Impact of 2oo3 Architecture Recovery on the Safety Integrity of a Safety Function

Karol Rástočný
Department of Control and Information Systems
University of Žilina, Faculty of Electrical Engineering and Information Technology
Žilina, Slovakia
karol.rastocny@uniza.sk

Juraj Ždánsky
Department of Control and Information Systems
University of Žilina, Faculty of Electrical Engineering and Information Technology
Žilina, Slovakia
juraj.zdansky@uniza.sk

Milan Medvedík
Department of Control and Information Systems
University of Žilina, Faculty of Electrical Engineering and Information Technology
Žilina, Slovakia
milan.medvedik@uniza.sk

***Abstract* — One of the basic features of a safety function is the safety integrity level. This feature also affects the technical solution of the system that implements the safety function. One of the parameters that affect the safety integrity of a safety-relevant system is its recovery to the original state after a failure has occurred. The method of recovery a safety-relevant system after the occurrence of a failure to its original state depends not only on its technical solution, but also on the method of its operation. The paper deals with the influence of various methods of recovery on the safety integrity of the safety function, which is implemented by an electronic safety-relevant system with a 2oo3 architecture.**

Keywords — recovery, safety, safety function, SIL, SRES

I. INTRODUCTION

Several processes in industry or transport are associated with a certain risk and thus the occurrence of an adverse event that can result in personal injury, significant material damage or environmental damage. Risk reduction to an acceptable value is achieved using technical and organizational safety measures. The technical measures also include safety related electronic systems (SRES), which implement the so-called safety features. One of the basic safety features of SRES is safety integrity, which according to [1] expresses the probability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated duration. It would be more appropriate (and more accurate) to use the term "ability" instead of "probability". This ability is expressed through the safety integrity level (SIL) - SIL 1 to SIL 4. SIL does not relate to SRES, but to the safety function (SF), which is implemented by SRES. The SRES may implement (and usually does) multiple SFs, and each SF may or may not be implemented with a different SIL. According to [1], safety integrity consists of three parts - systematic safety integrity (SysF-SI), software safety integrity (SW-SI) and hardware safety integrity (HW-SI). It can be stated that the SRES hardware can have mainly random failures, but also systematic failures and software only systematic failures. For this reason, the integrity of safety against systematic failures (SysF-SI) and the integrity of safety against random failures (RanF-SI) can be considered as is considered in [2]. It is generally assumed that in the case of SRES, SysF-SI forms a non-quantifiable part of SI and RanF-SI forms a quantifiable part of SI (the occurrence of random failures can be expressed, for example, by a random failure rate). SF must meet the requirement for both SysF-SI and RanF-SI levels. The fact that the SF has the required level of SysF-SI is proven by the application of appropriate (prescribed) measures to prevent errors and failures in the development of SRES, which implements the SF [1], [2]. That SF has the required level of RanF-SI is proven by calculating the dangerous failure rate of the SF. There are several methods that can be used to calculate dangerous failure probability of the safety function (DFP of SF), or dangerous failure rate of the safety function (DFR of SF).

Very commonly used methods include the modified Reliability Block Diagram (RBD) [3] and Fault Tree Analysis (FTA) [4] methods, which are primarily intended for the analysis of the reliability of technical objects. However, these methods do not allow to model the influence of some technical and operational properties of SRES on DFP of SF, or DFR of SF, which it implements. For example, these methods do not allow to model the influence of Diagnostic Coverage (DC) of fault states in the whole range of values ($0\% \leq DC \leq 100\%$), the influence of recovery, do not respect the order of occurrence of failures, change of SRES architecture. These shortcomings are largely eliminated by the method based on the use of the Markov chain (MC) [5], [6].

This paper deals with modeling the impact of the recovery method on the DFP of SF. The transition of the SRES from a safe (up) state to a dangerous (down) state is described by a homogeneous continuous-time Markov chain (CTMC). This means that the set of states in the model is countable, the intensities of transitions between states are constant and the transition from one state to another takes place continuously over time.

