Quantitative Assessment of the Diagnostics Effect on the Hardware Safety Integrity of the Safety-Related Electronic System Operating in Low Demand Mode of Operation

Karol RASTOCNY

Department of Control and Information Systems, Faculty of Electrical Engineering and Information Technology, University of Zilina, Univerzitna 1, Zilina, Slovak Republic

karol.rastocny@fel.uniza.sk

DOI: 10.15598/aeee.v17i2.3230

Abstract. *The paper deals with the quantitative assessment of the parameters influence of differently operating fault detection mechanisms on the hardware safety integrity of the safety function. It is considered that the safety function is implemented by an electronic safety-related system operating in low demand mode of operation. The quantitative assessment of the hardware safety integrity of the safety function is based on the use of homogeneous Markov chains. Proving the safety properties of the safety-related control system (proving, that the residual risk is acceptable) is a necessary condition for its implementation into an operation.*

Keywords

Analysis, diagnostics, Markov chain, safety.

1. Introduction

Safety integrity is ability of a safety-related system to achieve its required safety functions under all the stated conditions and within a stated duration. Safety integrity comprises two parts - systematic failure safety integrity and random failure safety integrity. Systematic failure safety integrity is the non-quantifiable part of the safety integrity and is not object of this paper. Random failure safety integrity is quantifiable part of the safety integrity and in [1] is designated as Hard-Ware Safety Integrity (HW-SI).

The random hardware failures are the main factor that influences the HW-SI. Therefore, from a safety point of view, it is very important to detect and negate any potentially dangerous failure as soon as possible (negation – enforcement of a safe state following the detection of a fault [1]) [2]. As the dangerous failure (in this paper) is considered the failure that causes a Safety Function (SF) transition into a dangerous state or increases the probability of the SF transition into a dangerous state. SF is an active safety measure for risk reduction and is implemented by the Electronic Safety-Related System (E-SRS). The detection and consecutive negation of the fault have a significant influence on the Safety Integrity Level (SIL) of the SF.

If the required HW-SI level of the SF is achieved by the structure with electronic components, an assessment of the HW-SI has to be based on quantitative analysis [1]. It is necessary to distinguish between the dependability and safety parameters of the E-SRS, but these parameters influence each other and a certain analogy can be found between them. Therefore, for the analysis of the consequences of the faults on the HW-SI, the modified methods, that were originally developed for the analysis of the dependability parameters, were used [3], [4] and [5]. These methods, however, generally do not allow the assessment of the simultaneous impact of multiple factors (failure rate, diagnostic coverage, detection time, restoration, changing the architecture after detection and negation of the fault, ...) on the HW-SI [6]. This inherent property will negatively affect especially the analysis of complex E-SRS. It is more appropriate to use a method based on Markov Chains with Continuous Time (CTMC), either alone [7], [8], [9], [10] and [11] or in combination with Markov Chains with Discrete Time (DTMC) [12].

A very important activity in the failures influence analysis on the HW-SI using the Markov analysis is model creation. For more complex system structure,

the automatic generating model is theoretically possible (under certain conditions), but practically excluded due to the explosion of states and transitions (the number of states significantly escalates with the number of system elements) [13]. The model creation depends on the analyst's experiences and his correct assessment of the operational and technical characteristics of the analysed system.

This paper presents the principles for solving problems related to the assessment of influence of fault detection mechanisms on the HW-SI of the SF by using the appropriate CTMC and DTMC combination. The proposed procedure is presented on a simple E-SRS that contains only two elements, in order to avoid negative influence of large number of CTMC and DTMC states on clarity of this procedure.

This paper builds on [12], which deals with the diagnostics influence on the HW-SI of the SF operating in continuous mode of operation.

2. General View on the Fault Detection Mechanisms

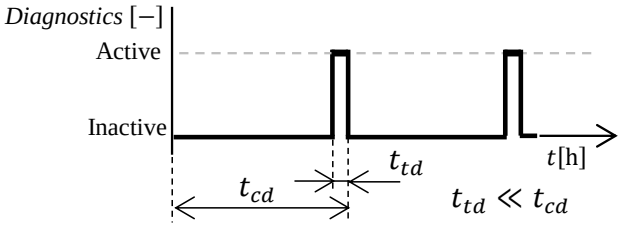
The E-SRS can contain one or more fault detection mechanisms that affect the dangerous state probability of analysed system. The fault detection mechanism can be characterized by the diagnostic coverage (the coefficient of diagnostic coverage is referred to as c) and the fault detection time t_d.

If the E-SRS contains one fault detection mechanism, this mechanism in principle can work so that detection of faults is performed:

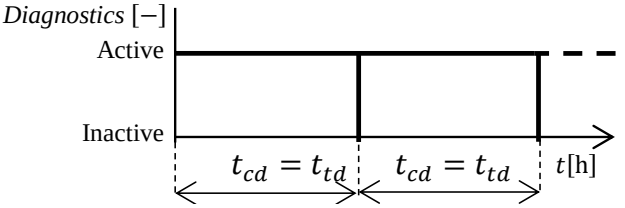
- Periodically (cyclically) and discreetly in time – always at the end of the diagnostic cycle (Fig. 1(a)), while $t_{cd} \gg t_{td}$. t_{cd} is the diagnostic cycle time (it can be identified with the maximum time of the fault detection) and t_{td} is the operation time of the fault detection mechanism.
- Periodically (cyclically) and continuously in time (Fig. 1(b)).

