Computing and Informatics, Vol. 37, 2018, 457–475, doi: 10.4149/cai_2018_2_457

MODELLING OF DIAGNOSTICS INFLUENCE ON CONTROL SYSTEM SAFETY

Karol RÁSTOČNÝ, Juraj ŽDÁNSKY, Mária FRANEKOVÁ

Faculty of Electrical Engineering, University of Žilina
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: {karol.rastocny, juraj.zdansky, maria.franekova}@fel.uniza.sk

Iveta ZOLOTOVÁ

Faculty of Electrical Engineering and Informatics, Technical University of Košice
Letná 9, 040 00 Košice, Slovakia
e-mail: iveta.zolotova@tuke.sk

Abstract. If the control system besides the standard control functions also realizes the functions (known as safety functions), failures of which can influence safety of the controlled process, then the control system may be a source of risk for assets, that are within the scope of the controlled process. Early detection of these failures and subsequent negation of their effects can have a significant influence on the safety integrity level of the safety function and thus also on the elimination of risks related to the controlled process. Therefore, the diagnostics is the means which, if appropriately applied, can increase not only the availability, but also the safety of the control system. The paper deals with using the homogeneous Markov chains to influence the evaluation of on-line diagnostics on the hardware safety integrity of the safety function, depending on the application method of several simultaneously operating diagnostics mechanisms and their basic parameters – the failures diagnostic coverage coefficient and the failure diagnostics time.

Keywords: Safety integrity, safety function, diagnostics, analysis, Markov process

1 INTRODUCTION

There are many cases in industry, when the controlled process can be a source of a significant danger that can result in personal injury, environmental damage or other undesirable consequences. If the risk related to the controlled process is bigger than the acceptable risk, then it is necessary to use appropriate measures to minimize this risk at least to the acceptable risk level [1, 2]. One of the technical measures is also the use of safety functions (SF), that are implemented by the safety related control system (SRCS). SF is function (risk reduction measure), that is intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a specific hazardous event [1].

From a safety point of view it is important to detect and negate any dangerous failure as soon as possible (negation – enforcement of a safe state following the detection of a failure). As the dangerous failure (in this paper) is considered the failure that causes the SRCS transition into a dangerous state or increases the probability of the SRCS transition into a dangerous state. The failure detection and subsequent negation of the failure consequences have significant influence on the safety integrity level (SIL) of the SF [1, 12, 13]. Therefore, the SRCS generally contains on-line functional diagnostics in addition to on-line test diagnostics (the SRCS is automatically on-line tested), especially if SFs are implemented with the SIL3 or SIL4 [4, 15].

To analyze the failures consequences on the hardware safety integrity, the methods that were originally intended for the analysis of the reliability – RBD (Reliability Block Diagram) and FTA (Fault Tree Analysis) are very often used. However, these methods do not allow a complex influence assessment of multiple properties of the SRCS on the hardware safety integrity of the SFs, which are realized by the SRCS. From this point of view, it is more appropriate to use for example the methods using the continuous-time Markov chain (CTMC), either alone [3, 14], or in a combination with the discrete-time Markov chain (DTMC) [6]. Also it is possible to use other methods, for example methods based on the Petri nets [7, 8, 9].

The publications, dealing with the failures on-line diagnostics influence on the hardware safety integrity, generally consider only one failure detection mechanism that operates continuously in time [5, 9, 15]. The failure detection mechanism, which operates discreetly in time, is considered only in case of periodic maintenance or repair of the system [4, 9, 10, 11, 16]. However, in practice it is possible that the SRCS contains more mechanisms for the failures detection, which vary by their parameters and the character of the activity. This paper deals with the analysis of the simultaneous operation of several mechanisms of the failures detection and their influence on the hardware safety integrity of the SF. The usage of the proposed method is presented on the SRCS with dual structure based on composite fail-safety with fail-safe comparison.

2 MARKOV CHAINS

Let us consider a stochastic process that fulfills the Markov property

$$\Pr\{X(t) \leq x \mid X(t_0) = x_0, X(t_1) = x_1, \ldots, X(t_n) = x_n\} = \Pr\{X(t) \leq x \mid X(t_n) = x_n\}$$

where $X(t)$ is the random variable, $t \in T$ (T is the time range) is the time parameter and is valid, that $0 \leq t_0 < t_1 < \cdots < t_n < t$.

If the value, which is acquired by $X(t)$, is called state and if the set of states is countable, then Markov process forms the Markov chain (MC). We distinguish two basic types of the MC:

- discrete-time Markov chain (DTMC);
- continuous-time Markov chain (CTMC).

The MC can be homogeneous or nonhomogeneous. In this paper a premise is accepted that the considered MC are homogeneous.