II. MODEL SRES – NO EFFECT ON DFP OF SF

If a high level of safety and SRES availability is required, SRES with a 2oo3 architecture is very often used [7]. It is a multi-channel architecture based on compound safety and with fail-safe comparison of data between SRES units (Fig. 1). The impact of architecture on safety and availability is also addressed [8]. For the sake of clarity of this paper, it is assumed that SRES consists of three hardware-identical and physically independent units - U1, U2, U3. Units U1, U2, U3 communicate with each other via internal buses C12, C13, C23. The SRES implements one SF, which is performed in a continuous mode, and a dangerous failure of the SRES can be considered a dangerous failure of the SF. A dangerous failure of the SRES should be the state where two units are in a fault state. SRES is characterized in

2021 International Conference on Applied Electronics (AE) | 978-80-261-0973-0/21/$31.00 ©2021 10.23919/AE51540.2021.9542892

ISBN 978-80-261-0973-0,

that if a fault state is detected in one unit, due to its negation, SRES transitions from architecture 2oo3 to architecture 2oo2 and remains in an up state. The influence of mutual communication of units U1, U2, U3 on SF safety is not the subject of this paper. The safety assessment of the communication system is addressed in [9].

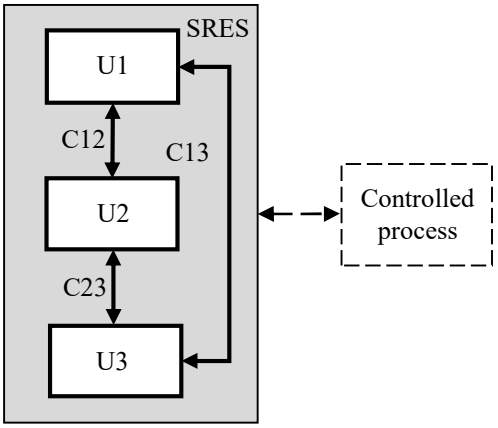

Fig. 1. Block diagram of a general architecture 2oo3

For a three-channel architecture with hardware-identical units,

$$\lambda_{U1} = \lambda_{U2} = \lambda_{U3} = \lambda, \tag{1}$$

where λ_{U1} is the random failures rate of the unit U1, λ_{U2} is the random failures rate of the unit U2 and λ_{U3} is the random failures rate of the unit U3.

Units U1, U2, U3 have identical mechanisms for detecting and negating fault states. These mechanisms are characterized by a fault state detection coefficient c, a fault state detection time t_d, and a fault state negation time t_N.

It is also true that:

$$\lambda = \lambda \cdot c + \lambda \cdot (1 - c), \tag{2}$$

where c is the diagnostic coverage coefficient, $\lambda \cdot c$ is the detectable failure rate and $\lambda \cdot (1 - c)$ is the undetectable failure rate.

In Fig. 2. a CTMC describing the transition of the SRES (according to Fig. 1) from fault-free state **1** to dangerous state **7** is shown.

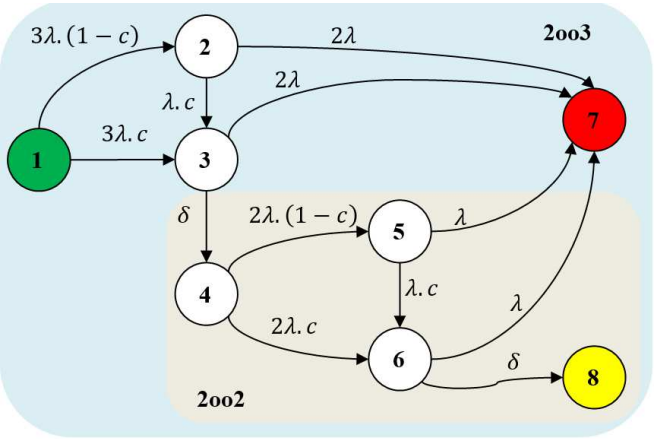

Fig. 2. Model of a general architecture 2oo3

TABLE I. shows the characteristics of the individual states of the CTMC in Fig. 2.

