Makes the Periodic Test the Systems Safety

Tashko A. Nikolov[1], Nikoleta H. Hristova[2]

Abstract - **The paper present the influence of several tests in the fault-tolerant control systems - absolute, relative and complete periodic tests, on the system reliability and safety. On the basis of some Markovian modelling techniques are offered generalised formula for obtaining the maximum safe period between system tests. On the one hand they avoid unnecessary over dimensioning and the resulting high manufacturing costs, while on the other hand it demonstrates a method of optimum distribution of the resource of the different tests in the fault-tolerant systems. Besides, it provides opportunities for additional comparative analysis of the different fail-safe and fault-tolerant structures.**

Keywords - **testing; failure detection; Markovian modelling**

I. Introduction

Stringent requirements on reliability and safety have been introduced for many technological processes in the fields of nuclear power, transport, space systems, chemical and other industries. These requirements affect the control systems as early in as design and development phase. They must take into account the growing requirements of the users, reflecting on their functionality and also they must be in line with the safety norms of the respective branch, national or international administrations. In many cases the safety requirements are determined in terms of the probability or mean time of a particular undesirable event occurrence.

The failure detection means in particular computer systems comprise three types of tests - *absolute, relative* and complete *periodic* ones [1, 8]. Let us assume that the failure detection facility in the three types of tests is *a, r* and *p*, respectively.

The absolute test has to detect failures for a period shorter than the system reaction time. The failure detection facility *a* of the absolute test is the probability of detecting the failure before the output of the result $(0 \le a \le 1)$.

The relative test consists of comparing two or more results from independent processing. The efficiency of the comparison r $(0 \le r \le 1)$ depends on the number of the compared information vectors N and on the dimensionality of these vectors n. If N=2, the probability of a wrong result obtaining is [8]:

$$(1-r) = (2^n - 1)/2^{2n} \qquad (1)$$

where: *n* is the length (in bits) of the output vector

In case of N=3, i.e. triple modular redundancy system (TMR), the probability for obtaining of two or three equivalent results is: $3\{1 \times (1/2^n) \times [(2^n - 1)/2^n]\}$ and $1 \times (1/2^n) \times (1/2^n)$ respectively.

The periodic test is a complete test of the system. It can be carried out both off-line (e.g. once a day, week or year) and on-line. In either case we can speak of a cycle of periodic test with duration T_{pt}. The failure detection facility *p* of the periodic test is the probability of failure detection at the complete testing (self testing) of the system $(0 \le p \le 1)$.

The purpose of the paper is to be established the requirements of the three types of test in order to be satisfied the safety criteria. The equations have to be valid for any kind of systems regardless of the number of redundant units and the used tests.

II. Modelling technique

When the system reaction after occurrence of a failure is in accordance with an adopted criterion of after-failure behaviour, the failure is considered to be *safe* [3, 4, 10], otherwise it is considered to be *dangerous.* The dangerous failure rate is marked by λ_d, the safety failure rate is marked by λ_s. Obviously, $\lambda_s + \lambda_d = \lambda$

Since normally the cycle of the periodic test is longer than the system reaction time we believe that a dangerous failure of the system appears after a failure has not been detected by the absolute and relative tests

$$\lambda_d = (1-a)(1-r)\lambda \qquad (2)$$

This, in a certain sense, is a worst-case assumption, because a new chance is given to the absolute and relative tests by the change of the information status [8].

Fig. 1 shows the model, described in [8]. From a dangerous state the system may be brought only into safety state with transition rate α. Consequently, an occurred dangerous failure can be detected only by the periodic test. Then for the restoration rate from a dangerous state we obtain:

$$\alpha = p / T_{pt} \qquad (3)$$

The probability for staying in each state is [2, 6]:

$$P_1 = \frac{\alpha\mu}{\mu(\alpha + \lambda_d) + \alpha\lambda} \qquad (4)$$

$$P_2 = \frac{\lambda_d \mu}{\mu(\alpha + \lambda_d) + \alpha\lambda} \qquad (5)$$

$$P_3 = \frac{\alpha\lambda}{\mu(\alpha + \lambda_d) + \alpha\lambda} \qquad (6)$$

