BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 2
Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0018

Mathematical Modeling and Examination of the Effects of Structural Redundancy in a Class of Computer-Based Fault Tolerant Systems

Mariya Hristova

Todor Kableshkov University of Transport, 1574 Sofia, Geo Milev str. 158, Bulgaria
Email: mhristova@vtu.bg

Abstract*:** *The present article models and examines k∨n systems, in particular Triple modular redundancy* (*2∨3*) *and 3∨5. The aim of the study is to derive mathematical models, which are used for determining the impact of structural redundancy* (*the number of channels n and the threshold of the quorum function k*) *on the reliability of the system. The probability of failure-free operation* ***p *and the Mean Time Between Failures* (*MTBF*) *are used as reliability indicators.*

***Keywords*:** *Real time systems, fault-tolerant systems, Safety Critical Systems* (*SCS*), *redundancy, triple modular redundancy, availability.*

1. Formulation of the problem

One class of systems for real-time control (Real Time Systems – RTS) with applications in various spheres of technology and life is intended for control of especially critical technological processes (Special Critical Technology Process or operation, SCTP). If SCTP go beyond their regulated functionality due to failures in their controlling systems, this may cause a loss of large human and material assets and/or inadmissible harming of the environment. Subject of enhanced requirements for reliability and safety is the hardware [1, 13] and software [2] of RTS of this class known as Safety Critical Systems (SCS). Special requirements are put also to the telecommunication systems, which must contain all necessary Safety related mechanisms [3, 4].

Depending on the nature of SCTP the technical solutions of SCS are subdivided into two main groups [5, 14]:

- ***Systems with fail-safe behaviour*.** This group comprises systems for which a criterion for safe post-failure behaviour may be defined. Most often, according to this

criterion the functionality of the system is restricted or the controlled process is stopped. These are interruptions of SCTP, during which the process stops and stays safely. A compulsion is created for removal of the failure and restoring operability so that the process could continue. These are known as systems with *fail-safe* behaviour, and their failures – as *safe* (*Safety*).

- ***Fault-tolerance systems*** – systems in which a desired post-failure behaviour cannot be defined [7, 12]. In aviation, aerospace transport, life support systems, etc., the nature of SCTP is such that every stopping of the process is inadmissible. They are often subject of requirements for high availability and continuity, which are most frequently achieved through ***redundancy***: structural, informational, temporal, functional, etc. [6, 8, 11]. By redundancy in this context is meant more than the necessary for the functioning of the system operable devices through which the errors and malfunctions of the elements are disguised.

For both types of systems a common criterion for belonging to SCS is the limit of the risk ensuing from possible failure. Safety standards regularize the admissible risk [1]. The standards are generally applicable, irrelevant to the technical solution of the system. The limit value of the risk is very low and may be reached with high reliability [14, 15] or through safe behaviour.

It is known that with redundancy a system can be built with randomly high pre-defined reliability. The question is, *at what price*? Certainly, with the increase of redundancy the resources and the price increase proportionally.

Subject of modeling and study in this paper is a class of computer-based systems from the second group, which have majoritarian ***fault-tolerance*** structure. Majoritarian structures are those consisting of n subsystems (building blocks, channels) with the same designation, each of which has the functionality defined for the system and its operability depends on the so-called ***quorum-function.*** The quorum digit (the correctness criterion) $k < n$ shows the number of the operable subsystems. The majoritarian system is operable when:

$$k = \left(\text{ent}\frac{n}{2} \right) + 1, \tag{1}$$

where ent is "entire part of " and

$$r = n - k \tag{2}$$

is structural redundancy.

With majoritarian structures based on the output building block (microcomputer, controller, software program) high reliability is achieved, but with n -multiple higher hardware and/or software resource. How efficient is this structural redundancy depends on how much it improves reliability. Here, the effect is marked with ξ and it is introduced as a digit showing how reliable the system is in comparison to the building block that may perform the same function.

When it comes to digital and computer-based majoritarian systems (Fig. 1), the input vector $X_i(x_1, x_2, \ldots, x_v)$ is submitted at a given moment for processing of all $\boldsymbol{n}$ building blocks. The output results are in the form of binary vectors and are compared in the majoritating device ***M*;** if $\boldsymbol{k}$ of them, $k = 1, 2, \ldots, n$, derive identical vectors $\boldsymbol{Y_i}$, the system validates the output vector $\boldsymbol{Y_i}$ as correct. It is accepted as operable and

remains operable when after failure one, two or more channels drop out until reaching the $n - k$ failure. In case of more failures the correctness criterion is breached and the majoritarian structure becomes inoperable.

