Robert PILCH
AGH University of Science and Technology, Kraków
pilch@agh.edu.pl

IMPACT OF TESTING OF ELEMENTS IN SAFETY RELATED SYSTEMS ON THE SAFETY INTEGRITY LEVEL (SIL)

Keywords

IEC-61508, probability of failure on demand, Markov model, safety integrity level.

Abstract

The paper presents a proposed methodology of calculating the PFD values for safety related systems, which accounts for the specific character of their operation and repair. The proposed method is based on Markov processes, and it allows one to account for the testing of elements after repair or renewal. This in turn allows one to determine an additional safety margin that occurs in real systems but not typically accounted for in commonly used calculation methods. Knowing these values enables a more deliberate designing of safety related systems and can allow obtaining higher SILs while using the same elements. The proposed model was used in calculations for exemplary systems, and the calculation results were compared to the results obtained according to recommendations of IEC-61508 and selected models presented in the literature. The paper also indicates the factors that affect the PFD and SIL values achieved by the safety related systems used in industry.

Introduction

Ensuring the required safety level is the basic aspect of the operation of contemporary technical systems. This issue is particularly important when an unexpected failure is a hazard to life, health, or the environment. In practice, this is typical for production, processing, and the transport of oil and gas, the chemical industry, the generation and transmission of power, and in other sectors such as railways. The operational safety requirements of a system are usually expressed as an acceptable compliance to risk levels, which is a condition of approval for operation. In many cases, the acceptable risk level can be achieved only by introducing additional systems, called "Safety Related Systems" (SRS). They continuously monitor selected parameters of a system, and when the limit values are reached or some specific symptoms occur, they implement preprogramed functions to prevent the occurrence of a hazardous event. The IEC-61508 series of standards were developed due to the practical significance of the problem. Their application is often required in the certification process of SILs achieved by safety related systems used in industry. In practice, the SRS most often comprise the E/E/PE systems (Electrical/Electronic/Programmable Electronic). Thus, reducing the risk to the acceptable level depends on the reliability of such systems. Consequently, acceptable average failure rates are specified for the safety related systems, i.e. The Probability of Failure on Demand (PFD) or The Probability of Failure per Hour(PFH), which ensure that the risk is reduced to the acceptable level. Relevant charts of PFD and PFH are usually expressed as SIL1– SIL4 (Safety Integrity Level) with values different by an order of magnitude [1].

The methodology presented in the standard is based on the reliability block diagrams [1, 2]. In order to account for additional aspects of operation of SRSs and to increase the accuracy of PFD calculation, some alternative computational models were proposed in the literature, which are mostly based on the Markov processes [3–6]. In [4], the calculation of the average downtime (t_{C1}) for an element in the proof test interval was presented and a method of determining this value, which is more accurate than the method presented in the standard, was included. Moreover, in [7, 8], the authors proved that different computational models lead to significantly different results. The SRSs used in industry usually have the k-out-of-n (koon) type reliability structures in which $n>3$ often occur. However, these cases are not presented in IEC-61508. Attempts were also made to develop generalized formulas for the PFD calculation in order to allow one to calculate the SILs for any SRS structures [9, 10]. Due to the assumptions made, such generalizations often give different PFD values for the same systems.

Moreover, the computational models proposed in the literature do not include the testing of elements after repair or renewal, which can significantly

reduce the PFD values. The testing of elements is widely used in the operation of SRSs; therefore, it makes sense to adapt the computational model to the operational practice. This paper presents a PFD computational model in which the elements are tested before they are installed in an SRS. The model is based on Markov processes. The paper also includes the calculation results and compares them with the results obtained using different computational models.

1. Basic assumptions used in the SIL calculation methodology

Basis assumptions and designations conforming to IEC-61508 are presented below.