[1] Tashko Nikolov is with Telecom Department at Technical University of Sofia, “Kliment Ohridsky” Blvd 8, 1756 Sofia, Bulgaria, E-mail: tan@tu-sofia.bg

[2] Nikoleta Hristova is with Telecom Department at Technical University of Sofia, “Kliment Ohridsky” Blvd 8, 1756 Sofia, Bulgaria, E-mail: nhh@tu-sofia.bg

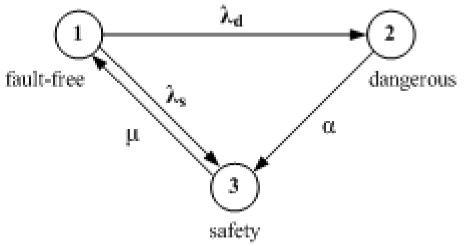

Fig. 1. Markovian graph of an element from the control system

In the model of safety control system the numbering of the states is rendered by an *N* numerical code, where *N* is the number of the modelling units. Each digit from this code can take one of the following values: 1, 2 or 3, which correspond to failure-free, dangerous and safety states of the element [6, 7, 2]. The transition rates in the graph can exist only between states whose codes differ in only one digit. That means the condition of ordinariness is being observed, e.g. in the time interval $(t, t+\Delta t)$ it is possible only one event to be realised.

The following Markovian graph (Fig. 2.) is obtained at a system consisting of two elements (e.g. 2-out-of-2 system) each described by a graph from Fig. 1.

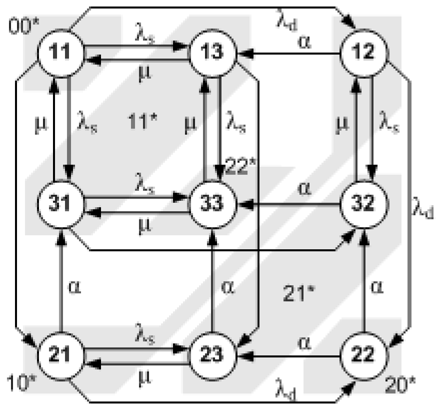

Fig. 2. Markovian graph of a 2-out-of-2 system

The probability for staying in any state is obtained by:

$$P_{a_s b_s c_s} = P_{a_s} \times P_{b_s} \times \ldots \times P_{k_s} \qquad (7)$$

where:

a, b,...,k are the numbers of the elements

$s \in \{1,2,3\}$ are the numbers of the states: failure-free, danger and safety.

Reducing this graph according to [5], on the principle of number of failures occurred - number of failures detected, we obtain the so-called "impersonified" model. Here the numbering of the states is presented by a two-digit code, the first digit showing the number of failures that have occurred, the second showing how many have been detected [2]. The model is called "impersonified" because there is no information about the certain failed element. However, this is of no significance in the case when systems of static redundancy with identical reserved elements are investigated. All indicators of the "impersonified" graphs are marked by *.

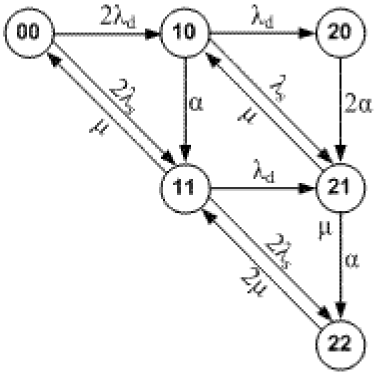

Fig. 3. "Impersonified" Markovian graph of a 2-out-of-2 system

$$\begin{aligned}
a^*_{00,10} &= \left[P_{11}(\lambda_d + \lambda_d)\right] / P_{11} = 2\lambda_d \\
a^*_{00,11} &= \left[P_{11}(\lambda_s + \lambda_s)\right] / P_{11} = 2\lambda_s \\
a^*_{11,00} &= \left[P_{13}(\mu + \mu)\right] / \left(P_{13} + P_{13}\right) = \mu \\
a^*_{22,11} &= \left[P_{22}(\mu + \mu)\right] / P_{22} = 2\mu
\end{aligned} \qquad (8)$$