If the E-SRS contains two fault detection mechanisms, it is necessary to assume, that these mechanisms differ from each other by the fault detection time and the diagnostic coverage. We can distinguish between:

- The "Rapid" detection Mechanism (RM), which is characterized by the diagnostic cycle t_{Rd} and the diagnostic coverage coefficient c_R.
- The "Slow" detection Mechanism (SM), which is characterized by the diagnostic cycle t_{Sd} and the diagnostic coverage coefficient c_S.



(a) Periodically and discreetly in time.



(b) Periodically and continuously in time.

Fig. 1: Operation of the fault detection mechanism.

Generally, E-SRS has also other support fault detection mechanisms that are not dominant with respect to HW-SI (they are designed, for example, for the fault localization).

3. The Hardware Safety Integrity of the Dual Structure – Operating in Low Demand Mode of Operation

Using the proposed method is presented on the E-SRS with dual structure based on composite fail-safety with fail-safe comparison. This is a structure that is very often used in practice.

The standard [1] requires to realize the HW-SI assessment individually for each SF. By reason of clarity of this paper, it is assumed that:

- The E-SRS implements only one SF. Based on this assumption, the dangerous state of the SF can be identified with dangerous failure of the E-SRS.
- The E-SRS comprises two hardware identical and independent units – R and L (Fig. 2). Based on this assumption it is valid, that $\lambda_R = \lambda_L = \lambda$, where λ_R (λ_L) is the hardware failure rate of the unit R (L).
- The functional specification of the SF is irrelevant from the view of the HW-SI.

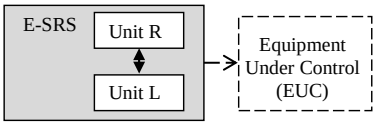


Fig. 2: Block diagram of a general dual structure.

Generally, the E-SRS with this structure has one or two detection mechanisms that have a major impact on the HW-SI.

3.1. Influence of One Fault Detection Mechanism

1) Fault Detection Mechanism Operates Periodically and Continuously in Time

If the fault detection mechanism operates periodically and continuously in time, the diagnostic influence on the HW-SI of E-SRS can be described by the model in Fig. 3.

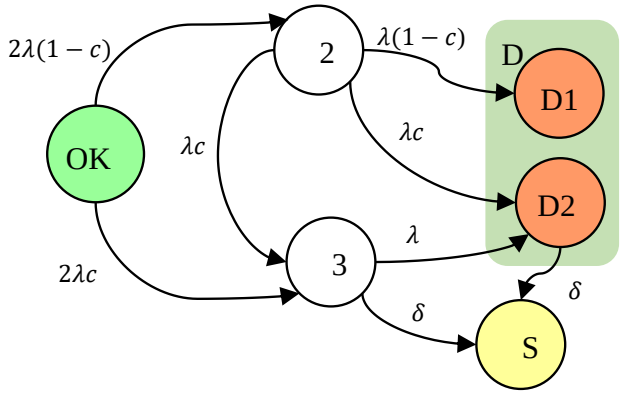


Fig. 3: The CTMC for the dual structure with the time-continuous fault detection – the low demand mode of operation.

The characteristic of the states in the model in Fig. 3 is listed in Tab. 1.

If the E-SRS operates in the low demand mode, so under certain conditions (if the SF is not required), a leaving the dangerous state D can be considered. Therefore, it is desirable to separate the dangerous state D on more qualitatively different substates. The state D (Fig. 3) contains these substates:

- D1 (5) – substate, in which is the E-SRS, when both units (R and L) have only the undetectable faults. This substate is necessary to consider as dangerous, because the E-SRS remains in this state until the time of requiring the SF. In case of the SF requiring, the EUC will not pass to the safe state.
- D2 (6) – substate, in which is the E-SRS, when both units have the fault (they can have even more faults), but at least one of these faults is detectable.

Tab. 1: The states in the CTMC in Fig. 3.

State	Characteristic
1 (OK)	E-SRS is functional. Neither the unit R nor the unit L has a random failure. Under this assumption $p_{\mathrm{OK}}\ (t=0)=1$.
2	Unit R or unit L has only the undetectable fault (one or more).
3	Unit R or unit L has the detectable faults. Units can have also the undetectable fault (one or more).
4 (S)	The safe (dysfunctional) state – the state after detection and negation of the fault.
D	The dangerous state – Unit R and unit L have a random failure.

The E-SRS can be in the state 3 or in the state D2 only when it has at least one detectable fault. It can be reasonably supposed, that the fault detection mechanism detects this fault, thereby the negation mechanism is activated and the E-SRS transits to the state S with the transition rate δ, which can be determined according to Eq. (1) – pessimistic approach:

$$\delta = \frac{1}{t_d + t_N}, \tag{1}$$

where t_d is the fault detection time (in this case $t_d = t_{cd}$, where t_{cd} is the duration time of one diagnostic cycle) and t_N is the time to negation of detected fault.