1. Each system with a "koon" structure consists of components which are identical and have constant failure rates (λ), constant repair rates (μ), and diagnostic coverage (DC) values.
2. Failure rate (λ) has a safe (λ_S) and dangerous component (λ_D); ($\lambda = \lambda_D + \lambda_S$).
3. Self-diagnostic tests performed at interval T_2 allow one to detect dangerous faults according to the diagnostics coverage (DC) value. Thus, dangerous failure rate (λ_D) is divided into detected dangerous failure rate ($\lambda_{DD} = DC \cdot \lambda_D$) and undetected dangerous failure rate ($\lambda_{DU} = (1 - DC) \cdot \lambda_D$); ($\lambda_D = \lambda_{DD} + \lambda_{DU}$).
4. Proof tests performed at interval T_1 allow one to detect and eliminate all types of failures that occur in the system.
5. Self-diagnostic test interval is strongly less than proof-test interval ($T_2 << T_1$). Both intervals are constant for all elements.
6. Mean time to restoration ($MTTR$) is identical for all elements and contains self-diagnostic test interval.
7. Detected and undetected faults can occur independently in each element.
8. Detected (β_D) and undetected (β) common cause failures are percentage components of detected and undetected faults, respectively (Fig. 1).

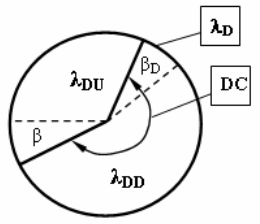

Fig. 1. Dangerous failure rate of an element

9. The determined mean probability of failure on demand (PFD) for each subsystem is less than 10^{-1}.
10. Average downtime due to undetected dangerous failures (t_{C1}) for each element is assumed as $t_{C1} = T_1/2 + MTTR$, and the average downtime due to detected dangerous failures (t_{C2}) is assumed as $t_{C2} = MTTR$.

2. Computational models of Safety Integrity Levels (SIL)

2.1. Reliability block diagram (RBD) method according to IEC-61508 (I)

The basic computational model used to evaluate the SILs is the reliability block diagram method presented in IEC-61508. According to this method, the failure rate and average downtimes for each element can be expressed as in Figure 2 [1].

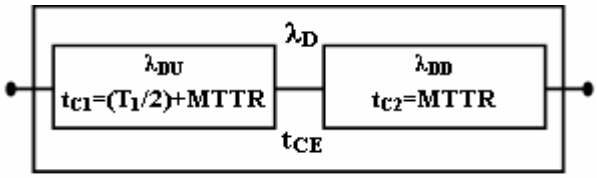

Fig. 2. Failure rates and average downtimes for a single element

Each element can be in the failure state due to two types of failures (detected and undetected by the self-diagnostic test). Thus, the average downtime of a single element due to both failure types (t_{CE}) is as follows [1]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} + MTTR = \\ = (1 - DC)\left(\frac{T_1}{2} + MTTR\right) + DCMTTR \tag{1}$$

The methodology also assumes a linear approximation of calculated PFD values using the following formula [1]:

$$PFD = (\lambda_D t_{CE}) \tag{2}$$

Instead of exponential formula in form:

$$PFD = 1 - e^{-\lambda_D t_{CE}} \tag{3}$$

This simplification is a result of the fact that, when the condition $\lambda_D t_{CE} << 1$ is fulfilled, the differences will be small and in each time will overstate the calculated PDF values. Hence, the error will always be made in the safe direction.

For the 1oo1 system, the PFD_{1oo1} is calculated according to formula (2), and for the 1oo2 case according to formula [1]:

$$PFD_{1oo2} = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \\ + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{4}$$

where t_{GE} – average downtime of the number of elements causing the failure state of the whole system.

The t_{GE} value for the1oo2 case is calculated according to formula as follows [1]:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} + MTTR \tag{5}$$

The aforementioned standard presents the formulas for the calculation of the PFD values of a few basic "koon" structures (1oo1, 1oo2, 2oo2, 1oo3, 2oo3) and the general methodology for the whole SRS as a serial structure consisting of three subsystems: sensor subsystem (S), logic subsystem (L),and final element subsystem(FE) [1]:

$$PFD = PFD_S + PFD_L + PFD_{FE} \tag{6}$$

The used method of the summation of the probabilities (not conforming to the reliability theory) gives results only slightly different from the correct calculation, because when the assumption ix is fulfilled, the values are less than 10^{-1}. The result of summation is always overestimated, so the error is made in the safe direction.

