Average Probability of Failure of Aperiodically Operated Devices

Krisztián Lamár, József Neszveda

Óbuda University, Kandó Kálmán Faculty of Electrical Engineering
Bécsi út 96/B, 1034 Budapest, Hungary
lamar.krisztian@kvk.uni-obuda.hu, neszveda.jozsef@kvk.uni-obuda.hu

Abstract: The aperiodically operated devices are typically non-operated or stored, usually in a powered-down state. The duration of being operated is much shorter than that of storage. These devices have to perform extremely reliably during usage, while the operation usually occurs under circumstances worse than the average. This paper proposes a calculation procedure of value jumps of failure rate caused by operating condition shifts, to determine the average probability of failure, based on the standards IEC 61511 and ANSI/ISA-84. In the suggested calculation method, a proposal is also made for taking the failure caused by the human factor during operation into account. It is known that the probability of successful operation is increasable with periodic diagnostic tests. The circumstances of diagnostic tests which interrupt the non-operated storage of the aperiodically operated devices differ from those described in the standards IEC 61511 and ANSI/ISA-84. As the repair rate given for the continuous technologies cannot be interpreted for diagnostic tests which interrupt the powered-down storage of the aperiodically operated devices, this paper suggests the implementation of the effect of tests into the calculation procedure as correction of state probabilities, and gives the required formulae. At last the article provides an easy algorithm for the suggested calculation method.

Keywords: Aperiodic Operation, Average Probability of Failure, Value Jumps of Failure Rate, Diagnostic Coverage, Reliability

1 Introduction

The standards IEC 61511 [1] and ANSI/ISA-84 [2] define the concepts of the safety integrity level (SIL) of the basic continuous technologies and their emergency/protective systems, thus enable the specialised authorities to determine or verify the reliability levels of devices and technologies.

The military and the disaster management use numerous devices containing electrical and mechanical components which are operated intermittently and are

stored powered down between two consecutive usages. The devices have to operate in continuous mode and extremely reliably during usage. In certain industries, such as manufacturing catalyst substances for the chemical industry, this kind of operation is also present, although in those cases the increased reliability is justified by the high expenses caused by failures. The intermittently operated, powered-down stored devices, technologies – furthermore aperiodically operated devices – have three distinguished operating conditions. These are:

- Mission period. The particularity of this condition is being relatively short (10–20 hours), and that the device or technology is operated in continuous mode. The devices of the military and the disaster management are often exposed to extreme strains (moving vehicle, outdoor operation) in this operating condition.
- Periodic diagnostic test. The particularity of this condition is being relatively short (less than 10 hours). The device or technology is operated similar to indoor continuous manufacturing technologies.
- Powered-down storage. In this condition, the operation of devices is somewhat similar to the emergency/protective devices as it is in standstill. On the other hand it differs, as the emergency/protective devices operate armed (in a standby condition), contrary to the aperiodically operated devices that do not function at all, thus their failures cannot be detected in this condition.

The aperiodic operation has numerous particularities that are not defined by the standards IEC 61511 and ANSI/ISA-84. The probability of failure values are various in different conditions. The duration of repairing the failures revealed by diagnostic tests which interrupt the powered-down storage state are not critical. It is practical to take the failure caused by the human factor into account during the mission period of the devices used by the military and the disaster management. The aim of this paper is to give a new investigation method that is in conform with the international standards and also takes the particularities of the aperiodic operation into account.

2 Average Probability of Failure

The standard IEC61511 has been worked out for continuous technologies. The continuous technologies can be split into high demand basic control and low demand emergency/protective control, based on the frequency of operation. The standard IEC 61511 separates strictly the concepts of the safety integrity level of the basic continuous technologies and their emergency/protective systems, and discusses them in two different time scales.

In low demand mode the failure appears when its operation is demanded. The probability of failure on demand (PFD [year^{-1}]) is the probability of the emergency system not working in accordance with standards in a potentially dangerous situation. The average probability of failure on demand is determined by the formula below, where "TI" stands for the period between the proof tests, which are the general overhauls of an device or technology in practice

$$PFD_{avg} = \frac{1}{TI}\int_0^{TI} PFD(t)dt \tag{1}$$

It occurs that the failure of the emergency/protective system indicates a spurious dangerous situation and this produces an unwanted safety operation that causes the spurious shutdown of the device. The probability of such shutdowns is called probability of failure to safety (PFS [year^{-1}]). The average probability of spurious shutdowns is:

$$PF_{avg}^{spurious} = \frac{1}{TI}\int_0^{TI} PFS(t)dt \tag{2}$$

In high demand mode the devices are observed and taken care of continuously by operative personnel. In these cases the measure of reliability is the average of the probability of dangerous failures (PF_D [h^{-1}]).