The probability of substate D1 can be calculated by solving the system of the differential equations:

$$\frac{\overrightarrow{dp(t)}}{dt} = \overrightarrow{p(t)} \cdot \mathbf{Q}, \tag{2}$$

on the basis of knowledge of the transition rate matrix

$$\mathbf{Q} = (Q_{ij}) \quad \text{for} \quad i,j \in \{1,\ldots,m\}, \tag{3}$$

and on the basis of knowledge of the initial distribution

$$\overrightarrow{P}_0 = \{p_1(t=0), p_2(t=0), \ldots, p_m(t=0)\}, \tag{4}$$

where q_{ij} is the transition rate from state i to state j and $q_{ii} = -\sum_{j=1, j\neq i}^{m} q_{ij}$ is the sojourn rate in state i, $\overrightarrow{p(t)} = \{p_1(t), p_2(t), \ldots, p_m(t)\}$ is distribution in time t, $p_i(t=0)$ is the probability of state i in time $t=0$ and m is the number of states.

2) Fault Detection Mechanism Operates Periodically and Discreetly in Time

If the fault detection mechanism operates periodically and discreetly in time - always at the end of the diagnostic cycle (Fig. 1(a)), the diagnostics influence on

the HW-SI of the E-SRS can be modelled using the combination of the CTMC and the DTMC.

The occurrence of random failures in time is continuous and independent of the fault detection mechanism. Therefore, the influence of the random failures on the safety integrity of E-SRS in time, when the fault detection mechanism is not active, can be described by the CTMC in Fig. 3 under assumption, that $\delta = 0$ (the transition to the state S is not possible).

The model in Fig. 3 (assuming that $\delta = 0$) can be described by Eq. (2) and Eq. (3) with the transition rate matrix

$$\mathbf{Q} = \begin{pmatrix} -2\lambda & 2\lambda(1-c) & 2\lambda c & 0 & 0 & 0 \\ 0 & -\lambda(1+c) & \lambda c & 0 & \lambda(1-c) & \lambda c \\ 0 & 0 & -\lambda & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (5)$$

and the differential equations system

$$\begin{aligned} p'_{\mathrm{OK}}(t) &= -2\lambda p_{\mathrm{OK}}(t), \\ p'_{2}(t) &= 2\lambda(1-c)p_{\mathrm{OK}}(t) - \lambda(1+c)p_2(t), \\ p'_{3}(t) &= 2\lambda c p_{\mathrm{OK}}(t) + \lambda c p_2(t) - \lambda p_3(t), \\ p'_{\mathrm{S}}(t) &= 0, \\ p'_{\mathrm{D1}}(t) &= \lambda(1-c)p_2(t), \\ p'_{\mathrm{D2}}(t) &= \lambda c p_2(t) + \lambda p_3(t). \end{aligned} \quad (6)$$

In this case, it is necessary to consider the state D as the dangerous state. The dangerous state probability in time, when the fault detection mechanism is not active, is the sum of the probabilities of the substate D1 and the substate D2.

The fault detection mechanism influence (Fig. 1) on the HW-SI of the E-SRS can be modelled using the DTMC (Fig. 4) and described by the transition probability matrix.

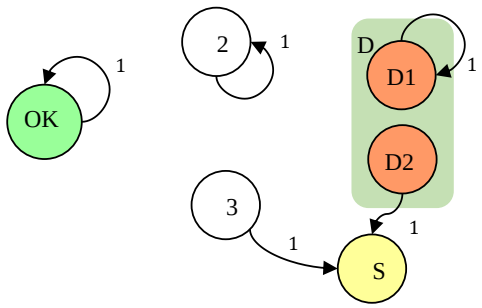


Fig. 4: The CTMC for the dual structure with the time-discrete fault detection – the low demand mode of operation.

Generally, the transition probability matrix is defined as follows:

$$\mathbf{P} = (P_{ij}) \quad \text{for} \quad i, j \in \{1, \ldots, m\}, \quad (7)$$

where p_{ij} is the transition probability of the system from state i to state j , q_{ii} is the sojourn probability in state i and m is the number of DTMC states.

For model shown in Fig. 4:

$$\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}. \quad (8)$$

Since the fault detection mechanism operates periodically, the initial probability distribution for the CTMC describing the random failures influence on the safety integrity in k-th cycle of diagnostics can be calculated using the DTMC:

$$\overrightarrow{P}_{k+1} = \overrightarrow{P}_k \cdot \mathbf{P}, \quad (9)$$

where $k \in \{0, \ldots, n\}$ and n is the number of diagnostic cycles.

Then for model in Fig. 4 is valid, that:

$$\begin{aligned} \overrightarrow{P_{k+1}(t=0)} = \Big\{ & p_{\mathrm{OK}}^{(k)}(t = t_{cd}), p_2^{(k)}(t = t_{cd}), 0, \\ & p_3^{(k)}(t = t_{cd}) + p_{\mathrm{S}}^{(k)}(t = t_{cd}) + p_{\mathrm{D2}}^{(k)}(t = t_{cd}), \\ & p_{\mathrm{D2}}^{(k)}(t = t_{cd}), 0 \Big\}, \end{aligned} \quad (10)$$

where $p_i^{(k)}(t = t_{cd})$ is the probability of the state i at the end of the k-th diagnostic cycle.

If in the time $t = 0$ is the E-SRS in the state OK (Fig. 4) then the initial distribution is

$$\overrightarrow{P_1(t=0)} = \{1, 0, 0, 0, 0, 0\}. \quad (11)$$

The dangerous state D probability decreases in consequence of the fault detection mechanism operation.

The dangerous state probability decreasing would reach the zero value, if $c = 1$.

Figure 5 shows the procedure for the CTMC/DTMC combination. This procedure is repeated for all diagnostic cycles.

