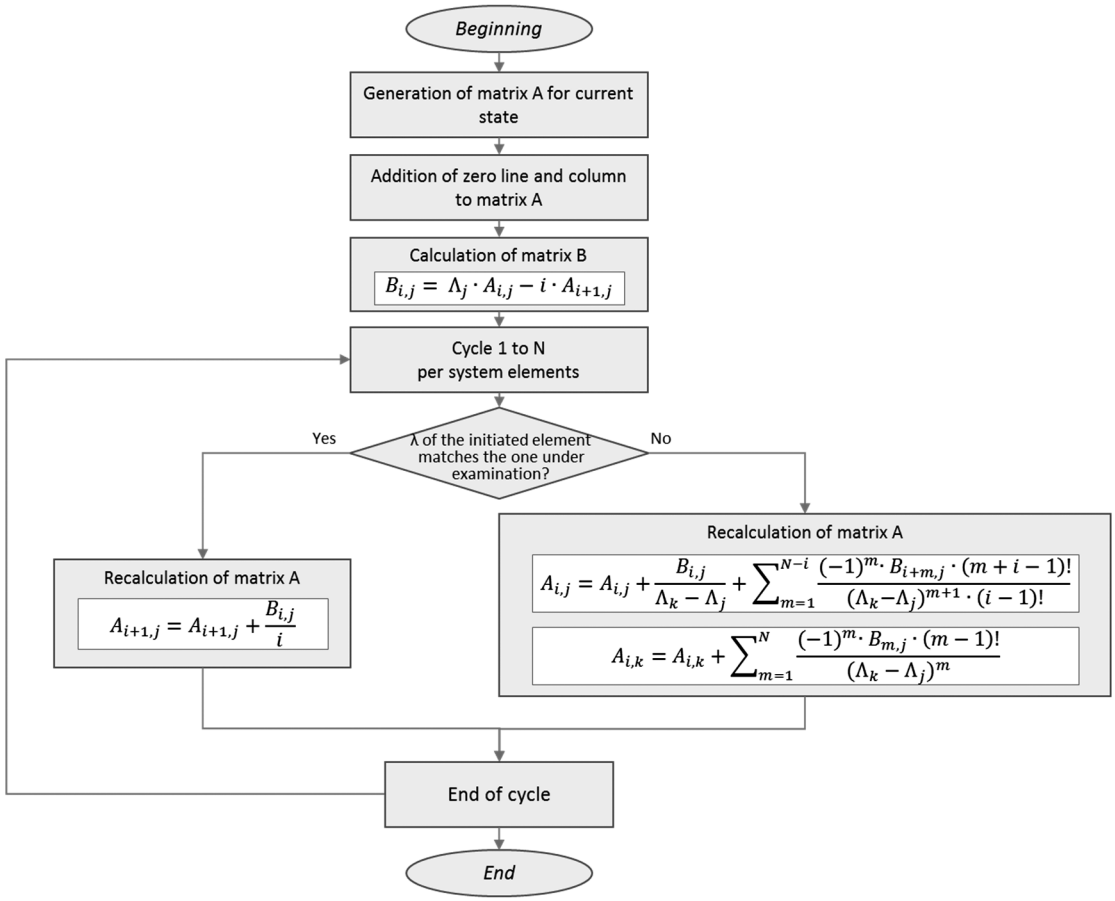


Figure 1. Diagram of analytic solution algorithm

i is the line index in the respective matrix;
j is the column index in the respective matrix;
k is the index of the initiated element of matrix Λ;
N is the number of elements in the initial system.

Conclusions

The paper develops and mathematically substantiates an algorithm that enables recurrent development of analytic expression for PNF calculation for a system of any number of elements in cold standby. The solution process consists in the recalculation of matrix coefficients using generalized formulas instead of numeric derivation and integration, which allows significantly reducing calculation time and increasing the accuracy of the results. In terms of data representation the algorithm is adapted for computer calculation.

References

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

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

3. Krivopalov DV. Osobennosti dinamicheskogo programmirovania v nadiozhnostnom proektirovanii programmnotekhnicheskikh sistem kosmicheskikh apparatov [Special aspects of dynamic programming in design for dependability of hardware and software systems of spacecraft]. In: Proceedings of the Fifth international science and technology conference Topical matters of space-based Earth remote sensing systems. Moscow (Russia); 2013 [in Russian].

4. Krivopalov DM, Yurkevich EV. Poluchenie funktsiy VBR v matrichnom vide dlia sistem s nenagruzhennym rezervirovaniem pri neodnotipnykh elementakh [Obtaining the PNF function in matrix form for cold standby systems under heterogeneous elements]. Dependability.

About the authors

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

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

Received on 29.08.2017

UDC 629.3.081.3
Original article
Dependability, vol. 17 no.4, 2017 DOI: 10.21683/1729-2646-2017-17-4-23-26

Interval estimation of reliability of one-off spacecraft

Anatoly Yu. Kolobov, *NPO Lavochkin, Khimki, Russia*
Evgeny V. Dikoun, *NPO Lavochkin, Khimki, Russia*

Anatoly Yu. Kolobov

Evgeny V. Dikoun

Abstract. Aim. *Many space technology products fall into the category of one-off (unique) or are manufactured in small batches of 3 to 5. In accordance with the regulatory documentation, the design and development activities in the space industry must involve quality assurance of products with interval estimation of dependability indicators. However, for one-off unique spacecraft that account for a fair share of the overall space industry product output, acquiring such estimates is associated with the problem of availability of original statistical data. That is due to the high cost of both the spacecraft itself and its testing, which does not allow testing large numbers of samples in the process of spacecraft development. In the context of restricted funding of the space industry, a practice has arisen that involves conduction each planned type of test on a single sample. The test samples have different configurations and versions of components (dimension and mass models, thermal analogues, etc.). In this case, it is impossible to acquire homogeneous statistical data in order to substantiate the compliance with the dependability requirements.* **Results**. *The article proposes a method of interval estimation of the probability of no-failure of a one-off spacecraft based on the results of flight tests using a priori information acquired at the stage of pre-delivery and acceptance testing. The authors compare the feasibility of using computational, experimental or computational and experimental methods of spacecraft dependability indicators evaluation. As initial data, electric and radio engineering and thermal vacuum tests results of spacecraft flight model are used. The fact that only the electric and radio engineering tests results are taken into consideration is due to the dependability of spacecraft being primarily defined by the dependability of the electronic equipment. The scope of tests (normally, about 50 for each spacecraft) allows obtaining highly reliable and informative estimates. This method can also be used at the stage of operation in order to evaluate and supervise dependability, e.g. after a year of operation. The correctness of aggregation of the a priori information and the information obtained at the said stage is verified with Fisher's Z-value.* **Conclusions**. *The proposed method allows estimating pointwise values of probability of no-failure of one-off spacecraft, lower confidence bounds and mean-square deviation of the probability of no-failure at the stages of pre-delivery and acceptance testing, flight testing and operation using a priori information. An example is given of interval estimation of probability of no-failure of one-off spacecraft based on the results of flight operations using a priori information obtained at the stages of pre-delivery and acceptance testing.*

Keywords: *one-off spacecraft, spacecraft, a priori information, interval estimation, probability of no-failure, lower confidence bound, flight tests.*

For citation: *Kolobov AYu, Dikoun EV. Interval estimation of reliability of one-off spacecraft. Dependability 2017;4: 23-26. DOI: 10.21683/1729-2646-2017-17-4-23-26*

Introduction

Regulatory documentation in the field of dependability requires implementation of interval estimation of dependability indicators (DI) of technical objects. For the most of engineering products acquiring of such estimates does not cause any difficulties, as it is always possible to collect required amount of statistical data, which allows obtaining correct estimation of DI.

However, many space technology products fall into the category of one-off (unique) or are manufactured in small batches of 3 to 5.

The high cost of both the spacecraft itself and its testing does not allow testing large numbers of samples in the process of spacecraft development. In the context of restricted funding of the space industry, a practice has arisen that involves conducting each planned type of test on a single sample. In this case, it is impossible to acquire homogeneous statistical data in order to substantiate the compliance with the dependability requirements [1,2].

It is proposed to implement Bayesian methods using a priori information when estimating dependability of one-off spacecraft.

Comparison of DI estimation methods

In accordance with regulatory documentation, when confirming the dependability, it is possible to use computational, computational and experimental or experimental methods. At the same time, every method has its own advantages and disadvantages.

The computational method is based on the usage of statistical data on failure rate of electronic components (ECs), assemblies, component parts of both specific models and their analogues.

The computational method has the following disadvantages [2]:

- lower level of detail of dependability structure diagram of radio-electronic devices with high failure rate of ECs (the number of failure rate of ECs in DI is as high as 120 000);
- use of summarized data on failure rate for component parts instead of specified sets of ECs;
- due to deterioration of data on failure rate of ECs, dependability assessments are underestimated, which complicates the confirmation of specified requirements for the product dependability;
- lack of reference data on dispersion of the failure rate of component elements doesn't allow obtaining interval estimation of DI dependability;
- estimation is carried out according to the project documentation. In this case there is no reference to the specific object of research.

The main problem of experimental methods (computational and experimental) is the problem with the set of presentative sample of initial data.

Due to the impossibility to obtain sufficient statistical homogeneous data due to financial restrictions, experimental methods are inapplicable for confirming of dependability requirements of one-off (unique) spacecraft.

Though computational and experimental methods have their own disadvantages, they do not have the disadvantages of individual computational and experimental methods.

Methodology of computational and experimental DI estimation taking into account a priori information

It is suggested to use the approach of step-by-step computational and experimental validation of probability of no-failure (PNF) of one-off (unique) spacecraft taking into account a priori information.

Figure 1 shows the algorithm of step-by-step estimation and control of dependability with a priori information of one-off spacecraft. When estimating PNF using this approach, estimates obtained at the previous step are used (i.e. estimation by integrated information are used in this case). The correctness of such data integration is estimated by Fisher's Z-criterion.

Estimations of dependability indicators obtained at the stages of pre-delivery (PT) and acceptance (AT) tests of spacecraft are used as a priori information for the flight tests (FT) stage. At the same time, information on the results of power and radio engineering tests (including tests in vacuum) of spacecraft at PT and AT stages is used as initial information for the estimation of PNF and its mean-square deviation.

The use of the results of power and radio engineering tests due to the fact that dependability of complex technical systems, operating under harsh conditions (such as spacecraft), is primarily determined by the dependability of electronic equipment. At the same time, the scope of tests (at the average, about 50 per one spacecraft) allows to obtain highly reliable and informative estimations.

Malfunctions which lead to the failure of spacecraft, are as follows:
- malfunctions that lead to the total loss of spacecraft efficiency;
- malfunctions that cause out-of-tolerance values of main operating parameters, specified in the technical requirements (TR).

In case several malfunctions are simultaneously identified as part of dependability estimation, they are considered a single failure. It is not allowed to consider one malfunction as repeated malfunctions of spacecraft caused by the same element.

Random faults of the software are considered self-repairing spacecraft operability disturbances and are not taken into account in the calculations.

The following failures are not taken into consideration:
- failures caused by another failure;
- failures caused by consumable materials running out of TR tolerances;
- failures caused by the violation of operating manual;
- failures caused by the influence of external factors not covered by the product TR;
- failures related to various experiments and caused by increased intensity of external influence in comparison with the requirements specified in TR;
- failures caused by the effect of ageing.

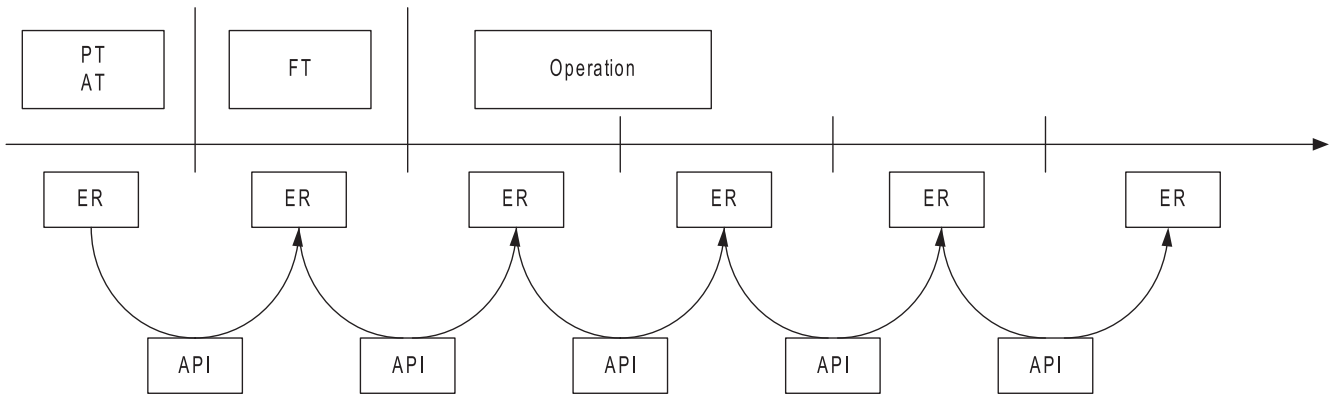


Figure 1. Algorithm of step-by-step estimation and supervision of dependability
PT – pre-delivery test; AT – acceptance test; FT – flight test; ER – estimation results; API – a priori information

Estimation of DI on the n test results at the PT and AT stages

The probability of no-failure (PNF) of spacecraft P_0 and its mean-square deviation (MSD) σ_{P0} based on n test results at the PT and AT stages is calculated by the following formula [3]:

$$\widehat{P}_0 = 1 - \frac{1}{2(n+2)};$$

$$\sigma_{P_0} = \frac{1}{2(n+2)}\sqrt{\frac{5n+7}{n+3}}.$$

If there are failures which were taken into account the estimation of dependability during tests ($m \neq 0$) is calculated using the following formula [4]:

$$\widehat{P}_0 = 1 - \frac{m}{n};$$

$$\sigma_{P_0} = \sqrt{\frac{\widehat{P}_0(1-\widehat{P}_0)}{n}}.$$

The lower confidence bound P_L for PNF at the specified confidence probability γ could be defined as:

$$\underline{P} = \widehat{P}_0 - t_p \cdot \sigma_p,$$

where t_p is Student's distribution for γ and n.

Estimation of probability of no-failure operation of spacecraft at the FT stage

Taking into account the preliminary information, obtained at the PT and AT stages, point value of PNF of spacecraft $\widehat{P}$ and its mean-square deviation σ_P are calculated according to the following formula:

$$\widehat{P} = \widehat{P}_0 + K_0 K_b \left| \widehat{P}_1 - \widehat{P}_0 \right|;$$

$$\sigma_P = \sqrt{(K_0 K_b)^2 \sigma_{P_1} + (1 - K_0 K_b)^2 \sigma_{P_0}^2};$$

$$K_0 = 1 - (\Phi(Z));$$

$$K_b = \frac{\sigma_{P_0}^2}{\sigma_{P_1}^2 + \sigma_{P_0}^2},$$

where $\widehat{P}$ and σ_P are the values of PNF of spacecraft and its MSD, determined by the FT results taking into account the preliminary information;

$\widehat{P}_1$ and σ_{P1} are the values of PNF and its MSD calculated in accordance with the FT results without taking into account the preliminary information;

$\widehat{P}_0$ and σ_{P0} are the values of PNF and its MSD calculated with preliminary information.

$\Phi(Z)$ is the table function of normal distribution [6];

Z is Fisher's Z-criterion.

$$Z = \frac{\left| \widehat{P}_1 - \widehat{P}_0 \right|}{\sqrt{\sigma_{P_1}^2 + \sigma_{P_0}^2}}.$$

Statistical homogeneity of the preliminary information and API results as well as the possibility to obtain the correct combined assessment of PNF are estimated in accordance with Fisher's Z-criterion. The condition $Z \leq 1.6$ is verified.

The lower confidence bound of DI with confidence probability γ is defined as

$$\underline{P} = \widehat{P} - t_P \sigma_P.$$

Estimations of dependability indicators obtained at PT and AT stages, i.e. $\widehat{P}_0$ and σ_{P_0} are used as preliminary information for the FT stage.

Estimation of PNF of spacecraft without taking into account of preliminary information

Estimation of DI is obtained in accordance with the following formulas

$$\widehat{P}_1 = \frac{n^* - m + 1}{n^* + 2};$$

$$\sigma_{P_1}^2 = \frac{n^{*2}\widehat{P}_1(1-\widehat{P}_1) + n^* + 1}{(n^*+3)(n^*+2)^2},$$

where n^* is the equivalent number of observed spacecrafts;

m is the number of failures which were taken into account during the observations.

$$n^* = \frac{24KN + \sum_{i=1}^{N} t_i (1-K)}{365\left[24K + t_{mp}(1-K)\right]},$$

where N is the number of days of spacecraft operation;

t_i is the duration of task performance of the spacecraft within i-th days;

t_{mp} is the specified average duration of task performance within 24 hours;

$$K = \frac{t_{mp}}{24 - t_{mp}}.$$

At the following DI control stages, the estimation of DI is carried out according to the scheme shown in Figure 1. At the same time, the estimation obtained at the previous stage is considered as a priori information.