With repairable systems big redundancy (when $\boldsymbol{n} > 5$) loses its meaning, because the running hours' time until failure $\mathrm{MTBF}_{k \vee n}$ (months, years) is hundreds and thousands of times greater than the recovery time of the failed unit $T_в$ (one-two hours). For this short time failures are slightly probable to occur and inoperability to be reached, which may be prevented by deeper reservation. Therefore, structures with very big redundancy are not implemented in practice, since such redundancy, apart from everything else, increases the price of reliability.

Most often $\boldsymbol{n}$ is brought down to the minimum limit of the majoritarian systems, the so-called *Triple modular redundancy* – system $2 \vee 3$, or in case of especially high requirements – system $3 \vee 5$. Therefore, the present analysis is limited within the systems $2 \vee 3$ and $3 \vee 5$.

The objective of this study is to derive mathematical models through which to quantify the influence of the redundancy contained in the structure on the reliability indicators of the system by establishing explicit dependences of the reliability enhancement on the size of redundancy.

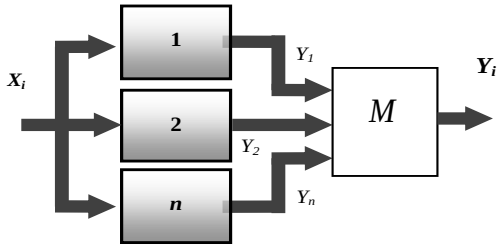

Fig. 1. Majoritarian structure

2. Summary of what is known from research literature

There are publications on modeling the reliability of majoritarian systems which allow to encompass and describe the systems characteristics [9, 10, 11]. This paper is based on known research results, and yet, it finds answers to problems of theoretical and practical significance that have not been yet investigated.

In literature, it is found the mathematical model of the reliability $P_{k \vee n}(t)$ of the studied systems depending on the probability of failure-free operation $\boldsymbol{p}$, respectively, the probability of failure $q = 1 - p$, and their structural units (they are assumed as equally reliable) [10]:

(3) $$P_{2\text{v}3}(t) = p^3 + 3p^2q,$$

(4) $$P_{3\text{v}5}(t) = p^5 + 5p^4q + 10p^3q^2,$$

where at intensity of failures $\lambda = \text{const}$ and ***t*** running hours (time) of failure $p(t) = e^{-\lambda t}$.

If calculations are made according to these formulas and graphs of dependences are drawn $P_{k \vee n}(t)$, the curves in Fig. 2 are obtained. It is evident that after a certain point t_{cr} the reliability of the system becomes smaller than that of the elements from which it is built. This is explained by the increasing influence of the large number of elements.

Depending on the average life time MTBF of the elements formulas are derived for the median time for running hours to failure MTTF_s of non-repairable systems and the median time between failures MTBF_s of repairable systems. In the context of this study attention should be paid to the results for repairable systems. It is established that in the general case the median time $\text{MTBF}_{k \vee n}$ between the failures of the system is ***"k*** from ***n"***:

$$\xi_{k \vee n} = \frac{1}{\frac{n!}{(n-k)!(k-1)!} K_{\text{a}}{}^{k-1} (1 - K_{\text{a}})^{n-k}}, \tag{5}$$

where K_{a} is the availability coefficient.

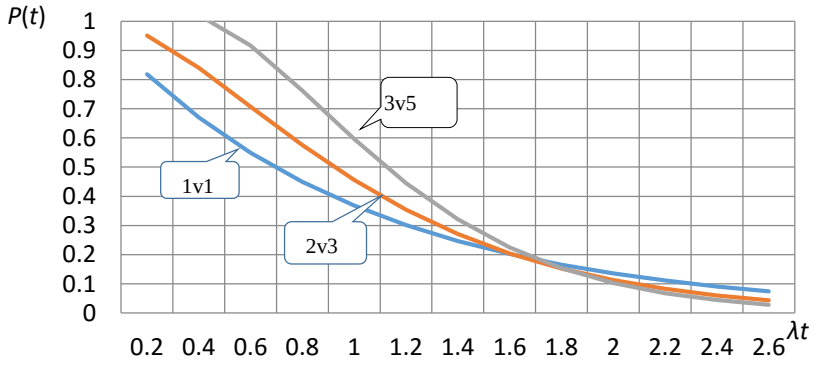

Fig. 2. Dependence of the reliability function of a majoritarian structure on redundancy upon simple majoritating