3.2. Influence of Two Fault Detection Mechanisms

If the E-SRS contains two fault detection mechanisms, it is theoretically possible to consider various combinations of the operation of these fault detection mechanisms, depending on their parameters and the mode of operation.

Typically, it is such a combination of fault detection mechanisms, when one mechanism (the RM) is

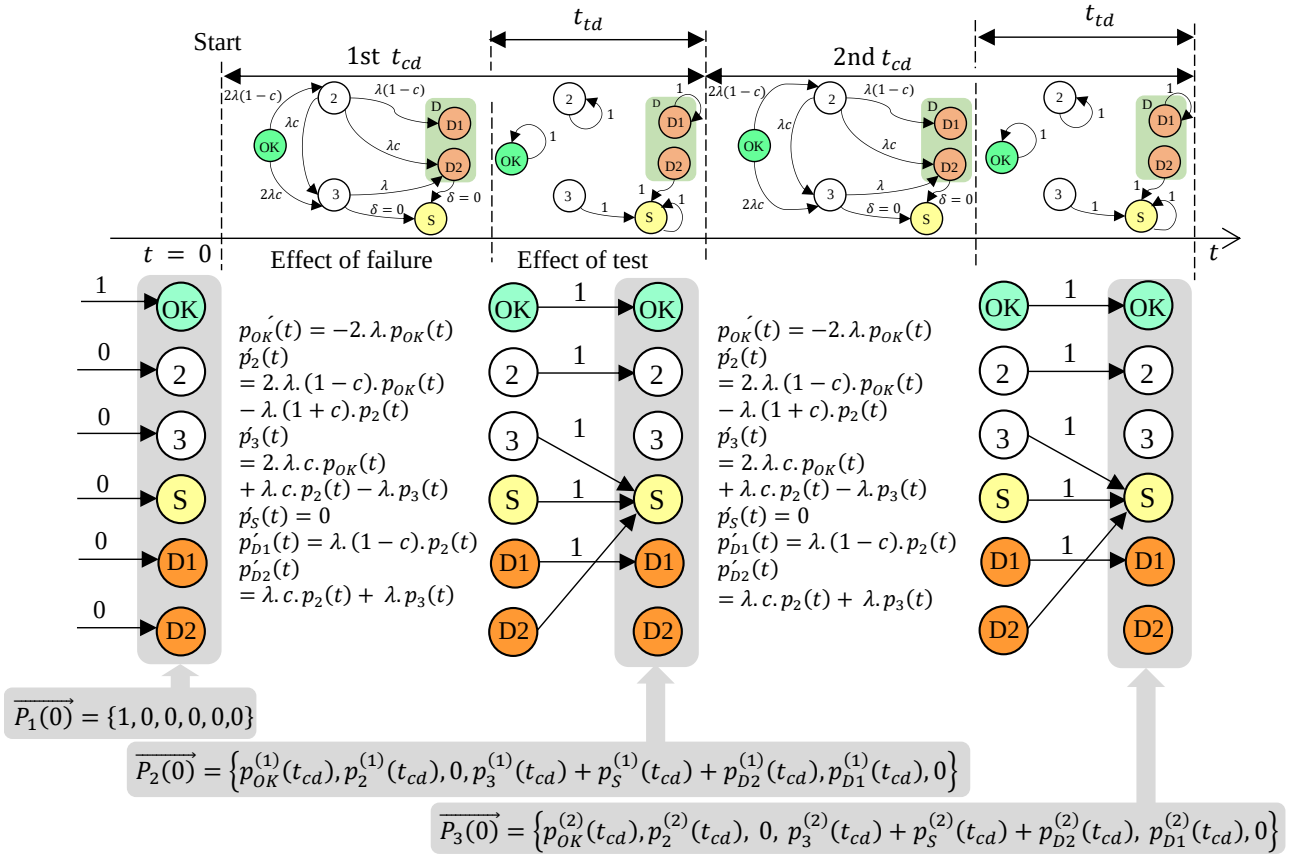


Fig. 5: The CTMC and DTMC combination.

intended for the detection of the maximum number of the faults in the shortest possible time interval and the second mechanism (the SM) is intended for the detection of a certain group of the faults, which are not detectable by the first mechanism. If the $t_{Sd} \gg t_{Rd}$, it is possible to proceed in such a way, that the RM operates continuously in time and the SM operates discretely in time.

Let both mechanisms operate discreetly in time. The model in Fig. 6 describes a behaviour of the E-SRS in time, when there is no operating fault detection mechanism (neither RM nor SM). The dangerous state D contains these substates:

- D1 – substate, in which is the E-SRS, when both units (R and L) have only the undetectable faults.
- D2 – substate, in which is the E-SRS, when one of the units (R or L) has at least one fault detectable by the RM (units can have also the undetectable faults or the faults detectable by the SM).
- D3 – substate, in which is the E-SRS, when one unit (R or L) has at least one fault detectable by the SM (units can have also the undetectable faults or the faults detectable by the RM).