Example. During power and radio engineering tests of the spacecraft at the PT and AT stages, 47 sessions were carried out. During 7 sessions, failures were identified.

The duration of FT was 180 days. Within 24 hours, the spacecraft operated for about 5 hours.

Task solving. For the PT and AT:

$$\widehat{P}_0 = 1 - \frac{7}{47} = 0,85,\ \sigma^2_{\widehat{P}_0} = \frac{0,85(1-0,85)}{47} = 0,0027.$$

where γ=0.9 $\underline{P} = 0,85 - 1,68 \cdot \sqrt{0,0027} = 0,76$

For the FT stage without taking into account a priori information:

$$K = \frac{5}{24-5} = 0,263,$$

$$n^* = \frac{180\left[24 \cdot 0.263 + 5(1 - 0?263)\right]}{365\left[24 \cdot 0.263 + 5(1 - 0?263)\right]} = 0,49.$$

For the FT stage with taking into account a priori information:

$$Z = \frac{|0,5984 - 0,85|}{\sqrt{0,0027 + 0,071}} = 0,92671,6,\ \Phi(Z)=0.822$$

K_0=1-0.822=0.178; $K_b = \frac{0,0027}{0,0027 + 0,071} 0,0366$

$$\widehat{P} = 0,85 + 0,178 \cdot 0,0366 \cdot 0,256 = 0,8516;$$

$$\sigma_P = \sqrt{\begin{matrix}(0,178 \cdot 0,0366)^2 \cdot 0,2664 + \\ +(1 - 0,178 \cdot 0,0366)^2 \cdot 0,0027\end{matrix}} = 0,0517.$$

where γ=0.9 and n=1 Student's distribution is t_{γ_n}=6,314

The lower bound of PNF of the spacecraft with confidence probability γ=0,9 according to the FT results is the following:

$$\underline{P} = 0,8516 - 6,314 \cdot 0,0517 = 0,5251.$$

References

1. Kolobov AYu, Dikoun EV. Obespechenie nadiozhnosti KA dlitelnogo funktsionirovania [Ensuring dependability of long-operation spacecraft]. In: proceedings of the International Conference and Russian Science School Systemic Problems of High Dependability, Mathematical Simulation and Innovation Technology of Vital Products (INNOVATIKA 2015). Part 1. Moscow (Russia); 2015. P. 16-18 [in Russian].

2. Kolobov AYu, Korchagin EN. Problemnye voprosy prognozirovania i podtverzhdenia nadiozhnosti KA dlitelnogo funktsionirovania [Problems related to predicting and confirming dependability of long-operation spacecraft]. In: Proceedings of the International Conference and Russian Science School INNOVATIKA 2014. Part 1. Moscow (Russia); 2015 [in Russian].

3. Dikoun EV, Kolobov AYu, Bodrov AV. Otsenka nadiozhnosti razgonnogo bloka "Fregat" [Dependability evaluation of the Fregat booster]. Mashinostroyenie: setevoy elektronny naouchny zhurnal 2016;4(3):73-77. ISSN 2310-0818. <http://indust-engineering.ru/issues/2016/2016-3-13.pdf> [in Russian].

4. Avduevsky VS et al. Technology dependability and efficiency: Reference book: In 10 volumes. Vol. 6. Moscow: Mashinostroenie; 1989 [in Russian].

5. Barbashov GV, Pham Duc Hung. Ouchiot apriornoy informatsii pri otsenke nadioznosti pirotekhnicheskikh sistem oupravlenia po vyborochnym ispytaniam [Accounting for a priori information in dependability evaluation of pyrotechnic control systems based on sampling tests]. Herald of the Saint Petersburg Institute of the Russian State Fire Service 2005;3(10):85-87 [in Russian].

6. Volkov LI, Shishkevich AM. Nadiozhnost letatelnykh apparatov [Aircraft dependability]. Moscow: Vysshaya Shkola; 1975 [in Russian].

7. Lukin VL, Sukhoruchenkov BI. Sposob kontrolia veroiatnosti bezotkaznoy raboty tekhnicheskikh system po rezultatam ispytaniy s ouchiotom vozmozhnykh defektov [Method of supervision of the probability of no-failure of technical systems based on the test results subject to possible defects]. Dvoynye teknologyy 2014;2.

About the author

Anatoly Yu. Kolobov, Candidate of Engineering, Associate Professor, Chief Specialist NPO Lavochkin, Khimki, Russia, e-mail: kolobov@laspace.ru.

Evgeny V. Dikoun, Deputy Head of Unit, NPO Lavochkin, Khimki, Russia, e-mail: dev@laspace.ru.

Received on 03.08.2017

Service Level Agreements and dependability

Viktor A. Netes, *Moscow Technical University of Communication and Informatics, Russia, Moscow*

Viktor A. Netes

Abstract. *The Service Level Agreement (SLA) is an efficient and proven tool for regulation of the relations between the supplier and the user of services that is designed to ensure their quality. Such agreements are well known and successfully used in the information and communication industry. They are also applicable in other areas. Essentially, SLA stipulates certain requirements for the service level of which the fulfilment is guaranteed by the provider. In case of SLA violation the service provider is usually financially liable. As a rule, in such cases the user is remunerated with a discount for services provided in the following accounting period. Dependability requirements are an important part of the SLA. The purpose of this paper is to familiarize a wide range of experts from various industries with the general matters of SLA application and the aspects related to the dependability requirements specification. The paper refers to the relevant documents of international standardization organizations (ITU, ISO/IEC, ETSI, TMForum) and the Russian standards. Recommendations are given for selecting the dependability indicators and standard values to be included in the SLA, as well as for defining the amounts of compensation payed by service providers to the customers in case of non-compliance with requirements for the availability factor. The availability factor is normally used in the SLA as the primary dependability indicator that defines the allowable total time of non-operability over the specified base period. Additionally, a client might be interested in restricting the duration of each individual downtime as well. For that purpose, the guaranteed recovery time can also be specified and exceeding this time would be deemed an SLA violation. The choice of the standard values for inclusion in the SLA is a search for a compromise between the intent to satisfy the user requirements and the wish to get ahead of the competition on the one hand and the requirement to ensure the feasibility of the assumed obligations and minimize the risk of SLA violation that involve financial and reputational losses on the other hand. Therefore, before proposing an SLA to a customer, a service provider must thoroughly analyze its actual ability to make sure that the probability of SLA requirements violation is sufficiently low. The computational or computational and experimental methods are suggested for its evaluation. The amount of compensation for a violation depends on its gravity, i.e. the achieved and the standard values of an indicator. In practice, this relation is usually expressed with a step (piecewise constant) function. A formula is proposed that expresses the theoretical relation between the relative amount of compensation for violation of the availability factor requirements and the severity of violation and the standard value of this indicator. It can be used in defining the technically substantiated reference for SLA conditions development and assessment, of which the value will be relevant to both the service providers and users.*

Keywords: *Service Level Agreement, standards, dependability indicators, availability, compensation.*

For citation*: Netes VA.Service Level Agreements and dependability. Dependability 2017;4: 27-30. DOI: 10.21683/1729-2646-2017-17-4-27-30*

The Service Level Agreement (SLA) is a tool to regulate the relations between the supplier and user of services that is designed to ensure their quality. Such agreements are well known and successfully used in the information and communication technologies (ICT) industry. Essentially, SLA stipulates certain requirements for the quality of service of which the fulfilment is guaranteed by the provider.Dependabilityrequirementsareusuallyamongstthem.

There are many publicationscovering the application of SLA in ICT (including several articles by the author [1-6]). However, such agreements are also applicable in other areas.In particular, [7]indicates the utility of their use in the housing and communal services, while[8]suggests the power supply services.Nevertheless, SLAs are generally little known outside the ICT industry.

The purpose of this paper is to familiarize a wide range of experts from various industries with the general matters of SLA application, relevant international and Russian regulatory documents, aspects related to the SLA dependability requirements specification. In particular, recommendations are given for selecting the dependability indicators and standard values to be included in the SLA, as well as for defining the amounts of compensation payed by service providers to the customers in case of non-compliance with the specified requirements.

The following documents of international industry organizations are devoted to the SLA application in telecom munications:International Telecommunications Union (ITU) Recommendations E.860 [9] and M.3342 [10],European Telecommunications Standards Institute (ETSI) Handbook EG 202009-3 [11], TM Forum (formerly TeleManagement Forum) HandbookGB917 [12]. A Russian standard was developed[13] based on these documents and the considerations outlined in [2].

In the informationtechnology (IT) industry the so-called InformationTechnologyInfrastructureLibrary(ITIL) became ratherwidespread. It was created in the second half of the 1980s by the order of the Great Britain Government and describes the best practical ways of organizing the work of companies or business units providing IT services.The process approach used in it complies with the ISO 9000 series standards.The seven volumes of the library describe the entire set of processes required to ensure the quality of IT services and the satisfaction of their users. The SLA application is amongst them.

Based on the ITIL, the British standard BSI 15000 was developed and was later adopted as an international standard ISO/IEC 20000 withalmost no changes.This standard consists of several parts, for the first two of which there are identical Russian standards [14, 15] ([15] is the translation of the ISO/IEC version of 2005, replaced with a new one in 2012).

Unfortunately, there are a number of terminological remarks to the standards [14, 15]. Firstly, they are not fully consistent, which is evident even in their names: the term "service management" is translated to Russian differently in [14] and [15]. Secondly, the translation of "SLA" in them is less logical and does not correspond with the term previously agreed in the telecommunications industryand stipulated in the standard [13].It is also worth mentioning that there is a third "SLA" translation in some publications.Another terminological flaw [14, 15] will be considered below.

As mentionedabove, SLA typically includes dependability requirements.Here one should pay attention to a certain inconsistency: SLAs are dedicated to services, but in the Russian [16] and international [17] standards dependability is defined as a property of a technical object.The idea that undertoday's conditions the concept of "dependability" should be extended to services has already been suggested (see, for example, [18]).The dependability of services is actually mentioned in the ISO/IEC 20000 standard and in several ITU Recommendations, the dependability indicators of gas transportation services are officially set forth in Russia [19].

However, within the framework of existing standards, we have to deal with a specific object, when considering dependability. The solution to this problem proposed in [20] is as follows. For each service, the so-called service frame is defined, that is a set of technologies involved in the service rendering. This service frame is the object, the dependability of which should be considered. Note that this method is not a pure formality, since it is still necessary to define the service frame, in particular, to calculate dependability at the design stage.

The main dependabilityindicatorused in the SLA is the availability factor(K_a). It can be viewed as the fraction of the availability time during the baseperiod. Let ussuppose that the standard value $K_{as} = 0.995$, and the baseperiod is one month (30 days).Then the allowable downtime (time of nonoperability) per month is $30 \cdot 24 \cdot (1 - 0.995)$ h = 3.6 h. Thus, if the total downtime per month does not exceed 3.6 hours, the SLA requirement for the availability factor is considered to be met, if it exceeds this value, there is a violation of the SLA.

Pre-planned periods ofmaintenance, measurement, switching, software updates,etc.are usually excluded from consideration. This corresponds to the definition of the availability factor [16].A note specifies that planned periods when the object is not used as intended can be excluded from consideration.This fact should be taken into account when drawing up the SLA wherethe frequency and duration of such planned interruptions in work should be stipulated.

Speaking of the availability factor, there is one more terminological inconsistency.In many publications in Russian, the term "availability" is translated in a way that is appropriate in a common parlance but does not correspond to the fixed term in the dependability theory. In addition, in telecommunications there is the term "accessibility", which is translated into Russian in the same way. The existence of two different concepts of the same term leads to confusion. This terminological misunderstanding was considered in detail in [21].

Unfortunately, that inexact translation is used in standards [14, 15]. One can also reproach the developers of the ISO/IEC 20000 standard, where instead of coming up with their

own definition of "availability" they should have used the definition from the international terminological standard with reference to it (at the time of development of ISO/IEC 20000 such standard was IEC 60050-191:1990, the precursor of [17])as prescribed by the standardization rules.

Besides the total downtime that characterizes the availability, a client might also be interested in restricting the duration of each individual downtime as well. For that purpose, the guaranteed recovery time can be specified and exceeding this time would also be deemed an SLA violation. Sometimes average recovery time is suggested for restricting the duration of downtime, however this indicator has a serious drawback that many meancharacteristics share:a long downtime can be compensated by a large number of short ones.Moreover, the normalization of the average recovery time can provoke a service provider into arranging several short breaks in order to compensate for the long downtime that has already occurred.It was mentioned in [22] that using the average recovery time as the standardized dependability indicatoris unadvisable.

An approximate algorithm of choosing the standard values for inclusion in the SLA was given in [2]. The solution to this problem is a search for a compromise between two conflicting aspirations. On the one hand, the intent to satisfy the user requirements and the wish to get ahead of the competition makes service providers set the standards high, but on the other hand there is the requirement to ensure the feasibility of the assumed obligations and minimize the risk of SLA violation that involve financial and reputational losses.

Therefore, before proposing an SLA to a customer, a service provider must thoroughly analyze its actual capabilities. It is also important to be able to evaluate the probability or rate of each SLA requirement violation in order to make sure that it is sufficiently low. If these characteristics prove to be unacceptable, then one has to lower the requirements or take measures to increase dependability. Since failures are rare in a well-functioning system, a direct experimental evaluation of the violations probability may take too long. Therefore, in such case it is reasonable to use the computational or computational and experimental evaluation methods for which the relations proposed in [3] can be used.

In case of SLA violation, the service provider is usually financially liable. As a rule, in cases of violation the user is remunerated with a discount for services provided in the following accounting period. The amount of compensation depends on the violation severity, i.e. how much the actual value of the indicator differs from the standard one. In practice, this relation between the amount of compensation and severity of violation is usually expressed with a step (piecewise constant) function. The following example is given in [9]: if the difference between the standard and the actual value of the availability factor expressed as a percentage is less than 2%, then the discount will be 15% of the rate, if this difference is 2 to 4%, the discount will be 30%, if the difference is more than 4%, the discount will be as high as 50%.

In practice,the amounts of compensation stipulated in SLAs vary significantly depending on the service provider (specific examples for communication services are given in [2]). To a large extent, they are determined by marketing policy and market conditions. Nevertheless, it is useful to be able to define the technically substantiated amounts of compensation that could be used as reference for SLA conditions development and assessment. This information can be relevant to both the service providers and users. In [4], a formula that expresses the relation between the amount of compensation for violation of the availability factor requirements and the severity of violation and the standard value of this indicator was proposed. It can be written as:

$$p = [1 - \log (1 - K_a)/\log (1 - K_{as})]\cdot 100\%,$$

where$p$is therelative amount of discount expressed as a percentage, $K_a$andK_{as}arethe actual and the standard values of the availability factor ($0 < K_a \le K_{as} < 1$), logarithm can be of any base. For example, if $K_{as} = 0.99$ and $K_a = 0.98$ than $p = 15\%$.

The main conclusions of this article are:

SLA is an efficient and proven tool for regulating the relations between the providers and users of services that is designed to ensure their quality. The application procedure for it has been established in a number of international and Russian standards.

Essentially, SLA stipulates certain requirements for the service level of which the fulfilment is guaranteed by the provider. In case of SLA violation the service provider is financially liable.

Dependability requirements are an important part of the SLA. The availability factor is normally used as the primary dependability indicator that defines the allowable total time of nonoperability over the specified base period. Additionally, the guaranteed recovery time can be specified.

The proposed formula expresses the theoretical relation between the relative amount of compensation for violation of the availability factor requirements and the severity of violation and the standard value of this indicator. It can be used in defining the technically substantiated reference for SLA conditions development and assessment.

References

1. Netes VA. Soglashenieobourovneobsluzhivaniaprirendetsifrovykhkanalov [Service Level Agreements under digital channel leasing]. Seti i sistemysviazi 2000;11:86–91 [in Russian].

2. Netes VA. Soglashenieobourovneobsluzhivania: standarty i realii [Service Level Agreements: standards and reality]. Vestniksviazi 2003;8:72–79 [in Russian].

3. Netes VA. Zadanietrebovaniyponadiozhnosti v soglasheniyakhobourovneobsluzhivania [Specification of dependability requirements in service level agreements]. Elektosviaz 2004;4:37–39 [in Russian].

4. Netes VA. Razmeryshtrafovzanarushenietrebovaniy k gotovnosti v SLA [Amounts of penalties for violation of

SLA availability requirements]. Elektrosviaz 2008;3:37–40 [in Russian].

5. Netes VA. SLA dlia VPN [SLA for VPN]. Vestniksviazi 2011;4:26–29 [in Russian].

6. Netes VA. Chtonuzhnodliaouspeshnogoprimenenia SLA [What is required for successful SLA application]. T-Comm–Telekommunikatsiii transport 2015;7:16–20 [in Russian].

7. ZelentsovLB, ZhernevskyKV, RylkovVI. Oupravleniepredostavleniem i podderzhkoyservisov v ZhKKh [Control of housing and public utilities services provision and support]. Ekonomicheskienaouki2010;1:329–333 [in Russian].

