Common-cause failures as major issue in safety of control systems

Juraj ILAVSKY [1], *Karol RASTOCNY* [2], *Juraj ZDANSKY* [2]

[1]Siemens s.r.o., CEE RU-SK IC-MOL RA ECZ, J. M. Hurbana 21, 010 01 Zilina, Slovak Republic
[2]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna 8215/1, 010 26 Zilina, Slovak Republic

juraj.ilavsky@siemens.com, karol.rastocny@fel.uniza.sk, juraj.zdansky@fel.uniza.sk

Abstract. *In order to gain an improvement of safety or availability measures of the safety-relevant control system through employment of redundancy a redundant system has to comply with the requirement on independence of redundant parts. If the requirements on the independence of redundant parts are unfulfilled, then a common-cause failure can directly cause a hazardous state on a system level through its effects on multiple redundant parts. Identification of sources and quantification of the common-cause failure parameters has been proved to be a formidable task. The latter problem, including other major safety-affecting factors lays in the focus of this paper. Our proposed technical safety analysis concept is extended, so now it partially covers elusive problems related to the common-cause failures.*

Keywords

Common-cause failure, safety model, SRCS.

1. Introduction

Nowadays it is rather common that a control system is used to perform not only its designated control functions, but also safety related functions. Such control system is often referred to as a safety-related control system (SRCS). If there is a single control function that partially performs both control and safety functions, then such a function shall be considered as safety relevant. Safety relevant function (or shortly "safety function") can be determined by a risk analysis. The higher is the risk bound with the controlled process, the more strict requirements are laid on safety of a SRCS. Safety integrity level (SIL) is a measure used to express the safety of the SRCS. SIL is defined for both functional and technical safety of the control system. While the functional safety assessment is qualitative and it is often based on functional test results, the technical safety is evaluated quantitatively with massive employment of mathematical methods. Technical safety is directly related to the combined probability of the hazardous failure of the individual safety functions due to a random failure. The SRCS is considered to be "safe" if it meets specified safety requirements together with requirements on their SIL. Fulfilment of these requirements can be achieved through consistent application of technical as well as organisational measures. If the safety is a key property of the SRCS - which basically is - then corresponding mathematical model must be created. It is very important that simultaneous effects of different kinds of factors affecting safety are comprehensively considered in the model. A list of the most important safety-affecting factors includes [1]:

- Independency of the SRCS channels (if it is a multi-channel system).
- Amount and method of redundancy applied in a system.
- Reliability of system elements.
- Diagnostics (which covers diagnostic coverage, time to detect and negate a failure).

Availability cannot be seen as directly related to safety; nevertheless it can significantly influence the safety of a SRCS, especially when the SRCS operates in the high-demand mode or continuous mode of operation. If the SRCS is partially disabled or completely unavailable, then a human operator assumes control. Failure probability of the human operator is known to be much higher than failure probability of the SRCS. If availability is a key factor in the SRCS operation too, then recovery of the SRCS (and its various forms, [2]) becomes rather important safety-affecting factor.

Each mathematical model has to consider actual parameters and characteristics of a real system (Fig. 1).

In the quantitative safety analysis these parameters include a definition of a system, its boundaries and architecture, identification of non-safety-related system elements (that can be excluded from the analysis), reliability measures of the system elements (e.g. failure rate λ, recovery rate μ), and diagnostic properties (diagnostic coverage coefficient c, time to detect a failure t_D). Quantified system parameters then represent input model parameters of the mathematical model. Output measures (safety measures) are most often probability of hazardous state P_H, or hazardous failure rate λ_H (which is derived from the former). If the evaluated results are compared to the reference measures, then achieved safety integrity level can be determined.