For the homogeneous DTMC the transition probability of the system from state i to state j can be calculated as the conditional probability, that the system in time $t = n + 1$ goes to state j, under the condition, that the system in time $t = n$ was in state i, i.e.

$$p_{ij} = \Pr\{X_{n+1} = j \mid X_n = i\}. \tag{1}$$

The homogeneous DTMC is completely defined, if the transition matrix (2) and the initial distribution (3) are defined.

$$\mathbb{P} = (p_{ij}) \text{ for } i, j \in \{1, \ldots, m\}, \tag{2}$$

$$\overrightarrow{P_0} = \overrightarrow{P_0(t=0)} = \{p_1(t=0), p_2(t=0), \ldots, p_m(t=0)\} \tag{3}$$

where $\overrightarrow{P_0}$ is the initial distribution at time $t = 0$, $p_i(t = 0)$ is the probability of state i at the time $t = 0$. The DTMC distribution in time $t = k + 1$ for $k \in \{0, \ldots, n\}$ is

$$\overrightarrow{P_{k+1}} = \overrightarrow{P_k} \cdot \mathbb{P}. \tag{4}$$

For the homogeneous CTMC the transition probability of the system from state i to j state can be calculated as the conditional probability, that the system in time $t = t + \Delta t$ goes to state j, under the condition, that the system in time t was in state i, i.e.

$$P_{ij}(t + \Delta t) = \Pr\{X(t + \Delta t) = j \mid X(t) = i\}. \tag{5}$$

The homogeneous CTMC is completely defined, if the transition rate matrix (6) and the initial distribution (3) are defined.

$$\mathbb{Q} = (q_{ij}) \text{ for } i, j \in \{1, \ldots, m\} \tag{6}$$

where q_{ij} is the transition rate from state i to state j and $q_{ii} = -\sum_{j=1,j\neq 1}^{m} q_{ij}$ is the sojourn rate in state i. If the CTMC is homogeneous, the transition rates are constant.

The CTMC distribution in time t can be calculated as a solution of the differential equations system (7) for the initial distribution (3)

$$\frac{\overrightarrow{\mathrm{d}P(t)}}{\mathrm{d}t} = \overrightarrow{P(t)} \cdot \mathbb{Q}. \tag{7}$$

3 GENERAL VIEW ON THE FAILURES DIAGNOSTICS

The SRCS can contain one or more failure detection mechanisms. The failure detection mechanism can be characterized by the failure detection time t_d and the diagnostic coverage coefficient c. For the hardware safety integrity evaluation the diagnostic coverage coefficient of the dangerous failures is relevant

$$c_D = \frac{\lambda_{dD}}{\lambda_D} \tag{8}$$

where λ_{dD} is the dangerous detectable hardware failure rate and c is the diagnostic coverage coefficient and λ_D is the dangerous failure rate.

In general, it is valid, that $\lambda_D = k \cdot \lambda, k \leq 1$. If the value k cannot be exactly proved for the application, it is necessary to choose the value k in accordance with the requirements of the relevant standards for the applications area.

If the SRCS contains one failure detection mechanism, this mechanism in principle can work by a schedule where the failure diagnostics operates:

- periodically and discreetly in time – always at the end of the diagnostic cycle (Figure 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 failure detection) and t_{td} is the operation time of the failure detection mechanism (the testing time); or
- periodically and continuously in time (Figure 1 b)).

If the SRCS contains two failure detection mechanisms, it is necessary to assume, that these mechanisms differ from each other by the failure detection time and the diagnostic coverage of the failures.

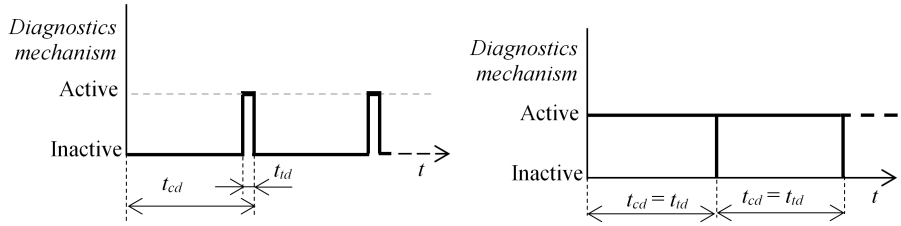
Let the system contains two failure detection mechanisms:

- the "rapid"detection mechanism (RM), which is characterized by the detection time t_{Rd} and the diagnostic coverage coefficient of the dangerous failures c_{DR};
- the "slow"detection mechanism (SM), which is characterized by the detection time t_{Sd} and the diagnostic coverage coefficient of the dangerous failures c_{DS}.

The Figure 2 shows the influence of these two diagnostics mechanisms on the overall diagnostic coverage of the dangerous failures. It shows, that

$$\lambda_D = \lambda_{uD} + \lambda_{dD\_R} + \lambda_{dD\_X} \tag{9}$$

where λ_D is the dangerous failure rate, λ_{uD} is the undetectable dangerous failure rate, λ_{dD_R} is the dangerous failure rate, which are detectable by the RM, λ_{dD_X} is the dangerous failure rate, which are detectable only by the SM.



a) Periodically and discreetly in time

b) Periodically and continuously in time

Figure 1. Operation of the failure detection mechanism

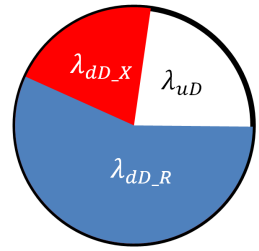


Figure 2. Diagnostic coverage of failures – two failure detection mechanisms

The probability of the failure detection by the SM, which was not detected by the RM, can be calculated according to the equation

$$Px = \frac{c_D - c_{DR}}{(c_D - c_{DR}) + (1 - c_D)} = \frac{c_D - c_{DR}}{1 - c_{DR}} \tag{10}$$

where c_D is the diagnostic coverage coefficient of the dangerous failures, which are detectable by the RM or SM and c_{DR} is the diagnostic coverage coefficient of the dangerous failures, which are detectable by the RM.