8. Krupsky AV. Kompleksny marketing energosbytovoykompaniinaosnovesoglasovannogoourovniapredostavleniaouslug i analizaklientskoyrentabelenosti [Comprehensive marketing of a power supply company based on an agreed service level and analysis of client profitability]. Fundamentalnieissledovania 2013;8-2:424–428 [in Russian].

9. ITU-T Recommendation E.860 (06/2002). Framework of a service level agreement.

10. ITU-T Recommendation M.3342 (07/2006). Guidelines for the definition of SLA representation templates.

11. EG 202009-3. User Group; Quality of telecom services; Part 3: Template for Service Level Agreements (SLA). 2007.

12. TM Forum GB917. SLA Management Handbook. Rel. 3.1, v. 1.2. 2012.

13. GOST R 55389–2012. System of national standards for quality of telecommunication services. Service Level Agreement (SLA).

14. GOST R ISO/IEC 20000-1-2013. Information Technology. Service management. Part 1. Service management system requirements.

15. GOST R ISO/IEC 20000-2-2010. Information Technology. Service management. Part 2. Code of practice.

16. GOST 27.002-2015. Industrial product dependability. Terms and definitions.

17. IEC 60050-192:2015. International electrotechnical vocabulary – Part 192: Dependability.

18. Shubinsky IB. A word from the Editor-in-Chief. Dependability 2015;1:3–4 [in Russian].

19. Rules of identification of dependability and service quality indicators of gas transportation in natural gas networks. Approved by decree of the Government of the RF no. 1074 dated 18.10.2014.

20. Netes VA. Virtualizatsia, oblachnyeouslugi i nadiozhnost [Virtualization, cloud services and dependability]. Vestniksviazi 2016;8:7–9 [in Russian].

21. Netes VA. Gotovnost i dostupnost–pochuvstvouyteraznitsu [Availability and accessibility: feel the difference]. Vestniksviazi 2005;8:22–26 [in Russian].

22. Dzirkal EV. Zadanie i proverkatrebovaniy k nadiozhnostislozhnykhizdeliy [Specification and verification of dependability requirements of complex products]. Moscow: Radio i sviaz; 1981 [in Russian].

About the author

Viktor A. Netes, Doctor of Engineering, Professor, Moscow Technical University of Communication and Informatics, Russia, Moscow, e-mail: vicnet@yandex.ru

Received on 09.06.2017

Research of the operational dependability of the *Lada Kalina* vehicle systems affecting traffic safety

Ilia V. Denisov, *AG and NG Stoletov Vladimir State University, Vladimir, Russia*
Alexey A. Smirnov, *AG and NG Stoletov Vladimir State University, Vladimir, Russia*


Ilia V. Denisov


Alexey A. Smirnov

Abstract. *The growing number of cars in the Russian Federation means that a large number of vehicles with different performance indicators get involved in the transportation process. One of those indicators is dependability that is a key characteristic of quality. A vehicle's operation is the primary test of its dependability, of which the indicators depend on the used design solutions and the manufacturing process. Defects occurring at various stages of vehicle manufacture significantly affect the dependability indicators. It must be noted that a vehicle is a source of increased hazard. A failure of a vehicle in operation due to a manufacturing defect or non-observance of operation conditions may cause an accident. Therefore it is extremely important to have at one's disposal information on the implemented systems reliability indicators that affect active safety. In this context, the research of automotive vehicles dependability in operation is a relevant scientific task, solving which will enable managing the technical condition of vehicles and ensure traffic safety.* **The aim** *of this research was to evaluate the operational dependability of the systems that directly affect the road safety of Lada Kalina with subsequent use of the obtained information in the development of automated systems for management of automotive vehicle technical condition in operation.* **The methods** *of research are based on the theoretical foundations of vehicle maintenance, the probability theory and mathematical statistics, experimental design theory. Standard methods of processing of statistical information on the operational dependability of vehicles were used. The data was obtained from official OAO AvtoVAZ dealerships in the Vladimir Oblast. As the result of research of the operational dependability of the systems that directly affect the road safety of Lada Kalina a list of defective components in the steering, braking, chassis, lighting and signalling systems was identified. Times to failure of parts, units and assemblies that limit the vehicle dependability, as well as the primary numerical characteristics of random distribution were determined. The defects identified at early stages of operation indicate design and manufacturing flaws of Lada Kalina.*
Conclusions: *In this paper the authors present the findings regarding the defects of the Lada Kalina systems that directly affect traffic safety. This information was obtained by means of analyzing vehicle failures within the warranty period that were recorded based on the owners' applications to the OAO AvtoVAZ dealerships an maintenance facilities in the Vladimir Oblast. Maintenance facilities, when performing diagnostic operations as part of routine maintenance, should take into consideration the list of the least dependable vehicle components given in this paper and directly affecting the traffic safety.*
The manufacturing factory should take note of the indicated defects and develop a plan of their elimination, as well as timely inform the consumers of the identified warranty-specific defects and recall the products.

Keywords: *automobile, Lada Kalina, VAZ-1118, dependability, steering, braking system, chassis, lighting system, defects, warranty period.*

For citation: *Denisov IV, Smirnov AA. Research of the operational dependability of the Lada Kalina vehicle systems affecting traffic safety. Dependability 2017;4: 31-35. DOI: 10.21683/1729-2646-2017-17-4-31-35*

Introduction

A review of current scientific publications [1] shows that today malfunctions of automotive vehicles account for 20 to 25 % of the total number of traffic accidents (TA). Failures of the braking and steering systems, chassis, lighting and signalling devices of vehicles reduce their dependability and cause high risk of situations that enable TAs.

In operation, it is extremely important to have at one's disposal information on the dependability of the components of the above systems as that enables the management of their technical condition. The country's leading colleges and automotive industry's research institutions in close cooperation with the manufacturers, operators and maintenance enterprises that collect and analyze initial information on failures of vehicle units and assemblies are now developing a system for managing the technical availability of transport vehicles.

As part of the automated system for vehicle technical condition management in operation under development [2, 3, 4] the task of this research was to evaluate the operational dependability of the systems that directly affect the road safety of *Lada Kalina*. The research involved official OAO AvtoVAZ dealers in the Vladimir Oblast. This paper presents the findings regarding the assigned task.

Findings regarding the operational dependability of *Lada Kalina*. The diagram in Figure 1 that illustrates mass defects of the steering system shows that non-acceptable steering rack displacements due to increased gear clearance account for the bulk of failures. Their elimination within the warranty period is predominantly performed by means of adjustment of gear transmission clearance or replacement of the whole mechanism. Cardan shaft knocking is caused by gaps in nail bearings of the U-joints.

Electromechanical power steering (EPS) defects account for one seventh of all of the system's defects. The unit is mechatronic and has a complicated design, therefore diagnosing its technical condition is especially labor-intensive and requires special methods and facilities [5]. In operation, defective EPS functioned incorrectly, i.e. allowed unintentional rotation of the steering wheel with the vehicle's deviation from the straight-line trajectory, as well as reduction of the maximum compensating torque.

The defect of the swivelling mechanism connector that ensures electrical connection between the airbag and the sound signal switch with the dashboard wiring harness is caused by broken spiral cable. In this case a reduced passive vehicle safety due to airbag failure can be observed.

Other steering failures in *Lada Kalina* are due to defects of the steering mechanism and its parts: increased gear transmission clearance and loss of case integrity.

Table 1. Mass defects of the steering system of Lada Kalina

Item	Name of defect	Number	$\overline{X}$, ths km	ν	σ
1	Steering rack displacement too high relative to case	40	17,5	0,68	11,9
2	Cardan shaft knocking	38	18,7	0,68	12,8
3	Electromechanical power steering disabled	26	21,2	0,64	13,5
4	Swivelling mechanism connector defect	21	16,6	0,77	12,7
5	Left steering knuckle out of size	19	18,6	0,58	10,8
6	Rack-to-lock gap out of size	12	15,0	0,94	14,2
7	Rupture of steering rack case	12	22,9	0,61	14,1
8	Steering column cover defect	11	6,9	0,82	5,7

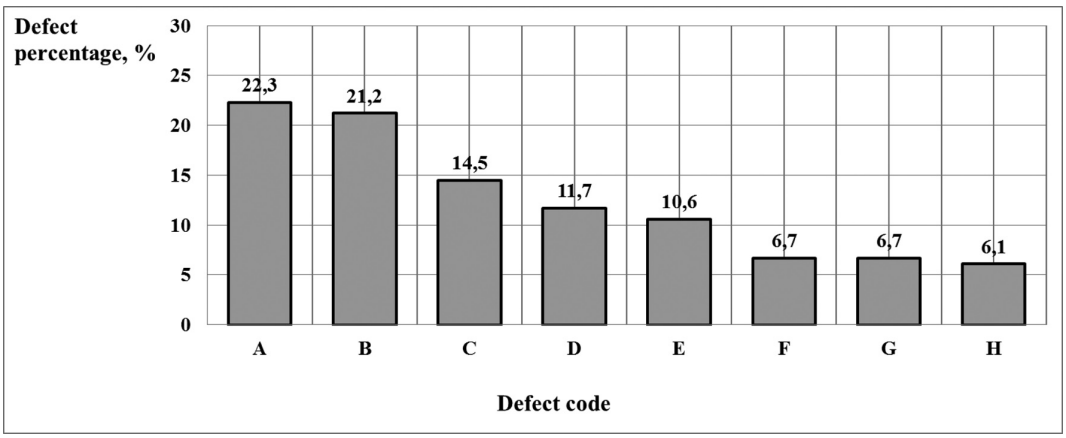


Figure 1. Defects of the steering system of Lada Kalina:
A: Steering rack displacement too high relative to case; B: Cardan shaft knocking; C: Electromechanical power steering disabled; D: Swivelling mechanism connector defect; E: Left steering knuckle out of size; F: Rack-to-lock gap out of size; G: Rupture of steering rack case; H: Steering column cover defect

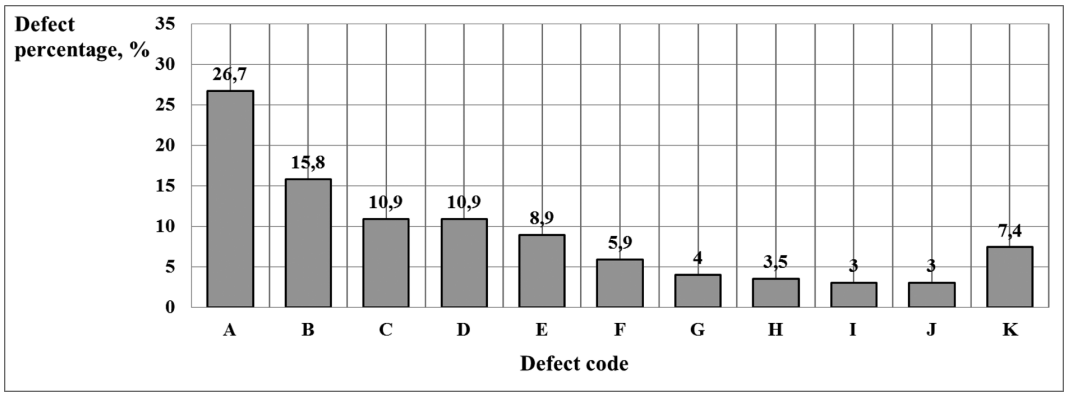


Figure 2. Defects of the braking system of Lada Kalina:
A: Loss of wheel cylinder integrity; B: Loss of main braking cylinder integrity; C: Loss of vacuum booster integrity; D: Main braking cylinder bleed off; E: Brake drum vibration/ovality; F: Vacuum booster wedging; G: Braking pressure regulator valve not adjusted; H: Right calliper leak; I: Rupture of cooling hose; J: Left calliper leak; K: Other defects

Table 2. Mass defects of the braking system of Lada Kalina:

Item	Name of defect	Number	$\overline{X}$, ths km	ν	σ
1	Loss of wheel cylinder integrity	54	25,6	0,54	13,8
2	Loss of main braking cylinder integrity	32	22,5	0,51	11,4
3	Loss of vacuum booster integrity	22	16,8	0,74	12,3
4	Main braking cylinder bleed off	22	15,5	0,65	10,1
5	Brake drum vibration/ovality	18	19,9	0,39	7,8
6	Vacuum booster wedging	12	6,2	1,37	8,5
7	Braking pressure regulator valve not adjusted	8	0,68	1,02	0,7
8	Right calliper leak	7	29,4	0,4	11,7
9	Rupture of cooling hose	6	5,0	1,16	5,8
10	Left calliper leak	6	28,9	0,57	16,3
11	Other defects	15	-	-	-

Figure 2 shows the percentage of vehicle braking system defects.

The figure shows that due to reduced performance of rubber components (sleeves and seals) the loss of wheel cylinder integrity accounts for a quarter of all failures. Braking fluid leaks and its bleeding off between brake circuits can also be observed in the main braking cylinder and front disk brake calliper. Thus, the defects of the main and wheel brake cylinders form over a half of all system failures.

Air intake into the vacuum booster cylinder and the wedging of its rod cause malfunction in sixteen out of a hundred vehicles with a failed braking system. Pressure regulator valve malfunctions were observed in only four percent of vehicles with the system's failures.

Among the «Other» malfunctions we should emphasize the defect of calliper seal, broken front brake block spring, failure of brake fluid level switch, as well as scuffing of rear brake friction pad.

Table 2 shows that times to failure of most brake control components correlate to the service interval as per the vehicle's log book, except for the main and wheel brake cylinders and brake hoses. In operation, those components must be checked as part of routine maintenance at service stations. It should be noted that of a special hazard to the vehicle owner and passengers are the brake hoses with the time to failure of just 5000 km and coefficient of variation of 1.16.

A special attention should be given to the braking pressure regulator valve installed in basic configurations of *Lada Kalina*. The average time to failure is about 700 km, which is unacceptably low. Premature blocking of lockup of rear axle brakes during braking caused by incorrect valve operation may cause skidding of the back wheels and loss of vehicle stability.

Figure 3 shows the distribution of chassis failures of the vehicle under investigation.

Defects of front suspension ball joint and destruction of rear brace joint that manifest themselves with knocking and clicking during vehicle acceleration are the most common in operation and require the replacement of components in order to eliminate the above defect symptoms.

Increased clearances in the supporting bearers of the right and left rotary racks cause knocking when passing bumps in the road, as well as distinctive creaking when the steering

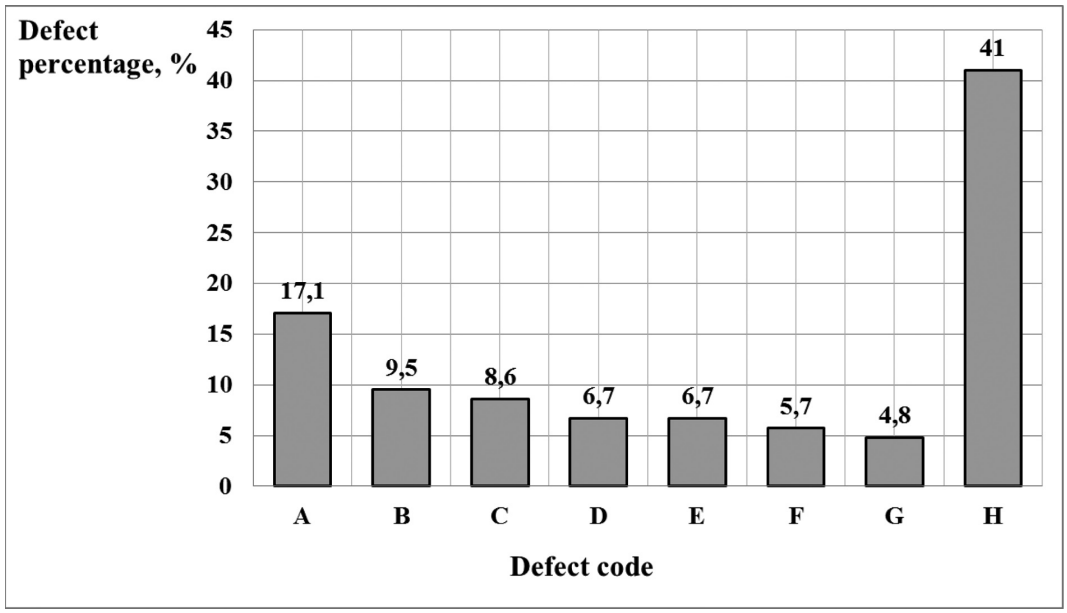


Figure 3. Defects of the chassis of Lada Kalina
A: Knocking/clicking in the front suspension during rotation; B: Knocking of the top mount of right front wheel support; C: Knocking of the top mount of left front wheel support; D: Rear wheel hub wobble; E: Destruction of rear brace joint of front suspension; F: Falling of rear suspension arm pad; G: Rear wheel hub bearing noise; H: Other defects

Table 3. Mass defects of the chassis of Lada Kalina

Item	Name of defect	Number	$\overline{X}$, ths km	ν	σ
1	Knocking/clicking in the front suspension during rotation	18	20,5	0,66	13,5
2	Knocking of the top mount of right front wheel support	10	22,9	0,67	15,4
3	Knocking of the top mount of left front wheel support	9	22,4	0,54	12,1
4	Rear wheel hub wobble	7	16,7	0,59	9,9
5	Destruction of rear brace joint of front suspension	7	22,9	0,51	11,7
6	Falling of rear suspension arm pad	6	20,5	0,66	13,6
7	Rear wheel hub bearing noise	5	14,4	0,7	0,69
8	Other defects	43	-	-	-

wheel is turned. The defect is due to the loss of component integrity that entails sand collection and excessive tear and wear of the ball and destruction of the retainer. Increased noise during rear wheels rotation and their wobble are due to gaps in the hub bearings that are eliminated by means of adjustment or replacement.