TABLE I. SRES STATES

State	Characteristics
1	SRES is in up state; neither of the three units is in a fault state.
2	SRES is in up state; one of the three units is in a fault state that is not detectable.
3	SRES is in up state; one of the three units is in a fault state that is detectable (consequence of at least one random fault).
4	SRES is in up state; one of the three units is in a fault state, which was detected (this unit was "isolated" from the other units due to negation and thus the architecture was changed SRES - from architecture 2oo3 to architecture 2oo2).
5	SRES is in up state and works in the 2oo2 architecture; one of the two units is in a fault state that is not detectable.
6	SRES is in up state and works in the 2oo2 architecture; one of the two units is in a fault state that is detectable (consequence of at least one random fault).
7	SRES is in down state (in a dangerous state) - at least two units are in a faulty state.
8	SRES is in down state (in a safe state) after the detection and negation of the fault state or after the interruption of the SRES operation.

The transition rate from state **3** to state **4**, or from state **6** to state **8** can be expressed by the relation

$$\delta = \frac{1}{t_d + t_N}, \tag{3}$$

where δ is the failure detection and negation rate of the fault state, t_d is the time of detection of the fault state and t_N is the time needed to negate the detected fault state. Depending on the area of application, the mean value of the fault detection time can also be used [1], [2].

The transition from state **2** to state **3** (or from state **5** to state **6**) corresponds to a situation where a detectable fault occurs in the unit (which is in an undetectable fault state). If the SRES operates in the 2oo3 architecture, it enters a dangerous state **7** when two of the three units are in a fault state; if the SRES operates in the 2oo2 architecture, it enters a dangerous state **7** when two of the two units are in a fault state.

The CTMC in Fig. 2. can be described by a system of differential equations (4) and a vector of initial probabilities (5).

$$\begin{aligned}
\frac{dp_1}{dt} &= -3\lambda \cdot p_1 \\
\frac{dp_2}{dt} &= 3\lambda \cdot (1 - c) \cdot p_1 - (2\lambda + \lambda \cdot c) \cdot p_2 \\
\frac{dp_3}{dt} &= 3\lambda \cdot c \cdot p_1 + \lambda \cdot c \cdot p_2 - (2\lambda + \delta) \cdot p_3 \\
\frac{dp_4}{dt} &= \delta \cdot p_3 - 2\lambda \cdot p_4 \\
\frac{dp_5}{dt} &= 2\lambda \cdot (1 - c) \cdot p_4 - (\lambda \cdot c + \lambda) \cdot p_5
\end{aligned} \tag{4}$$

$$\frac{dp_6}{dt} = 2\lambda \cdot c \cdot p_4 + \lambda \cdot c \cdot p_5 - (\lambda + \delta) \cdot p_6$$
$$\frac{dp_7}{dt} = 2\lambda \cdot p_2 + 2\lambda \cdot p_3 + \lambda \cdot p_5 + \lambda \cdot p_6$$
$$\frac{dp_8}{dt} = \delta \cdot p_6 ,$$

where p_i is the probability of state i in the model.

If at time $t = 0$ the SRES is in state 1, then the vector of initial probabilities is

$$\overrightarrow{P_0(t=0)} = \{1, 0, 0, 0, 0, 0, 0, 0\}. \quad (5)$$

States **7** and **8** are absorption states. The analysis of the impact of random failures on the DFP of SF, or DFR of SF, ends when one of this state is reached.

III. Model SRES – effect of recovery on DFP of SF

SRES can remain in the 2oo2 architecture for the maximum time allowed, which results from the SRES availability requirement. Within this time interval, the SRES must be recovered to the original 2oo3 architecture. Recovery from 2oo2 to 2oo3 can take place:

- without interruption of operation, by replacing a unit with a detected fault state with a new unit;
- after interruption of operation and subsequent replacement of a unit with a detected fault state with a new unit;
- after interruption of operation and subsequent replacement of all three units.