The probabilities for staying in the separate states are:

$$\begin{aligned}
P^*_{00} &= P_{11} = P_{a_1}P_{b_1} = P_1^2 \\
P^*_{10} &= P_{12} + P_{21} = P_{a_1}P_{b_2} + P_{a_2}P_{b_1} = 2P_1P_2 \\
P^*_{11} &= P_{13} + P_{31} = P_{a_1}P_{b_3} + P_{a_3}P_{b_1} = 2P_1P_3 \\
P^*_{21} &= P_{23} + P_{32} = P_{a_2}P_{b_3} + P_{a_3}P_{b_2} = 2P_2P_3 \\
P^*_{22} &= P_{33} = P_{a_3}P_{b_3} = P_3^2
\end{aligned} \qquad (9)$$

When the system has at least one detected failure, it is in a safety state. Consequently, states 11, 21 and 22 are of the safety type. When unidentified failures emerge in both elements, there is no right result criterion and that is why state 20 is considered to be dangerous, while states 00 and 10 are considered as failure-free.

The graph of a multi-channel system (NMR system) is shown on Fig. 4.

In general, the formula for finding the probability for staying in each state is:

$$P^*_{ij} = \frac{n!}{(n-i)!(i-j)!\,j!}\left(P_1^{n-i} P_2^{i-j} P_3^{j}\right) \qquad (10)$$

where:

n - number of elements

i - number of occurred failures

j - number of detected failures

P_1 - probability for a failure-free state of separate element

P_2 - probability for a dangerous state of separate element

P_3 - probability for a safety state of separate element

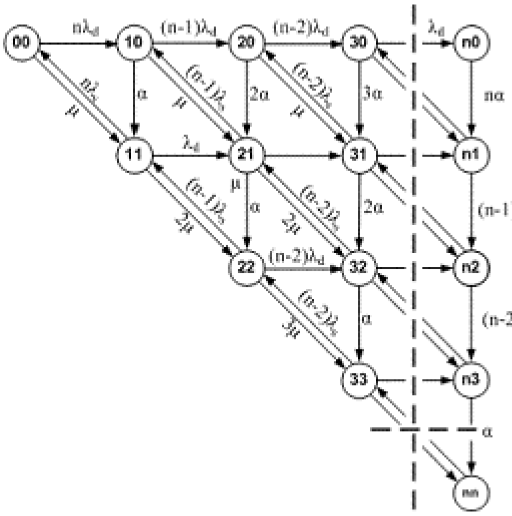

Fig. 4. "Impersonified" graph of NMR

III. Mean time for detection of an unidentified failure

The problem of finding the admissible time for the existence of an unidentified failure comprises: *Designing a periodic test of such failure detection facility p and period T_{pt} satisfying the safety criteria, e.g. probability for dangerous failure of the system.*

The time required is the reciprocal value of the sum of the transition rates going out of the dangerous state of the system, e.g. the mean time for staying in a dangerous state [6, 5].

System 2-out-of-2 (NMR; N=2)

The dangerous state of the 2-out-of-2 System is 20, with probability $P_{20}^{*} = P_2^2$. Corresponding to Eq. (9) from Eq. (5) is obtained:

$$\alpha = \frac{\lambda_d \mu (1-P_2)}{P_2(\lambda+\mu)} \tag{11}$$

$$T_d = 1/\alpha = \frac{P_2(\lambda+\mu)}{\lambda_d \mu (1-P_2)} \tag{12}$$

where: T_d is the mean time for staying in a dangerous state.

The problem may be reduced to the evaluation of the mean time for staying in a dangerous state (T_d=1/α) as a function of probability for a dangerous failure of the individual element P_2, while in its turn P_2 may be presented as a function of the probability for dangerous failure of the system Q_d. That leads to obtaining implicitly the dependence $\alpha = f(Q_d)$ for various types of systems (e.g. N=1,2,3,...).