2.2. Computational model based on Markov processes (II)

An alternative method to calculate the SIL is the model based on Markov processes. Their main advantages include better computation accuracy. Among the disadvantages, one can name computational complexity, which increases along with the growing number of elements and difficulties in accounting for common cause failures.

The states transition diagram for a single element (1oo1 system) according to the basic computational model based on Markov processes is presented in Figure 3 [4].

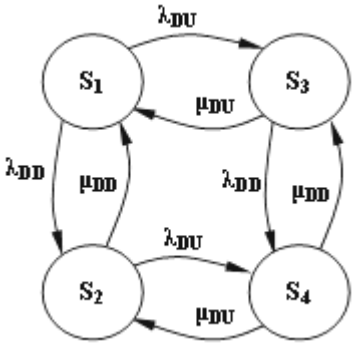

Fig. 3. States transition diagram for a single element [4]

States S_i in the diagram mean:
S_1 – operating state – no detected and undetected failures,
S_2 – failed state – detected failure of the element,
S_3 – failed state – undetected failure of the element,
S_4 – failed state – detected and undetected failure of the element.

Respective element repair rates are assumed as follows:

$$\mu_{DD} = \left(t_{C2}\right)^{-1} = MTTR^{-1} \tag{7}$$

$$\mu_{DU} = \left(t_{C1}\right)^{-1} = \left(\frac{T_1}{2} + MTTR\right)^{-1} \tag{8}$$

Differential equations for the presented diagram can be written as follows:

$$\begin{cases} P_{S_1}^{'}(t) = -(\lambda_{DD} + \lambda_{DU})P_{S_1}(t) + \mu_{DD}P_{S_2}(t) + \mu_{DU}P_{S_3}(t) \\ P_{S_2}^{'}(t) = -(\lambda_{DU} + \lambda_{DD})P_{S_2}(t) + \lambda_{DD}P_{S_1}(t) + \mu_{DU}P_{S_4}(t) \\ P_{S_3}^{'}(t) = -(\lambda_{DD} + \mu_{DU})P_{S_3}(t) + \lambda_{DU}P_{S_1}(t) + \mu_{DD}P_{S_4}(t) \\ P_{S_4}^{'}(t) = -(\mu_{DD} + \mu_{DU})P_{S_4}(t) + \lambda_{DU}P_{S_2}(t) + \lambda_{DD}P_{S_3}(t) \end{cases} \tag{9}$$

The solution of the system of equations in the assumed time horizon allows one to determine the probability that the element is in the failure state ($P_f(t)$):

$$P_f(t) = P_{S_2}(t) + P_{S_3}(t) + P_{S_4}(t) \tag{10}$$

The average probability of failure on demand (PFD) can be calculated from formula [4]:

$$PFD = \frac{1}{T_1}\int_0^{T_1} P_f(t)dt \tag{11}$$

In "koon" systems, when n>1, the states transition diagram is built analogously; however, when the number of elements (n) increases, the number of the systems states (i) grows very rapidly – according to formula [8]:

$$i = 4^n \tag{12}$$

Hence, for greater values of n, it is advisable to develop a computer algorithm to generate states transition diagrams and solve differential equations.

2.3. Proposed computational model with testing of elements after repair (III)

Models I and II do not account for the testing of elements after repair and before resuming operation. In practice, the repaired elements are tested for correct functioning before they are again put into operation. This allows one to detect and eliminate all types of dangerous failures of an element during the repair. In the case of a replacement of an element, it can be assumed that a new element is free of any defects or it can be additionally tested before it is put to operation.

The proposed computational Model III is based on Markov processes. Unlike the classic Model II, it accounts for the testing of each element following its failure and repair. It was assumed that the test effectiveness is 100%, so all failures are detected, and after the repair (or replacement), the element is fully renewed. The other significant difference is that the PFD values are always calculated in the time interval [0-T_1]. Consequently, if an element succumbs only to a failure that is undetectable by the self-diagnostic test, it is not renewed. The proof test, which detects all failures, is done only after the time T_1. However, this happens outside the time interval that, according to the standard, is included in the calculations. This is exactly the assumption made in Model III. Taking into account the assumptions, the Markov states transition diagram for a single element according to the proposed model is presented in Figure 4.