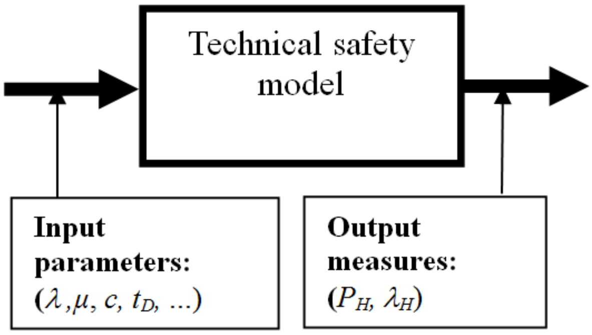
Technical safety model
Input parameters: (λ, μ, c, t_D, ...)
Output measures: (P_H, λ_H)

Fig. 1: The principle of the quantitative safety modelling.

2. General Approach to the Technical Safety Analysis of the SRCS

As a matter of fact, no mathematical method has been primarily developed for the safety analysis purpose. Methods used for the reliability or dependability analyses were modified instead; and used in the quantitative safety analysis process. A rough discrimination of mathematical methods can classify these methods into following categories:

- Static and dynamic.
- Analytical and numerical.
- Combined and hierarchical methods.

2.1. Common Safety Analysis Methods

Static methods (also referred to as combinatorial methods) represent a system as a set of independent, but logically connected functional blocks. Static methods can reveal dependencies between failures of the respective functional blocks and failure of the overall system. The most common combinatorial methods are reliability block diagram method (RBD) and (static) failure tree analysis (FTA). These methods are recommended by many standards (e.g. IEC 61508) and can be easily adopted in the safety analysis.

Dynamic models, commonly known as state-oriented methods, can take into consideration not only structure, but behaviour as well (either in normal operation or in a faulty state). The system is described by the set of states and the behaviour of the system is introduced to the model through the set of transitions between the states. External or internal events (e.g. failure, recovery, maintenance, and reconfiguration) can initiate a transition.

The common state-oriented methods include Continuous time Markov Chains (CTMC), [3], Petri nets [4], and various formal language-based methods. In some cases, these methods do not produce analytical solution, so the employment of the numerical method like Monte Carlo is necessary.

2.2. Complex Safety Analysis Methods

Hierarchical model is basically a complex model that combines more than one method used on different levels of the system decomposition, while the results of the analysis on the lower level are used as input parameters for the analysis on the higher level. Basic hierarchy can be seen even in the most simple safety analysis methods - for instance, the RBD method can use the failure rate of the system elements as an input parameter, while these failure rates can be assessed or estimated with the help of another quantitative method.

This approach is not uncommon, especially when more complex safety critical system is being analysed. Another example is covered in [5], in which a convenient combination of RBD and Markov analysis is used to achieve better modelling power in the case of complex repairable systems.

The concept of hierarchy can be employed also with the single quantitative method. Correct system decomposition becomes very important in this case, since it can make the whole safety analysis process more transparent and therefore less prone to human errors. From this point of view, the Petri nets hold a special position, since they allow the creation of multi-layer models that still can be examined analytically. The ProFunD concept [6] that integrates functional description with dependability issues is quite well defined in this field and adopted by the [4] standard.

2.3. Markov Chain Based Approach to the Safety Analysis

Markov chains are nowadays widely used in many fields, so their use in the technical safety analysis is not surprising. In addition, the combination of the Continuous Time Markov Chain (CTMC) and the Discrete Time Markov Chain (DTMC) can be conveniently applied in the safety analysis process, so the modelling power of the both methods is joined and even more safety-affecting factors can be considered in the analysis at the same time (even though some restrictions naturally apply [7], [2]). Basically, the CTMC covers stochastic part of system behaviour (e.g. failure effects, corrective maintenance) and deterministic part of system behaviour (like preventive maintenance) is covered withthe DTMC method. With this combination it is even possible to approximate non-homogenous Markov Chain by the finite set of homogenous Markov chains.

The CTMC-based safety analysis involves both quantitative and qualitative part of the analysis. The qualitative part of the analysis covers definition of the system state-space. The total number of states is heavily dependent on the number of considered system parameters (failure rate, diagnostic coverage, time to detect and negate a failure and so on), on the total number of system channels and the depth of system decomposition; in the case of multi-channel system also on the possibility of the system reconfiguration, when failure of one channel is detected, negated and faulty channel is isolated (for instance the reconfiguration from the 2-out-of-3 structure to the 2-out-of-2 structure).