For the system $2 \vee 3$

$$\text{MTBF}_{2 \vee 3} = \frac{1}{H_{\text{s}}} = \frac{\text{MTBF}}{6K_{\text{a}}(1 - K_{\text{a}})}, \tag{6}$$

and for the system $3 \vee 5$

$$\text{MTBF}_{3 \vee 5} \frac{\text{MTBF}}{30K_{\text{a}}{}^{2}(1 - K_{\text{a}})^{2}}. \tag{7}$$

3. Effect of the structural redundancy on the system's availability

The new investigations of this paper use already established research results from previous publications of the author, as well as such by other authors.

The probability of failure-free operation ***p,*** respectively – for failure $q = 1 - p$ of the structural units of the majoritarian system is a probability for them to be in the respective state. If this probability is reviewed as availability, and after sufficient operation time, as availability coefficient K_a, the availability parameters can be substituted in (3) and (4) and the formulas for repairable systems can be obtained:

Availability of the system $2 \vee 3$ is

(8) $K_{a2v3} = K_{a2v3}^3 + 3K_a^2(1-K_a)$, respectively: $K_{a2v3} = K_a^2(3-2K_a)$.

Availability of the system $3 \vee 5$:

(9) $$K_{3v5} = K_a^5 + 5K_a^4(1-K_a) + 10K_a^3(1-K_a)^2.$$

The enhancement of the availability K_{a2v3} of the system as compared to the availability of the individual channel K_a can be established through their relationship:

(10) $$\xi_a = \frac{K_{a2\vee3}}{K_a} = \frac{K_a^2(3-2K_a)}{K_a} = K_a\left(3-2K_a\right).$$

The task to investigate the effect from the enhancement of fault tolerance is limited to studying the function (10) $\xi = f(K_a)$, shown in Fig. 3.

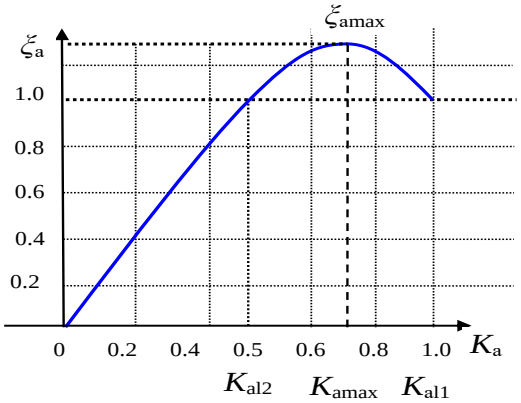

Fig. 3. Enhancement of availability through majoritating "2 of 3"

The variables in this function are probabilities and change within the range 0-1. It is evident that the effect from the fault tolerance devices (three instead of one information processing channels), depends on the availability of the individual elements. When the availability of the element, which is growing from 0, reaches a value K_{al}, the availability of the system grows and reaches that of the channel: $K_{a2v3} = K_a$, then $\xi_a = 1$. Then it continues to grow and always remains bigger

than that of the channel until reaching a maximum $\xi_{\text{a max}}$, after which it asymptotically decreases and at $K_{\text{a}} \approx 1$ it approximates 1. In order to find these characteristic points:

1. A quadratic equation obtained from the condition $\xi_{\text{a}} = 1$ is solved:

(11) $$K_{\text{a}}\left(3 - 2K_{\text{a}}\right) = 1.$$

It has roots: $K_{\text{a}11} = 1$; $K_{\text{a}12} = 0.5$.

This means that at availability $K_{\text{a}} > 0.5$ the system $2 \vee 3$ becomes more reliable than each of the channels from which it is built. At $K_{\text{a}} = 1$ it equalizes to that of absolutely reliable channel, but the availability is already 1.