$$PF_{Davg} = \frac{1}{T}\int_0^{T} PF_D(t)dt \tag{3}$$

The nature of aperiodically operated devices is that failures are critical only during the mission period, however, in those cases any kind of shutdown can be fatal therefore it is not adequate to take only dangerous failures and emergency shutdowns into consideration. This end, contrary to standard IEC 61511, the PF_{avg}^{sum} value should be calculated, which gives the average PF of every failure causing shutdown, during the T mission period starting from T_B moment for devices. Until T_B moment the devices were stored and interrupted with diagnostic tests.

$$PF_{avg}^{sum} = \frac{1}{T}\int_{T_B}^{T_B+T} PF(t)dt \tag{4}$$

3 Handling the Operating Condition Shifts

Currently there are internationally approved, standardised reliability calculation methods for the continuously operated and the emergency/protective devices and

technologies. Their principal [3] is that the λ failure rate is constant during operation. It is also common that the distribution of probability of failure (PF) is considered exponential [4].

$$PF(t) = 1 - e^{-\lambda t} \tag{5}$$

The λ failure rate of aperiodically operated devices and technologies varies in different operating conditions. FARADIP [5] database includes the probability of failure values for devices, subassemblies and components. According to the database the benchmark is the failure rate of devices installed indoor steadily, lacking any harmful vibration and temperature fluctuation, thus its coefficient is 1. The failure rate of inactive or powered-down storage condition is $\lambda_S = C_S \cdot \lambda$, where $C_S = 0.1$, as for the lack of mechanical and thermal effects decreases the λ failure rate, assuming that the storage is professional and the powered-down condition is shorter than one year. The failure rate of active devices used for outdoor and/or moving applications is $\lambda_A = C_A \cdot \lambda$, where $C_A = 4$.

The three operating conditions of aperiodically operated devices correspond with the classifications above. In figure 1.a, the probabilities of failure of individual operating conditions are shown; in figure 1.b the failure rate jumps can be seen with distorted time scale. Subscript "A" stands for the active operation of the mission period hereafter.

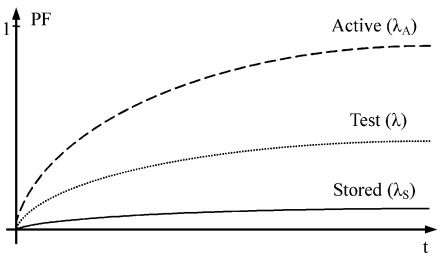

Figure 1a
Probability of failure of operating conditions

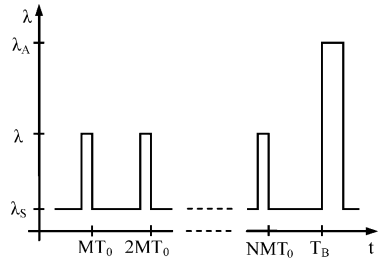

Figure 1b
Failure rate jumps

During mission period, the device can be investigated with any calculation method [3] developed for continuous technologies.

"T_0" is a time base small enough that the time-discrete calculation of formula (4) results in a reasonably low error. "N" is the number of tests, and "n" is the ordinal number of the actual test. "MT_0" is the duration of non-operated condition between two tests (including the test itself), and "m" is the m^{th} interval of this period. "QT_0" is the duration between the last test and the beginning of the mission, and "q" is the q^{th} interval of this period. "KT_0" is the mission period, and

"k" is the k^{th} interval of this period. Finally, $T_B = N \cdot M \cdot T_0 + Q \cdot T_0$ stands for the time elapsed until the beginning of the mission period. Now, formula (4) can be rewritten in time-discrete form:

$$PF_{avg}^{sum} = \frac{\sum_{k=N \cdot M+Q}^{N \cdot M+Q+K} PF(k \cdot T_0)}{K+1} \tag{6}$$

For the correct determination of formula (6), it is necessary to calculate the initial probability of failure value $PF(N \cdot M \cdot T_0 + Q \cdot T_0)$.