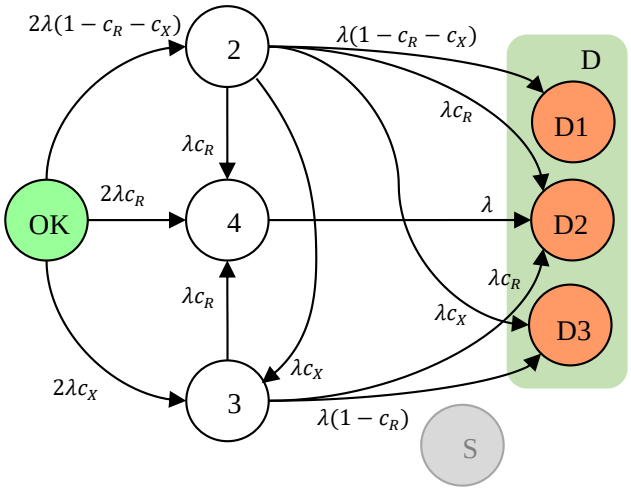


Fig. 6: The reduced CTMC for the dual structure with the time-discrete fault detection – the low demand mode of operation and with two fault detection mechanisms in time, when they are not active.

The diagnostic coverage coefficient of the faults, which are detectable only by the SM is defined as:

$$c_X = P_X \cdot (1 - c_R), \tag{12}$$

where P_X is the probability of the failure detection by the SM, which was not detected by the RM. If the

probability P_X cannot be believably determined, it is possible to use pessimistic approach and the assumption, that $P_X = 0$.

The E-SRS is in the state 4 (Fig. 6), when the first E-SRS fault is detectable by the RM (transition from the state OK to the state 4), or when in unit, which already has the fault undetectable by the RM, occurs the fault detectable by the RM (transition from the state 2 to the state 4 or transition from the state 3 to the state 4).

The E-SRS reaction to the fault detection mechanisms (RM, SM) is shown in Fig. 7. If $r = 1$, $s = 0$, the model corresponds to the E-SRS reaction to the RM. If $r = 0$, $s = 1$, the model corresponds to the E-SRS reaction to the SM.

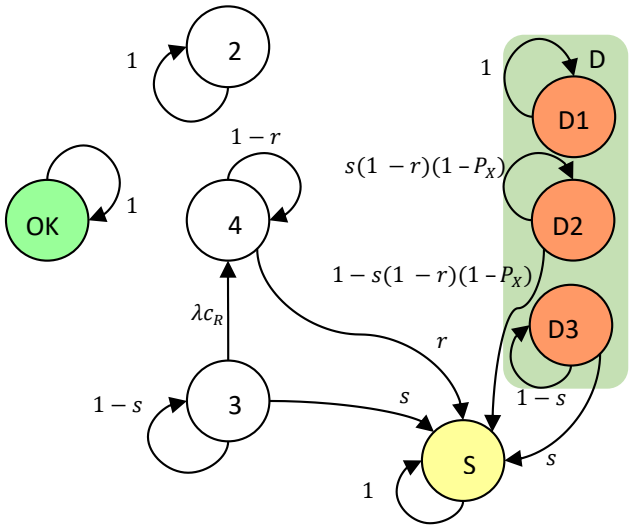


Fig. 7: The DTMC for the dual structure with the time-discrete fault detection – the low demand mode of operation and with two fault detection mechanisms.

The E-SRS (Fig. 7) is in the state 4 or in the state D2, when it has the fault detectable by the RM. Therefore, due to the fault detection by the RM ($r = 1$, $s = 0$) and the negation of its consequences, the E-SRS transits from the state 4 and D2 to the state S.

The E-SRS (Fig. 7) containing the fault detectable by the SM is in the state 3 or D3 and with a certain probability also in the state D2. Therefore, due to the fault detection by the SM ($r = 0$, $s = 1$) and the negation of its consequences, the E-SRS transits from the state 3 to the state S and from the state D3 to the state S with the probability 1. The E-SRS leaves the state D2 with the probability P_X.

If the inequality $t_{Sd} \gg t_{Rd}$ is valid, then given to the SM activity, the RM activity can be considered as continuous in time and it is possible to describe its influence on the HW-SI by the model in Fig. 8. The system transits into state S after detection and negation of fault by the RM and the rate of transition into

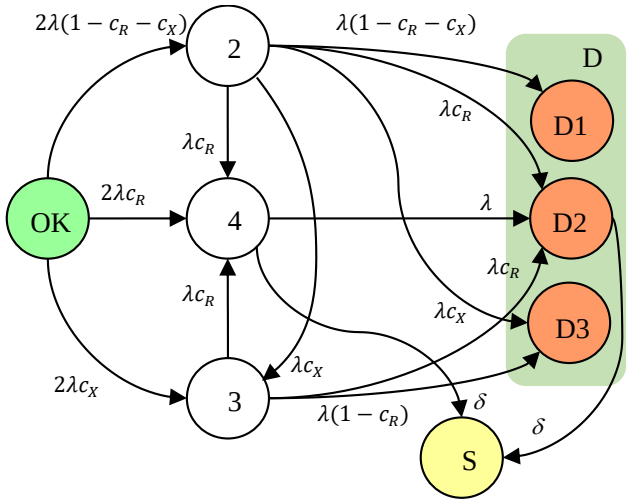


Fig. 8: The CTMC for the dual structure with the time-discrete fault detection – the low demand mode of operation and with two fault detection mechanisms, when they are active.

state S can be determined according to the Eq. (1). In mathematical description of the models in Fig. 6, Fig. 7 and Fig. 8 it is necessary to proceed the same as in Subsec. 3.1.

4. The Results of the Experiment

The aim of this part of the paper is to highlight the influence of the differently operating fault detection mechanisms and their properties (diagnostic coverage, fault detection time) on the dangerous failure probability of the SF ($p_D(t)$).