Table 3 shows mean times to failure of defective vehicle chassis components.

Figure 4 shows the percentage distribution of lighting and signalling devices of *Lada Kalina*: Mass defects of lighting devices associated with the loss of integrity of headlamp units, tail lights and fog lights manifest themselves in the form of misting of their glasses in operation caused by ingress of moisture and are due to distortional stress at the mounting spots on the vehicle body.

Failures of auxiliary stop signals are caused by failures of one or more semiconductor elements. Table 4 shows information on the operational dependability of a vehicle's lighting components.

Conclusion. The findings regarding the dependability of *Lada Kalina* safety system elements within the warranty period are an important part of the vehicle's technical condition management system. The defects identified at early stages of operation indicate design and manufacturing flaws.

Maintenance facilities, when performing diagnostic operations as part of routine maintenance, should take into consideration the list of the least dependable vehicle components given in this paper and directly affecting the traffic safety.

The manufacturing factory should take note of the indicated defects and develop a plan of their elimination, as well as timely inform the consumers of the identified warranty-specific defects and recall the products.

References

Denisov IlB, Smirnov AA. Issledovanie vliyaniya tekhnicheskogo sostoyaniya avtotransportnykh sredstv na dorozhno-transportnouyou avariynost v Rossiyskoy Feder-

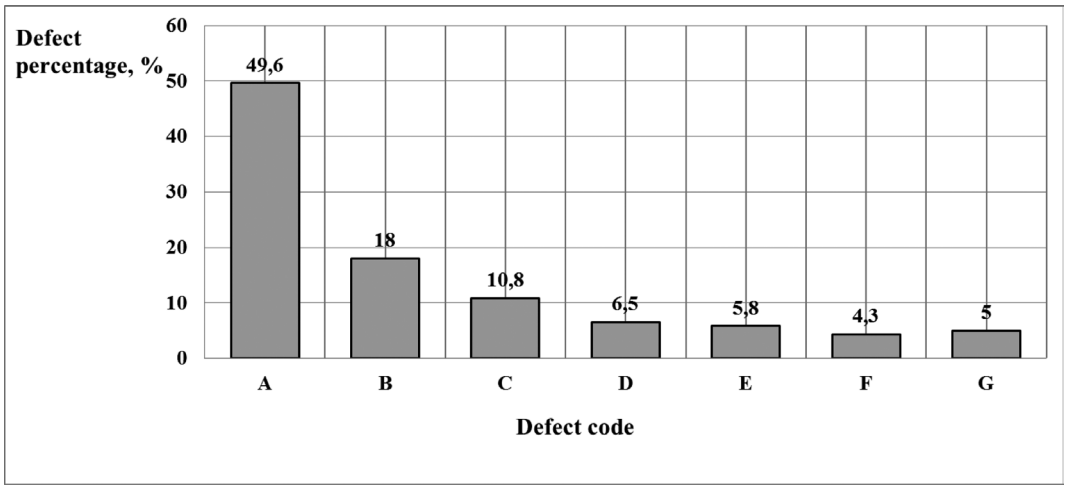


Figure 4. Defects of the lighting system of Lada Kalina:
A: Loss of integrity of left headlamp unit; B: Loss of integrity of right headlamp unit; C: Defect of right tail light; D: Defect left tail light; E: Loss of integrity of fog light; F: Defect of auxiliary stop signal; G: Other defects

Table 4. Mass defects of the lighting system of *Lada Kalina*:

Item	Name of defect	Number	$\overline{X}$, ths km	ν	σ
1	Loss of integrity of left headlamp unit	69	10,8	0,73	7,9
2	Loss of integrity of right headlamp unit	25	13,9	0,85	11,8
3	Defect of right tail light	15	19,7	0,51	10,1
4	Defect of left tail light	9	18,3	0,82	15,0
5	Loss of integrity of fog light	8	15,3	0,97	14,8
6	Defect of auxiliary stop signal	6	19,7	0,94	18,6
7	Other defects	7	-	-	-

atsii [Research of the effect of the condition of automotive vehicles on the rate of traffic accidents in the Russian Federation]. In: Zakharov DA, editor. Proceedings of the VIII Russian national research and practice conference Organization and Safety of Road Traffic. Tyumen (Russia): TyumGNGU; 2015. p. 71-77 [in Russian]. ISBN 978-5-9961-1027-8.

Bazhenov YuV, Denisov IlB, Denisov IvV. Veroyatnostnaya model predotkaznogo sostoyaniya avtomobilia [The probabilistic model of an automobile's prefailure state]. Biulleten transportnoy informatsii 2010;9(183):35-38 [in Russian].

Denisov IlV, Denisov IvV. Innovatsionnyi podkhod k obespecheniyou bezopasnoy ekspluatatsii avtotransportnykh sredstv [An innovative method of ensuring safe operation of automotive vehicles. In: Anisimov IA, editor. Proceedings of the international research and practice conference Matters of Transportation Systems Operation. Tyumen (Russia): TyumGNGU; 2010. p. 85-88 [in Russian]. ISBN 978-5-9961-0277-8.

Denisov IlV. Naouchnie predposylki avtomatizatsii tekhnologicheskikh protsessov oupravlenia rabotosposobnostiu avtotransportnykh sredstv v ekspluatatsii [Scientific premises of automation of operability management processes of automotive vehicles in operation]. In: Proceedings of the XVI International research and practice conference Topical Matters of Automotive Vehicles Operation. Vladimir (Russia): Vladimir State University Publishing; 2014 [in Russian]. ISBN 978-5-9984-0549-5.

Denisov IlV, Smirnov AA. Metodika diagnostirovania elektromekhanicheskogo ousilitelia roulevogo oupravlenia bezredouktornogo tipa [Method of diagnosing direct action electromechanical power steering]. Elektronika i elektrooboroudovanie transporta 2016;5:22-25 [in Russia].

About the authors

Ilia V. Denisov, Candidate of Engineering, AG and NG Stoletov Vladimir State University, Senior Lecturer in Automotive Transportation, Vladimir, Russia, e-mail: denisoviv@mail.ru

Alexey A. Smirnov, AG and NG Stoletov Vladimir State University, second year master degree student, Vladimir, Russia, e-mail: AlexiFoX@yandex.ru

Received on 19.12.2016

Models of malicious software and fault tolerance of information communication networks

Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*
Sergey V. Kupin, *4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia*
Dmitry S. Kupin, *Bauman MSTU, Moscow, Russia*


Sergey M. Klimov


Sergey V. Kupin


Dmitry S. Kupin

Abstract. *The aim of this paper is to develop a model that would enable a standardized representation of malicious software's structure, functions and to get a quantitative estimation of the fault tolerance of information and telecommunication networks affected by malicious software. The paper shows the relevance and importance of the malicious software models and evaluation of the fault tolerance of information and telecommunication networks affected by malicious software. Malicious software refers to software systems able to covertly deploy, establish unauthorized virtual data communication channel, self-propagate, self-modify, conduct unauthorized collection of information on the network and information technology interference against it. The structural and functional model of malicious software developed in this paper is composed of the following set of diagrams and function descriptions: structures of covert deployment and malicious software installation using electronic mail, structural and functional diagram of the main module of malicious software and covert deployment modules, structural and functional diagram of malicious software while implementing malicious functions, malicious software certificate. The diagrams detail the standard functions, operating procedures and information interaction of malicious software modules of the external and internal networks via an unauthorized virtual data communication channel. Primary malicious software modules are considered through the example of the Careto targeted computer attack. The model of fault tolerance of information and telecommunication networks affected by malicious software is described by indicators that characterize the ability of the networks and information security facilities to maintain and recover specified probabilistic and temporal characteristics over the period of malicious software activity. The following indicators are considered: probability that information and telecommunication networks and information security facilities maintain the specified probabilistic and temporal characteristics over the period of malicious software activity, probability that information and telecommunication networks and information security facilities recover the probabilistic and temporal characteristics after the effects of malicious software activity, factor of operation availability of information and telecommunication networks to perform the specified probabilistic and temporal characteristics under malicious software activity at an arbitrary moment in time, mathematical expectation of the duration of malicious software activity, mathematical expectation of the recovery time of the probabilistic and temporal characteristics of information and telecommunication networks and information security facilities. It is assumed that the values of the parameters required for the calculation of the indicators of the fault tolerance model of information and telecommunication networks were obtained as the result of a testbed simulation of the networks affected by malicious software. In the conclusion it is noted that the developed models enable the identification of the general structure of covert deployment and installation of attacking malicious software using electronic mail, structural and functional diagram of the main module of malicious software and covert deployment modules, structural and functional diagram of malicious software while implementing malicious functions, malicious software certificate, as well as evaluate the fault-tolerance of information and telecommunication networks and information security facilities affected by malicious software, quantify the probabilistic and temporal fault tolerance, recoverability and availability characteristics of networks.*

Keywords: *malware, information and telecommunication networks, information security facilities, fault tolerance.*

For citation: Klimov SM, Kupin SV, Kupin DS. Models of malicious software and fault tolerance of information communication networks. Dependability 2017;4: 36-43. DOI: 10.21683/1729-2640-2017-17-4-36-43

Introduction

Today, the highest threat comes from targeted computer attacks organized by intruders using covertly deployable and self-propagating malicious software (malware, MW). Such software is not always quickly detectable by state-of-the-art information security facilities (ISF) such as antivirus protection, computer attack detection, prevention and recovery systems. Usually, intruders exploit zero-day vulnerabilities in many programs of operating systems (OS), network services and protocols for covert deployment of MW elements into information and telecommunications networks (ITCN).

MW shall refer to a software system for covert deployment, establishment of unauthorized virtual data communication channels, self-propagation, self-modification and implementation of massive targeted information technology interference (computer attack) against ITCN for the purpose of disrupting information security and operational stability.

MW systems have difficult to analyze software implementation, their development and execution involves considerable information resources, they use algorithms for compression, encryption and masking of destructive actions. Today's massive targeted computer attacks, such as WannaCry in 2017, that involve MW affect hundreds of thousands of computers worldwide and disrupt the operational stability of ITCN of the banking, energy, healthcare, communication, transportation and other critical industries [1-2].

This paper proposes a structural and functional model of MW that was developed involving the analysis of the Careto targeted computer attack's source code set forth in the Kaspersky Laboratory analytical findings. Additionally, the paper interprets a standard structural model and functions of a wide range of MW.

Careto facilities enabled the intruder to attack 380 unique objects in 31 countries. Using Careto the intruders stall information on computer facilities, private encryption keys, VPN settings, SSH settings, RDP files, as well as files of various data formats. Typically, MW deployment is performed via the Internet, suitable ITCN communication equipment and unauthorized connection of external data storage device [3].

The Careto MW system is installed in the network with the installation module and provides the intruder with remote access to the ITCN without the user's knowledge, performs a set of commands received from the remote control server in order to collect information on the network, vulnerable services and stored data. In case of successful ITCN penetration the Careto installation module extracts the components required for correct Careto operation and subsequent deployment in the network.

Essentially, Careto and similar programs enable two types of computer incidents in the ITCN:

1. Penetration and organization of unauthorized, virtual, covert channel for collection, transmission and processing of information on the ITCN.

2. Covert deployment of MW elements in the ITCN and implementation of massive targeted interference.

Massive targeted MW interference against the ITCN vulnerabilities cause practically immediate (in case of data communication via fiber-optic channels) disruption of functional stability of the ITCN even if ISF are in place.

In order to ensure the functional stability of ITCN affected by MW, it is required to develop models that will define standard MW structures and functions, allow implementing them in the form of testbed simulation models [4] and quantify ITCN resilience when affected by destructive actions [5-7].

ITCN simulation models allow reproducing the most time-critical regulations and control cycles, while ISF models enable developing the respective information security facilities. The most rational configuration of the testbed for verification of ITCN behavior under MW would be a set of data processing centers, information systems based on virtual machines, MW simulators interconnected by means of network communication equipment.

ITCN fault tolerance shall be understood as the ability of the network and ISF to ensure compliance with the specified regulations of control cycles performance (probabilistic and temporal characteristics) under MW within the given time interval.

The presence of potential vulnerabilities in the modern ITCN enables MW deployment and implementation of destructive actions that disrupt functional stability. Therefore, the development of models allowing formalizing the structure and operation process of MW, evaluate ITCN fault tolerance under MW is of relevance.

Problem definition

The following was developed as part of this paper's preparation:

1. MW structural and functional model including the following components:

– general MW system structure;

– structure of MW covert deployment and installation using electronic mail;

– structural and functional diagram of Careto main module and covert deployment modules (SGH, SBD);

– structural and functional diagram of the MW module (SGH) that describes the primary functional capabilities of the MW system;

– MW certificate.

2. Model of ITCN fault tolerance under MW based on experimental testing of ITCN segments and appropriate ISF with simulation of MW against them.

Figure 1 shows the general structure of MW of which the components are distributed over the internal and external networks and interact over the unauthorized virtual data communication channel (established by the intruder). There are known Careto codes for 32 and 64-bit Windows and Linux operating systems (OS), as well as other types of MW for mobile applications of Android and Apple iOS [1,3].

MW structure includes external facilities for controlling the modules deployed in the internal network based on MW control server and delivery (translation) and information interaction module. The MW modules deployed in the ITCN collect data on the network configuration (accessible IPs, MAC addresses and port numbers of communication equipment), type of operating system and ISF, intercept information from the display (user's desktop image), keyboard and connected storage media. The delivery module issues control commands for implementation of destructive functions by the modules deployed in the internal network and then delivers the collected information to the MW control server and stores it in a database. The MW server enables the implementation of the offensive functions of computer attacks against ITCN by means of selection out of a database and sending of a code of special program exploits to the vulnerabilities of the target internal network. Additionally, MW can use various Metasploit Framework tools, e.g. in order to increase MW privileges in the operating system.

The following primary MW modules operate in the internal network:

1. Covert MW elements deployment (loading drivers) and interaction modules that include the facilities for initial access to ITCN elements, covert downloading onto the operating system and ISF evasion, as well as interface programs for organization of information interaction with the external network and between the modules of the internal network.

2. Modules of covert self-propagation of MW in ITCN in the form of software tools for system administrator privileges management, load facilities that ensure interception of operating system traps, covert transition to MW code execution and priority imposing of its functions implementation.

3. Modules of data collection, preparation and implementation of ITCN attacks, of which the key functions consist in the operation of a set of implant programs that intercept wire and wireless network traffic, keystrokes, sessions and keys during programs operation, extract information from computer equipment, save screenshots and control file operations. The malicious module generates the input data on the target ITCN required for interaction, enables deployment of the remaining components of the MW system and delivers the computer attack code to the target ITCN elements.

4. MW self-modification modules are program components that ensure MW adaptation to the parameters of the hardware and software environment of the target ITCN by means of extraction and deployment of programs required for the organization of an unauthorized connection to the network, OS versions, as well as sending a request to the MW server with input data for additional malicious modules.

5. MW covertness modules, i.e. a set of modules that conceal MW actions by means of fake software certificates and electronic signature, internal and external traffic encryption, removal of traces of MW in computer files and memory.

Figure 2 shows the MW covert deployment and installation structure using electronic mail.

Covert deployment, self-propagation and installation of MW are performed as follows. The intruder prepares a phishing e-mail message that contains a link to a malicious network resource. When the link is opened by the user, MW is deployed in the open segment of the ITCN. Then the user is redirected to a legitimate network resource in order to conceal the fact that the system is compromised.