The methods developed for continuous technologies are not able to take the effect of storage into account. When calculating the initial probability of failure the multiple jumps of λ failure rate during this period have to be minded. It also has to be taken into account that the repairing of failures revealed by diagnostic tests increase the probability of successful operation. From among the calculation methods of reliability, it is the Markov analysis that allows the temporal changes of λ failure rate to be calculated with [3]. The jumps of the λ failure rate can be handled with a time-discrete calculation method.

The Markov model is a graph (Figure 2). Its nodes represent the states of the system and its edges represent the probability of transition from one state to another at the end of the next T_0 period. The Markov model of 1oo2D structure of control systems [6] – which are efficient for both dangerous and safe failures – includes six states considering failures.

An aperiodically operating device with a 1oo2D control structure can get from faultless operation (1) into reduced (faulty yet operable) states (2), (3), (4), (5) or shutdown due to a failure (6). Based on the nature of failures [1], failure states are distinguished as safe and detected (SD), dangerous and detected (DD), safe but undetected (SU) finally dangerous and undetected (DU) ones.

The $\lambda_{x,y}$ failure rate, corresponding with the given state (x), defines the probability of transition into another state (y). The model shown in Figure 2 considers every shutdown by any reason dangerous, therefore the system can get into shutdown (6) from any reduced failure state or from the faultless state equally. The probability of transition into a yet operable failure state has to be taken into account with double coefficient because of the dual redundancy.

The model shown in Figure 2 does not include the μ repair rate defined by the standards [1] and [2], which in fact can be integrated into the Markov model easily. The reason is that the mission period of aperiodically operated devices is short and the operation often takes place on a previously unknown site, therefore it is assumed that during mission period, there is no chance or time to repair the device.

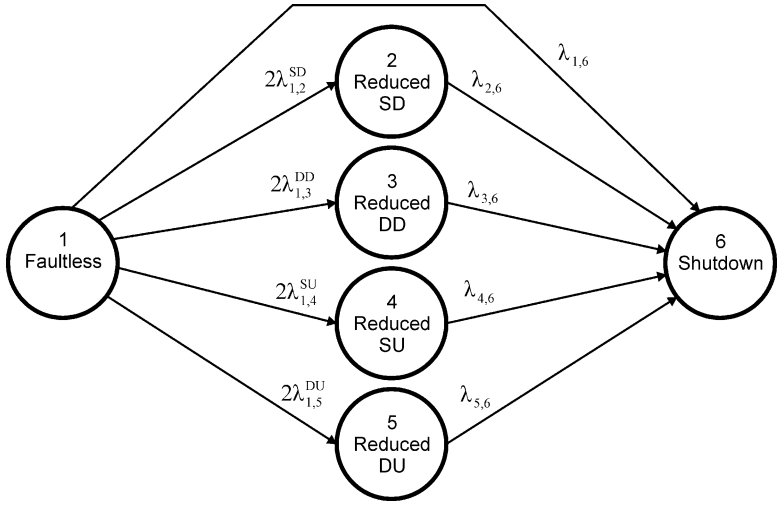

Figure 2
The simplified (contracted) Markov model of the 1oo2D structure

If the λ failure rate is constant, the **S** vector of state probabilities at the (iT_0) moment is:

$$\mathbf{S}(iT_0) = \mathbf{S}(T_0) \cdot \mathbf{T}^{i-1} \tag{7}$$

where $\mathbf{S}(T_0)$ is the first row of the **T** transition probability matrix, which can be written based on Figure 2.:

$$T = \begin{vmatrix} 1-\sum_{j=2}^{6}\lambda_{1,j} & 2\lambda_{1,2}^{SD} & 2\lambda_{1,3}^{DD} & 2\lambda_{1,4}^{SU} & 2\lambda_{1,5}^{DU} & \lambda_{1,6} \\ 0 & 1-\lambda_{2,6} & 0 & 0 & 0 & \lambda_{2,6} \\ 0 & 0 & 1-\lambda_{3,6} & 0 & 0 & \lambda_{3,6} \\ 0 & 0 & 0 & 1-\lambda_{4,6} & 0 & \lambda_{4,6} \\ 0 & 0 & 0 & 0 & 1-\lambda_{5,6} & \lambda_{5,6} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} \tag{8}$$

In case the device's $\mathbf{S}((i-1)T_0)$ state probabilities at the preceding $(i-1)T_0$ moment are known the recursive formula below may be applied instead of formula (7).