In reality it is necessary to assume, that some of the dangerous failures are covered by both failure detection mechanisms and also that there can be a part of failures, which are not covered by any failure detection mechanism. In general, the diagnostic coverage of the failures covered by the SM can be significantly lower than the diagnostic coverage of the failures covered by the RM, because the SM may be intended for detection of certain failures, which are not detectable by the RM.

Generally, it is possible to say, that:

- $c_D > c_{DR}$; if $c_D = c_{DR}$, it does not make any sense to apply the SM and $P_X = 0$;
- if $c_{DR} < 1$ and at the same time $c_D = 1$, then $P_X = 1$.

If the SRCS contains more failure detection mechanisms, a simplified method can be also used as the parameters estimation of the failure diagnostics, based on pessimistic premise that

$$c_D = \max\{c_{Di}\} \text{ for } i =\in \{1, \ldots, n\},$$
$$t_{cd} = \max\{t_{cdi}\} \text{ for } i =\in \{1, \ldots, n\} \tag{11}$$

where c_{Di} is the diagnostic coverage coefficient of dangerous failures, which are detectable by i^{th} failure detection mechanism; t_{cdi} is the maximum time of the dangerous failure detection, which is detectable by i^{th} failure detection mechanism and n is a number of failure detection mechanisms.

4 THE HARDWARE SAFETY INTEGRITY OF THE DUAL STRUCTURE

In practice, SRCS with dual structure based on composite fail-safety are often used with fail-safe comparison. The standard [1] requires to realize the hardware safety integrity evaluation not for the system, but individually for each SF. Due to clarity reason of this paper it is assumed that the SRCS comprises two hardware identical and physically independent units – unit R and unit L (Figure 3), which control the EUC. Let both these units participate in realization of one SF and each unit may contain several elements – for example sensors, logic, actuators. On this premise, the dangerous state of the SRCS can be identified with dangerous failure of the SF.

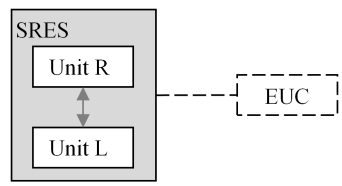


Figure 3. Block diagram of a general dual structure

In general, the SRCS with this structure has the RM, which is based on mutual data comparison of the units R and L after each operation cycle (comparative mechanism) and in many cases also the SM, which is focused on the failures, which are not detectable by the comparative mechanism.

As it is the dual structure with identical units, it is valid:

$$\lambda_L = \lambda_R = \lambda \tag{12}$$

where λ_L is the hardware failure rate of the unit L and λ_R is the hardware failure rate of the unit R.

5 THE DANGEROUS FAILURE PROBABILITY OF THE SF

In general, the SF can be performed in the low demand mode of operation or in the high demand mode of operation (in continuous mode of operation) [1].

If the SF operates in the continuous mode, then as the dangerous state of the SRCS is considered the state, which terminates the ability to realize its SF in compliance with the safety requirements specifications. In this case, the analysis of the SRCS failure consequences ends when the dangerous state is reached – it is necessary to identify the dangerous state of the SRCS with the dangerous state of the EUC.

In this paper it is considered, that the SF operates in the continuous mode and occurrence of the electronic elements failures can be regarded as the continuous random process, which follows the exponential distribution law. It is also taken into account the pessimistic assumption, that

$$\lambda_D = \lambda, \qquad c_D = c, \qquad c_{DR} = c_R, \qquad c_{DS} = c_S \tag{13}$$

where c is the overall diagnostic coverage coefficient of the failures, $c_R(c_S)$ is the diagnostic coverage coefficient of the failures covered by the RM (SM).

A. Influence of One Diagnostics Mechanism – Continuous Mode of Operation

If the method based on the MC is used for the hardware safety integrity evaluation, then for the dual structure (Figure 3) with hardware identical units can be used the CTMC, which is shown in Figure 4.

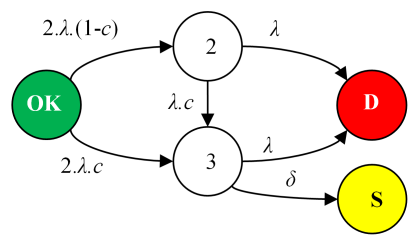


Figure 4. The Markov model for the dual structure with the time-continuous failure detection – continuous mode of operation and with one failure detection mechanism

It is a simplified approach to the hardware safety integrity evaluation, which can be used just when the SRCS has the failure detection mechanism. This failure detection mechanism operates continuously in time and the SRCS operates in the continuous mode.

The characteristic of the states in the model in Figure 4 is listed in Table 1.

State	Characteristic
OK	SRCS is functional; neither one unit has the failure.
2	Unit R or unit L has only the undetectable failures (one or more).
3	Unit R or unit L has the detectable failures (one or more); units can have also the undetectable failures (one or more).
S	The safe (dysfunctional) state – the state after detection and negation of the failure. The EUC is in state, which is not dangerous.
D	The dangerous state – both units have the failure.