A. *Recovery without interruption of SRES operation - replacement of one unit*

The transition of the SRES from the 2oo2 architecture to the 2oo3 architecture by replacing a unit with a detected fault state without interruption of operation can only take place if the SRES has a learning feature. The ability to learn is necessary for the new unit to be able to establish cooperation with other units.

Let the SRES due to the detection and negation of the fault state for example in unit U1 it goes to state **4** (change of architecture 2oo3 to architecture 2oo2) (Fig. 3.). If the SRES is in state **4**, then after replacing the U1 unit, the SRES goes to state **1** (return to architecture 2oo3). The rate of the transition from state **4** to state **1** is given by the relation

$$\mu = \frac{1}{T_{2oo2}}, \quad (6)$$

where T_{2oo2} is the maximum time allowed that SRES can spend in the 2oo2 architecture.

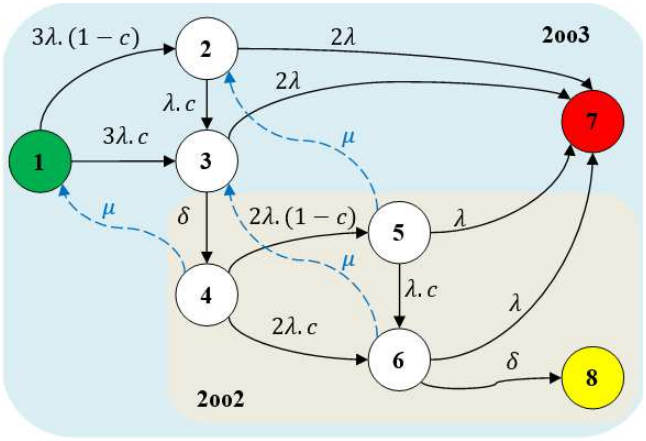

Fig. 3. SRES model – replacement of one unit without interruption of operation

During the work of SRES in the 2oo2 architecture, the occurrence of a fault in another unit is not excluded – for example unit U2. The following scenarios are possible:

- an undetectable fault occurs in the U2 unit before replacing the U1 unit; the SRES goes to state **5** and after replacing the U1 unit, goes from state **5** to state **2** (not state **1**);
- a detectable fault occurs in unit U2 before replacing unit U1; The SRES goes to state **6** and after replacing the unit U1 it goes from state **6** to state **3** (not to state **1**);
- if a fault state in unit U2 has been detected and negated before replacing unit U1, the SRES goes into down state (state **8**).

The CTMC in Fig. 3. can be described by a set of differential equations (7) and a vector of initial probabilities (5).

$$\begin{aligned}
\frac{dp_1}{dt} &= -3\lambda \cdot p_1 + \mu \cdot p_4 \\
\frac{dp_2}{dt} &= 3\lambda \cdot (1 - c) \cdot p_1 - (2\lambda + \lambda \cdot c) \cdot p_2 + \mu \cdot p_5 \\
\frac{dp_3}{dt} &= 3\lambda \cdot c \cdot p_1 + \lambda \cdot c \cdot p_2 - (2\lambda + \delta) \cdot p_3 + \mu \cdot p_6 \\
\frac{dp_4}{dt} &= \delta \cdot p_3 - (2\lambda + \mu) \cdot p_4 \\
\frac{dp_5}{dt} &= 2\lambda \cdot (1 - c).p_4 - (\lambda \cdot c + \lambda + \mu) \cdot p_5 \\
\frac{dp_6}{dt} &= 2\lambda \cdot c \cdot p_4 + \lambda \cdot c \cdot p_5 - (\lambda + \delta + \mu) \cdot p_6 \\
\frac{dp_7}{dt} &= 2\lambda \cdot p_2 + 2\lambda \cdot p_3 + \lambda \cdot p_5 + \lambda \cdot p_6 \\
\frac{dp_8}{dt} &= \delta \cdot p_6 .
\end{aligned} \quad (7)$$