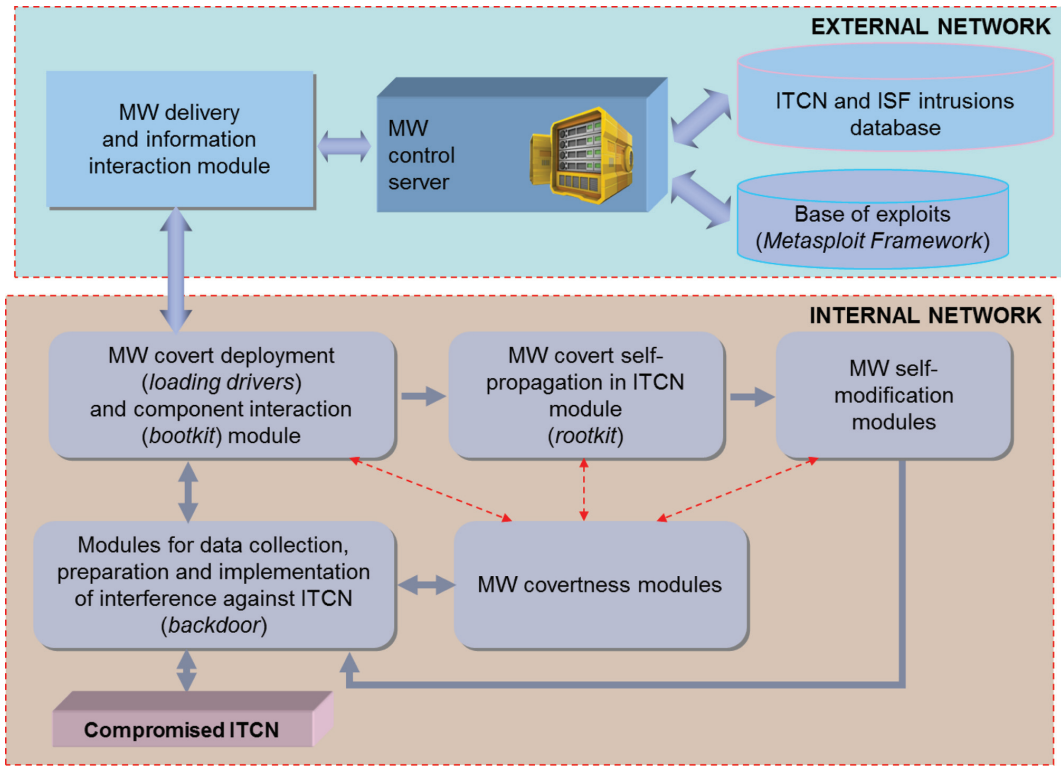


Figure 1. General MW system structure

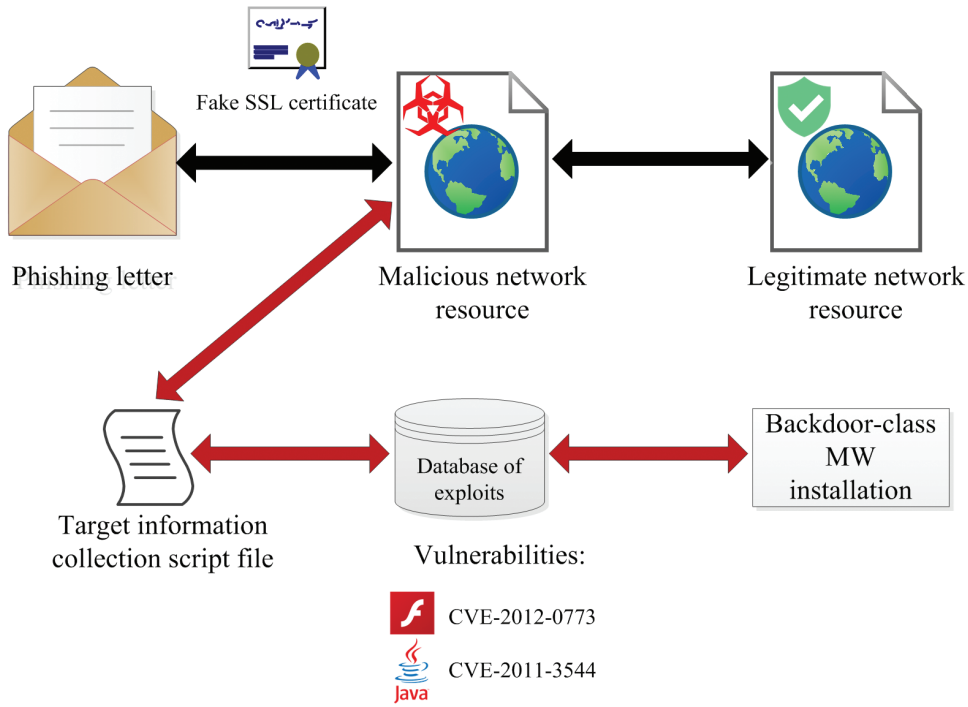


Figure 2. Structure of MW covert deployment and installation using electronic mail

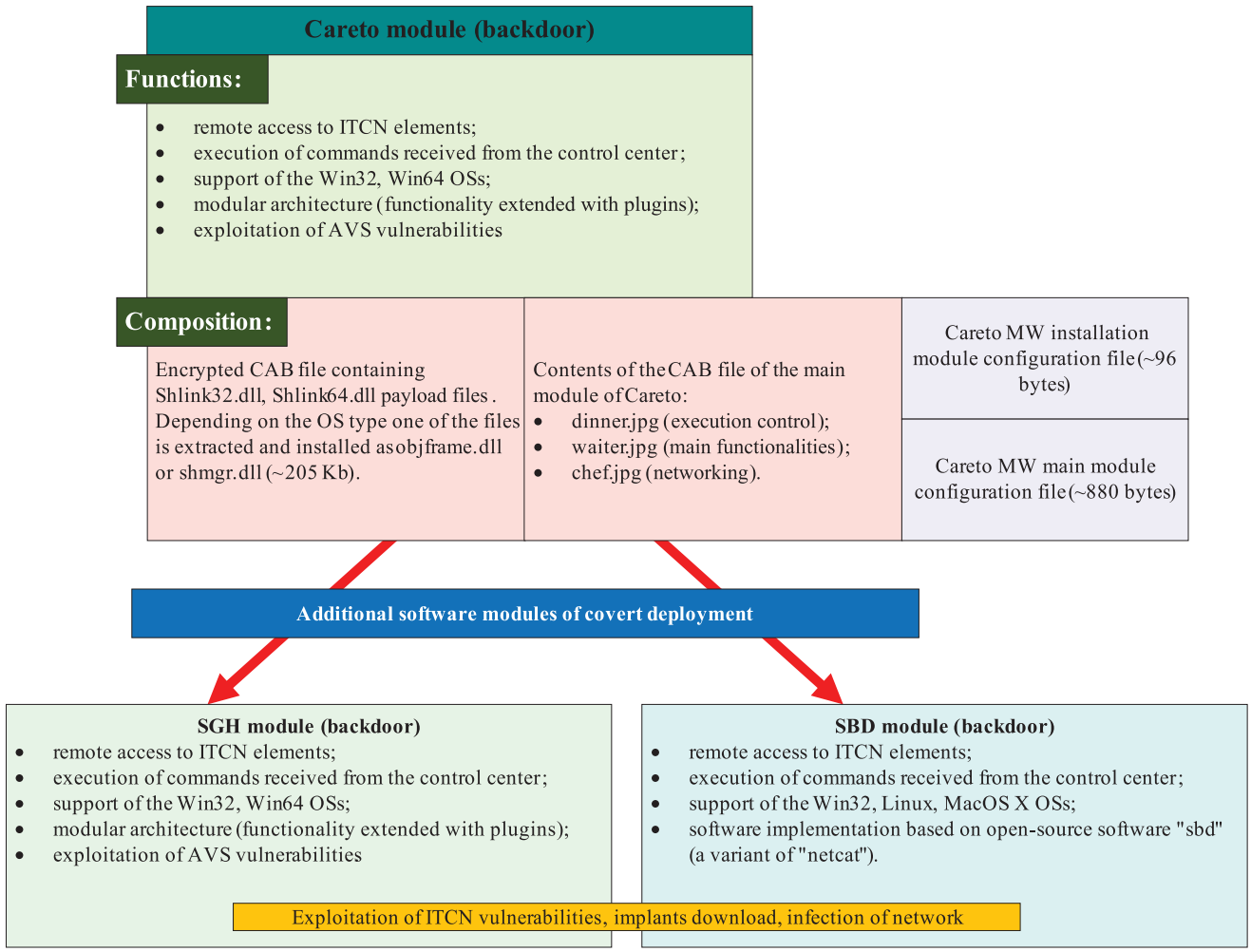


Figure 3. Structural and functional diagram of main MW module and covert deployment modules (exemplified by Careto)

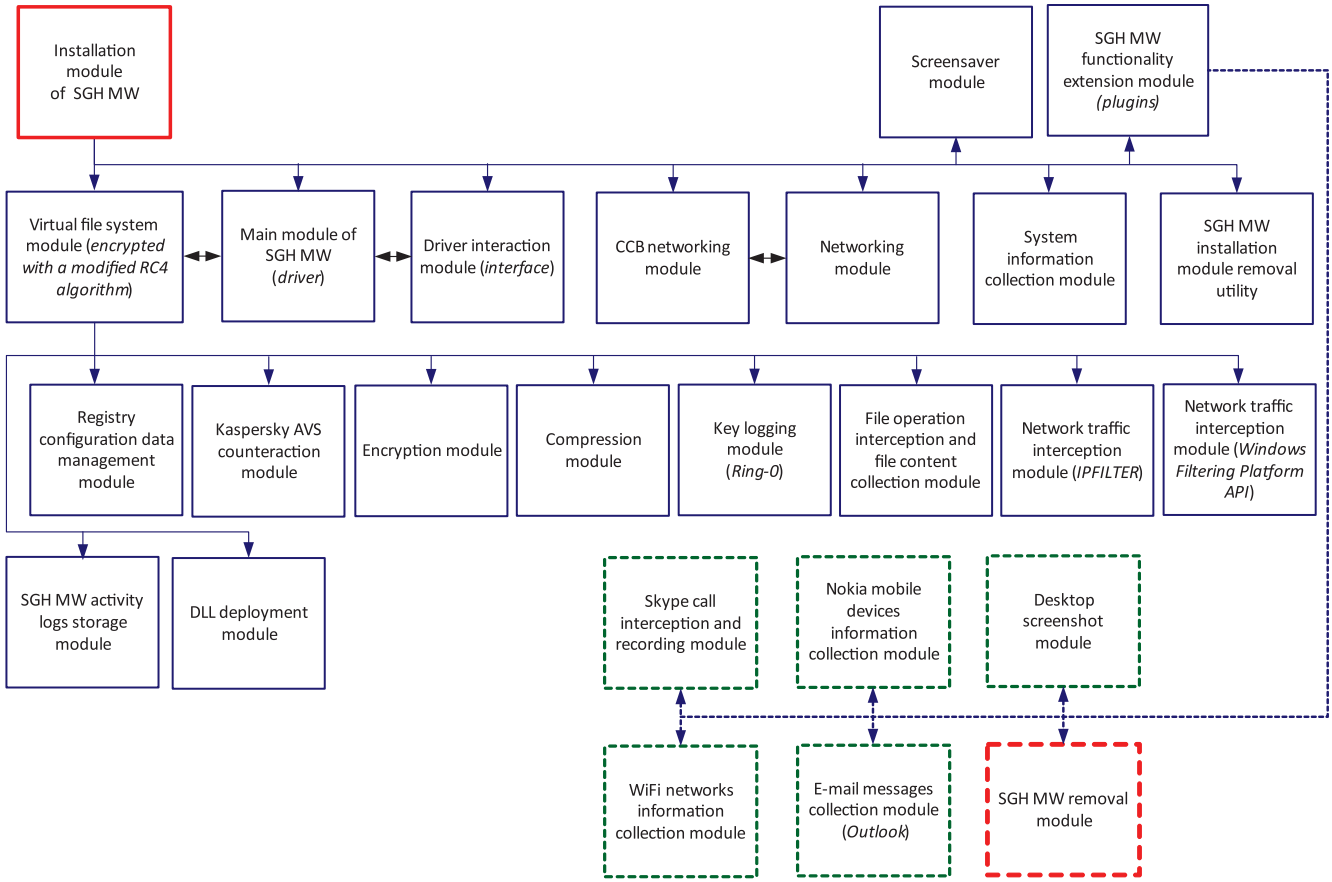


Figure 4. Structural and functional diagram of the MW module (SGH) that describes the primary functional capabilities of the MW system

In order to mask the MW the intruders use subdomains based on malicious network resources. The purpose of the masking mechanism is used on the assumption that if the name of the network resource is very long the browser cuts the name from the end leaving the name of the subdomain.

Then, by using a script file for collection of information on the targets within the ITCN, data on the vulnerabilities and information resources available for intrusion is prepared. For instance, vulnerabilities in Adobe Flash products (vulnerability code CVE-2012-0773) and Java (vulnerability code CVE-2011-3544) are used. Based on the information collected in the ITCN, the required exploit is selected out of the database and loaded as an extension of a browser. Then it is forwarded to the ITCN to ensure the installation of a backdoor-class MW. After a successful compromise of the ITCN the user is redirected to a legitimate network resource, e.g. a news portal.

It is assumed that during its penetration into the ITCN the content of the malicious message evades the standard ITF. The intruder specifies a unique link to a certain exploit and sends it to the user in the phishing letter. The user then loads it. In order to mask the links to exploits, the links are shortened using respective services.

The structural and functional diagram of the main MW module and covert deployment modules (exemplified by Careto) is given in Figure 3. As it can be seen in Figure 3, Careto mainly consists of the main module that performs the initial deployment in the ITCN and the modules for organization of unauthorized data communication channels, covert propagation and implementation of information technology interference (SGH and SBD).

Figure 4 shows the structural and functional diagram of the SGH MW module that describes the primary functional capabilities of the MW system. This type of MW is one of the modules for data collection, preparation and implementation of backdoor-class interference against ITCN. This module provides the intruder with covert remote access to the ITCN, performs various commands received from the MW remote control server. As Careto has the capability to download additional SGH and SBD MW, it can be concluded that the structural and functional diagram, as well as the description of the SGH modules completely characterizes the malicious functions of the whole Careto MW system.

Let us present the primary malicious function of MW, as exemplified by the SGH module of Careto, with a description of the functions of its component modules as follows:

Screensaver module that waits for the moment when the desktop with the name “screen-saver” becomes available, then creates another desktop with its own name, loads the default browser. The «DllEnumClass» function removes the screensaver module or deletes its name from the configuration information, depending on the version of the Windows OS.

Functionality extension module that reads the list of additional SGH modules from the configuration information,

Table 1. Standard MW vulnerabilities certificate

MW description elements	MW description
Name	Careto
Type	backdoor, modular
Detection date	2014
Brief description	The MW covertly deploys and provides the intruder with a remote access to the ITCN, performs various commands received from the remote control server
MW target	public agencies and businesses
Hazard level	High
MW structure	- installation module - main module - remote control center networking module - functional module - execution control module of the functional and network module - removal module - system information collection and data authentication module (additional modules may be downloaded from the remote control center).
Primary functionality	- configuration file and payload file encrypted with a modified RC4 algorithm; - inclusion into startup group as a COM object; - injection of malicious code into explorer.exe, iexplore.exe, firefox.exe, chrome.exe processes; - rerecording of the code sections of the system libraries; - safe closure of module engines; - reception and transmission of data is encrypted with AES and RSA algorithms; - launch of executable files with certain arguments; - reception of CAB file, extraction of file and subsequent launch with a certain argument; - extraction of executable module from CAB file and subsequent launch in the memory; - modification of configuration file, change of remote control server; - collection of information on ITCN and transmission to the remote control server; - complete removal of MW from ITCN.
ITCN compromise indicators	**(Files, fragment)** %AppData%\Microsoft\objframe.dll|shmgr.dll|Shlink(32|64).dll **(Registry, fragment)** [HKLM\Software\Classes\CLSID\{E6BB64BE-0618-4353-9193-0AFE606D6F0C}\InprocServer32] = «%System%\browseui.dll» **(Networks, fragment)** hxxp://202.75.58.153/cgi-bin/commcgi.cgi User-Agent field: Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)
Detection method	**(Virus protection facilities, fragment)** Kaspersky: Trojan.Win32|Win64.Careto.*
Possible elimination measures	- OS reinstallation and formatting of data storage media; - manual check of ITCN compromise indicators (startup group elements, network interaction, file system activity, OS log files analysis); - antivirus facilities update and complete check of ITCN.
Information on MW	https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

loads those modules and regularly polls them, sends the results to the remote control server via the interface provided by the network interaction module.

Driver interaction module that represents an interface for the user level "scimap.sys" driver.

Module for network interaction with the remote control server that establishes connection with the network interaction module by means of the above channel specified in the SGH module's configuration information, performs network interaction with the remote control server.

Network interaction module that provides network features to other SGH modules via the above channel.

System information module that collects low-level information on the ITCN (list of files on the disk, base address of

the PE format files created after the specified date, hardware and software platform characteristics).

Registry configuration data management module that creates normalized configuration information for the SGH module that is used by the other modules.

Antivirus protection counteraction module.

Encryption module that provides cryptographic features to the other modules (AES-128, RC4 encryption algorithms).

Compression module that provides compression features to the other modules (LZNT1 compression algorithm).

Keystroke interception module, a keylogger that operates in kernel mode.

File operations interception and content collection module that intercepts file operations, collects information and file contents in accordance with filter rules.

Network traffic interception module that provide network traffic interception facilities.

SGH activity log files storage module that creates two storage files based on the acquired information collected by other modules and saves them in the ITCN activity log in the form of entries with timestamps and text information.

DLL deployment module that registers the function of management of the events of process creation and loading of library into the process space based on loading rules that define the location of the deployed DLL libraries and list of names of the target processes for deployment.

Skype calls interception and recording module that intercepts a number of Skype functions and data while masking itself as a system library.

Nokia mobile devices information collection module that steals information from Nokia mobile devices.

Desktop screenshot creation module that creates desktop screenshots and records the cursor positions.

Wi-Fi networks information collection module that collects information on wireless networks accessible via the Wi-Fi interface of the compromised ITCN.

Electronic mail messages collection module uses the Microsoft Outlook interface and prompts it from the intercepted OLE2 system functions.