If the failure rate of the system elements would have been the only input parameter, then maximal number of the system states, that need to be considered in the analysis would be given by a combination of operational and disabled (or degraded) states of all considered elements. Some of these states can be considered to be hazardous. The total number of system states (and transitions between them) increases with the number of the input parameters or system elements. This property adds up to the complexity of the model, which on the other hand lessens its readability and comprehensibility. An analyst is therefore challenged, or even overwhelmed by a large number of system states, which simultaneously increases the probability of their mistake during safety analysis. Algorithmisation of this process is problematic, as hazardous state is very specific and general definition is virtually impossible. An automation of this process was satisfactory in the dependability analysis, which was the aim of the work described in [8]. The task of quantitative analysis of the model which consists of a large number of states is analytically unmanageable, so in such case a reasonable numerical method supported by the user-friendly software must be used instead.

Technical safety of any multi-channel SRCS can be analysed with the help of state-space concept illustrated in the Fig. 2. General concept can be expanded and detailed with respect to specific architecture of the system under analysis.

The SRCS can be during its useful life present in one of these states (as seen in the Fig. 2):

- Initial failure-free state (F) - safe state. It is reasonable to assume that in the instant $t = 0$ the probability of this state equals to unity.
- Degraded operational state (N) - safe state. In this state one or more failures are present in the system. These failures though have no effect on required SRCS functions, so in this state the safety of the controlled process is not endangered.
- Fail-safe state (S). This is an absorbing state, which is reached when the failure of the SRCS is detected and negated. SRCS is disabled, yet the safety of the controlled process is not primarily endangered.
- Hazardous state (H). This is an absorbing state that is reached by the SRCS after hazardous failure (or hazardous combination of failures). In this state, the SRCS is disabled and the safety of the controlled process can be endangered.

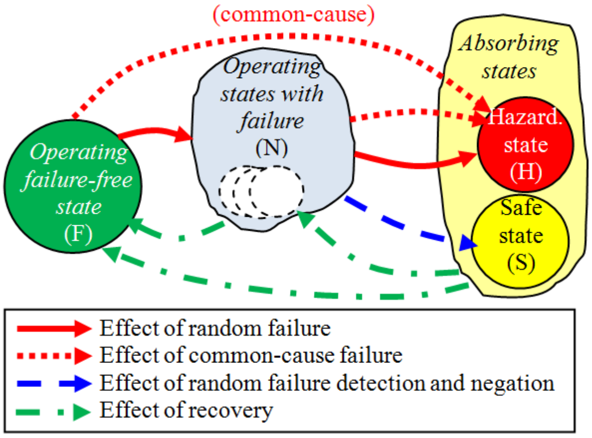
(common-cause)
Absorbing states
Operating states with failure (N)
Hazard. state (H)
Operating failure-free state (F)
Safe state (S)
Effect of random failure
Effect of common-cause failure
Effect of random failure detection and negation
Effect of recovery

Fig. 2: General state-space of the SRCS safety model including most important effects of safety-affecting factors.

If the SRCS does not possess failure detection mechanisms, then the CTMC model contains just one absorbing state - hazardous state - and the hazardous failure rate $\lambda_H(t)$ can be expressed as:

$$\lambda_H(t) = \frac{\dfrac{dP_H(t)}{dt}}{1 - P_H(t)}, \qquad (1)$$

in which $P_H(t)$ is the probability of the hazardous state H.

If the model contains two absorbing states, then the hazardous failure rate can be evaluated with the help of the following equations:

$$P_{HS}(t) = P_H(t) + P_S(t),$$

$$\lambda_H(t) = \frac{\frac{dP_{HS}(t)}{dt}}{1 - P_{HS}(t)} \cdot \frac{P_H(t)}{P_{HS}(t)}, \tag{2}$$

in which $P_H(t)$ is the probability of the safe state S. The proof of the equation (2) can be found in the paper [1].