Table 1. States of the model in Figure 4

The SRCS can go from the state OK to the dangerous state D on a trajectory, which depends on the sequence of the failures occurrence and their detectability (detectable or undetectable).

The characteristic of the transitions in the model in Figure 4 is listed in Table 2.

Transition	Characteristic
OK $\rightarrow$ 2	Transition is realized, if the undetectable failure occurs in unit L or unit R.
OK $\rightarrow$ 3	Transition is realized, if the detectable failure occurs in unit L or unit R.
2 $\rightarrow$ D	Transition is realized due to the failure occurrence in the unit (L or R), which is without failure.
2 $\rightarrow$ 3	Transition is realized due to the detectable failure occurrence in the unit, which already has the undetectable failure.
3 $\rightarrow$ D	Transition is realized due to the failure occurrence in the unit (L or R), which is without failure.
3 $\rightarrow$ S	Transition is realized due to the detection and negation of the failure occurrence.

Table 2. Transitions in the model in Figure 4

The transition rate from the state 3 to the state S can be expressed by the equation

$$\delta = \frac{1}{t_d/2 + t_N} \tag{14}$$

where δ is the failure detection and negation rate, t_d is the failure 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 needed to the detected failure negation. Using the mean value of the failure detection time is not accurate, but acceptable in practice [1, 2]. In case of

the pessimistic approach, the transition rate from the state 3 to the state S can be expressed by the equation

$$\delta = \frac{1}{t_d + t_N}. \tag{15}$$

CTMC in Figure 4 can be described by the transition rate matrix (16) and the differential equations system (17):

$$\mathbb{Q} = \begin{pmatrix} -2\lambda & 2\lambda \cdot (1-c) & 2\lambda \cdot c & 0 & 0 \\ 0 & -\lambda \cdot (1+c) & \lambda \cdot c & 0 & \lambda \\ 0 & 0 & -\lambda - \delta & \delta & \lambda \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{16}$$

$$\begin{aligned} p'_{OK}(t) &= -2\lambda \cdot p_{OK}(t), \\ p'_2(t) &= 2\lambda \cdot (1-c) \cdot p_{OK}(t) - \lambda \cdot (1+c) \cdot p_2(t), \\ p'_3(t) &= 2\lambda \cdot c \cdot p_{OK}(t) + \lambda \cdot c \cdot p_2(t) - (\lambda + \delta) \cdot p_3(t), \\ p'_s(t) &= \delta \cdot p_3(t), \\ p'_D(t) &= \lambda \cdot p_2(t) + \lambda \cdot p_3(t). \end{aligned} \tag{17}$$

If in the time $t = 0$ the SRCS is in the state OK (Figure 4), then the initial vector

$$\overrightarrow{P_0(t=0)} = \{1, 0, 0, 0, 0\}, \tag{18}$$

and the dangerous state probability [5]

$$\begin{aligned} p_D(t) = e^{-2\lambda.t} - 1 + \frac{2\delta}{(\lambda \cdot c - \delta) \cdot (1+c)}(e^{-\lambda \cdot (1+c) \cdot t} - 1) \\ - \frac{2\lambda^2 \cdot c}{(\lambda \cdot c - \delta) \cdot (\lambda + \delta)}(e^{-(\lambda+\delta) \cdot t} - 1). \end{aligned} \tag{19}$$

If $c = 0$, then

$$p_D(t) = 1 - 2e^{-\lambda \cdot t} + e^{-2\lambda \cdot t}. \tag{20}$$

If $c = 1$, then

$$p_D(t) = \frac{e^{-2\lambda \cdot t}\lambda \cdot (\delta - \delta \cdot e^{2\lambda \cdot t} + \lambda + \lambda \cdot e^{2t \cdot \lambda} - 2\lambda \cdot e^{-(\delta - \lambda) \cdot t})}{(\lambda + \delta)(\lambda - \delta)}. \tag{21}$$

At the latest in time, when the probability value of the state D achieves the critical limit (the maximum allowed value related to the acceptable risk), it is necessary to terminate the SRCS operation and execute the proof-test. The influence of the proof-test on the hardware safety integrity of the SRCS is described in [9, 10, 11, 16].

If the SRCS operates in the continuous mode and the failures diagnostics operates periodically and discreetly in time – always at the end of the diagnostic cycle (Figure 1 a)), then the diagnostics influence on the hardware safety integrity of the SRCS can be modelled using the multi-phase Markov model – combination of the CTMC and the DTMC.

The failures influence on the hardware safety integrity of the SRCS in time, when the failure diagnostics mechanism is not active, can be described by the model in Figure 5. The failures occurrence is continuous in time, but the failure detection is not possible and therefore the transition from the state 3 to the state S is not possible. The state S in the model in Figure 5 is mentioned only by the reason of representation of a compatibility with the model in Figure 4.