$$\mathbf{S}(iT_0) = \mathbf{S}((i-1)T_0) \cdot \mathbf{T} \tag{9}$$

The jumps of λ failure rate can be taken into account with constant coefficients $\lambda_S = C_S \cdot \lambda$ and $\lambda_A = C_A \cdot \lambda$ (Figure 1.b). $\mathbf{T}_S$ shall stand for the transition probability matrix of the powered-down storage condition, $\mathbf{T}$ for test mode among normal circumstances, and $\mathbf{T}_A$ for mission period. Subtracting the **I** unit matrix from the $\mathbf{T}$ transition probability matrix yields the **P** probability of failure matrix, which consists only of λ failure rate values, therefore the **P** probability of failure matrix can be multiplied by constant values (C_S or C_A). Adding the **I** unit matrix to the $\mathbf{P}_S$ or the $\mathbf{P}_A$ probability of failure matrix after the multiplication yields the new $\mathbf{T}_S$ or $\mathbf{T}_A$ transition probability matrix.

$$\mathbf{T}_S = (\mathbf{T} - \mathbf{I}) \cdot C_S + \mathbf{I}, \text{ and } \mathbf{T}_A = (\mathbf{T} - \mathbf{I}) \cdot C_A + \mathbf{I} \tag{10.1}$$

Of course the procedure can be inverted:

$$\mathbf{T} = (\mathbf{T}_S - \mathbf{I}) \cdot \frac{1}{C_S} + \mathbf{I}, \text{ and } \mathbf{T} = (\mathbf{T}_A - \mathbf{I}) \cdot \frac{1}{C_A} + \mathbf{I} \tag{10.2}$$

If λ_S failure rate jumps to λ_A value at $(i-1)T_0$ moment, then the $C_{SA} = \frac{C_A}{C_S}$ coefficient has to be applied in order to convert the $\mathbf{T}_S$ transition probability matrix into the $\mathbf{T}_A$ transition probability matrix.

If there are three interconvertible transition probability matrices assigned to the three operation conditions of the aperiodically operated devices, the condition shifts can be handled as transition probability matrix conversions.

$$\mathbf{S}((N \cdot M + Q + k)T_0) = \mathbf{S}(0) \cdot \mathbf{T}_S^M \cdot \mathbf{T}^P \cdot \mathbf{T}_S^M \cdot \mathbf{T}^P \cdots \mathbf{T}_S^M \cdot \mathbf{T}^P \cdot \mathbf{T}_S^Q \cdot \mathbf{T}_A^k \tag{11}$$

"PT_0" is the average value of the time needed for the test and the repair. N, M, Q and k are defined previously. Formula (11) still excludes the result of repair.

4 Human Factor

Since any shutdown of military or disaster management device may be fatal, the human factor has to be integrated into the probability of failure investigation. From among the numerous investigation methods [7], it is practical to choose one that is considerable with the jumps of the λ failure rate. The TESEO method is suitable, as it estimates by how much the human action raises the probability of failure, by empirically analysing the reasons leading to a failure caused by humans. TESEO defines carefully described categories for the competency of the

staff, the complexity of the task, the operability of the device as well as the time available for the decision, and assigns coefficients to them [8].

Table 1 presents some typical cases and gives the corresponding C_H factor that raises the failure rate.

Table 1

Conditions of carrying out the task during the mission period

Competency of the staff and the device	C_H
Well motivated and highly trained staff Totally familiar task, optimally maintained device	1.112
Highly trained staff without any stress or personal conflict Fairly simple task, well maintained device	1.224
Staff expanded with improperly trained persons Complex task, sufficiently maintained device	1.640
Staff is improperly trained but able to carry out the task Miscellaneous task, improperly maintained device	3.560

The C_H coefficient, which describes the competency of the staff and the device, can be taken into account with the formulae (10) where C_S has to be replaced by $C_S C_H$ and C_A by $C_A C_H$. The $C_{SAH} = \frac{C_A}{C_S} \cdot C_H$ coefficient converts the $\mathbf{T}_S$ transition probability matrix into the $\mathbf{T}_A$ transition probability matrix.

5 Periodic Diagnostic Tests

The purpose of periodic test is detecting and repairing the failures. The periodically executed diagnostic tests and repairs are capable of increasing the reliability of devices [9]. In diagnostic test condition which interrupts the non-operated storage condition of the aperiodically operated devices, the operative personnel carry out a prescribed sequence of actions. These actions are executed among normal circumstances, and mainly inspect the operation of the actuators in the control system. When the operative personnel detect a failure, the device is being repaired. The result of repair is reviewed by executing another prescribed sequence of actions. This method differs from the test mode carried out during continuous operation, as in reasonable time-limit the duration of test and repair is not critical.