3. Mathematical Implementation of Significant Safety-affecting Factors

A majority of electronic SRCS's is made of electronic components, which are not subject to mechanical deterioration. Such components fail randomly, thus the time to failure is random variable with exponential distribution (as far as the useful life of the SRCS is concerned, during which aging processes are not dominant). Parameter of this distribution (failure rate) can be obtained directly from the supplier of the components, or calculated from the operational statistical data (if available) or determined through reliability test. Safety analysis is focused only on a set of failures that can (alone, or in combination) have hazardous effect on controlled process. The problem is, that it is virtually impossible to determine full set of potentially hazardous failures, so simplifying assumption is usually taken - it is assumed, that all failures of the control system are potentially hazardous. Such assumption also simplifies safety assessment process, since the proof that individual failures have not hazardous consequences is not needed. The reason why such assumption can be applied is explained by the following equation:

$$\lambda_{iK} \leq \lambda_i, \tag{3}$$

in which λ_{iK} is a hazardous failure rate of the i-th SRCS component (on chosen level of decomposition, e.g. it could be a level of system channels), λ_i is a failure rate of the i-th SRCS component.

If diagnostic mechanisms are implemented in the CRCS, then it applies that:

$$\begin{aligned} \lambda_{iM} &\leq \lambda_i \cdot (1 - c), \\ \lambda_{iD} &\leq \lambda_i \cdot c, \end{aligned} \tag{4}$$

in which λ_{iM} is a failure rate of undetectable failures of the i-th SRCS component, λ_{iD} is a failure rate of detectable failures of the i-th SRCS component and c is a diagnostic coverage coefficient (identical for both channels).

Time t_D to detect a failure of a component determines transition rate to the safe state S.

In general, many perspectives must be taken into consideration when a recovery of a system is to be implemented into a mathematical model. Recovery can be seen as:

- Partial recovery of a SRCS that is after failure operational, but in a degraded state.
- A recovery of a disabled SRCS.
- A recovery after a preventive maintenance.

Various vantage points to modelling of the effects of random failures, diagnostics and recovery on SIL of a SRCS have been provided in papers [2], [7], [9]. These publications provide a firm ground for the creation of comprehensive mathematical model, even of a complex system. However, the more complex a system is (especially a multi channel system), the more important step is to assess a common-cause failure (CCF) effects on safety.

The modelling of CCF effects on safety of a SRCS can present a problem, because the origin of CCF is not easily identifiable. On the contrary, there are many sources of CCF failures and if they occur randomly, the probability distribution of their occurrence can be only estimated at best.

Systematic analysis shows, that a CCF failure can have its origin in:

- physical (internal or external),
- functional (internal or external),
- process domain.

In practical applications, single CCF often fits into more than one category from the three mentioned above. If the SRCS is designed to have identical channels, then failure detection mechanisms have little or no counter-acting effect on safety-related consequences of CCFs.

Principal step in the analysis of CCF effects on a SRCS safety is identification of those SRCS components, whose failure possible leads to a hazardous state. Those components are often the redundant parts of multi-channel systems. The Fig. 3 and the Fig. 4 show an example of this kind of situation in the case of two-channel system with identical channels that is operated in 2-out-of-2 operation (2oo2). Such system is assumed to be operational only if both channels work identically. In both cases (the Fig. 3 as well as the Fig. 4) any CCF that causes identical but faulty operation of both channels will lead to a hazard.