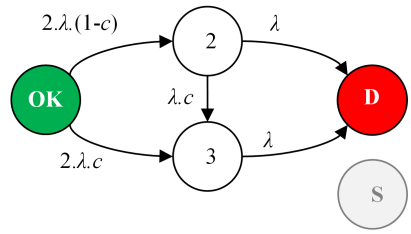


Figure 5. The reduced CTMC model for the dual structure with the time-continuous failures detection – continuous mode of operation and with one failure detection mechanism in time, when it is not active

The model in Figure 5 can be described by the differential equations system

$$\begin{aligned} p'_{OK}(t) &= -2\lambda \cdot p_{OK}(t), \\ p'_2(t) &= 2\lambda \cdot (1-c) \cdot p_{OK}(t) - \lambda \cdot (1+c) \cdot p_2(t), \\ p'_3(t) &= 2\lambda \cdot c \cdot p_{OK}(t) + \lambda \cdot c \cdot p_2(t) - \delta \cdot p_3(t), \\ p'_s(t) &= 0, \\ p'_D(t) &= \lambda \cdot p_2(t) + \lambda \cdot p_3(t). \end{aligned} \tag{22}$$

The failure detection mechanism influence (Figure 1 a)) on the hardware safety integrity of the SRCS provided, that $t_d \to 0$ (theoretical, but acceptable assumption) can be modelled using the DTMC (Figure 6) and described by the transition probability matrix

$$\mathbb{P} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{23}$$

Using the matrix (23), is possible to calculate the initial distribution for solution of the differential equations system (22) for the next diagnostic cycle

$$\overrightarrow{P_{n+1}(t=0)} = \overrightarrow{P_n(t=t_{cd})} \cdot \mathbb{P} \tag{24}$$

where n is the test cycle order ($n = 1$ after putting the SRCS into operation), $\overrightarrow{P_n(t=t_{cd})}$ is solution of the differential equations system (22) with the initial distribution (18) in the time $t = 0$ or the initial distribution calculated according to (24) in the time $t = t_{cd}$ (after the execution of n^{th} test cycle).

$$\overrightarrow{P_n(t)} = \left\{ p_{OK}^{(n)}(t), p_2^{(n)}(t), p_3^{(n)}(t), p_s^{(n)}(t), p_D^{(n)}(t) \right\}. \tag{25}$$

The initial distribution for the next $(n+1)$ cycle

$$\overrightarrow{P_{n+1}(t=0)} = \left\{ p_{OK}^{(n)}(t=t_{cd}), p_2^{(n)}(t=t_{cd}), 0, p_3^{(n)}(t=t_{cd}) + p_s^{(n)}(t=t_{cd}), \right.$$
$$\left. p_D^{(n)}(t=t_{cd}) \right\}. \tag{26}$$

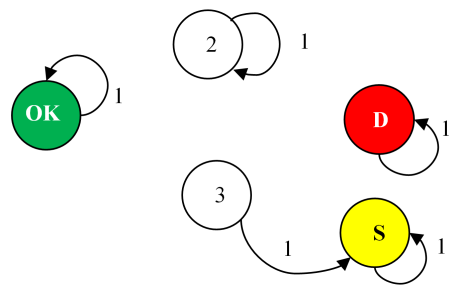


Figure 6. The DTMC model for the dual structure with the time-discrete failures diagnostics – continuous mode of operation and with one failure detection mechanism

B. Influence of Two Diagnostics Mechanisms – Continuous Mode of Operation

If the SRCS contains two failure detection mechanisms, then it is possible to consider various combinations of operation of these failure detection mechanisms according to the parameters and the operation mode. Generally, it is such a combination of the failure detection mechanisms, that one mechanism is intended for the detection of the maximum number of failures in the shortest possible time interval (the RM) and the second mechanism (the SM) is intended for the detection of a certain group of failures, which are not covered by the first mechanism.

The analysis of the failure consequences on the hardware safety integrity can be based on the same principles as in the case of one failure detection mechanism. Although it is possible to proceed in a number of ways, the most suitable are the following ones:

1. If the failure detection time is approximately the same for both the mechanisms, thus it is possible to proceed in such a way, as if the SRCS contains only one failure detection mechanism with the diagnostic coverage coefficient, which can be calculated according to the (10) (if the P_x is unknown, is necessary to choose $P_x = 0$) and the failure detection time, which can be determined according to the (11).
2. It is possible to divide the set of failures on two subsets (X, Y) and make the analysis for each of them separately. The final probability of the dangerous state

$$p_D(t) = p_{DX}(t) + p_{DY}(t) - p_{DX}(t) \cdot p_{DY}(t), \tag{27}$$

   provided, that the dangerous state occurrence probability in consequence of the failures from the first subset $p_{DX}(t)$does not influence the dangerous state occurrence probability in consequence of the failures from the second subset $p_{DY}(t)$ and vice versa.
3. 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.

If it is valid, that $t_{Rd} \ll t_{Sd} \ll t_{proof}$ (t_{proof} is the maximum time value between two proof tests; in extreme cases that can be identified with the useful life of the SRCS), not only the failures diagnostics of the RM, but even the failures diagnostics of the SM can be considered as the continuous-time process. Then the SRCS reaction to the failures occurrence can be described by the CTMC, which is shown in Figure 4.

The transition rate from the state 3 to the state S (Figure 4) can be determined according to the (14) or (15). If the failure is detectable by the RM, then $t_d = t_{Rd}$. If the failure is detectable by the SM, then $t_d = t_{Sd}$. Real value of the $t_d \in \langle t_{Rd}, t_{Sd} \rangle$. In case of pessimistic approach, it can be assumed, that $t_d = t_{Sd}$. The diagnostic coverage coefficient of the failures can be determined according to the (10). The dangerous state probability can be calculated according to the (19) for the time interval $t \in \langle 0, t_{proof} \rangle$ and if the proof-test is perfect, this curve will be repeated periodically [9].