B. *Recovery after interruption of SRES operation – replacement of one unit*

The CTMC in Fig. 4. describes the scenario where the recovery of SRES to the original state occurs after the

interruption of SRES operation, either by transition from state **6** to state **8** after detection and negation of the fault state, or by the intervention of a maintenance worker (transition from state **4** and from state **6** to state **8** with rate μ_1, or from state **5** to state **9** with rate μ_1; state **9** represents the state when an undetectable fault remains in the system after the intervention of the maintenance worker). The maintenance worker will replace the unit with the detected fault state (if SRES is in state **4**), or another unit with the detected fault state (if SRES is in state **6**). After replacing the unit (units), the maintenance worker will put the SRES into a up state (transition from state **8** to state **1** and transition from state **9** to state **2** with rate μ_2).

It is also true that:

$$\begin{aligned} T_{2oo2} &\geq T_1 + T_2, \\ \mu_1 &= \frac{1}{T_1}, \\ \mu_2 &= \frac{1}{T_2}, \end{aligned} \tag{8}$$

where T_{2oo2} is the maximum allowed time, that the SRES can spend in the 2oo2 architecture, T_1 is the time required to stop the SRES after the transition to the 2oo2 architecture and T_2 is the time required to bring the SRES to a up state after the SRES is stopped by a maintenance worker.

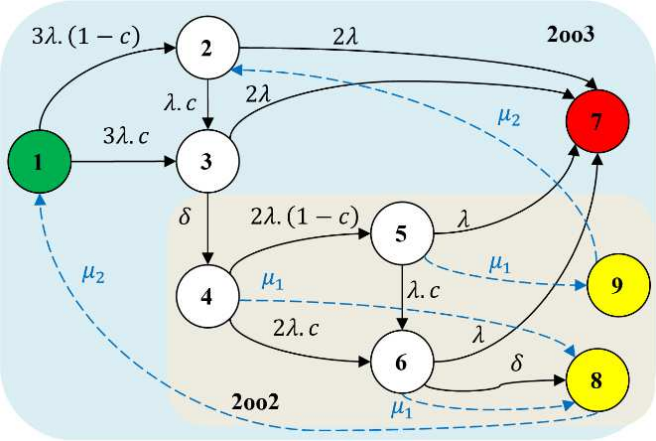

Fig. 4. SRES model – interruption of SRES operation and replacement of one unit

The CTMC in Fig. 4. can be described by a system of differential equations (9) and a vector of initial probabilities (10).

$$\begin{aligned} \frac{dp_1}{dt} &= -3\lambda \cdot p_1 + \mu_2 \cdot p_8 \\ \frac{dp_2}{dt} &= 3\lambda \cdot (1-\mathrm{c}) \cdot p_1 - (2\lambda + \lambda \cdot c) \cdot p_2 + \mu_2 \cdot p_9 \\ \frac{dp_3}{dt} &= 3\lambda \cdot c \cdot p_1 + \lambda \cdot c \cdot p_2 - (2\lambda + \delta) \cdot p_3 \\ \frac{dp_4}{dt} &= \delta \cdot p_3 - (2\lambda + \mu_1) \cdot p_4 \\ \frac{dp_5}{dt} &= 2\lambda \cdot (1-c) \cdot p_4 - (\lambda \cdot c + \lambda + \mu_1) \cdot p_5 \\ \frac{dp_6}{dt} &= 2\lambda \cdot c \cdot p_4 + \lambda \cdot c \cdot p_5 - (\lambda + \delta + \mu_1) \cdot p_6 \\ \frac{dp_7}{dt} &= 2\lambda \cdot p_2 + 2\lambda \cdot p_3 + \lambda \cdot p_5 + \lambda \cdot p_6 \\ \frac{dp_8}{dt} &= \mu_1 \cdot p_4 + (\delta + \mu_1) \cdot p_6 - \mu_2 \cdot p_8 \\ \frac{dp_9}{dt} &= \mu_1 \cdot p_5 - \mu_2 \cdot p_9 \,. \end{aligned} \tag{9}$$

$$\overrightarrow{P_0(t=0)} = \{1,0,0,0,0,0,0,0,0\} \tag{10}$$

If, after the replacement of the unit with the detected fault state, a complete check test of the remaining two units was carried out, the situation would essentially correspond to a recovery with the replacement of all three units. However, it can be assumed that the time of down state of the SRES would be extended.