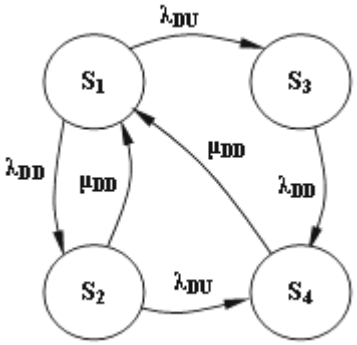

Fig. 4. States transition diagram for a single element according to Model III

States S_i in the diagram are the same as in Model II (only S_1 is the operating state). The set of differential equations can be written as follows:

$$\begin{cases} P_{S_1}^{'}(t) = -(\lambda_{DD} + \lambda_{DU})P_{S_1}(t) + \mu_{DD}P_{S_2}(t) + \mu_{DD}P_{S_4}(t) \\ P_{S_2}^{'}(t) = -(\lambda_{DU} + \mu_{DD})P_{S_2}(t) + \lambda_{DD}P_{S_1}(t) \\ P_{S_3}^{'}(t) = -\lambda_{DD}P_{S_3}(t) + \lambda_{DU}P_{S_1} \\ P_{S_4}^{'}(t) = -\mu_{DD}P_{S_4}(t) + \lambda_{DU}P_{S_2}(t) + \lambda_{DD}P_{S_3}(t) \end{cases} \tag{13}$$

After solving the set of differential equations in time interval [0-T_1], the PFD value is calculated according to formulas (10) and (11).

For the 1oo2 system, the Markov states transition diagram according to Model III will have 16 states, and it is not presented here due to its size. The system of differential equations was also solved in the Matlab software.

3. Calculation example and comparison of results

In order to compare the results according to three presented models (I, II, III), calculations were made for selected "koon" structures of the SRSs used in practice. The calculations were made for a few failure rates λ_D, for time intervals T_1, and diagnostic coverage (*DC*). In all cases, it was assumed that *MTTR* = 24 [h] and $\beta = \beta_D = 0$. All results are presented in Tables 1, 2, and 3.

Selected calculation results are also presented as charts. Figures 5–8 present the results for different values of λ_D and T_1 at constant *DC*. Figures 9–10 present the results for different values of λ_D and *DC* at constant T_1.

Table 1. PFD values obtained according to models I, II and III if DC = 0.8

"koon"	λ_D [1/h]	DC = 0.8								
		T_1 = 17520 [h]			T_1 = 13140 [h]			T_1 = 8760 [h]		
		I	II	III	I	II	III	I	II	III
1oo1	1.66E-7	2.948E-4	1.685E-4	2.937E-4	2.221E-4	1.272E-4	2.211E-4	1.494E-4	8.593E-5	1.485E-4
	1.66E-6	2.948E-3	1.683E-3	2.912E-3	2.221E-3	1.271E-3	2.197E-3	1.494E-3	8.588E-4	1.479E-3
	1.66E-5	2.948E-2	1.662E-2	2.677E-2	2.221E-2	1.259E-2	2.062E-2	1.494E-2	8.534E-3	1.417E-2
	1.66E-4	2.948E-1	1.475E-1	1.377E-1	2.221E-1	1.150E-1	1.215E-1	1.494E-1	8.026E-2	9.746E-2
1oo2	1.66E-7	1.167E-7	3.335E-8	1.144E-7	6.637E-8	1.898E-8	6.474E-8	3.016E-8	8.633E-9	2.910E-8
	1.66E-6	1.167E-5	3.326E-6	1.122E-5	6.637E-6	1.894E-6	6.380E-6	3.016E-6	8.622E-7	2.882E-6
	1.66E-5	1.167E-3	3.237E-4	9.284E-4	6.637E-4	1.856E-4	5.531E-4	3.016E-4	8.505E-5	2.620E-4
	1.66E-4	1.167E-1	2,502E-2	2,158E-2	6,637E-2	1,525E-2	1,717E-2	3,016E-2	7,445E-3	1,138E-2