The Fig. 3 illustrates an example of a scenario, in which simultaneous faulty operation of both channels (redundant components) is caused by an internal cause (e.g. a systematic failure that has its origin in mistake in software design phase - which is at the same time functional aspect). Another possible source of CCF would be in this case unwanted short-circuit between the redundant channels - that would be a physical cause. The latter case implies that a CCF failure rate is closely bound to a failure rate of redundant components. The CCF part of failure rate can be modelled through so-called β-factor. Basically, β-factor is a real number between $< 0, 1 >$, which express a ratio between CCF failure rate and total failure rate of a redundant component. It can be stated that:

$$\begin{aligned} \beta &= \frac{\lambda_{iCCF}}{\lambda_i}, \\ \lambda_i &= \beta \cdot \lambda_i + \lambda_{iR}, \end{aligned} \tag{5}$$

in which λ_i is a total failure rate of i-th component, λ_{iR} is the failure rate of i-th component and β is common-cause failure coefficient. This approach is very simplified, but it can and it also is used to model CCF effects on safety.

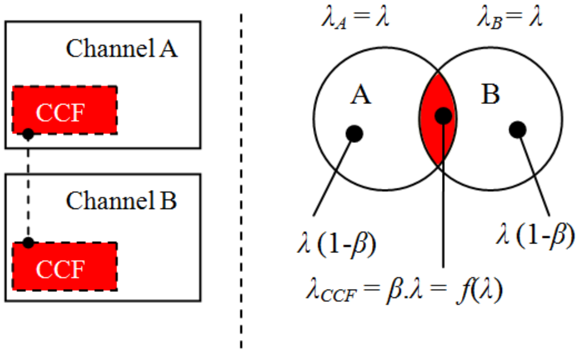
Channel A
CCF
Channel B
CCF
$\lambda_A = \lambda$
$\lambda_B = \lambda$
A
B
$\lambda\,(1\text{-}\beta)$
$\lambda\,(1\text{-}\beta)$
$\lambda_{CCF} = \beta.\lambda = f(\lambda)$

Fig. 3: Common-cause failure of the redundant channels that origins inside the system boundary.

Environment outside the system itself can also present possible source of CCF failures (in dependence on the definition of the system boundary). The cause that initiates simultaneous faulty operation of redundant components (SRCS channels) origins outside the system boundary (illustrated in the Fig. 4). Possible source of such CCF is a common power source or electromagnetic interference for instance. Failure rate of the CCF failures is in this case completely unrelated to a failure rate of the redundant components, so the CCF failure rate must be determined independently.

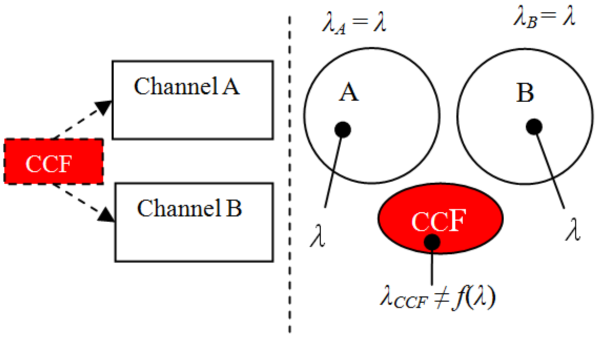

Fig. 4: Common-cause failure that origins in the system environment.

4. Case Study

The effects of CCF can be demonstrated on a simple example of 2oo2 system that operates with identical channels (Fig. 3). Such system can be (for the safety analysis purposes) under specific circumstances (100 % diagnostic coverage of the potentially hazardous failures, negligible time to detect a failure, constant random failure rate) described by a simple CTMC model pictured in the Fig. 5.

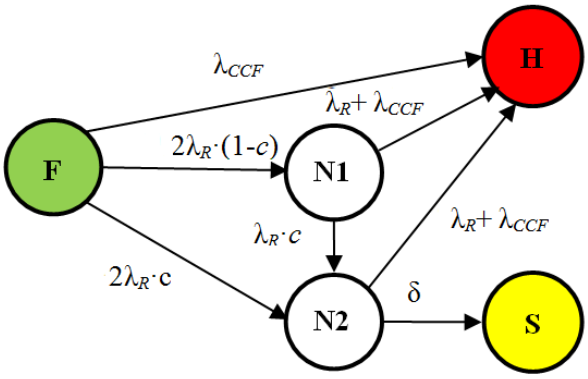
λ_{CCF}
H
$\lambda_R + \lambda_{CCF}$
F
$2\lambda_R\cdot(1\text{-}c)$
N1
$\lambda_R\cdot c$
$\lambda_R + \lambda_{CCF}$
$2\lambda_R\cdot c$
N2
δ
S

Fig. 5: The CTMC model of the SRCS with 2-out-of-2 structure that implements CCF model.