C. *Recovery after interruption of SRES operation – replacement of all three units*

The model in Fig. 5. describes the scenario when SRES working in the 2oo3 architecture switches, after detecting and negating a fault state of one unit, to the 2oo2 architecture. The SRES must complete work on the 2oo2 architecture by the predetermined time T_{2oo2}. Within this time interval, the SRES operation is safely interrupted (transition from state **4** to state **8**, transition from state **5** to state **8** and transition from **6** to state **8**). After replacing all three units, the SRES is recovered to up state from state **1**. The SRES is "as good as new".

The assumption that after the replacement of all three units goes from state **8** to state **1** (state **8** would not be absorbent) does not correspond to reality. After recovery to the 2oo3 architecture, the SRES would not be considered "as good as new" - with a certain probability greater than 0 it remains in states **2**, **3**, **7**.

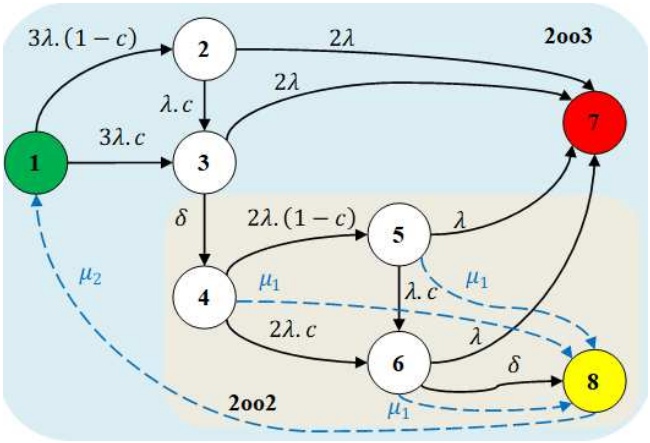

Fig. 5. SRES model – interruption of SRES operation and replacement of three units

The CTMC in Fig. 5. can be described by a system of differential equations (11) and a vector of initial probabilities (5).

$$\begin{aligned} \frac{dp_1}{dt} &= -3\lambda \cdot p_1 + \mu_2 \cdot p_8 \\ \frac{dp_2}{dt} &= 3\lambda \cdot (1-\mathrm{c}) \cdot p_1 - (2\lambda + \lambda \cdot c) \cdot p_2 \end{aligned}$$

$$\frac{dp_3}{dt} = 3\lambda \cdot c \cdot p_1 + \lambda \cdot c \cdot p_2 - (2\lambda + \delta) \cdot p_3$$
$$\frac{dp_4}{dt} = \delta \cdot p_3 - (2\lambda + \mu_1) \cdot p_4$$
$$\frac{dp_5}{dt} = 2\lambda \cdot (1 - c) \cdot p_4 - (\lambda \cdot c + \lambda + \mu_1) \cdot p_5 \qquad (11)$$
$$\frac{dp_6}{dt} = 2\lambda \cdot c \cdot p_4 + \lambda \cdot c \cdot p_5 - (\lambda + \delta + \mu_1) \cdot p_6$$
$$\frac{dp_7}{dt} = 2\lambda \cdot p_2 + 2\lambda \cdot p_3 + \lambda \cdot p_5 + \lambda \cdot p_6$$
$$\frac{dp_8}{dt} = \mu_1 \cdot p_4 + \mu_1 \cdot p_5 + (\delta + \mu_1) \cdot p_6 - \mu_2 \cdot p_8 .$$