Table 2. PFD values obtained according to models I, II and III if DC = 0.93

"koon"	λ_D [1/h]	DC = 0.93								
		T_1 = 17520 [h]			T_1 = 13140 [h]			T_1 = 8760 [h]		
		I	II	III	I	II	III	I	II	III
1oo1	1.66E-7	1.058E-4	6.156E-5	1.054E-4	8.033E-5	4.711E-5	7.999E-5	5.488E-5	3.266E-5	5.457E-5
	1.66E-6	1.058E-3	6.153E-4	1.045E-3	8.033E-4	4.709E-4	7,949E-4	5,488E-4	3,265E-4	5,434E-4
	1.66E-5	1.058E-2	6.126E-3	9.626E-3	8.033E-3	4.694E-3	7.475E-3	5.488E-3	3.258E-3	5.219E-3
	1.66E-4	1.058E-1	5.864E-2	5.076E-2	8.033E-2	4.541E-2	4.506E-2	5.488E-2	3.185E-2	3.667E-2
1oo2	1.66E-7	1.520E-8	4.398E-9	1.455E-8	8.817E-9	2.563E-9	8.338E-9	4.161E-9	1.220E-9	3.841E-9
	1.66E-6	1.520E-6	4.394E-7	1.428E-6	8.817E-7	2.561E-7	8.220E-7	4.161E-7	1.220E-7	3.805E-7
	1.66E-5	1.520E-4	4.352E-5	1.186E-4	8.817E-5	2.542E-5	7.155E-5	4.161E-5	1.214E-5	3.472E-5
	1.66E-4	1.520E-2	3.960E-3	2.896E-3	8.817E-3	2.367E-3	2.327E-3	4.161E-3	1.156E-3	1.575E-3

Table 3. PFD values obtained according to models I, II and III if DC = 0.99

"koon"	λ_D [1/h]	DC = 0.99								
		T_1 = 17520 [h]			T_1 = 13140 [h]			T_1 = 8760 [h]		
		I	II	III	I	II	III	I	II	III
1oo1	1.66E-7	1.853E-5	1.221E-5	1.847E-5	1.489E-5	1.015E-5	1.484E-5	1.125E-5	8.076E-6	1.120E-5
	1.66E-6	1.853E-4	1.221E-4	1.834E-4	1.489E-4	1.015E-4	1.476E-4	1.125E-4	8.076E-5	1.117E-4
	1.66E-5	1.853E-3	1.220E-3	1.716E-3	1.489E-3	1.014E-3	1.409E-3	1.125E-3	8.072E-4	1.086E-3
	1.66E-4	1.853E-2	1.211E-2	1.065E-2	1.489E-2	1.007E-2	9.831E-3	1.125E-2	8.030E-3	8.629E-3
1oo2	1.66E-7	5.068E-10	1.615E-10	4.115E-10	3.352E-10	1.099E-10	2.598E-10	1.988E-10	6.838E-11	1.432E-10
	1.66E-6	5.068E-8	1.614E-8	4.050E-8	3.352E-8	1.099E-8	2.569E-8	1.988E-8	6.837E-9	1.423E-8
	1.66E-5	5.068E-6	1.612E-6	3.476E-6	3.352E-6	1.097E-6	2.305E-6	1.988E-6	6.829E-7	1.334E-6
	1.66E-4	5.068E-4	1.586E-4	1.199E-4	3.352E-4	1.083E-4	1.028E-4	1.988E-4	6.758E-5	7.927E-5

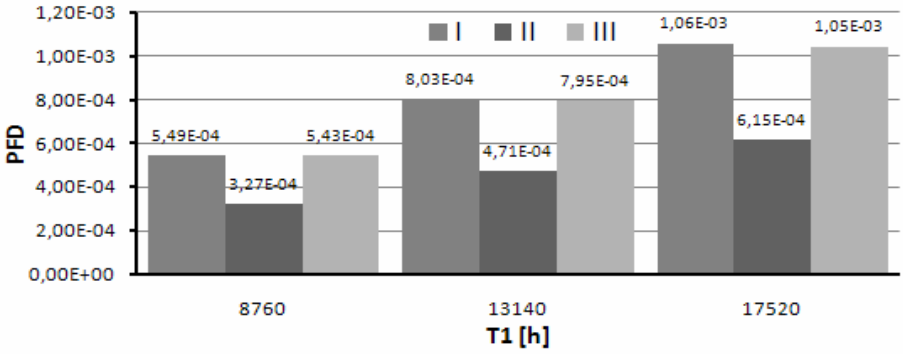

Fig. 5. PFD of the 1oo1 system according to models I, II, III for λ_D = 1.66E-6 [1/h] and DC = 0.93