This makes possible:

1. Simplification of the problem for more complex systems (NMR, N>2).
2. Formulation of requirements both on the parameters of the periodic control and on the safety of the individual elements.

The analytical investigation of the dependencies for 2-out-of-2 is shown on Fig. 4., where Q_{dav} is the dangerous acceptable value.

System 2-out-of-3 (TMR)

We have a dangerous failure in TMR system when the difference between the number of the occurred failures and those that have been detected is larger or equal to two. Then the dangerous states are 20, 30 and 31. Consequently, for the probability of a dangerous failure we obtain:

$$Q_d = P_{20}^{*} + P_{30}^{*} + P_{31}^{*} \tag{13}$$

$$Q_d = 3P_1P_2^2 + P_2^3 + 3P_2^2P_3 \tag{14}$$

$$Q_d = P_2^2(3-2P_2) \tag{15}$$

$$2P_2^3 - 3P_2^2 + Q_d = 0 \tag{16}$$

The solution of Eq. (16) constitutes the formation of the criterion for safety for the individual elements of the general safety criterion for the system.

Three real roots are obtained in such a case, two of which are identical [10]. The results are graphically shown on Fig. 4.

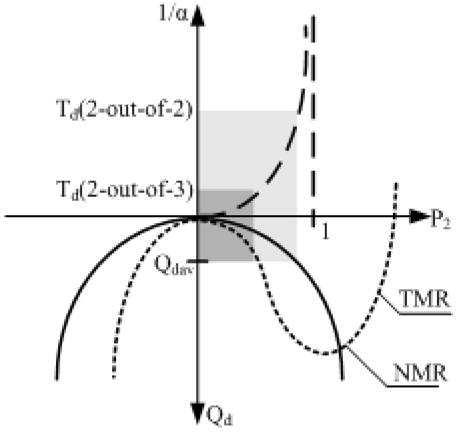

Fig. 4. Dependence between the mean time of staying in a dangerous state and the probability for dangerous failure by TMR

From Eq. (5) it is possible to be obtained certain dependence (Fig. 5.) between the three types of failure detection means – absolute test, relative test and complete periodic test. One may recognise easily that the absolute and relative tests are not present (e.g. *a=0* and *r=0*), there is a determined value *A* for the time duration of the periodic complete test, by which the safety norm can be observed.

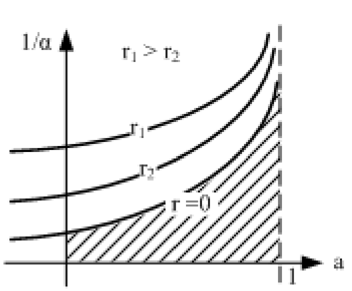

Fig. 5. Dependence between the time duration of the periodic test and the failure detection facility of the absolute and relative tests

$$1/\alpha_{(a=0)} = \frac{P_2(\lambda+\mu)}{(1-r)(1-P_2)\lambda\mu} \tag{17}$$

When $a = 0$ and $r = 0$ we obtain the following:

$$A = \frac{P_2(\lambda+\mu)}{(1-P_2)\lambda\mu} = \frac{P_2}{P_1(1-P_2)\lambda} \tag{18}$$

IV. Examples

Example 1.

A 2-out-of-2 system with the following indicators of the individual elements is given:

- Failure rate - $\lambda = 10^{-5}$ h^{-1}
- Repair rate - $\mu = 1$ h^{-1}
- Failure detection facility of the absolute test - $a = 0.5$
- Failure detection facility of the periodic test - $p = 0.95$
- Compared information vectors - $N = 2$
- Order of the compared vectors - n =8 bits
- Safety norm of the system - $Q_{dav} = 10^{-12}$

The maximum admissible time for detecting a hidden failure is required.

Procedure:

Step 1.: Calculation of the failure detection facility of the relative test from Eq. (1):

$$r = 1 - \frac{2^n - 1}{2^{2n}} = 1 - \frac{2^8 - 1}{2^{16}} = 0.9961$$

Step 2.: Calculation of the dangerous failure rate from Eq. (2):

$$\lambda_d = (1-a)(1-r)\lambda = 1.95 \times 10^{-8}, h^{-1}$$

Example 2.