6 THE EXPERIMENTAL RESULTS AND DISCUSSION

Let us suppose that the SF is implemented by the dual structure based on composite fail-safety with fail-safe comparison, as it is shown in Figure 3. The SRCS in compliance with functional specification of the SF controls EUC. The unit R and the unit L are hardware identical. Their failures rate $\lambda = \lambda_L = \lambda_R = 2 \times 10^{-5}$ h^{-1}. The functional specification of the SF is irrelevant from the view of hardware

safety integrity analysis of the SRCS. Let the supposed time interval, in which the dangerous failure probability of the SF ($p_D(t)$) will be calculated, be 1 year (it can be, e.g., the time interval between the proof tests).

The SRCS operates in such a way that if the failure is detected, the safety reaction is triggered and the SRCS transits to the state S (interruption of the SRCS operation). The transition rate of the SRCS to the state S is determined according to the (15).

A. One Failure Detection Mechanism

Let the SRCS have one failure detection mechanism with the diagnostic coverage coefficient of the failures $c = 0.99$, which operates in such manner that the diagnostic test is triggered every 0.5 h. The time duration of test and the time of reaction to the failure is negligible with respect to the considered time interval 0.5 h.

If the SF is performed in continuous mode of operation and the diagnostic cycle time (the failure 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 relation derived for the model in Figure 4. The time dependence ($p_D(t)$) is shown in Figure 7.

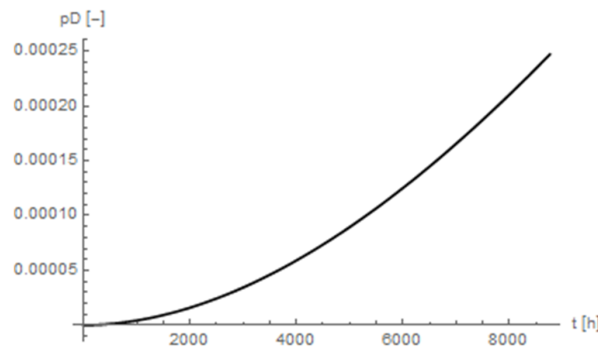
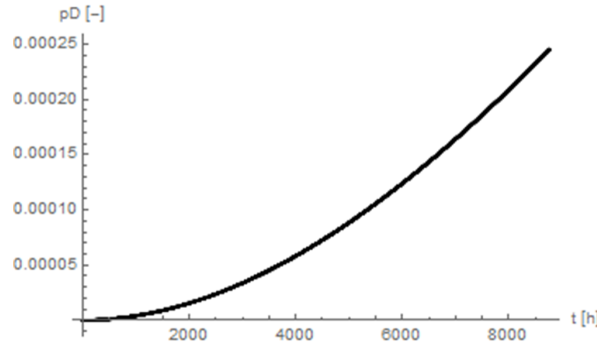


Figure 7. The dangerous failure probability of the SF; one failure detection mechanism; continuous mode of operation – calculation using the CTMC model (Figure 4)

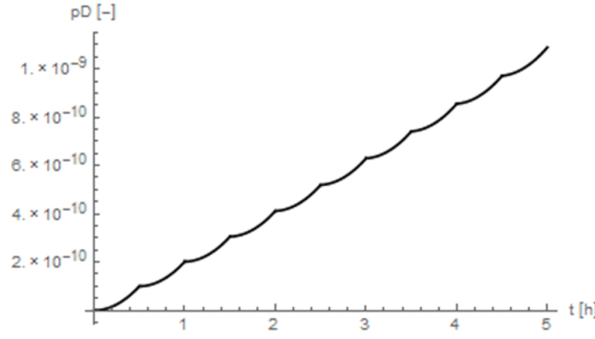
The dangerous failure probability of the SF can be calculated also using the relations derived from models in Figure 5 and Figure 6 (CTMC/DTMC combination). The time dependence $p_D(t)$ is shown in Figure 8 a). Modelling of the dangerous failure probability of the SF using the CTMC/DTMC combination is closer to reality, but the calculation is significantly more time-consuming than in case of using only the CTMC model.

Figure 8 b) shows only the shortened time frame of the dangerous failure probability of the SF calculated using the CTMC/DTMC, to achieve observability of

the influence of the time-discreet diagnostic method on the monitored variable $-p_D(t)$.



a) The whole time frame



b) The shortened time frame

Figure 8. The dangerous failure probability of the SF; one failure detection mechanism; continuous mode of operation – calculation using the CTMC/DTMC model (Figures 5, 6)

The failures diagnostic coverage influence on the dangerous failure probability of the SF can be seen in Figure 9. The results confirm the known fact, that failures diagnostic coverage under 60 % does not significantly influence the hardware safety integrity of the SF. The failures diagnostic coverage influence is significant, if $c \to 1$.

B. Two Failure Detection Mechanisms

Let us assume that the SRCS has two failure detection mechanisms. Let one failure detection mechanism (RM) operate in such manner that the diagnostic test is triggered every 0.5 h and its diagnostic coverage coefficient of the failures $c = 0.9$.