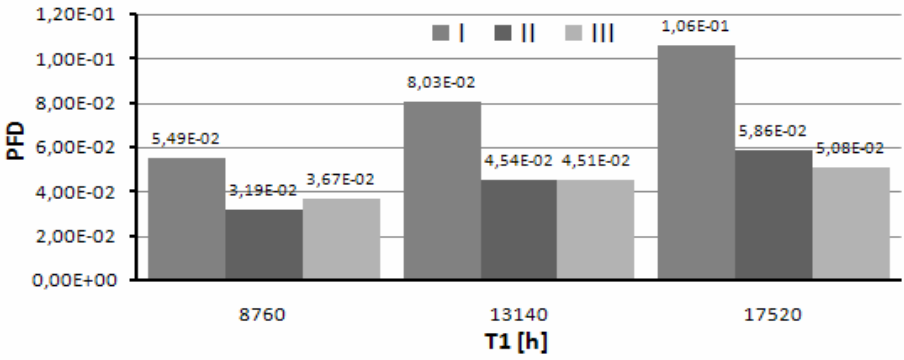

Fig. 6. PFD of the 1oo1 system according to models I, II, III for λ_D = 1.66E-4 [1/h] and *DC* = 0.93

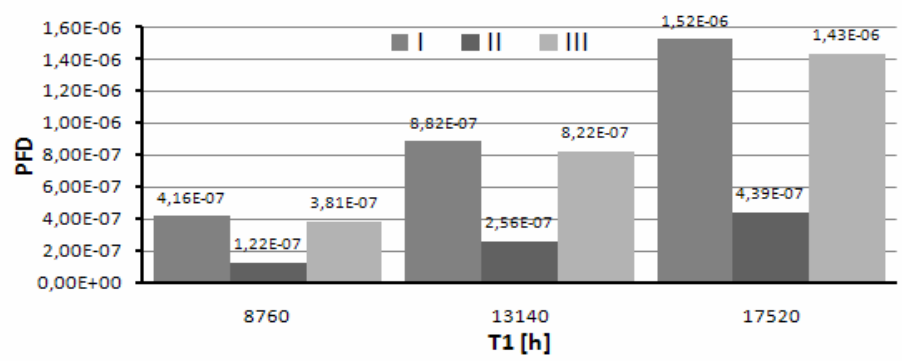

Fig. 7. PFD of the 1oo2 system according to models I, II, III for λ_D = 1.66E-6 [1/h] and *DC* = 0.93

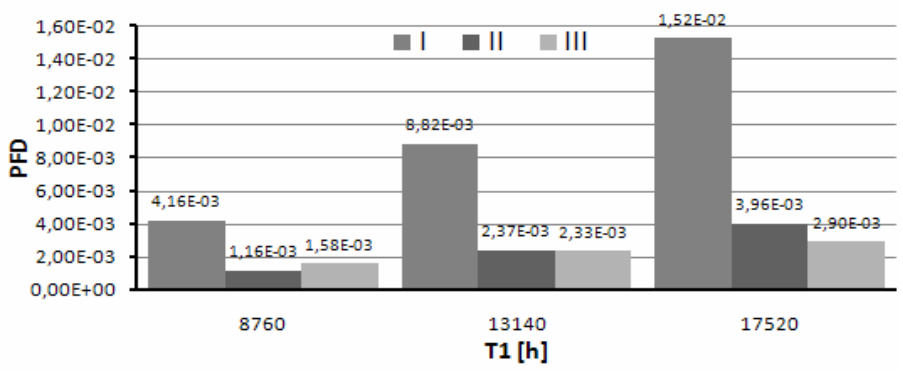

Fig. 8. PFD of the 1oo2 system according to models I, II, III for λ_D = 1.66E-4 [1/h] and *DC* = 0.93