Let the SF be realized by the dual structure based on composite fail-safety with fail-safe comparison (Fig. 2). Let:

- $\lambda = \lambda_L = \lambda_R = 2 \cdot 10^{-5}$ h^{-1} (the unit R and the unit L are hardware identical).
- The considered time interval, in which the dangerous failure probability of the SF will be calculated, is 10 years (it can be e.g. the time interval between two proof tests of the E-SRS).
- The time to negation of a detected fault is negligible ($t_N \ll t_d$).

The E-SRS operates so that if the fault is detected, the safety reaction is triggered and the E-SRS transits to the state S (the SF is required). The transition rate to the state S is determined according to the Eq. (1).

The calculations were performed in the Mathematica SW tool.

4.1. One Fault Detection Mechanism

Let the E-SRS have one fault detection mechanism with the diagnostic coverage coefficient $c = 0.99$, which operates so that the diagnostic test is triggered every 0.5 h. The time duration of test and the time of negation is negligible given to the considered time interval 0.5 h.

If the SF operates in low demand mode of operation and the time of the diagnostic cycle (the fault detection time) is significantly less than the time between two proof tests ($t_{cd} \ll t_{proof}$), the dangerous failure probability of the SF can be calculated according to the Eq. (2) for the model in Fig. 3. The time dependence $p_D(t)$ is shown in Fig. 9.

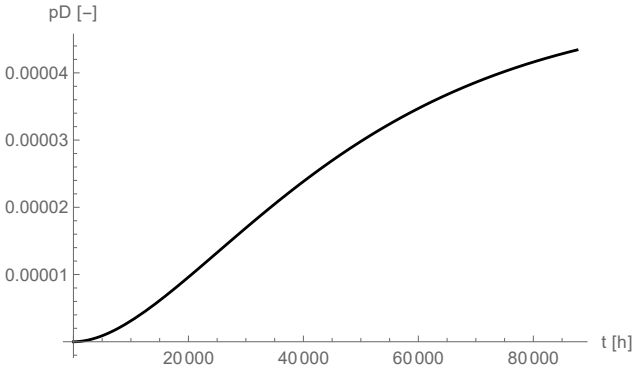


Fig. 9: The dangerous failure probability of the SF; one fault detection mechanism; calculation using the CTMC (Fig. 3).

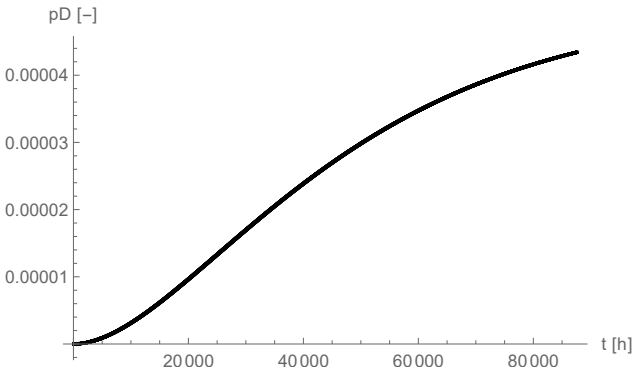


Fig. 10: The dangerous failure probability of the SF; one fault detection mechanism; calculation using the CTMC/DTMC (Fig. 3 and Fig. 4).

The dangerous failure probability of the SF, which operates in the low demand mode of operation, can be calculated also using the relations derived from the models in Fig. 3 (under assumption, that $\delta = 0$) and Fig. 4 (CTMC/DTMC combination). The time dependence $p_D(t)$ is shown in Fig. 10. Modelling of the dangerous failure probability of the SF using the CTMC/DTMC combination is closer to reality, but the calculation is significantly more time-consuming than in case of using only the CTMC.

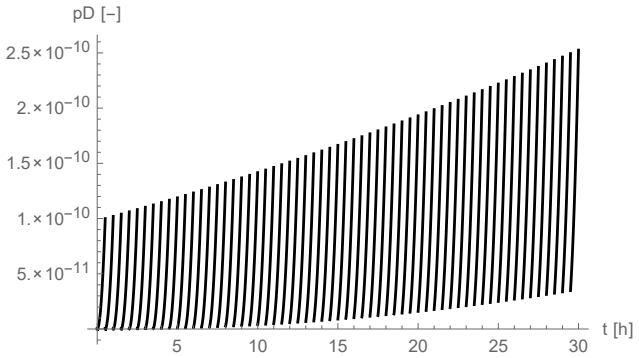


Fig. 11: The dangerous failure probability of the SF; one fault detection mechanism; calculation using the CTMC/DTMC (Fig. 3 and Fig. 4) in the shortened time frame for $c = 0.99$.

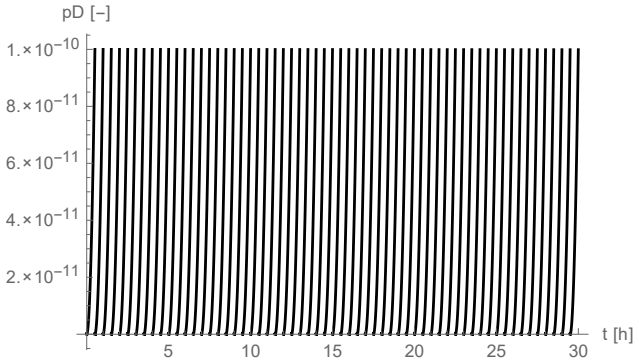


Fig. 12: The dangerous failure probability of the SF; one fault detection mechanism; calculation using the CTMC/DTMC (Fig. 3 and Fig. 4) in the shortened time frame for $c = 1$.