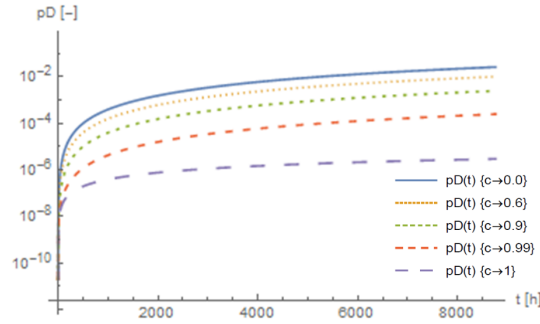


Figure 9. The failures diagnostic coverage influence on the dangerous failure probability of the SF; one failure detection mechanism

Let the next failure detection mechanism (SM) operate in such manner that the diagnostic test is triggered every 10 h. Let the SM cover 90 % of the failures, which are not covered by the RM ($c_x = 0.09$).

If the SF is performed in continuous mode of operation and the diagnostic cycle time (the failure 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 relation derived for the model in Figure 4. The time dependence $p_D(t)$ is shown in Figure 10. The comparison of the graphs in Figure 7 and in Figure 10 shows that even if the diagnostic coverage coefficient is the same in both cases, the SRCS with two failure detection mechanisms has worse safety properties. Deterioration of the safety properties is caused by the bigger failure detection time.

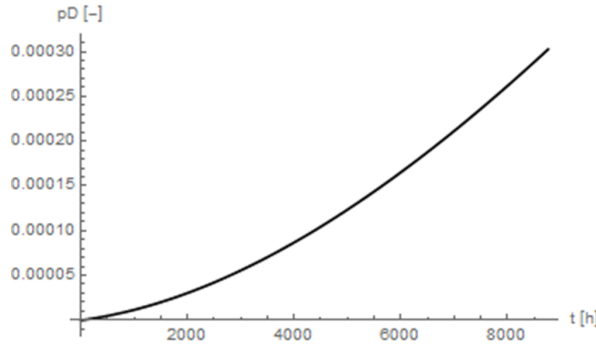


Figure 10. The dangerous failure probability of the SF; two failure detection mechanisms; continuous mode of operation – calculation using the CTMC model (Figure 4)

7 CONCLUSIONS

In the paper, the basic idea how to solve problem related to the evaluation of differently operating failure detection mechanisms to the hardware safety integrity of the SF is analyzed. Solution of this problem is based on the appropriate CTMC and DTMC combination. All the factors were respected in the presented models that significantly influence the hardware safety integrity of the SF.

In order to underline the significance of the problem, the obtained results are presented as a simple dual structure with two elements. In practice, there are often much more complex structures, when the SF is realized by bigger number of elements, which are not only on the process level of control, but also on the higher levels. This leads to the fact, that the SF is realized by parts of the SRCS with different structures. In such cases the model creation is difficult – the number of states in the model increases markedly, thus showing a tendency to increase the probability of mistakes made by the analyst. A successful solution of this problem lies in the decomposition of the SF hardware realization on modules with simple structures and in appropriate using of combination of the different analysis methods when integrating the partial results.

The dangerous failure probability of the SF can be calculated based on the models presented in this paper. In practical use, on the basis of knowledge of the dangerous failure probability, it is necessary to calculate the variable, which is required by relevant standards given to the application area. For example, [1] requires to determinate the average probability of dangerous failure on demand of the SF (PFD_{avg}) in low demand mode of operation, or the average frequency of dangerous failure of the SF (PFH) in high demand mode of operation or continuous mode of operation.

The ideas mentioned in this paper have practical importance and they can be properly used for the hardware safety integrity evaluation of the SF, which has more complex hardware structure and several (at the same time operating) failure detection mechanisms.

Acknowledgment

This work was supported by the Educational Grant Agency of the Slovak Republic (KEGA) No. 034ŽU-4/2016 "Implementation of Modern Technologies Focusing on Control Using the Safety PLC into Education" (45 %) and particularly by the project No. 008ŽU-4/2015 "Innovation of HW and SW Tools and Methods of Laboratory Education Focused on Safety Aspects of ICT within Safety Critical Applications of Processes Control" (45 %), and by the grant VEGA 1/0663/17 (10 %).

REFERENCES

[1] EN 61508:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

[2] EN 61511:2004. Functional Safety – Safety Instrumented Systems for the Process Industry Sector.

[3] Holub, P.—Börcsök, J.: Advanced PFH Calculations for Safety Integrity Systems with High Diagnostic. XXII International Symposium on Information, Communication and Automation Technologies (ICAT 2009), Bosnia, 2009, pp. 1–8. ISBN 978-1-4244-4220-1, doi: 10.1109/ICAT.2009.5348449.

[4] Iden, J.: Assessing the Effects of Diagnostic Failures on Safety-Related Control Systems. International Automatic Control Conference (CASC), Taiwan, 2014, pp. 23–28. ISBN 978-1-4799-4586-3, doi: 10.1109/CACS.2014.7097156.

[5] Ilavský, J.—Rástočný, K.—Ždánsky, J.: Common-Cause Failures as Major Issue in Safety of Control Systems. Advances in Electrical and Electronic Engineering, Vol. 11, 2013, No. 2, pp. 86–93. ISSN 1804-3119, doi: 10.15598/aeee.v11i2.748.