2. The curve $\xi = f(K_{\text{a}})$ has a maximum that can be obtained through classical minimax method as the first differential quotient of the function (10) is equalized to zero:

(12) $$\frac{d\xi}{dK_{\text{a}}} = 3 - 4K_{\text{a}} = 0.$$

The derivation of the equation shows that the extreme of the curve will be obtained at:

(13) $$K_{\text{a ext}} = 0.75.$$

The value of enhancement under (10) at this value is

(14) $$\xi_{\text{a max}} = 1.125.$$

4. Modeling the effect of redundancy over the lifetime of majoritarian systems

It is already noted, that a comparative quantity ξ_{t} is introduced, in order to establish the effect of redundancy on the "lifetime" of the system. The comparative quantity is a digit defined as a relation of the average time $\text{MTBF}_{k \vee n}$ between the failures of the majoritarian system to the average time between the failures of its elements MTBF:

(15) $$\xi_{\text{t}} = \frac{\text{MTBF}_{k \vee n}}{\text{MTBF}}.$$

The equation (16) is obtained for the general case by substituting from (3) in (15). It shows the effect of redundancy on the lifetime of the majoritarian system, that is, the introduced enhancement:

(16) $$\xi_{tk\vee n} = \frac{1}{\binom{n}{k} k K_a^{\,k-1} (1-K_a)^{n-k}}.$$

Applied to the system $2 \vee 3$, this formula is reduced to:

(17) $$\xi_{t2\vee3} = \frac{1}{6K_a(1-K_a)}.$$

For the system $3 \vee 5$:

(18) $$\xi_{t3\vee5} = \frac{1}{30K_a^{\,2}(1-K_a)^2}.$$

Let us study the functions $\xi_{2\vee3}(K_a)$ and $\xi_{3\vee5}(K_a)$.

4.1. Study of $\xi_{2\vee3}(K_a)$

If the analytical expression of the enhancement of lifetime (17) is studied with the methods of mathematical analysis, it will be established that $\xi_{t2\vee3}(K_a)$ decreases with the availability coefficient K_a of the elements from which the system is created. It is evident that the function is extreme: it has a minimum at a critical value of the availability coefficient of the element $K_{a\ cr}$ and values $\xi_{t2\vee3} \to \infty$, when $K_a \to 1$ and $K_a \to 0$. In addition, at other two characteristic values of availability $(K_{ar1}$ and $K_{ar2})$ enhancement is nullified $(\xi_{t2\vee3} = 1)$, which means that the lifetime of the system is equalized to that of the element.

4.2. Determination of K_{acr}

In order to find the critical lowest value of availability K_{acr}, equation (17) should be studied following the minimax method for determination of extreme. Easier, and yet equivalent, is the derivation through annulling the first differential quotient of the function in the denominator $6K_a(1-K_a)$:

$\frac{d\left(6K_a(1-K_a)\right)}{dK_a} = 0$, $(1-K_a) - K_a = 0$. $K_{acr2\vee3} = 0.5$ is obtained.

The function $\xi_{t2\vee3}(K_a)$ is graphically interpreted in Fig. 4. In case of high reliability of the structural unit $K_a \approx 1$ it has a very high value $\xi_{t2\vee3} \to \infty$. At $K_a = 0.5$ the relation reaches its minimal value $\xi_{t2\vee3} = 0.666$ and again grows symmetrically relative to this minimal point. Due to the small values of the

availability $K_a < 0.5$, which are not often found in practice, the curve is not of practical interest in its subsequent course.

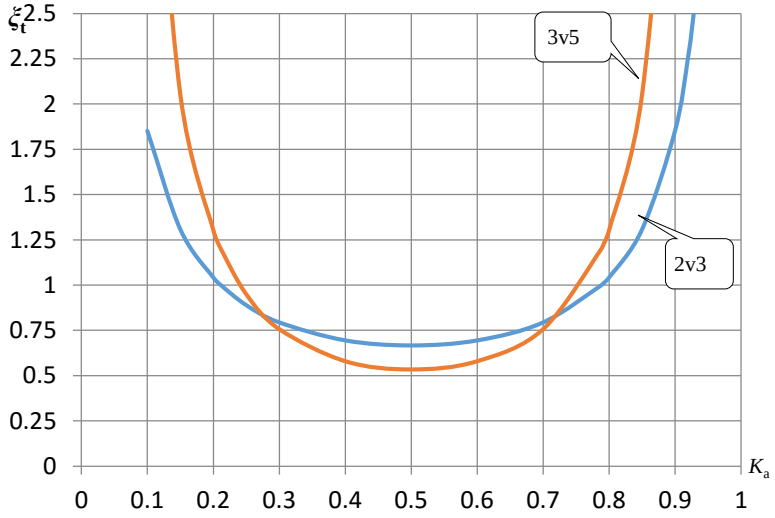

Fig. 4. Increase of the lifetime of the majoritarian system depending on the availability of structurally building element