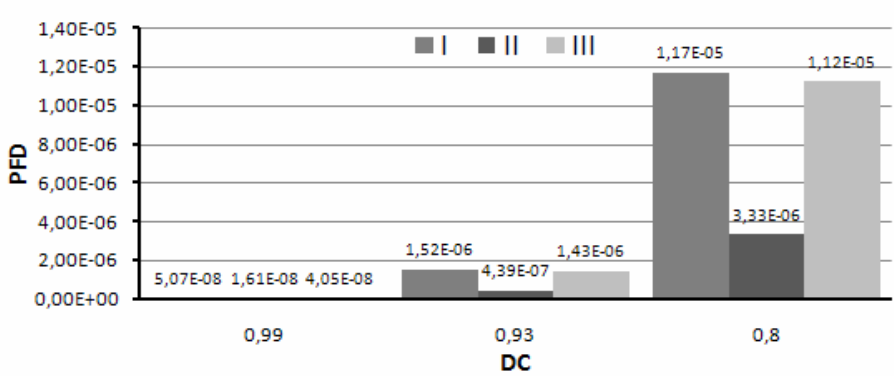

Fig. 9. PFD of the 1oo2 system according to models I, II, III for λ_D = 1.66E-6 [1/h] and T_1 = 17520 [h]

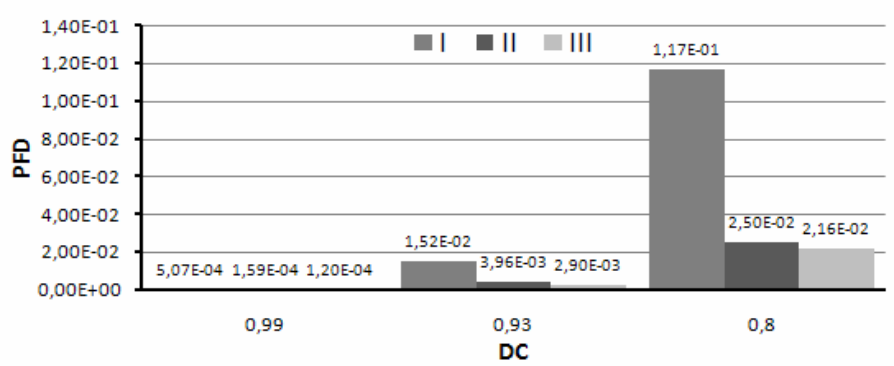

Fig. 10. PFD of the 1oo2 system according to models I, II, III for λ_D = 1.66E-4 [1/h] and T_1 = 17520 [h]

The obtained results indicate that, irrespective of the system structure and values of parameters (λ_D, T_1, *DC*), the PFD values obtained according to IEC-61508 (Model I) are greater than the values obtained according to the proposed Model III with the testing of elements after repair. These differences grow with increasing time interval T_1, with increasing dangerous failure rate λ_D, and with decreasing diagnostic coverage *DC*. In the extreme case, the PFD values according to Model I are even five times greater than the PFD calculated according to Model III (Fig. 8).The PFD calculated according to classic Markov model (Model II) have the least values in the majority of cases. However, this is a result of the fact that this model does not account for the repair of undetected failures before the time of proof test T_1 that, in practice, is in principle impossible. Thus, these results cannot be treated as fully credible and in the real system such little PFD values will not be possible to obtain. In the case of

longer test intervals T_1 and higher failure rates (λ_D in the 10^{-4} order of magnitude), the testing of elements (Model III) gives better results than Model II (Fig. 6, Fig. 8, Fig. 10). This indicates a substantial impact of testing the elements after repair.