[6] Mechri, W.—Simin, C.—BenOthman, K.: Switching Markov Chains for a Holistic Modeling of SIS Unavailability. Reliability Engineering and System Safety, Vol. 133, 2015, pp. 212–222. ISSN 0951-8320, doi: 10.1016/j.ress.2014.09.005.

[7] Liu, B.—Ghazel, M.—Toguyéni, A.: Model-Based Diagnosis of Multi-Track Level Crossing Plants. IEEE Transactions on Intelligent Transportation Systems, Vol. 17, 2016, No. 2, pp. 546–556. ISSN 1524-9050, doi: 10.1109/TITS.2015.2478910.

[8] Liu, Y.: Discrimination of Low- and High-Demand Modes of Safety-Instrumented Systems Based on Probability of Failure on Demand Adaptability. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, Vol. 228, 2014, No. 4, pp. 409–418. ISSN 1748-006X.

[9] Kleyner, A.—Volovoi, V.: Application of Petri Nets to Reliability Prediction of Occupant Safety Systems with Partial Detection and Repair. Reliability Engineering and System Safety, Vol. 95, 2010, No. 6, pp. 606–613. ISSN 0951-8320, doi: 10.1016/j.ress.2010.01.008.

[10] Rástočný, K.—Ilavský, J.: Effects of a Periodic Maintenance on the Safety Integrity Level of a Control System. In: Schnieder, E., Tarnai, G. (Eds.): Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2010). Springer-Verlag, 2010, Part 2, pp. 77–85. ISBN 978-3-642-14261-1.

[11] Rástočný, K.—Ilavský, J.: Effects of Recovery on the Safety of a Safety-Related Control System. IEEE International Conference on Applied Electronics (AE), Pilsen, Czech Republic, 2011, pp. 321–324. ISBN 978-80-7043-865-7.

[12] Rástočný, K.—Franeková, M.—Zolotová, I.—Rástočný, K. Jr.: Quantitative Assessment of Safety Integrity Level of Message Transmission Between Safety-Related Equipment. Computing and Informatics, Vol. 33, 2014, No. 2, pp. 343–368. ISSN 1335-9150.

[13] Rástočný, K.—Franeková, M.—Holečko, P.—Zolotová, I.: Modeling of Hazards Effect on the Safety Integrity of Open Transmission Systems. Computing and Informatics, Vol. 35, No. 2, 2016, pp. 470–496. ISSN 1335-9150.

[14] Innal, F.—Dutuit, Y.—Rauzy, A.—Signoret, J.-P.: New Insight into the Average Probability of Failure on Demand and the Probability of Dangerous Failure Per Hour of Safety Instrumented Systems. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, Vol. 224, 2010, No. 2, pp. 75–86. ISSN 1748-006X.

[15] Ustoglu, I.—Kaymakci, O. T.—Börcsök, J.: Effects of Varying Diagnostic Coverage on Functional Safety. International Symposium on Fundamentals of Electrical Engineering (ISFEE), Romania, 2014, pp. 1–6. ISBN 978-1-4799-6820-6, doi: 10.1109/ISFEE.2014.7050581.

[16] Velten-Philipp, W.—Houtermans, M.: The Effect of Diagnostic and Periodic Proof Testing on the Availability of Programmable Safety Systems. Proceedings of the 10th WSEAS International Conference on Communications, Athens, 2006, pp. 180–186. ISBN 960-8457-47-5.

Karol Rástočný graduated at the Department of Signalling and Communication Systems of the Faculty of Mechanical and Electrical Engineering, Technical University of Transport and Communications, Žilina, Slovakia in 1982. He defended is Ph.D. in the field of safety analysis in 1995. Since 2008 he has been working as Professor at the Department of Control and Information Systems at the Faculty of Electrical Engineering, University of Žilina. His professional orientation covers solving problems of functional and technical safety of safety related control systems, preferably oriented to railway domain.

Juraj Ždánsky graduated at the Department of Information and Safety Systems of the Faculty of Electrical Engineering, University of Žilina in 2003. He received his Ph.D. degree at the University of Žilina in 2007 in the field of automation with specialization on safety control. Since 2014 he has been working as Associated Professor in the Department of Control and Information Systems at the Faculty of Electrical Engineering, University of Žilina. His professional orientation covers solving problems in functional and technical safety of safety related control systems, preferably oriented to industry.

Mária Franeková graduated at the Department of Telecommunications of the Faculty of Electrical Engineering, Slovak Technical University of Bratislava, Slovakia in 1985. She defended her Ph.D. in the field of channel coding applications in 1995. Since 2011 she has been working as Professor at the Department of Control and Information Systems at the Faculty of Electrical Engineering, University of Žilina, Slovakia. Her scientific research is focused on secure and safety-related communication systems, safety analysis, safety and cryptography techniques used within control of safety-critical processes in transport (railway and road) and in industry.

Iveta Zolotová graduated at the Department of Technical Cybernetics of the Faculty of Electrical Engineering, Technical University of Košice, Slovakia in 1983. She defended her C.Sc. in the field of hierarchical representation of digital image in 1987. Since 2010 she has been working as Professor at the Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Slovakia. Her scientific research is focused on networked control and information systems, supervisory control, data acquisition, human machine interface and web labs. She also investigates issues related to digital image processing.