SGH malware removal module that completely deletes MW elements from the ITCN.

We shall define the standard certificate of MW activities implementation against ITCN vulnerabilities using the GOST R 56546-2015 (Table 1) and the example of the Careto MW that describes the key features of its operation and recommendations for the elimination of ITCN vulnerabilities.

Subsequently, it is suggested to use the standard MW certificate in investigations of computer incidents and design of adaptive MW detection facilities based on their behavioural analysis as part of a system for computer attack detection, prevention and recovery.

The ITCN fault tolerance model is required to insure the network's functional dependability when affected by MW. It is based on experimental tests of functional analogues of ITCN segments and associated ISF that involved testbed simulation of MW attacks against them. The model consists of a set of indicators defined by formulas (1-5):

1. Probability of ITCN and ISF maintaining the specified probabilistic and temporal characteristics over the MW period:

$$P_M^{ITCN}(t_{MW}) = \left[1 - \prod_{i=1}^{N} P_{MWi}(t_{MW})\right] \sum_{j=1}^{N} P_{ISFj}(t_{MW}) \sum_{k=1}^{N} P_{Ek}(t_{MW}), \quad (1)$$

where t_{MW} is the time of MW action;

P_{MWi} is the probability of i-th successful MW action against ITCN and ISF elements, N is a sequence of natural numbers;

P_{ISFj} is the probability of successful prevention and detection of MW by the j-th ISF element;

P_{Ek} is the probability of successful elimination of the k-th vulnerability in the ITCN and ISF.

2. Probability of recovery of the probabilistic and temporal characteristics of ITCN and ISF affected by MW:

$$P_{rec}^{ITCN}(t_{rec}) = \left\{1 - \prod_{i=1}^{N}\left[1 - S_{ITCNi} e^{-\lambda_{ISF\,i}\, t_{rec}}\right]\right\} \cdot \left\{1 - \prod_{j=1}^{N}\left[1 - S_{ISFj} e^{-\mu_{ISF\,j}\, t_{rec}}\right]\right\}, \quad (2)$$

where t_{rec} is the recovery time of ITCN and ISF characteristics;

S_{ITCN}, S_{ISF} are the weight numbers of [0, …, 1] that characterize the number of sensors in the ITCN and ISF that detected and countered the MW modules;

λ_{ITCN} is the recovery rate of ITCN elements;

μ_{ISF} is the recovery rate of ISF components;

3. The coefficient of ITCN and ISF operational availability to perform specified probabilistic and temporal characteristics under MW at an arbitrary moment in time.

$$K_A^{ITCN} = \frac{t_{ITCN}}{\sum_{i=1}^{N}\left(t_{ITCNi} + t_{fi}^{MW}\right)}, \quad (3)$$

where t_{ITCN} is the time period of ITCN operability;

t_r^{MW} is the period of faults (failures) as the result of MW activity.

4. The mathematical expectation of the MW action time:

$$m_{MW} = \frac{\sum_{i=1}^{N} t_{MWi}}{N_{tot}^{MW}}, \quad (4)$$

where t_{MWi} are the i-th values of MW action time;

N_{tot}^{MW} is the total number of measurements of MW action time as part of testbed simulation.

5. The mathematical expectation of recovery time of the probabilistic and temporal characteristics of ITCN and ISF:

$$m_{rec} = \frac{\sum_{j=1}^{N} t_{recj}^{ITCN} + \sum_{j=1}^{N} t_{recj}^{ISF}}{N_{rec}^{ITCN} + N_{tot}^{ISF}}, \quad (5)$$

where t_{recj}^{ITCN} is the recovery time of the j-th ITCN element;

t_{recj}^{ISF} is the recovery time of the j-th ISF element;

N_{tot}^{ITCN} is the total number of measurements of ITCN elements recovery when affected by MW;

N_{tot}^{ISF} is the total number of measurements of ISF components recovery when affected by MW.

Conclusion

The paper suggests models that allow identifying the general structure of covert deployment and installation of MW using electronic mail, structural and functional diagram of the main MW module and covert deployment modules (using the example of the Careto MW), structural and functional diagram of MW when implementing malicious functions, MW certificate, as well quantifying the probabilistic and temporal characteristics of fault tolerance, recoverability and availability of ITCN affected by MW.

References

1. Levtstov V., Demidov N. Anatomia targetirovannoy ataki [Anatomy of a targeted attack]. Information Security 2016;2:36–39.

2. Zagorsky A.V., Romashkina N.P., editors. Ougrozy informatsionnoy bezopasnosti v krizisakh i konfliktakh XXI veka [Information security threats in the XXI century's crises and conflicts]. Moscow: IMEMO RAS; 2015 [in Russian].

3. Unveiling "Careto" – The Masked APT. Kaspersky Llab's Analytical materials. <https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf>

4. Klimov S.M., Astrakhov A.V., Sychiov M.P. Metodicheskie osnovy protivodeystvia kompiuternim atakam. Elektronnoye ouchebnoe izdanie [Basic methods of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013 [in Russian].

5. Shubinsky I.B. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016 [in Russian].

6. Kapur K., Lamberson L. Reliability in engineering design. Moscow: Mir; 1980.

7. Velichko V.V., Popkov G.V., Popkov V.K. Modeli i metody povyshenia zhivuchesty sovremennykh sistem sviazi [Models and methods of improving the resilience of present day communication systems]. Moscow: Goriachaia linia-Telekom; 2016 [in Russian].

About the author

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia, e-mail: klimov.serg2012@yandex.ru.

Sergey V. Kupin, Researcher, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, Russia, e-mail: serkup1970@mail.ru.

Dmitry S. Kupin, teacher, Bauman MSTU, Korolyov, Russia, e-mail: t3ft3lb@gmail.com.

Received on 08.06.2017

UDC 629.3.081.3
Original article
Dependability, vol. 17 no.4, 2017 DOI: 10.21683/1729-2646-2017-17-4-44-48

Evaluation methods and ways of improving the operational dependability of mass airflow sensors in engines

Mikhail V. Gorban, *North Caucasus Federal University, Institute of Service, Tourism and Design (Branch), Pyatigorsk, Russia*
Evgeny A. Pavlenko, *North Caucasus Federal University, Institute of Service, Tourism and Design (Branch), Pyatigorsk, Russia*


Mikhail V. Gorban


Evgeny A. Pavlenko

Abstract. *The design of today's car engine electronic control system practically always includes an engine load sensor. Normally, its role is played by the intake manifold absolute pressure sensor or the mass airflow sensor. Film mass airflow sensors are the most common ones. The sensor is installed in the intake between the air filter and the throttle plate of the engine intake manifold. In the process of operation the sensor is exposed to pollution and ageing of the gauging element due to interaction with dust particles and motor oil fumes in the airflow. That causes the output signal to deviate from the reference values and consequently inaccurate calculation of the fuel blend composition by the electronic engine control system. Given the design of the sensors, they cannot be repaired and are replaced with new ones. A new sensor is quite costly. Given the above, it is obvious that the subject is of relevance. The aim of the paper is to find methods of evaluation and ways of improving the operational dependability of film mass airflow sensors installed in modern automobiles. The evaluation of sensor operability is based on the voltage of the sensor output signal. Using a diagnostic scanner plugged into the automobile's diagnostics port in the analog-to-digital converter channel viewing mode the voltage of the sensor output signal is recorded, the fuel blend long-lasting correction factor is evaluated, and the presence of error codes associated with the malfunction of mass airflow sensor in the memory of electronic control unit is verified. A digital oscilloscope is used for measuring the voltage at the moment of ignition lock activation and the resting voltage at zero airflow, as well as the transient time. Based on the obtained findings it becomes obvious that the operational dependability of such sensors can only be improved by correcting the calibration tables of the mass airflow sensor stored in the memory of the engine control unit. Using a mass airflow sensor test stand, input data is prepared for the correction procedure. The reference and tested sensors are installed on the same vacuum pump nozzle, and the airflow rate is changed gradually. Under a fixed airflow rate the sensors' output voltage is measured. The resulting data is summarized in a table and processed with the Chip Tuning PRO calibration software. As can be seen, one of the causes of the loss of the sensors' operational dependability is the pollution of the sensing element. The layer of pollution on the sensing element reduces the coefficient of heat transmission between the airflow and the sensor's gauging element. Based on the conducted research, the paper presents the results of changing sensor output signal in operation as compared to the reference values, suggests a method of correction of the calibration table of mass airflow sensor parameters in the engine control program stored in the memory of the electronic control unit, provides recommendations regarding the methods of evaluation and ways of improving the sensors' operational dependability.*

Keywords: *mass airflow sensor; diagnostic parameters; resting voltage; transient time; calibration table.*

For citation: *Gorban MV, Pavlenko EA. Evaluation methods and ways of improving the operational dependability of mass airflow sensors in engines. Dependability 2017;4: 44-48. DOI: 10.21683/1729-2646-2017-17-4-44-48*

In modern automobiles, in order to identify the air consumption by the engine, a film mass airflow sensor (MAFS) is installed between the air filter and the throttle plate. The MAFS indications are one of the basic parameters used by the electronic control unit (ECU) for identifying the engine load, calculating the required amount of fuel and optimal ignition dwell angle [1].

The Bosch HFM5 film MAFS is the most common type found in Lada automobiles [2,3]. The sensor signal is a voltage that varies between 0 and 5V. The voltage value of the sensor's output signal depends on the size of the airflow passing through the sensor. In case of zero air consumption when the engine is off the sensor's output voltage is supposed to be about 1V. When the engine is on, air flows though the sensor, and the higher the air consumption the higher is the value of the sensor's output voltage.

The operating history of such sensors in Lada automobiles has shown that after about 50 to 70 thousand kilometers the MAFS stops measuring the air consumption correctly. In such cases traction and dynamic performance of the automobile deteriorates, fuel consumption increases, crankshaft rotation becomes uneven when idling, starting of engine is complicated, etc. [4,5].

The sensitivity of the sensor's gauging element reduces due to the pollution with sludge in the airflow, and abrasive wear by dust particles. Measurement accuracy also deteriorates, which ultimately entails incorrect calculation of the fuel-air mixture. Given the design of the sensors, they cannot be repaired and are replaced with new ones. A new sensor is quite costly.

Given the above, it is obvious that the subject is of relevance as it consists in finding methods of evaluation and ways of improving the operational dependability of film MAFS installed in modern automobiles.

We have examined the MAFS operation using an experimental installation (Fig. 1) and in an automobile. Sensor parameters were measured with an MT-10 diagnostic scanner and an Autoscope IV digital USB oscilloscope.

The evaluation of sensor operability was based on the voltage of the sensor output signal. Using the diagnostic scanner plugged into the automobile's diagnostics port in the analog-to-digital converter channel viewing mode the voltage of the sensor output signal was recorded, the fuel blend long-lasting correction factor was evaluated, the presence of MAPS-specific error codes in the ECU memory was verified.

Table 1. Measurement results of the sensors under consideration

Ths km travelled in service	Resting voltage, V	Transient time, ms	Long-term correction factor	Availability of fault code, Yes/No
0 (new sensor)	1.000	2.8	1.0	No
45	1. 05	14.8	1.03	No
60	1.142	22.88	1.1	No

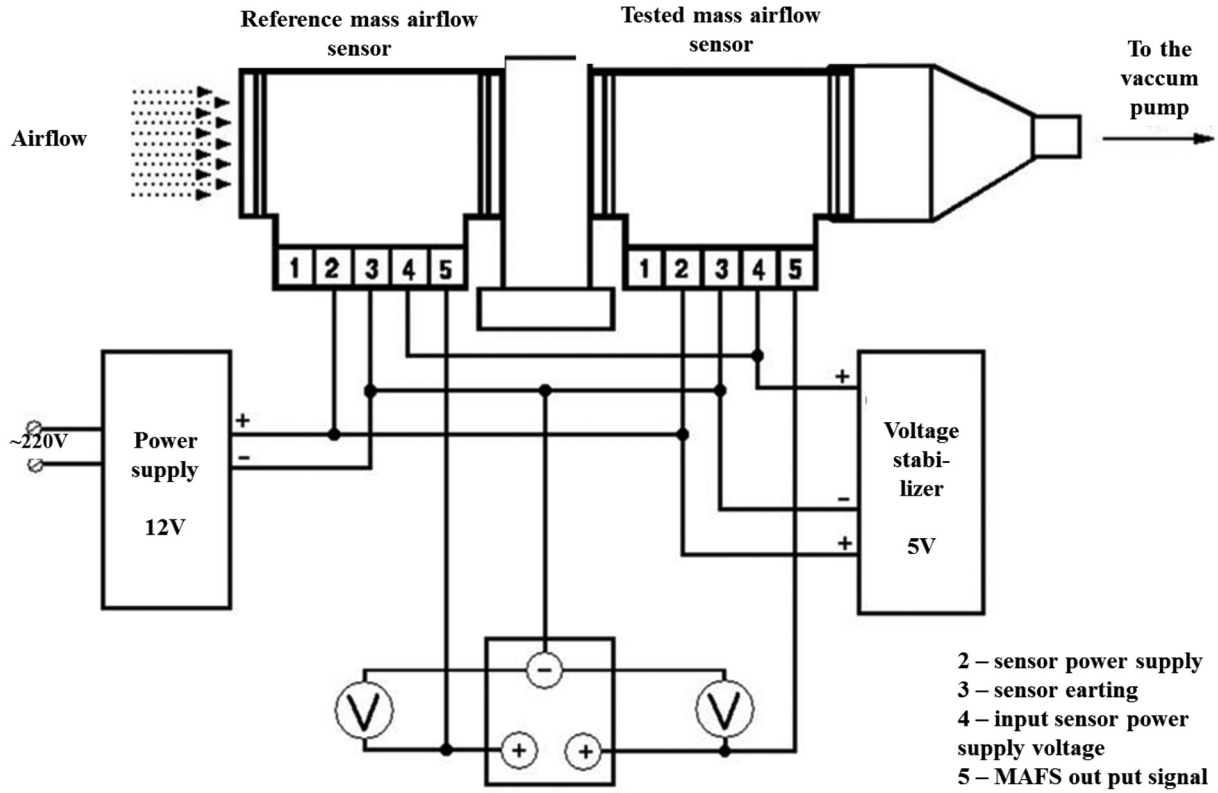


Figure 1. Diagram of the mass airflow sensor test stand

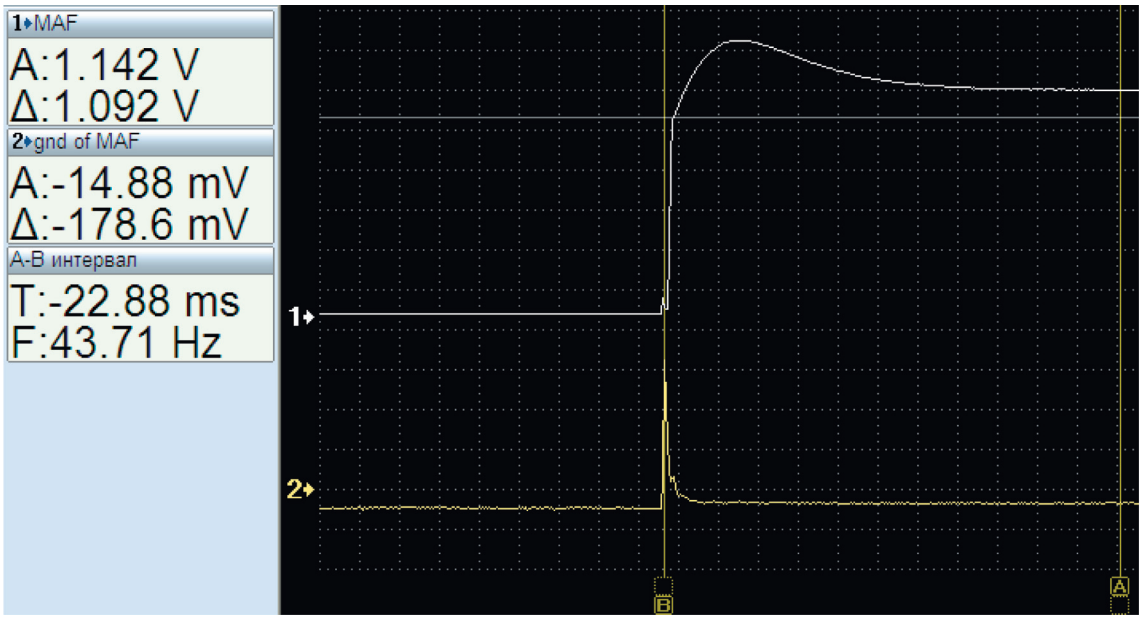


Figure 2. An output voltage oscillogram of a sensor from an automobile that had travelled 60 ths km.