The strongest effect of the redundancy, hundreds of thousands of times "longer life", is obtained at values closer to 1, i.e., at very high availability of the building element. Since with the linear scale on Fig. 4 this cannot be accounted, on Fig. 5 this part of the curves is shown in decimal logarithmic scale, in which $\xi_{t2\vee3}(K_a)$ becomes almost linear dependence with a slant increasing pro rata to the majoritarian threshold k.

4.3. Determination of K_{ar1} and K_{ar2}

The effect of the redundancy $\xi_{2\vee3} = 1$ is zero when in equation (17) $6K_a(1-K_a) = 1$ is put. This is the condition under which $\mathrm{MTBF}_{2\vee3} = \mathrm{MTBF}$. The values of availability when this condition is fulfilled can be found. The expression is reduced to the quadratic equation:

(19) $$6K_a^2 - 6K_a + 1 = 0,$$

the roots of which are: $K_{ar1} = 0.789$ and $K_{ar2} = 0.211$. At these values median time is reached between the failures of the system equaling that of the elements: $\mathrm{MTBF}_{2\vee3} = \mathrm{MTBF}$.

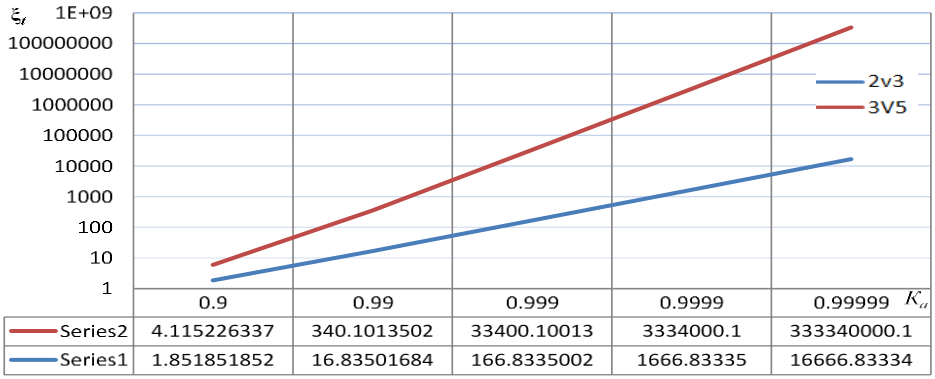

Fig. 5. $\xi_{t2\vee3}(K_a)$ in logarithmic scale

The enhancement is $\xi_{t2\vee3}=166$ at values of the availability typical for computer-based structural elements K_a = 0.999, i.e., by such number of times longer life. Enhancement also drops abruptly irrespective of this very strong effect of enhancement at high reliability, when availability decreases. Enhancement is the lowest at the critical value $K_{a\,cr}$.

5. Study of system $3\vee5$

The study of $\xi_{t3\vee5}(K_a)$ is performed following the same order.

5.1. Determination of $K_{a\,cr}$

The extreme points of the denominator of (18) are sought,

$$\frac{d\left(30K_a^{\,2}(1-K_a)^2\right)}{dK_a}=0,$$

$$30.2K_a(1-K_a)^2-30K_a^{\,2}2.(1-K_a)=0;\;\;(1-K_a)-K_a=0,$$

$$K_{a\,cr3\vee5}=0.5. \tag{20}$$

That is, the critical point is at the same value of the availability. By substituting in (18) we find that the minimum point, which the relation will reach, is

$$\xi_{t3\vee5}=0.533.$$

5.2. Determination of the critical points

An equation of the fourth degree is derived:

$$30K_a^{\,2}(1-2K_a+K_a^{\,2})-1=0,$$

Only the roots of the quadratic equation are of interest:

$$K_a^{\,4}-60K_a^{\,3}+30K_a^{\,2}-1=0.$$

They are: $K_{ar1} = 0.2111$, $K_{ar2} = 0.7889$. The other two roots are imaginary.