Using the CTMC/DTMC combination is demonstrated by "width" (saw-tooth shape) of the line in the graph in Fig. 10, what is caused by change of $p_D(t)$ value due to the operation of the RM. Influence of the RM can be observed more clearly in Fig. 11 and Fig. 12, where only a short period of time (0 to 30 hours) is shown, in order to observe the influence of time-discrete diagnostics method on observed value - $p_D(t)$.

4.2. Two Fault Detection Mechanisms

The graph in Fig. 13 shows the probability of the dangerous failure of the SF during one year of operation. Because this time interval is significantly larger than the considered time of the diagnostic period of the RM mechanism or SM mechanism ($t_{Rd} = 0.5$ h, $t_{Sd} = 10$ h), so the impact of the diagnostic coverage is demonstrated by "width" of the line – as in Fig. 10.

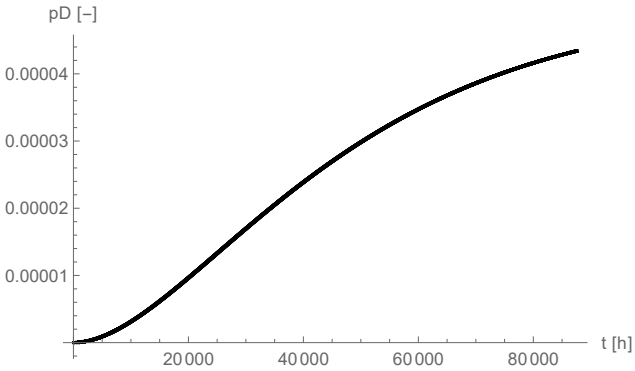


Fig. 13: The dangerous failure probability of the SF; two fault detection mechanisms; calculation using the CTMC/DTMC (Fig. 7 and Fig. 8) for $c_R = 0.9$ and $c_X = 0.09$.

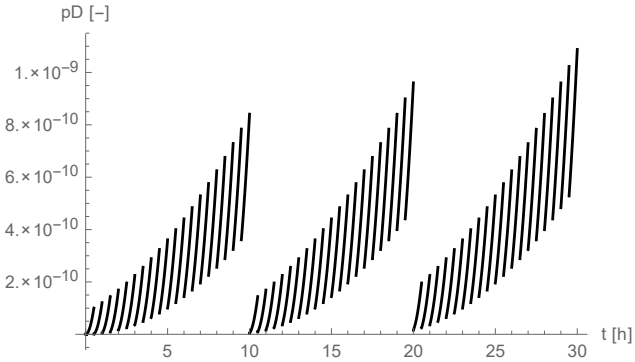


Fig. 14: The dangerous failure probability of the SF; two fault detection. mechanisms; calculation using the CTMC/DTMC (Fig. 6 and Fig. 7) in the shortened time frame for $c_R = 0.9$, $c_X = 0.09$, $t_{Rd} = 0.5$ h and $t_{Sd} = 10$ h.

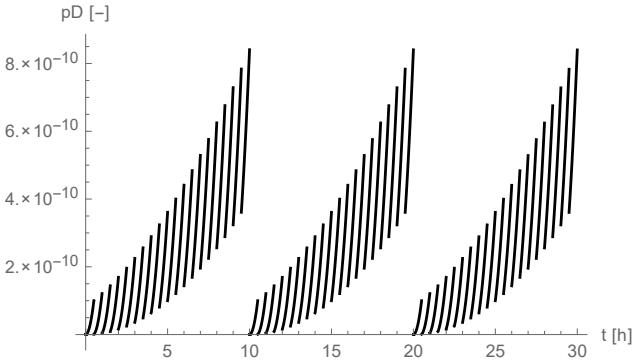


Fig. 15: The dangerous failure probability of the SF; two fault detection mechanisms; calculation using the CTMC/DTMC (Fig. 6 and Fig. 7) in the shortened time frame for $c_R = 0.9$, $c_X = 0.1$, $t_Rd = 0.5$ h and $t_{Sd} = 10$ h.

The probability of the dangerous failure of the SF (Fig. 13, Fig. 14 and Fig. 15) is calculated according to the relations derived from the models in Fig. 7 and in Fig. 8.

Real view at the operation of two fault detection mechanisms, which operates discreetly in time, and the diagnostic coverage influence, is obvious from the graphs in Fig. 14 and in Fig. 15.

5. Conclusion

have significant influence on the HW-SI of the SF. The restoration process is not directly visible on the considered models because the restoration process can begin only when the fault is detected and negated. In the paper, author assumes the dual structure of the E-SRS with the fail-safe property (Fig. 4) and therefore, after the detection and negation of the fault is the E-SRS operation interrupted and the E-SRS transits to the down state. The restoration process has no influence on the HW-SI of the SF (it has influence on the E-SRS availability). The E-SRS has the structure 2oo3 (three-channel structure) with such a property, that the detection and negation of the fault leads to the isolation of defective part of the E-SRS and to the change of the E-SRS structure (to the dual structure), so then the existence of the restoration even during the up state of the E-SRS can be assumed [14].