Meaning of the states pictured in the Fig. 5 corresponds with the meaning of the states illustrated in the diagram in the Fig. 2. The diagram in the Fig. 5 shows random hardware failure rate λ_R (λ_R describes single channel; both channels are identical thus both have equal values of hardware failure rate) and rate, with which the system reaches the safe state δ, which can be easily determined by:

$$\delta = \frac{1}{t_D}, \tag{6}$$

in which t_D is a time to detect failure (it is safe to assume with maximal time to detect a failure, not a mean time; if diagnostic checks follow cyclic schedule, then t_D is a duration of single cycle).

Given the fact that $\lambda_{CC} << \lambda_R$, then the diagram pictured in the Fig. 5 can be modified in a way shown in the Fig. 6.

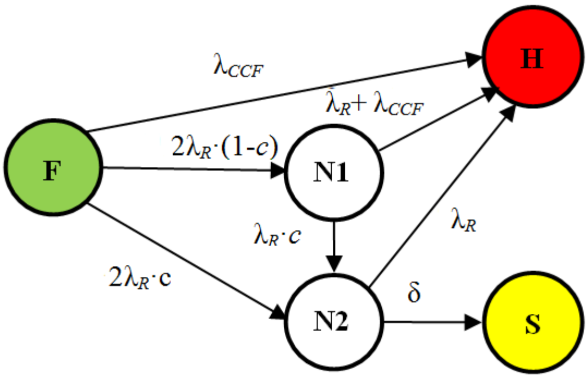

Fig. 6: Simplified CTMC model of the SRCS with 2-out-of-2 structure that implements CCF model.

The diagram in the Fig. 6 can be further divided into two sub-diagrams; each is pictured in the Fig. 7 and Fig. 8 respectively.

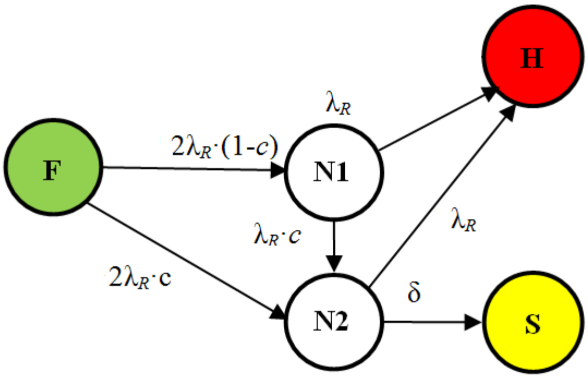

Fig. 7: Sub-diagram - no CCF effects modelled.

The diagram shown in the Fig. 7 is basically a CTMC model of a standard two-channel (2oo2) SRCS without CCF effects implemented. This model can be described by an infinitesimal generator matrix (7) and linear differential equation system (8). More information on how equation (9) can be used to evaluate the probability of hazardous state derived from the differential equations system and initial probability distribution vector (10), and on safety properties of SRCS with 2oo2 architecture can be found in [12]:

$$\mathbf{A} = \begin{pmatrix} -2\,\lambda_R & 2\,(1-c)\lambda_R & 2\,c\,\lambda_R & 0 & 0 \\ 0 & -\lambda_R - c\,\lambda_R & c\,\lambda_R & \lambda_R & 0 \\ 0 & 0 & -\lambda_R - \delta & \lambda_R & \delta \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (7)$$

$$\frac{d}{dt}\vec{P}(t) = \vec{P}(t) \cdot \mathbf{A}, \quad (8)$$

where $\vec{P}(t)$ is absolute probability distribution vector.