The state probabilities, at starting the n^{th} diagnostic test in $n \cdot M \cdot T_0 = i$ moment, applying the model in Figure 2, is:

$$\mathbf{S}(i) = [s_1(i) \quad s_2(i) \quad s_3(i) \quad s_4(i) \quad s_5(i) \quad s_6(i)] \tag{12}$$

When analysing the effect of the interruptive test, it is assumed that the operative personnel are capable to reveal only the detectable – including shutdown causing – failure states; all the other states are presumed and documented as successful operation. In the moment of test, the device is either operating faultlessly or can get into a particular failure state.

Let the value of average probability of detected failures to be introduced. According the model in Figure 2, the operative personnel detect a failure in the average of tests with the probability given by formula (13).

$$s_{avg}(i) = \frac{1}{3}\{s_2(i) + s_3(i) + s_6(i)\} \tag{13}$$

It is suitable to be calculated with in every further test, assuming that during the life cycle of the device the signed differences between the average and the real values are balanced, therefore the calculation error is negligible.

The efficiency of test is described with the diagnostic coverage. When calculating the diagnostic coverage (DC) for aperiodically operated devices, contrary to standards [1] and [2], not only the ratio of detected and all dangerous failures ($DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$) has to be considered, but the ratio of all detected and all failures, as during mission period a shutdown of any reason can be fatal. Therefore the modified diagnostic coverage is:

$$DC_M = \frac{\sum \lambda_{0D}}{\sum \lambda_{total}} \tag{14}$$

Assuming that the initial state is recovered during repairs, the repair of revealed failures may reset the state probabilities to the $\mathbf{S}(1)$ values succeeding the commissioning [10]. However, this value is reduced by the DC_M value of diagnostic coverage. If the operative personnel reveal and repair the failures with the average probability of detected failures s_{avg}, the result of repairs is the average probability of recovery (v_{avg}), which, according to the model in Figure 2, is:

$$v_{avg}(i) = \frac{DC_M}{3}\{s_2(i) - s_2(1) + s_3(i) - s_3(1) + s_6(i) - s_6(1)\} \tag{15}$$

In the i+1 moment following the test, the probability of successful operation is increased by the value of average probability of recovery caused by repair. Accordingly, the probability of detectable failure states decrease. The failure states can be repaired with the probability of their occurrence, therefore the distribution of the average probability of recovery (v_{avg}) among the individual failure states is carried out weighted by the failure states' probability of occurrence. For example the probability of recovery from the (2) failure state in the model of Figure 2 is:

$$v_{avg}(i)\frac{s_2(i)}{s_2(i)+s_3(i)+s_6(i)} = v_{avg}(i)\frac{s_2(i)}{3s_{avg}(i)} \tag{16}$$

As a result of repairs, the device's state probabilities change, thus the elements of the $\mathbf{S}(i)$ vector corresponding the successful operation and detectable failure states have to be corrected. In the model of Figure 2, these values are $s_1(i)$, $s_2(i)$, $s_3(i)$ and $s_6(i)$.

The probability of successful operation is increased by the value of average probability of recovery caused by the repair.

$$s_1(i+1) = s_1(i) + v_{avg}(i) \tag{17.1}$$

The values of detectable failures have to be corrected:

$$s_2(i+1) = s_2(i) - v_{avg}(i)\frac{s_2(i)}{3s_{avg}(i)} = s_2(i)\left\{1 - \frac{v_{avg}(i)}{3s_{avg}(i)}\right\} = s_2(i)w(i) \tag{17.2}$$

$$s_3(i+1) = s_3(i) - v_{avg}(i)\frac{s_3(i)}{3s_{avg}(i)} = s_3(i)\left\{1 - \frac{v_{avg}(i)}{3s_{avg}(i)}\right\} = s_3(i)w(i) \tag{17.3}$$

The non-detected failure states keep their original values.

$$s_4(i+1) = s_4(i) \tag{17.4}$$

$$s_5(i+1) = s_5(i) \tag{17.5}$$

The value of detectable failure causing shutdown has to be corrected:

$$s_6(i+1) = s_6(i) - v_{avg}(i)\frac{s_6(i)}{3s_{avg}(i)} = s_6(i)\left\{1 - \frac{v_{avg}(i)}{3s_{avg}(i)}\right\} = s_6(i)w(i) \tag{17.6}$$

At first approach, the T_0 time base was considered as unit. As the repair is considered as a correction of state probabilities, the actual time has no meaning, because it is assumed that it is much shorter than the period of powered-down storage and the repair is not carried out during the mission period.