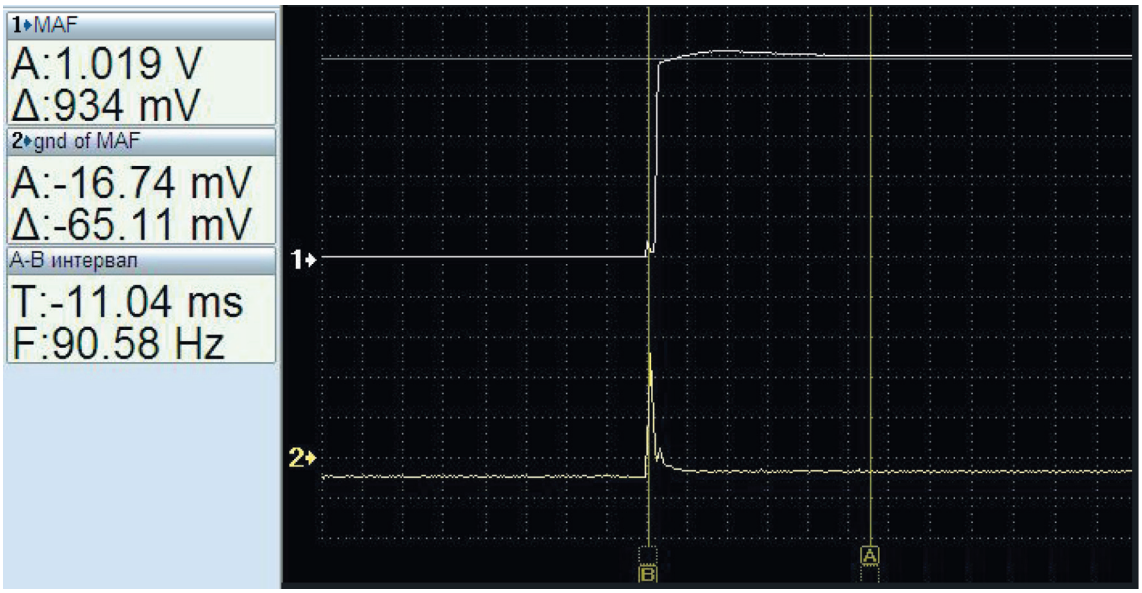


Figure 3. Output voltage oscillogram of a sensor from an automobile that had travelled 60 ths km after the cleaning of the sensing element

The digital oscilloscope was used for measuring the voltage at the moment of ignition lock activation and the resting voltage at zero airflow, as well as the transient time.

The measurement of the resting voltage and transient time involved Bosch HFM5 sensors of automobiles with different kilometer performance figures. A new sensor was used for comparison of the results. The findings are given in Table 1.

According to the Bosch manuals the tolerance of the resting voltage variation are within 0.98 – 1.02V. If the voltage is not within the tolerances, the sensor should be replaced. The table shows that only the new sensor's voltage is within the tolerances. However, practice has shown that sensors with the resting voltage of 1.05V remain in operation and dependable. Therefore, 1.05V can be identified as the upper threshold of resting voltage.

A more complete evaluation of operational dependability was conducted using an oscillograph based on the results of measurement of the transient time after MAFS energization. Hence the sensor's signal output was connected to the first channel, while the sensor mass was connected to the second channel.

Reaching the resting voltage takes some time required for the heating-up of the sensor's thermistor. If the transient process happens within 1 to 10 ms, the sensor can be deemed operable.

Figure 2 shows an oscillogram of a MAFS from an automobile that had travelled 60 ths km.

The figure shows that the resting voltage was 1.142V, while the transient time was 22.88 ms. Those values are outside of the allowed tolerances. Under such values the fuel mixture is significantly enriched and the control unit – upon

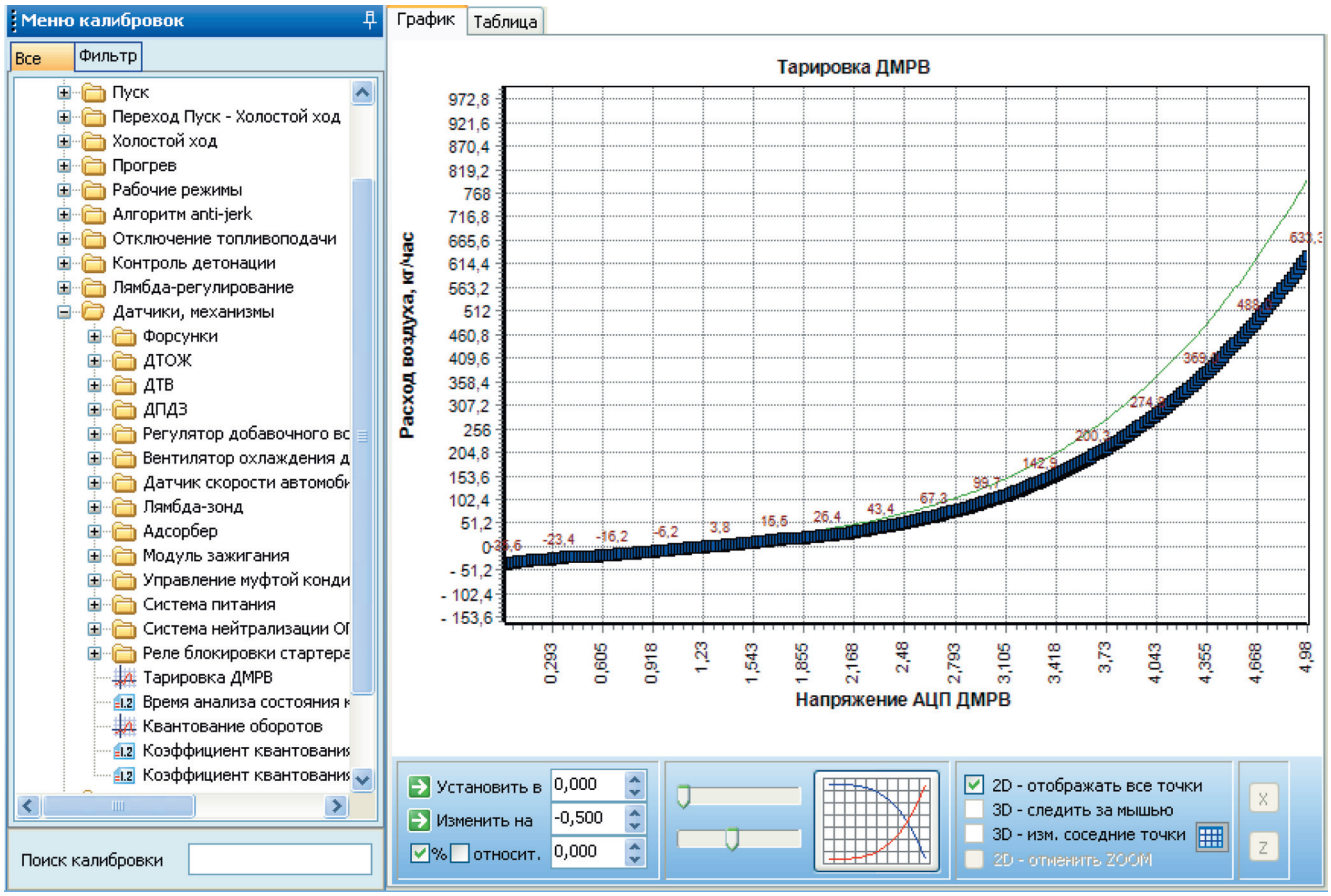


Figure 4. MAFS calibration map in Chip Tuning PRO 7

the oxygen sensor's command – starts increasing the factor of self-teaching correction in order to insure the stoichiometric ratio. Table 1 shows that under the voltage of 1.142V the long-term correction factor becomes equal to 1.1.

One of the causes of the loss of the sensors' operational dependability is the pollution of the sensing element. The layer of pollution on the sensing element reduces the coefficient of heat transmission between the airflow and the sensor's gauging element. Therefore it would be advisable to evaluate the effect of cleaning of the sensor's sensing element on the change of its performance.

Figure 3 shows the output voltage oscillogram of a sensor after cleaning. The MAFS was washed with the special Mass air flow liquid. The liquid is safe and sufficiently active. After the cleaning the sensor's sensing element was dried with a jet of compressed air.

The oscillogram shows that after the cleaning the sensor's resting voltage fell to 1.019V, i.e. within the tolerances. The transient time was 11.04 ms, which is insignificantly higher than the acceptable 10 ms.

It is suggested improving the operational dependability of such sensors by correcting the MAFS calibration table stored in the memory of the engine control unit.

Using the mass airflow sensor test stand (Fig. 1), input data was prepared for the correction procedure. The reference (new) and tested sensors were installed on the same vacuum pump nozzle, and the airflow rate was changed gradually. Under a fixed airflow rate the sensors' output voltage was measured. The resulting data was summarized in a table and processed with the Chip Tuning PRO 7 calibration software. Table 2 shows the test results for a new sensor and one from an automobile that had travelled 60 ths km after the washing.

Table 2. Results of the tests of sensors under consideration

Reference MAFS, V	Tested MAFS, V
1.00	1.019
1.64	1.73
3.73	4.36

In Chip Tuning PRO 7, the firmware file stored in the memory of the control unit was opened and the MAFS calibration map was loaded. The calibration map in Figure 4 is a characteristic curve of air consumption Q_a and output voltage of the mass airflow sensor U_{out}.

Table 2 shows that if the air consumption Q_a = 0 kg/h the reference sensor reads the voltage U_{out} = 1.00V, while for the tested sensor the value is 1.019V. Therefore the correction must be performed in such a way as to ensure that if U_{out} = 1.019V the air consumption was Q_a = 0 kg/h. The last line of the table corresponds with the voltage of the reference sensor U_{out} = 3.73V, while for the tested sensor U_{out} = 4.36V. The voltage U_{out} = 3.73V corresponds with the

air consumption Q_a = 271.9 kg/h. Therefore the correction must be performed in such a way as to ensure that if U_{out} = 4.36V the air consumption was 271.9 kg/h.

The correction procedure was performed in two stages. At the first stage, the initial curve was shifted parallel to the y axis (Figure 4), so when U_{out} = 1.019V the air consumption Q_a = 0 kg/h. At the second stage of correction, the shifted curve must be rotated about the point of air consumption Q_a = 0 kg/h turning the curve to the value when if U_{out} = 4.36V the air consumption is Q_a = 271.9 kg/h.

Figure 4 shows two graphs that reflect MAFS calibration before and after correction. The calibration map obtained after the correction is saved in the ECU's firmware file.

Based on the findings it can be argued that the self-diagnostics system of the engine control unit is unable of identifying the reduction of the time of MAFS reaction to changing air consumption. Therefore, this malfunction cannot be identified by reading the malfunction codes from the control unit and can be ascertained only by means of estimation of the correction factors of fuel feed using a scanner and measurement of the transient time with an oscillograph.

MAFS operational dependability can be improved by cleaning the sensors' sensing elements with special cleaning solutions and subsequent correction of the MAFS calibration maps stored in the memory of the electronic control units.

References

1. Reif K. Datchiki v avtomobile. Seria: Avtomobilnaya tekhnika. Bosch. Tipy datchikov, oustroystvo, printsyp raboty [Sensors in automobiles. Series Automotive engineering. Bosch. Types of sensors, design, operating principles]. Moscow: Izdatelstvo: Za rouliom.

2. Maintenance and repair manual. VAZ-2111, 212114-11 engine control system with distributed sequential fuel injection, EURO 2 toxicity standard. AvtoVAZ technical development directorate; 2004.

3. Vzaimozameniaemost novykh ouzlov i detaley avtomobiley VAZ [Interchangeability of new units and parts of VAZ automobiles]. Izdatelstvo: Tretiy Rim; 2003.

4. Plaksin AM, Gritsenko AV, Grakov FN, Glemba KV, Lukomsky KI. Diagnostirovanie sistemy vpuska avtomobilnykh dvigateley vnutrennego sgorania metodami testovogo diagnostirovania [Diagnosing intake systems of automotive internal combustion engines by means of testing]. Fundamentalnye issledovania 2014;8-5:1053-1057.

5. Gritsenko AV, Larin ON, Glemba KV. Diagnostirovanie datchikov massovogo raskhoda vozdukha legkovykh avtomobiley [Diagnosing mass airflow sensors in cars]. Herald of the South Ural State University. Engineering Series 2013;13 (2):113-118.

About the authors

Mikhail V. Gorban, Candidate of Engineering, senior lecturer in transportation vehicles and processes, North Caucasus Federal University, Institute of Service, Tourism and Design (Branch), Pyatigorsk, Russia, e-mail: gorban.mihail@mail.ru.

Evgeny A. Pavlenko, Candidate of Engineering, senior lecturer in transportation vehicles and processes, North Caucasus Federal University, Institute of Service, Tourism and Design (Branch), Pyatigorsk, Russia, e-mail: evgeneip@bk.ru.

Received on 06.02.2017

UDC 629.3.081.3
Original article
Dependability, vol. 17 no.4, 2017 DOI: 10.21683/1729-2646-2017-17-4-49-52

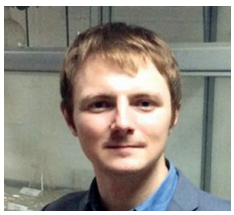
Study of conductive materials by means of a multi-frequency measurement system based on microminiature eddy current transformers

Sergey F. Dmitriev, *Altai State University, Altai Krai, Barnaul, Russia*
Alexey V. Ishkov, *Altai State University, Altai Krai, Barnaul, Russia*
Alexander O. Katasonov, *Altai State University, Altai Krai, Barnaul, Russia*
Vladimir N. Malikov, *Altai State University, Altai Krai, Barnaul, Russia*
Anatoly M. Sagalakov, *Altai State University, Altai Krai, Barnaul, Russia*


Sergey F. Dmitriev


Alexey V. Ishkov


Alexander O. Katasonov


Vladimir N. Malikov


Anatoly M. Sagalakov

Abstract. *A measurement system has been developed that is based on an eddy current transformer and allows evaluating the applicability of the eddy current method for detecting local defects of products made of an aluminium-magnesium alloy. The paper describes the design of a microminiature eddy current transformer (ECT) with an excitation, measurement and compensation windings that uses a pyramidal core that enables localization of the magnetic field within an area about 2500 square мм. The distinctive feature of the measurement system consists in the ability to detect deep defects (up to 5 mm). The paper sets forth the primary parameters of the transformer that enable the magnetic field localization (shape, material and size of the core, number of the windings and number of loops). It also describes the process of preparation and application of several ECTs with different core and winding parameters. That allowed the ETCs generating different electromagnetic fields and reacting to the changes in that field with varied efficiency. Optimal ECT size for identifying defects in aluminium-magnesium alloys was established (pyramidal shape of the core, base 400 мм in diagonal, edge 4 mm long, 20 loops of the excitation winding, 200 loops of the measurement winding, 200±40 loops of the compensation winding). The paper describes the design of the measurement system and the measurement method that allows finding defects with the linear size of 0.25 mm situated 5 mm below the surface or more depending on the signal received from the eddy current transformer. The measurement system includes two microminiature transformers controlled by special C++ software. Voltage to the excitation winding was applied by an integrated rectangular wave generator. This setup allowed creating a magnetic field with minimal noise. The voltage of the excitation winding varied from 2 to 3V. The transformers output signal was processed in a hardware filtering system described in this paper. The distinctive feature of the measurement system is the synchronous change of the measurement signal generation frequency and filtration frequency. That enables efficient extraction of the useful signal that carries information on the defects of the tested object. The paper sets forth data that demonstrate the dependence of the amplitude part of the signal from the defects of various sizes and experimentally establishes the limit defect sizes under which such measurements are possible. The research covered objects in the form of aluminium-magnesium plates (94% Al, 3% Mg). Amplitude changes due to the linear sizes of the defects and the depth of their situation. The nature of such changes allows identifying the defects' parameters. Depending on the size and depth of the defects, the change of the amplitude associated with the transformer passing above the defect were from 2.5V (for a defect 0.25 mm wide situated 1 mm from the surface) to 0.1V (for a defect 0.25 mm wide situated 5 mm from the surface).*

Keywords: *eddy current transformer, aluminium-magnesium, core, defect, alloys.*

For citation: *Dmitriev SF, Ishkov AV, Katasonov AO, Malikov VN, Sagalakov AM. Study of conductive materials by means of a multi-frequency measurement system based on microminiature eddy current transformers. Dependability 2017;4: 49-52. DOI: 10.21683/1729-2646-2017-17-4-49-52*

Introduction

Methods and means of non-destructive eddy current testing are used for detecting defects in products made of any conductive materials. Such measurement allows – if necessary – testing each manufactured product at the factory.

The duraluminium and aluminium-magnesium alloys are widely used in today's production, most widely in the aerospace and other industries. Due to the combination of their strength and light weight, those alloys are also widely used in the production of high-speed trains including Shinkansen, as well as a number of other machine construction industries. Duraluminium is also frequently used in the electrical, chemical and food industries, as well as radio engineering and construction. The D16AM alloy is used in extreme conditions of low temperatures, the D16T duraluminium is highly ductile, which is the reason of its widespread application in shipbuilding.

Quality control of such alloys and products made out of them becomes a relevant matter. Research in this area is in constant development.

The analysis of current research shows a trend to size reduction (miniaturization) of eddy current transformers (ECT) used in quality control of alloys [1-6]. One of the methods allows developing 5*5 mm transformers with the wire diameter of 0.15 mm. However, such transformers do not enable the required depth of magnetic field penetration and localization for local measurement in heterogeneous conductive media. Ferrite cores are often used in order to increase the magnetic field localization. This design solution ensures a significant reduction of eddy current scattering. It also enables the depth of field penetration of 2.5 mm.