Based on the performed investigations, it is evident that both majoritarian systems have one and the same qualities and do not differ in principle. By increasing the redundancy from $2 \vee 3$ to $3 \vee 5$ particular characteristics are strengthened: the effect of enhancement grows, but only at the high values of the reliability of the building component, whereas at low values it deteriorates below that of $2 \vee 3$.

6. Inferences

1. The smaller the availability of the element is, the weaker the effect of the redundancy will be. At small values of the availability of the building element the reliability of the system decreases and becomes lower than the latter. At $K_a = 0.5$ such result is reached that system $2 \vee 3$ becomes more efficient than system $3 \vee 5$.

2. At high availability coefficient $K_a = 0.9999$ the lifetime of a majoritarian system as compared to that of its building components is increased by several orders: for $\xi_{t2 \vee 3} = 1666.8$, $\xi_{t3 \vee 5} = 3\ 334\ 000$.

7. Conclusion

Result of the conducted research is the analysis of the effect of structural redundancy in majoritarian systems, which have been established. Some new dependences are studied, which allow for drawing the conclusion that majoritarian systems have substantial effect for increasing reliability. The expenses for structural redundancy are beneficial only when the initial reliability of the building blocks constituting such systems is sufficiently high. The quantitative values of the effect allow the experts, developers, designers, specialists designing SCS of this class to optimize their solutions and defend their designs.

References

1. BS EN 50126-1:1999**,** Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Basic requirements and Generic Process, BSI, ISBN 9780580717512, European Committee for Electrotechnical Standardization, 1999.
2. Standard: CENELEC – EN-50128 Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems, European Committee for Electrotechnical Standardization, Brussels, 2011.
3. Standard: CENELEC – EN 50159 Railway Applications – Communication, Signalling and Processing Systems – Safety-Related Communication in Transmission Systems, European Committee for Electrotechnical Standardization, Brussels, 2010.
4. Franeková, M., P. Lüley. Modelling of Failure Effects within Safety-Related Communications with Safety Code for Railway Applications, Mechanic, Transport, Communication, Art. ID 1213, VII 27 – VII 34, 2015.
5. Hristov, H., W. Bo. Safety Critical Computer Systems: Failure Independence and Software Diversity Effects on Reliability of Dual Channel Structures. – Information Technologies and Control, 2014, No 2, pp. 9-18.

6. L e e, P. A., T. A n d e r s o n. Fault Tolerance: Principles and Practice. – Springer Science & Business Media, 2012, pp. 51-62.
7. L i, Z., J. T i a n, P. Z h a o. Software Reliability Estimate with Duplicated Components Based on Connection Structure. – Cybernetics and Information Technologies, Vol. **14**, 2014, No 3.
8. D u b r o v a**,** E. Fault-Tolerant Design. New York, Springer Verlag, 2013, DOI 10.1007/978-1-4614-2113-9.
9. S h e, X., K. S. M c E l v a i n. Time Multiplexed Triple Modular Redundancy for Single Event Upset Mitigation. – IEEE Transactions on Nuclear Science, 2009.
10. H r i s t o v, H., G. P o p o v, M. H r i s t o v a. Comparative Reliability Analysis for Fault-Tolerant Microprocessor Structures. – In: Proc. of 2nd International Scientific Conference "Computer Science", Greece, 2005, pp. 48-53.
11. H r i s t o v, H., M. H r i s t o v a. Modeling Reliability of Fault Tolerant Systems with Homogeneous Reservation. – Sci. J. Mechanics, Transport, Communications, Vol. **1**, 2013, No 3, art. 0862, ISSN 1312-3823.
12. K o r e n, I., C. M. K r i s h n a. Fault-Tolerant Systems. San Francisco, CA, USA, Morgan Kaufmann Publishers, Inc., ©2007, ISBN:0120885255.
13. P r a d h a n, D. K. Fault-Tolerant Computer. Prentice Hall, 1996, ISBN:0-13-057887-8.
14. S h o o m a n, M. L. Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design. by John Wiley & Sons, Inc., 2002, pp 83-144, ISBN: 9780471293422.
15. L i, W., Z. L i u , X. J i n, Y. S h i. Reliability Estimation Based on the Degradation Amount Distribution Using Composite Time Series Analysis. – Cybernetics and Information Technologies, Vol. **13**, 2013, No 3.