Conclusions

The obtained results and their analysis indicate that significant differences in the PFD values can occur depending on the computational model used. The widely used Model I according to IEC-61508 does not account for testing the elements after a repair. However, the effect obtained as a result can be significant and can be observed based on the proposed Model III. In practical applications, the goal should always be that the computational model reflects the reality to the maximum extent possible. Hence, when the elements are tested after repair, the proposed Model III will be preferred. Using Model I will not be an error, but it may result in a significant overestimation of PFD values and excessive safety margins. In some cases, it may even give a result that the system does not fulfil the required SIL when in reality it does. Using Model II, on the other hand, may lead to over-optimistic results that the real system will not fulfil.

The observed impact of changing the models' parameters allows one to draw conclusions that reducing the PFD values of a system and achieving higher SILs is possible by means of the following:

– A reduction of the dangerous failure rate (λ_D);
– An increase of diagnostic coverage (DC) and the resulting decrease of dangerous and undetected failure rate (λ_{DU}) of an element;
– A reduction of the proof test interval (T_1);
– Testing the elements after repair; and,
– A change of the system "koon" structure, e.g. increasing the number of elements n at constant value of k.

References

1. IEC-61508. Functional safety of electrical/electronic/programmable electronic safety-related systems.
2. Guo H., Yang X.: A simple reliability block diagram method for safety integrity verification. Reliability Engineering and System Safety. 2007, 92, 1267–1273.
3. Bukowski J.V., Goble W.M.: Using Markov models for safety analysis of programmable electronic systems. ISA Transactions. 1995, 34, 193–198.

4. Zhang T., Long W., Sato Y.: Availability of systems with self-diagnostic components – applying Markov model to IEC 61508-6. Reliability Engineering and System Safety. 2003, 80, 133–141.
5. Knegtering A., Brombacher A.C.: Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by the IEC 61508 standard for functional safety. Reliability Engineering and System Safety. 1999, 66, 171–175.
6. Langeron Y., Barros A., Grall A., Bérenguer C.: Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules. Journal of Loss Prevention in the Process Industries. 2008, 21, 437–449.
7. Rouvroye J.L., Brombacher A.C.: New quantitative safety standards: different techniques, different results? Reliability Engineering and System Safety. 1999, 66, 121–125.
8. Młynarski S., Pilch R., Smolnik M., Szkoda M., Szybka J.: Evaluation of the safety integrity level (SIL) due to the guidelines of EN 61508 and with the use of Markov processes. Journal of Konbin. 2015, 35, 73–84.
9. Jahanian H.: Generalizing PFD formulas of IEC 61508 for KooN configurations. ISA Transactions. 2015, 55, 168–174.
10. Chebila M., Innal F.: Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. Journal of Loss Prevention in the Process Industries. 2015, 34, 167–176.

Wpływ testowania elementów w układach związanych z bezpieczeństwem na poziom nienaruszalności bezpieczeństwa (SIL)

Słowa kluczowe

IEC-61508, prawdopodobieństwo niewykonania funkcji bezpieczeństwa, model Markowa, poziom nienaruszalności bezpieczeństwa.

Streszczenie

W artykule przedstawiono zaproponowaną metodykę obliczeń prawdopodobieństw PFD dla układów związanych z bezpieczeństwem, uwzględniającą specyfikę ich eksploatacji i odnawiania. Zaproponowana metoda oparta jest na procesach Markowa i umożliwia uwzględnienie faktu testowania elementów po wykonaniu ich naprawy lub odnowy. Pozwala to na wyznaczenie wartości dodatkowego zapasu bezpieczeństwa występującego w rzeczywistych układach, ale niewynikającego ze stosowanych zazwyczaj metod obliczeniowych. Znajomość tych wartości umożliwia bardziej świadome projektowanie struktur układów związanych z bezpieczeństwem oraz może

pozwolić na uzyskanie wyższych poziomów SIL przy zastosowaniu tych samych elementów. Na podstawie opracowanego modelu wykonano obliczenia dla przykładowych układów, a wyniki porównano z wynikami uzyskanymi według zaleceń IEC-61508 oraz wybranych modeli prezentowanych w literaturze. Wskazano również czynniki, które wpływają na wartości prawdopodobieństw PFD oraz poziomy SIL osiągane przez stosowane w przemyśle układy związane z bezpieczeństwem.