IV. Case Study - Simulation Results

Let SF be implemented by SRES with architecture 2oo3, as shown in Fig. 1. Units U1, U2, U3 are hardware identical. Their of random failures rate is $\lambda = \lambda_{U1} = \lambda_{U2} = \lambda_{U3} = = 2 \cdot 10^{-6}\ \mathrm{h}^{-1}$ and the coefficient of diagnostic coverage $c = 0{,}99$. The functional specification of the SF is irrelevant from the point of view of the RanF-SI analysis of the SRES. Let the assumed time interval within which the probability of a dangerous SF failure ($DFP(t)$) is calculated, or the dangerous failure rate of the SF ($DFR(t)$) is 20 years (useful life of SRES). A proof test during the useful life of the SRES is not expected. SRES works so that if a fault is detected, a safe response is triggered - either the architecture is reconfigured (architecture change 2oo3 to 2oo2), or SRES goes to state **8** (in architecture 2oo2) and SRES operation is interrupted. The failure detection and negation rate $\delta = 1\ \mathrm{h}^{-1}$.

In TABLE. II. to TABLE. V. shows the results of calculations for individual models shown in Fig. 2 to Fig. 5.

TABLE II. Without recovery to original architecture (calculation according to CTMC in Fig. 2.)

$\lambda = 2 \cdot 10^{-6}\ h^{-1}; c = 0{,}99; \delta = 1\ h^{-1}$

μ [h^{-1}]	$DFP(176000)$ [-]	$DFR(176000)$ [h^{-1}]
0	2,141050731635·10^{-3}	2,277466·10^{-8}

TABLE III. Recovery to original architecture (calculation according to CTMC in Fig. 3.)

$\lambda = 2 \cdot 10^{-6}\ \mathrm{h}^{-1}; c = 0{,}99; \delta = 1\ \mathrm{h}^{-1}$

T_{2oo2} [h]	$DFP(176000)$ [-]	$DFR(176000)$ [h^{-1}]
12	2,689515400022·10^{-3}	2,6072179·10^{-8}
24	2,689403471833·10^{-3}	2,6072091·10^{-8}
48	2,689179827635·10^{-3}	2,6071919·10^{-8}
62	2,689049555763·10^{-3}	2,6071819·10^{-8}

TABLE IV. Recovery to original architecture (calculation according to CTMC in Fig. 4.)

$T_2 = 0{,}5$ h; $\lambda = 2 \cdot 10^{-6}\ \mathrm{h}^{-1}; c = 0{,}99; \delta = 1\ \mathrm{h}^{-1}$

T_1 [h]	$DFP(176000)$ [-]	$DFR(176000)$ [h^{-1}]
11,5	2,689554293809·10^{-3}	2,607164·10^{-8}
23,5	2,689490475171·10^{-3}	2,607102·10^{-8}
47,5	2,689363270059·10^{-3}	2,606978·10^{-8}
61,5	2,689288487472·10^{-3}	2,606906·10^{-8}

TABLE V. Recovery to original architecture (calculation according to CTMC in Fig. 5.)

$T_2 = 0{,}5$ h; $\lambda = 2 \cdot 10^{-6}\ \mathrm{h}^{-1}; c = 0{,}99; \delta = 1\ \mathrm{h}^{-1}$

T_1 [h]	$DFP(176000)$ [-]	$DFR(176000)$ [h^{-1}]
11,5	2,689432637915·10^{-3}	2,607045·10^{-8}
23,5	2,689241499715·10^{-3}	2,606860·10^{-8}
47,5	2,688859930030·10^{-3}	2,606489·10^{-8}
61,5	2,688637582815·10^{-3}	2,606273·10^{-8}

The comparison of the results shows that none of the considered methods of recovery the SRES to the original architecture has a significant impact on $DFP(t)$, or $DFR(t)$. Even the results of $DFP(t)$, or $DFR(t)$ are more favorable for SRES without recovery to the original architecture than with recovery. This is a logical consequence that the analysis does not end with state **8**, but continues with a return to state **1**, increasing the probability of transition to state **7**.

Since the changes are insignificant, they are better visible from the data given in the tables (Tables II. to Table V.) than would be visible in the graphs. For illustration only, Fig. 6. shows the course of $DFP(t)$ for recovery SRES from architecture 2oo2 to architecture 2oo3 (Fig. 5).