The procedures described in this document were practically used as part of the validation report for the Kernel of the JAZZ system (product of AZD Praha). In the Kernel analysis, three different fault detection mechanisms have been respected, which have an impact on the HW-SI of the Kernel [15].

Acknowledgment

This paper has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number 016ZU-4/2018: Modernization of teaching methods of management of industrial processes based on the concept of Industry 4.0.

References

[1] EN IEC 61508. *Functional safety of electrical/ electronic/programmable electronic safety-related systems.* Brussels: CENELEC, 2010.

[2] ZDANSKY, J., K. RASTOCNY and J. HRBCEK. Influence of Architecture and Diagnostic to the Safety Integrity of SRECS Output Part. In: *International Conference on Applied Electronics.* Pilsen: IEEE, 2015, pp. 179–182. ISBN 978-8-0261-0385-1.

[3] DING, L., H. WANG, K. KANG and K. WANG. A novel method for SIL verification based on system degradation using reliability block diagram. *Reliability Engineering & System Safety*. 2014, vol. 132, iss. 1, pp. 36–45. ISSN 0951-8320. DOI: 10.1016/j.ress.2014.07.005.

[4] DING, L., H. WANG, J. JIANG and A. XU. SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram. *Reliability Engineering & System Safety*. 2017, vol. 165, iss. 1, pp. 170–187. ISSN 0951-8320. DOI: 10.1016/j.ress.2017.03.005.

[5] FITHRI, P., N. A. RIVA, L. SUSANTI and B. YULIANDRA. Safety Analysis at Weaving Department of PT. X Bogor Using Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). In: *5th International Conference on Industrial Engineering and Applications*. Singapore: IEEE, 2018, pp. 382–385. ISBN 978-1-5386-5748-5. DOI: 10.1109/IEA.2018.8387129.

[6] IDEN, J. Assessing the effects of diagnostic failures on safety-related control systems. In: *International Automatic Control Conference*. Kaohsiung: IEEE, 2014, pp. 23–28. ISBN 978-1-4799-4584-9. DOI: 10.1109/CACS.2014.7097156.

[7] HOLUB, P. and J. BOERCSOEK. Advanced PFH Calculations for Safety Integrity Systems with High Diagnostic. In: *XXII International Symposium on Information, Communication and Automation Technologies*. Bosnia: IEEE, 2009, pp. 69–76. ISBN 978-1-4244-4220-1. DOI: 10.1109/ICAT.2009.5348449.

[8] ILAVSKY, J., K. RASTOCNY and J. ZDANSKY. Common-cause Failures as Major Issue in Safety of Control Systems. *Advances in Electrical and Electronic Engineering*. 2013, vol. 11, iss. 2, pp. 86–93. ISSN 1804-3119. DOI: 10.15598/aeee.v11i2.748.

[9] LIU, Y. L., M. RAUSAND and H. JIN. Modeling and reliability assessment of a 3-channel safety-instrumented system. In: *International Conference on Industrial Engineering and Engineering Management*. Hong Kong: IEEE, 2012, pp. 2098–2102. ISBN 978-1-4673-2945-3. DOI: 10.1109/IEEM.2012.6838116.

[10] MECHRI, W., C. SIMON and K. BENOTHMAN. Switching Markov chains for a holistic modeling of SIS unavailability. *Reliability Engineering & System Safety*. 2015, vol. 133, iss. 1, pp. 212–222. ISSN 0951-8320. DOI: 10.1016/j.ress.2014.09.005.

[11] RASTOCNY, K., J. ZDANSKY, J. BALAK and P. HOLECKO. Diagnostics of an output interface of a safety-related system with safety PLC. *Electrical Engineering*. 2017, vol. 99, iss. 4, pp. 1169–1178. ISSN 0948-7921. DOI: 10.1007/s00202-017-0624-1.

[12] RASTOCNY, K., J. ZDANSKY, M. FRANEKOVA and I. ZOLOTOVA. Modelling of diagnostics influence on control system safety. *Computing and Informatics*. 2018, vol. 37, iss. 2, pp. 457–475. ISSN 1335-9150. DOI: 10.4149/cai_2018_2_457.

[13] BALAK, J. and K. RASTOCNY. Use of tensor construction of Markov chains when evaluating observed feature of E-SRS. In: *ELEKTRO*. Mikulov: IEEE, 2018, pp. 1–6. ISBN 978-153864759-2. DOI: 10.1109/ELEKTRO.2018.8398309.

[14] GABRIEL, T., A. HILDEBRANDT and U. MENCK. PFD Calculation Considering Imperfect Proof Tests. *Chemical Engineering Transactions*. 2016, vol. 48, iss. 1, pp. 637–642. ISSN 2283-9216. DOI: 10.3303/CET1648107.

[15] RASTOCNY, K. Quantitative analysis of the Kernel. Project JAZZ. *Validation Report - technical safety principle JAZZ*. AZD Praha, 2018. Contract SOD-007-18-40.

About Authors

Karol RASTOCNY was born in Petrovice, Slovak Republic. He graduated at the Department of Signalling and Communication Systems of the Faculty of Mechanical and Electrical Engineering, Technical University of Transport and Communications, Zilina, Slovak Republic in 1982. He defended is Ph.D. in the field of safety analysis in 1995. Since 2008 he has been working as a Professor at the Department of Control and Information Systems at the Faculty of Electrical Engineering and Information Technology, University of Zilina. His professional orientation covers solving problems of functional and technical safety of safety-related control systems.