For algorithmizability, the $\mathbf{v}(i)$ vector-variable including the average increase of the probability of successful operation is introduced.

$$\mathbf{v}(i) = [v_{avg}(i) \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \tag{18.1}$$

For handling the $w(i) = 1 - \frac{v_{avg}(i)}{3s_{avg}(i)}$ factor the $\mathbf{w}(i)$ vector-variable is introduced:

$$\mathbf{w}(i) = [1 \quad w(i) \quad w(i) \quad 1 \quad 1 \quad w(i)] \tag{18.2}$$

The corrected state probabilities following the repair of failures detected during the tests can be calculated with the vector operation below:

$$\mathbf{S}_{\text{corr}}(i) = \left\{\text{Diag}\left(\mathbf{w}^{T}(i)\right)\mathbf{S}(i)\right) + \mathbf{v}^{T}(i)\right\}^{T} \tag{19}$$

6 Algorithmization

The values of the state probabilities from commissioning till the beginning of the mission period are necessary for determining the required frequency of periodic diagnostic tests and/or the required value of diagnostic coverage. The effect of repairs, which is excluded in formula (11), has to be taken into account at this point. If the duration of the test and the repair is still considered as unit (T_0), the steps of calculating the state probabilities before, during and after the test mode are as follows:

T_0 period preceding the test (storage condition):

$$\mathbf{S}((M-1)T_0) = \mathbf{S}((M-2)T_0) \cdot \mathbf{T}_S \tag{20.1}$$

T_0 period of the test (normal mode):

$$\mathbf{S}(MT_0) = \mathbf{S}((M-1)T_0) \cdot \mathbf{T} \tag{20.2}$$

The result of the test, thus the correction:

$$\mathbf{S}_{\text{corr}}(MT_0) = \left\{\text{Diag}\left(\mathbf{w}^{T}(MT_0)\right)\mathbf{S}(MT_0)\right) + \mathbf{v}^{T}(MT_0)\right\}^{T} \tag{20.3}$$

T_0 period following the test (storage condition):

$$\mathbf{S}((M+1)T_0) = \mathbf{S}_{\text{corr}}(MT_0) \cdot \mathbf{T}_S \tag{20.4}$$

The formulae (20) describe the effect of the test executed in the MT_0 moment, but of course any test carried out at any $n \cdot MT_0$ moment can be handled similarly.

Standards [1] and [2] give the safety integrity level (SIL) values referring to T_0=1 [hour] time base when investigating continuous operation, and referring to T_{year}=1 [year] when investigating emergency/protective systems. The storage condition interrupted with periodical tests differs from the operation modes above.

The λ failure rates of the Markov model (Figure 2) are presented for normal, continuous mode in the [5] databases, therefore primarily the $\mathbf{T}$ transition probability matrix is determined where the λ failure rate values correspond with the T_0=1 [hour] time base. In formulae (11) and (20) the $\mathbf{T}$, $\mathbf{T}_S$, $\mathbf{T}_A$ transition probability matrices are shown corresponding with the T_0=1 [hour] time base. In the case of T_0=1 [hour] time base, the period of the diagnostic test and the repair is

being realistically considered PT_0 long. The determination of the first $N(M-1+P)+Q-1$ set of state probabilities requires significant computing resources.

If the result of the test mode is taken as correction of state probabilities into account, the duration of the test, as far as it is much shorter than the non-operated condition, is irrelevant. Choosing a T_{10}=10 [hours] period is useful, because the test and the repair are executable in such term, the number of calculation operations is reduced and it does not add further rounding problems, as follows.

If $\lambda_S = C_S \cdot \lambda = 0.1 \cdot \lambda$ and $T_{10} = 10 \cdot T_0$, then:

$$\lambda_S \cdot T_{10} = \lambda \cdot T_0 \tag{21}$$

Thus calculating with T_{10}=10 [hours] time base in the case of powered-down condition converts the $\mathbf{T}_S$ transition probability matrix right into the $\mathbf{T}$ transition probability matrix, and this does not imply any further rounding error. The introduction of the ten-hour (T_{10}) time base modifies the duration between two tests to $M_{10}T_{10}$, and the duration between the last test and the beginning of the mission period to $Q_{10}T_{10}$.