$$\begin{aligned} P_H^{2oo2}(t) = e^{-2\lambda_R t} - 1 + \\ + \frac{2\delta}{(\lambda_R - \delta)\cdot(1+c)} \cdot (e^{-2\lambda_R t(1+c)} - 1) - \\ - \frac{2\lambda_R^2 c}{\lambda_R c - \delta \cdot \lambda_R + \delta} \cdot (e^{-(\lambda_R + \delta)t} - 1). \end{aligned} \quad (9)$$

$$\vec{P}(t) = \{1, 0, 0, 0, 0\}. \quad (10)$$

The diagram in the Fig. 8 shows simple 2-state diagram that illustrates the transition of the SRCS from failure-free state (F) into a hazardous state (H) caused solely by a CCF.

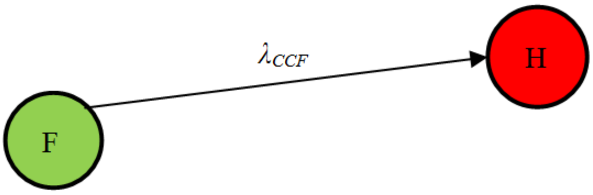

Fig. 8: Subdiagram - only the CCF effect modelled.

Based on the diagrams pictured in the Fig. 6, Fig. 7, and Fig. 8 the total failure rate can be evaluated as:

$$\lambda_H = \lambda_{CCF} + \lambda_H^{2oo2}, \quad (11)$$

in which λ_H^{2oo2} is transition rate of the system from the (F) state into the (H) state (as seen in the Fig. 7), which can be evaluated using the equations (2) and (9).

In adherence to the standards [10] and [11] it can be assumed that β-factor of real SRCS could fall between 0 to $0,2$ (mainly depending on applied failure-avoiding measures. Therefore evaluations can be performed in a following fashion (given the equation (5) and the fact that $\lambda_{CC} << \lambda_R$):

$$\lambda_{CCF} = \frac{\beta}{1-\beta} \cdot \lambda_R. \quad (12)$$

The plot in the Fig. 9 shows the CCF effect on the probability of the hazardous state of the SRCS under analysis (modelled by the CTMC in the Fig. 6). Typical values of the β-factor have been chosen. When the measure has been evaluated, it was assumed, that $\lambda_R = 2,5 \cdot 10^{-5}\ \mathrm{h}^{-1}$, $c = 1$ and $\delta = 1\ \mathrm{h}^{-1}$.

When the equations (2) and (11) are applied on the probability of the hazardous state $P_H(t)$, hazardous failure rate λ_H can be obtained as a result. The same SRCS and the same typical values of the β-factor have been chosen. The result of the analysis is pictured in the Fig. 10.

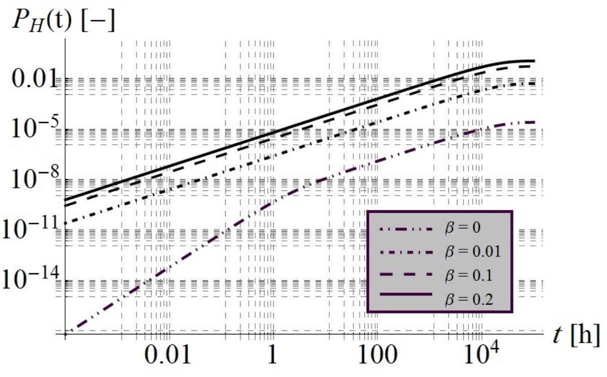

Fig. 9: Probability of the hazardous state of the system.

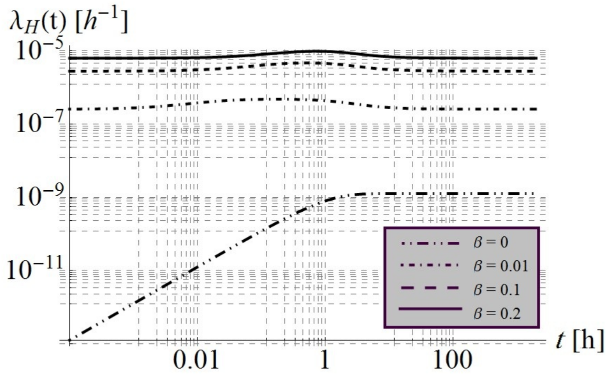

Fig. 10: Hazardous failure rate in dependence on different β-factor values.