A TMR system each element of which has the same parameters as in Example 1 is given. The maximum admissible time for the detection of a hidden failure is also required.

Procedure

Step 1: Calculation the failure detection facility of the absolute test from Eq. (3):

$$r = 1 - \frac{(2^n - 1)(3 \times 2^n - 2)}{2^{2n}} = 0.9884$$

Step 2: Calculation the dangerous failure rate from Eq. (8)

$$\lambda_d = (1-a)(1-r)\lambda = 5.28 \times 10^{-8}, h^{-1}$$

Step 3: Calculation the probability P_2 for a dangerous failure by each element depending on the safety criterion Eq. (16):

$$Q_d = (3 - 2P_2)P_2^2 = 10^{-12}$$

$$P_2 = 5.75 \times 10^{-7}$$

Step 4: Calculation the mean time T_d for staying in a dangerous state depending on Eq. (12):

$$T_d = 1/\alpha = \frac{P_2(\lambda+\mu)}{\lambda_d \mu (1-P_2)} = 9.9, h$$

Step 5.: Determination the maximum duration of the periodic system test from Eq. (3):

$$T_{pt} = p/\alpha = 0.95 \times 9.9 = 9.4, h$$

Table I. shows results about the maximum duration in dangerous state of the system for the two types of systems depending on the dimensionallity of the information vector. All other conditions are the same.

TABLE I

Dependence of the T_D on the dimensionallity

***n*,bit**	**4**	**5**	**6**	**7**	**8**	**…**	**16**
***T*$_d$(*N*=2),h**	3.33	6.66	13.3	25	51.3	…	13333
***T*$_d$(*N*=3),h**	0.68	1.28	2.5	4.8	9.9	…	2555

V. Conclusion

On the basis of some Markovian modelling techniques are offered generalised formula for obtaining the maximum safe period between system tests. On the one hand they avoid unnecessary over dimensioning and the resulting high manufacturing costs, while on the other hand they avoid unnecessary over dimensioning and the resulting high manufacturing costs, while on the other hand it demonstrates a method of optimum distribution of the resource of the different tests in the fault-tolerant systems. Besides, it provides opportunities for additional comparative analysis of the different fail-safe and fault-tolerant structures. The dependencies shown in the paper between the value of the safety norm and the time parameters of the failure detection means could be applied in many practical cases. This dependence may be used not only for analysis of fault-tolerant computer systems (e.g. aeroplanes, nuclear power plants etc.)

References

[1] Görke,W., *Fehlertolerante Rechensysteme*, Oldenburg Verlag München Wien, 1989

[2] Johnson,B.W., *Design and Analysis of Fault Tolerant Digital Systems*, Addison-Wesley Publishing, 1989.

[3] Redmil, F.J., *Dependability of critical computes systems*, Elsevier Applied Science, 1988 Part 1; 1989 Part 2.

[4] Bishop, P.G., *Dependability of critical computes systems*, Elsevier Applied Science, 1990 Part 3.

[5] Kochs, H.-D., *Zuverlässigkeit elektronischer Anlagen*, Springer, Berlin, 1984.

[6] Kuo W., Zuo M., *Optimal Reliability Modelling*, John Wiley&Sons, 2003.

[7] Nikolov,T., *Investigating the safety of control systems*, Dissertation, Technical University of Sofia, 1991.

[8] Echtle,K., B.Hinz, T.Nikolov, Hardware Fault Detection by Diverse Software, Hardware and Software Fault Tolerance in Parallel Computing Systems, ELLIS HORWOOD, London, 1992, pp.313-326

[9] Bronstein,I.N., K.A.Semendjajew, Taschenbuch der Mathematik, Verlag Harri Deutsch.

[10] Laprie, J.C., (ed.), Dependability: basic conceptsand terminology in English, French, German, Italian and Japenese, Wien, Springer, 1992