There are several known designs of laid-on eddy current transformers, of which the working surface is made in the form of a plain surface or a hemisphere. This surface ensures satisfactory contact between the transformer and the tested surface, yet the voltage applied to the transformer significantly depends on the curvature of the tested surface. Additionally, the transformer's operation is significantly affected by the edge effect, which prevents testing parts of complex shape and small size. In order to solve this problem, ECT is often equipped with an additional core, one of the ends of which is shaped as a truncated cone. The disadvantage of this solution is that despite the higher magnetic field localization the core design is significantly more complex. That decreases the measurement accuracy of the controlled parameter due to the fact that the transformer's input signal significantly depends on the interaction between the two cores that can unpredictably affect the enhancement of the eddy current field that carries the information on the tested objects [7].

Manufacturing such instruments requires the deployment of special production lines, which causes a significant growth of the price of the final product. In order to reduce the instrument's price it has been suggested to substitute the expensive hardware units with PC software.

Sensor design

A microminiature eddy current transformer has been developed for local testing of physical parameters as part of research of the properties of aluminium alloy plates and welds. The advantage of this transformer (that the comparable devices do not have) is the capability to perform local measurements within areas of about hundreds of мms and about 5 mm deep. The measurement parameter is the conductivity of the material and its distribution over the surface and depth of the tested object [8].

The excitation winding with the diameter $D_1 = 0.12ч0.13$ mm of the microminiature transformer consists of 10 loops of copper wire with the cross-section area of 5 мм^2. The measurement winding with the diameter of 0.05ч0.08 mm consists of 130 loops of copper wire with the cross-section area of 20 мм^2. In order to minimize the effect of the excitation winding on the resulting signal, the design includes a compensation winding with the cross-section area of 5 мм^2 that is connected to the measurement winding in such a way that the voltage of the excitation winding is calculated based on the result. The winding is placed around the pyramidal core made of ferrite 2000 NMZ with the relative magnetic permeability of $\mu_{max= 500}$ or (if higher magnetic field localization is required) of 81NMA alloy annealed using a special technique. The core is a four-face pyramid 1 mm high and 0.2 mm-long base edges. The measurement winding is at the tip of the pyramid, which improves the magnetic field localization. The performance characteristics of the developed transformers enable efficient magnetic field localization and applicability for analysis of defects 250 мm or larger in size. The transformers also ensure significant depth of penetration into the tested object when operating at sufficiently low frequencies.

A laid-on ECT consists of a pyramidal core. The pyramidal cores are covered with wire windings. The windings are treated with a compound at the infiltration temperature of 200 degrees Celsius; the wire diameter is $1.5Ч10^{-6}$ m. The measurement winding is at the tip of the pyramid; the winding diameter is 0.05 mm; the number of loops varies between 100 and 200. In the middle of the pyramid is the excitation winding that consists of one loop. The compensating winding is on a movable frame and consists of 100 loops. 10 ECTs were created and tuned in order to subtract the voltage induced by the generator winding to the measurement winding. The aim of creating various ECTs is obtaining a magnetic field of different strengths, hence the

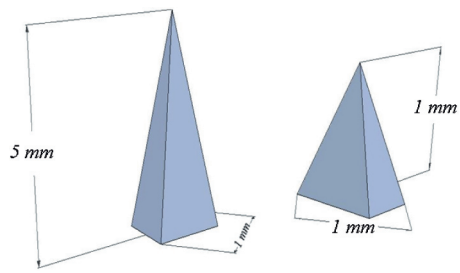


Figure 1. Cores of different sizes

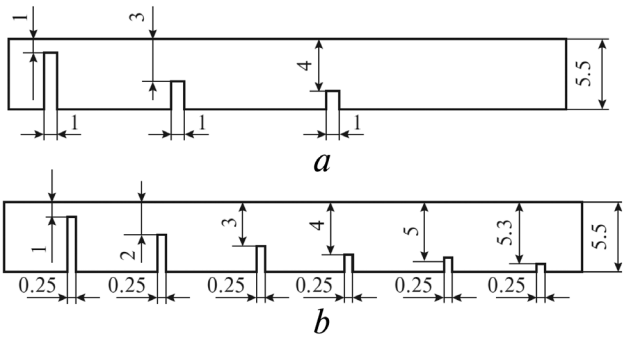


Figure 2. Plates nos 1 and 2 (side views)

size differences from core to core. The correlation between the base diagonal and edge of the pyramid varies from 1:1 to 1:10 (Fig. 1).

The ECTs designed using cores having identical correlations between the base diagonal (400 мm) and edge length (4 mm) were calibrated using semiconductors with known conductivity. Thus, the ECTs have identical geometrical parameters of the cores and identical loop counts of the excitation (20 loops), measurement (200 loops) and compensating (200±40 loops) windings.

The measurement system based on a microminiature eddy current transformer operates in the following manner. The computer software operates the generator that generates a series of rectangular voltage pulses with the repetition frequency f1 required for the operation of the eddy current transformers. The voltage pulses from the generator outputs are transmitted to two integrators connected in series and then to the input of the power amplifier. From the amplifier outputs the pulses are sent to the excitation windings of the eddy current transformers. The difference between the output voltages of the measurement windings of the transformers carries the information on structural heterogeneity of the tested object that falls within the coverage of the eddy current transformers. It is identified and amplified in a special microphone amplifier. The signal, having passed two serially connected quality low-frequency filters and two serially connected selective amplifiers, arrives to an amplitude detector. Then the signal is transmitted to the computer via an analog-to-digital amplifier. Owing to simultaneous control of the frequency of the generated signal at the excitation winding and cut-off frequency of the filtration system, as well as selective amplification the useful signal is extracted. The latter carries information on the distribution of conductivity within the object, including its defects [9-10]. Software control allows changing the operation frequency of the measurement system in such a way as to enable reliable recording of the signal received from the measurement winding.

Experimental results

In order to evaluate the maximum depth of situation and linear dimensions of defects that justify the use of eddy current test method, samples with model defects were prepared.

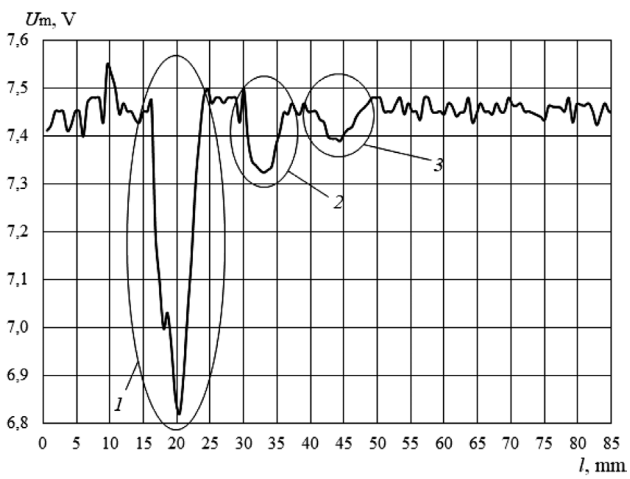
The samples were Al-Mg alloy plates (94% Al, 3% Mg). The thickness of the first plate was 5.5 mm, it contained three defects in the form of 1 mm thick cuts 1, 3 and 4 mm deep (Fig. 2.a). The thickness of the second plate was 5.5 mm, it contained six defects in the form of 0.25 mm thick cuts 1, 2, 3, 4, 5 and 5.3 mm deep (Fig. 2.b).

In order to identify the sensor's sensitivity to defects inside metal, the scanning was performed from the defect-free side of the sample.

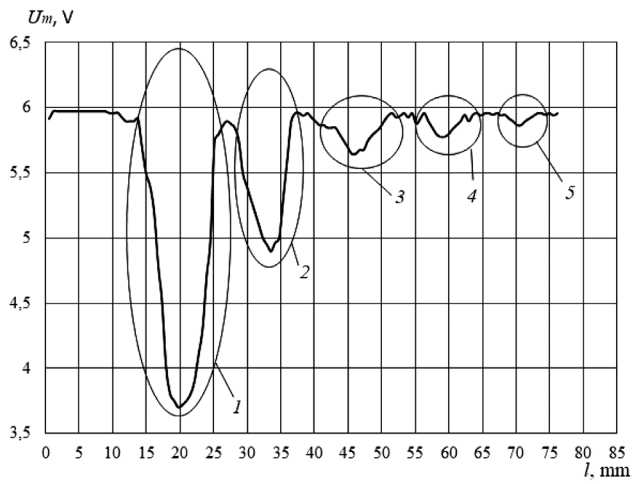
During the experimentation with the first plate, the amount of induced voltage at the excitation winding of the transformer was 2V.

The research results of the first plate with 1 mm defects under signal frequency of 500 Hz and amplitude of 2V ensured evident detection of all three cuts based on the drop of signal amplitude (Fig. 3.a): for the first defect it was about 0.75V, for the second one it was 0.2V, and 0.1V for the third one.

The research results of the second plate under signal frequency of 500 Hz and amplitude of 3V ensured the detection of five defects (Fig. 3.b.). The drop of signal amplitude



a)



b)

Figure 3. Scanning results of plates no. 1 (a) and no. 2 (b). U is the voltage applied to the measurement winding of the voltage transformer, l is the coordinate of the transformer relative to the beginning of the tested object

for the first defect was about 2.5V, 1V for the second one, 0.4V for the third one, 0.2V for the forth one and 0.1V for the fifth one. No signal response change was registered for the sixth defect due to its small value.

The results of the experiment show the efficiency of the developed measurement system for detection of defects 0.25 mm wide or higher situated up to 5 mm below the surface.

Conclusion

The developed measurement system based on microminiature eddy current transformers enables higher electromagnetic field localization compared to the previously available systems.

The pyramidal shape of the core, a system of bandpass filters and selective amplification enabled a significant reduction of the noise level and significant penetration depth of eddy currents into the object under examination. The developed eddy current transformers enable efficient scanning of welds of titanium alloys and quality analysis. Scanning of defects in aluminium alloys allows detecting defects with linear size of about 100 мм situated up to 5 mm deep from the surface. The developed software automates the measurements and provides for real-time modification of the device's operation frequency.

The activities were conducted with the support of the Russian Foundation for Basic Research (project code 17-48-220044, Development and research of highly efficient composite nanostructured seal coatings).

References

1. Prance RJ, Clark TD, Prance H. Ultralow noise induction magnetometer for variable temperature operation. Sens. Actuators 85: 361–364.

2. Prance RJ, Clark TD, Prance H. Compact room temperature induction magnetometer with super conducting quantum interference level field sensitivity. Rev. Sci. Instrum. 74: 3735–3739.

3. Semenov VS, Ryabtsev AP, Mudrov AE. Electromagnetic flaw detection and testing methods in Siberian Physicotechnical Institute and Tomsk State University. Vestn. Tekhn. Gos. Univ. 2003;278:48–54.

4. Barbato L, Poulakis N, Tamburrino A, Theodoulidis T. Ventre. solution and extension of a new benchmark problem for eddy current nondestructive testing. IEEE Trans. Magn. 2015;51 (7):1–1.

5. Rocha, Tiago J, Ramos HG, Ribeiro AL, Pasadas DJ. Magnetic sensors assessment in velocity Induced eddy current testing, Measurement 2015.

6. Litvinenko AA, RU Patent no. 2231287.

7. Lee KH, Baek MK, Park IH. 2012 Estimation of deep defect in ferromagnetic material by low frequency eddy current method. IEEE Transactions on Magnetics 48:3965-3968.

8. Klyuev VV. Nerazrushayushchii kontrol' [Nondestructive Testing]. Moscow: Mashinostroenie; 2003, vol. 2, books 1–2 [in Russian].

9. Malikov VN, Davydchenko MA, Dmitriev S F, Sagalakov AM. Subminiature eddy-current transducers for conductive materials research. In: Proc. of Int. Conf. on Mechanical Engineering, Automation and Control Systems. Tomsk (Russia); 2015 [in Russian].

10. Dmitriev SF, Malikov VN, Sagalakov AM, Shevtsova LI, Katasonov AO. Subminiature eddy current transducers for studying semiconductor material. Journal of Physics: Conference Series 643.

About the authors

Sergey F. Dmitriev, Associate Professor, Candidate of Engineering, Altai State University, Senior Lecturer in general and experimental physics, Altai Krai, Barnaul, Russia, e-mail: dmitrsf@gmail.com

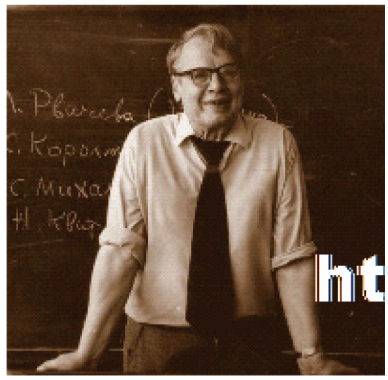
Alexey V. Ishkov, Doctor of Engineering, Professor, Altai State University, Professor of structural materials technology and machine maintenance, Barnaul, Russia, e-mail: buvarton@mail.ru

Alexander O. Katasonov, Altai State University, student, Altai Krai, Barnaul, Russia, e-mail: ivenir4000@gmail.com

Vladimir N. Malikov, Doctor of Engineering, Professor, Altai State University, lecturer in general and experimental physics, Altai Krai, Barnaul, Russia, e-mail: osys11@gmail.com

Anatoly M. Sagalakov, Doctor of Physics and Mathematics, Professor, Altai State University, Professor of general and experimental physics, Altai Krai, Barnaul, Russia, e-mail: sagalakovam@mail.ru

Received on 18.08.2017



Gnedenko e-Forum

International Group on Reliability

http://Gnedenko-Forum.org/

Dear colleagues!

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

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

"Reliability: Theory and Applications".

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

Join Gnedenko Forum!

Welcome!

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

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

Alexander Bochkov, PhD

a.bochkov@gmail.com

Membership is free.

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

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 107078, Moscow, 5 Orlikov lane, Office 755, 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:

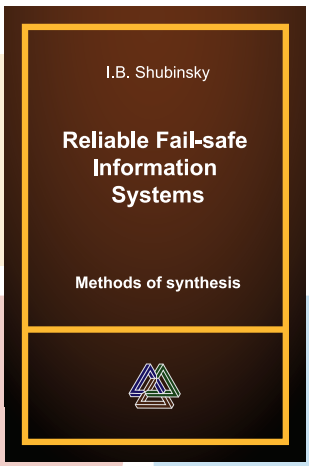
- Through the agency «Rospechat»
  – for the first half of the year: an index 81733;

- 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: E.Patrikeeva@gismps.ru

НАДЁЖНОСТЬ
DEPENDABILITY SCIENTIFIC-TECHNICAL JOURNAL
ISSN 1729-2646

REPRESENTS



Publication can be purchased through the editorial board of Journal Dependability Ltd.

+7 (495) 967-77-05, ext.186
+7-916-105-81-31
(Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Journal Dependability Ltd,
109029, Moscow,
Nizhegorodskaya str.27, bldg.1, office 209
Tel./fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Igor B. Shubinsky

RELIABLE FAIL-SAFE
INFORMATION SYSTEMS
Methods of synthesis

Copy deadline 12.02.2016. format of the edition 70x100/16.
Offset printing. Offset paper. Conv. Sheet. P. 17,55.
Circulation of 700 copies. Order number 1452.

I.B.Shubinsky

Reliable Fail-safe Information Systems

2016

The book describes conceptual provisions to ensure structural and functional reliability of information systems at all stages of a life-cycle. It represents different types of redundancy taking into account limited efficiency of the failure detection system. Under these conditions a broad-based assessment of their efficiency is performed, with determination of capabilities of structural redundancy with an endless number of standby facilities. Ways to ensure functional reliability of software are represented, including the recommendations for the development of software programs requirement specification, with the description of the process of a reliable program architecture development and well proven rules and recommendations used for design and implementation of software, as well as for integration with system hardware.

The book also presents theoretical and practical provisions of adaptive fault tolerance (active protection) of information systems, including the methods and disciplines of active protection, as well as the ways of implementation. A method of synthesis of active protection and the results of research of information system reliability with various disciplines of active protection are offered. There are also certain assessments of the efficiency of active protection in relation to the traditional methods of structural redundancy.

You can find the description of the principles to ensure functional safety of information systems, with a substantiation of the possibility to restart independent channels in two-channel safe systems. The rules of determination of the allowed time for a guaranteed detection of single and double hazardous failures are developed, including the method of synthesis of a combined two-level information system developed with higher functional safety requirements.

To prove the conformance of reliability with functional safety the method of accelerated field testing of the information system has been developed. The book contains the description of this method, including the example of its practical implementation. You will also find the information about the procedures of certification tests based on the requirements of information safety and software certification conformance.

A checklist of the most complex and significant subjects is provided at the end of each chapter. The book is primarily intended for experts who are engaged in practical development, manufacture, operation and updating of information. It is intended for researchers in the field of structural reliability of different discrete systems, academic staff, post-graduate students and students specializing in the field of information systems and as well as those working in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
By phone +7 (495) 967-77-05, ext. 186; +7-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

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