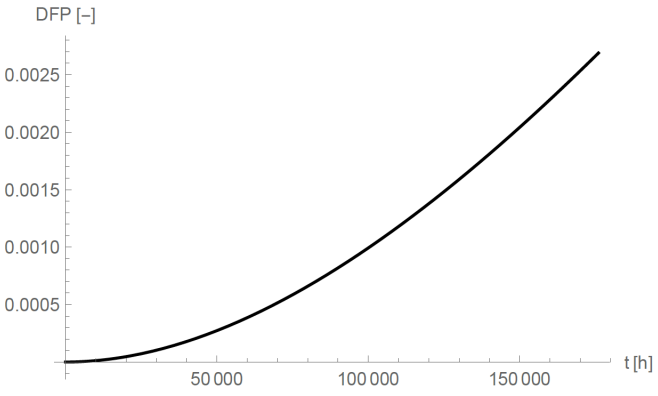

Fig. 6. Probability of dangerous failure – calculation according to the model in Fig. 5. for $T_1 = 47{,}5$ h; $T_2 = 0{,}5$ h; $\lambda = 2 \cdot 10^{-6}\ \mathrm{h}^{-1}; c = 0{,}99;$ $\delta = 1\ \mathrm{h}^{-1}$.

V. Conclusion

The paper considers ways to recovery SRES from the 2oo2 architecture to the original 2oo3 architecture, which are possible. Theoretically, there are other ways to recovery to the original architectures, but these are practically out of the question because they would lead to a degradation of the properties of SRES with the 2oo3 architecture. When choosing an appropriate recovery method, it should be borne in mind that the recovery method affects not only the integrity of the safety (albeit minor), but the availability and (organizational and technical) maintenance of the SRES. A comprehensive assessment of the impact of recovery to the original architecture on the availability and safety integrity of SRES is not the subject of this paper.

The results presented in this paper refute the often-presented claim that recovery has a positive effect on the integrity of safety of SF. Such a statement is justified only if the recovery to the original architecture follows a regular check (perfect proof test).

Acknowledgment

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number 008ŽU-4/2019: Modernization and expansion of educational possibilities in the field of safe controlling of industrial processes using the safety PLC.

References

[1] EN 61508, "Functional safety of electrical/ electronic/programmable electronic safety-related systems," 2010.

[2] EN 50129, "Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling," 2018.

[3] EN 61078, "Analysis techniques for dependability - Reliability block diagram and boolean methods," 2006.

[4] EN 61025, "Fault tree analysis," 2007.

[5] K. Rástočný, J. Ždánsky, M. Franeková and I. Zolotová, "Modelling of the Diagnostics Influence on the Safety of the Control System," In: The journal Computing and Informatics, Vol. 37, No. 2, ISSN 1335-9150, pp. 457–475, 2018.

[6] H. Ahangari, F. Atik, Y.I. Ozkok, S.O. Ata, O. Ozturk, "Analysis of design parameters in safety-critical computers," In Journal IEEE Transactions on Emerging Topics in Computing, Volume 8, Issue 3, ISSN 2168-6750, p. 712-723, 2020.

[7] A.C. Torres-Echeverría, S. Martorell and H.A. Thompson, "Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing," In: The journal Reliability Engineering and System Safety, Vol. 96, Issue 5, ISSN 0951-8320, pp. 545–563, 2011.

[8] P.Cuninka, P. Zavacky and M. Stremy, "Influence of Architecture on Reliability and Safety of the SRCS with Safety PLC," Proceedings of 2nd International Conference on Mathematics and Computers in Sciences and in Industry, Sliema, Malta, ISBN: 978-147998673-6, p. 225-230, 2015.

[9] K. Rástočný, M. Franeková, I. Zolotová and K. Rástočný, Jr., "Quantitative assessment of safety integrity level of message transmission between safety-related equipment," In: The journal Computing and Informatics. Vol. 33, No. 2, ISSN 1335-9150. pp. 343 – 368, 2014.