T_{10} period preceding the test (storage condition):

$$\mathbf{S}((M_{10}-1)T_{10}) = \mathbf{S}((M_{10}-2)T_{10}) \cdot \mathbf{T} \tag{22.1}$$

Assuming that the average duration of the test and the repair is $PT_0 = T_{10} = 10$ [hours]. The T_{10} period of the test:

$$\mathbf{S}(M_{10}T_{10}) = \mathbf{S}((M_{10}-1)T_{10}) \cdot \mathbf{T} \tag{22.2}$$

The result of the test, thus the correction:

$$\mathbf{S}_{corr}(M_{10}T_{10}) = \left\{ \mathrm{Diag}\left(\mathbf{w}^T(M_{10}T_{10})\mathbf{S}(M_{10}T_{10})\right) + \mathbf{v}^T(M_{10}T_{10}) \right\}^T \tag{22.3}$$

T_{10} period following the test:

$$\mathbf{S}((M_{10}+1)T_{10}) = \mathbf{S}_{corr}(M_{10}T_{10}) \cdot \mathbf{T} \tag{22.4}$$

During mission period, it is still recommended to determine the state probabilities referring to the T_0=1 [hour] time base, therefore the primarily determined $\mathbf{T}$ transition probability matrix has to be converted into $\mathbf{T}_A$ transition probability matrix. The value of C_H can be picked out of Table 1 according to the particular situation.

$$\mathbf{T}_A = (\mathbf{T} - \mathbf{I}) \cdot C_A \cdot C_H + \mathbf{I} \tag{23}$$

After that, with the recursive operations of formulae (24), the time-discrete sequence of the vectors of state probabilities, during the KT_0 mission period can

be figured out. The initial values at the $T_B = (N \cdot M_{10} + Q_{10}) \cdot T_{10}$ beginning of the mission period are:

$$\mathbf{S}((N \cdot M_{10} + Q_{10}) \cdot T_{10}) = \mathbf{S}((N \cdot M_{10} + Q_{10} - 1) \cdot T_{10}) \cdot \mathbf{T} \tag{24}$$

Restoring T_0=1 [hour] time base, formula (24) is rewritten as:

$$\mathbf{S}((N \cdot M + Q) \cdot T_0) = \mathbf{S}((N \cdot M_{10} + Q_{10}) \cdot T_{10}) \tag{25.0}$$

The first two steps of the recursive operations are:

$$\mathbf{S}((N \cdot M + Q + 1) \cdot T_0) = \mathbf{S}((N \cdot M + Q) \cdot T_0) \cdot \mathbf{T}_A \tag{25.1}$$

$$\mathbf{S}((N \cdot M + Q + 2) \cdot T_0) = \mathbf{S}((N \cdot M + Q + 1) \cdot T_0) \cdot \mathbf{T}_A \tag{25.2}$$

The k^{th} step of the recursive operations is:

$$\mathbf{S}((N \cdot M + Q + k) \cdot T_0) = \mathbf{S}((N \cdot M + Q + k - 1) \cdot T_0) \cdot \mathbf{T}_A \tag{25.k}$$

Now, the average probability of failure applied for the aperiodically operated devices according to formula (6) can be determined. The sixth (S6) state probabilities of the KT_0 mission period, which stand for the shutdown, are sufficient for the calculation.

$$PF_{avg}^{sum} = \frac{\sum_{k=N \cdot M+Q}^{N \cdot M+Q+K} s_6(k \cdot T_0)}{K+1} \tag{26}$$

Conclusion

The concept of aperiodically operated devices and the characteristics of their operation have been defined. It has been shown that if the operation mode shifts are taken into account by the jumps of the λ failure rate, the time-discrete Markov model is applicable. Different transition probability matrices belong to the different operation conditions. The rule of conversion between these matrices has been given. This rule is capable of taking the failure caused by the human factor also into account. By analysing the effect of diagnostic test and repair interrupting the non-operated condition, a proposal for the modified interpretation of the diagnostic coverage has been given. Also by analysing the effect of diagnostic test and repair, it has been recommended that the increase of the probability of successful operation should be taken into account with correction of state probabilities. Finally, – due to their recursive nature – a well-programmabe algorithm of the equations has been given, and the average probability of failure applied for the aperiodically operated devices was determined. In order to decrease the need of computing resources, a proposal has been given for a time base conversion that does not affect the calculation accuracy. Based on this work further investigations may be performed, i.a. a computer simulation program can be written for the analysis of diagnostic coverage and the impact of the test

frequency. These results will be published later, and can be the basis of a commercial product, that will support the military and the disaster management to determine and improve the reliability of their aperiodically operated devices.

References

[1] IEC 61511, International Standard, Functional safety – Safety instrumented systems for the process industry sector, International Electrotechnical Commission (IEC), 2002

[2] ANSI/ISA-84.00.01-2004, American National Standard, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, International Society of Automation (ISA), 2004

[3] ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques, International Society of Automation (ISA), 2002

[4] Goble, W., M., Cheddie, H. L., Safety Instrumented System Verification: Practical Probabilistic Calculation, International Society of Automation (ISA), 2005

[5] http://www.technis.org.uk (Available: 03-02-2013)

[6] Scott, M., Adler, B., How to select a safety PLC, On-line Technical Paper, http://www.isa.org/Content/Microsites838/Safety_Division/Home818/ISA_2004_Safety_Papers/How_to_Select_a_Safety_PLC.pdf, International Society of Automation (ISA), 2004 (Available: 03-02-2013)

[7] Humphreys. P. (editor), Human Reliability Assessor's Guide: A Report by the Human Factors in Reliability Group (Reports: SRDA-R11), AEA Technology, 1995

[8] Smith, D. J., Reliability, Maintainability, and Risk: Practical Methods for Engineers, 8th edition. Butterworth-Heinemann, 2011

[9] Bukowski, J. V., Modeling and Analyzing the Effects of Periodic Inspection on the Performance of Safety-Critical Systems. IEEE Transactions on Reliability, Vol. 50, No. 3, pp. 321-329, 2001

[10] Goble, W. M., Bukowski, J. V., Brombacher, A. C., How Diagnostic Coverage improves safety in programmable electronic systems, ISA Transactions, Vol. 36, No. 4, pp. 345-350, 1997

[11] Jadlovská, A., Jajčišin, Š., Predictive Control Algorithms Verification on the Laboratory Helicopter Model, Acta Polytechnica Hungarica, Vol. 9, No. 4, pp. 221-245, 2012

[12] Bokor, Z., Integrating Logistics Cost Calculation into Production Costing, Acta Polytechnica Hungarica, Vol. 9, No. 3, pp. 163-181, 2012

[13] Sárosi J., New Force Functions for the Force Generated by Different Fluidic Muscles, Transactions on Automatic Control and Computer

Science, Scientific Bulletin of the "Politehnica" University of Timisoara, Vol. 57(71), No. 3, pp. 135-140, 2012

[14] Varga, A., Rácz, E., Kádár, P., New Experimental Method for Measuring Power Characteristics of Photovoltaic Cells at Given Light Irradiation, Proceedings of 8th IEEE International Symposium on Applied Computational Intelligence and Informatics, SACI 2013, Timisoara, Romania, pp. 405-409, 2013

[15] Pachter, M., State Estimation for Discrete Systems, Military Operations Research, Vol.16, No. 3, pp. 23-31, 2011

[16] Rădac, M.-B., Precup R.-E., Petriu, E. M., Preitl, S., Experiment-based Performance Improvement of State Feedback Control Systems for Single Input Processes, Acta Polytechnica Hungarica, Vol. 10, No. 3, pp. 5-24, 2013

[17] Sven Guzman, M., Pohl, E. A., Schneider, K., Rainwater, C., Application of Reliability Methods to Social Networks, Military Operations Research, Vol. 17, No. 4, pp. 51-58, 2012

[18] Grosselin, K., Bayesian Estimates of the Rideshare Reliability Effect, Military Operations Research, Vol. 17, No. 4, pp. 39-49, 2012

[19] Novak-Marcincin, J., Janak, M., Barna, J., Torok, J., Novakova-Marcincinova, L., Fecova, V., Verification of a Program for the Control of a Robotic Workcell with the use of AR, International Journal of Advanced Robotic Systems, Vol. 9, Art. No. 54, 2012

[20] Kolozsi, G., Changes of "UT" Specifications, Korrozios Figyelo, Vol. 51, No. 1, pp. 15-19, 2011

[21] Durovsky, F., Fedak, V., Integrated Mechatronic Systems Laboratory, Proceedings of the 14th International Power Electronics and Motion Control Conference (EPE-PEMC 2010), pp. S51-S55, 2010

[22] Horváth, L., Rudas, I. J., New Method of Knowledge Representation and Communication for Product Object Modeling, Proceedings of the 12th WSEAS International Conference on Applied Computer Science ACS-12, pp. 75-80, 2012