In order to put the dominance of the CCF over other system parameters into perspective, the plot pictured in the Fig. 11 has been created. It presents failure rate tolerance areas for different β values ($\beta = 0$, $\beta = 0,2$). The failure rate margin has been set to $\lambda_R =< 2,5 \cdot 10^{-5}$ h^{-1}, $2,5 \cdot 10^{-6}$ h^{-1} $>$. The plot clearly says, that CCF effects on the safety integrity are dominant, even over the effects of failure rate of the respective channels. The large the β value is, the less important is the absolute value of the failure rate of the SRCS redundant channels.

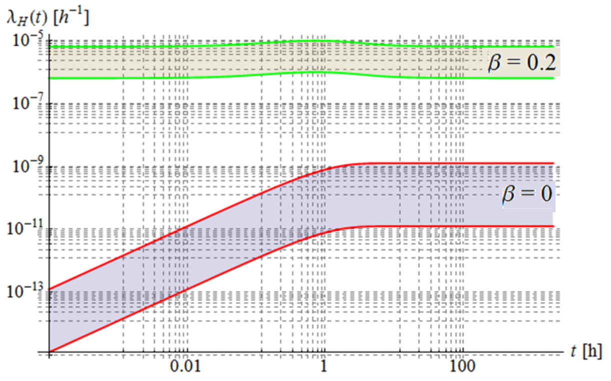

Fig. 11: Hazardous failure rate with specified margins of channel failure rate.

5. Conclusion

The effects of the factors on the SRCS safety that are mentioned in this paper are heavily dependent on each other. The employment of simple methods (like RBD or FTA) for this purpose is constrained, since those simple methods need to create standalone model for each considered system parameter. Revelation of mutual influences between system parameters is therefore a formidable task for such methods. In conclusion, only local optimisation of the given architecture with regard to the respective factor is achievable. On the other hand, Markov chain-based models can comprehensively describe effects of multiple factors on the safety of the SRCS. However, practical experiences still show that best results of the safety analysis are achieved through the use of convenient combination of methods. If a combination of mathematical methods is used, then a great attention is to be paid to mathematical conditions and assumptions related to all combined methods.

CCF failures have a strong impact on the safety and their estimation and mathematical description is often inaccurate. That is why the subjective attitude of the safety evaluator could also be significant, which is rather unacceptable. Therefore if the SRCS requires SIL 4 category safety requirements, then prove is to be made, that no CCF related effects influence the safety, or at least that their influences are negligible. Such prove can be done through the application of satisfactory technical (exclusion of physical and functional causes) and organisational (exclusion of process-related issues) measures that aim for the reduction of possible CCF sources.

Acknowledgment

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0388/12 "Quantitative safety integrity level evaluation of control systems in railway application".

References

[1] RASTOCNY, K. and J. ILAVSKY. Quantification of the Safety Level of a Safety-critical Control System. In: *International Conference on Applied Electronics (AE), 2010*. Pilsen: IEEE, 2010, pp. 1–4. ISBN 978-80-7043-865-7. ISSN 1803-7232.

[2] RASTOCNY, K. and J. ILAVSKY. *Effects of a Periodic Maintenance on the Safety Integrity Level of a Control System **. Berlin Heidelberg:

Springer-Verlag, 2010. ISBN 978-3-642-14260-4. DOI: 10.1007/978-3-642-14261-1_8.

[3] IEC 61165 Ed. 2.0 b. *Application of Markov techniques*. New York: IEC, 2008.

[4] DIN IEC 62551. *Analysemethoden fur Zuverlassigkeit, Petrinetz-Modellierung*. Berlin: IEC, 2008.

[5] KNEGTERING, B and A.C. BROMBACHER. Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by the IEC 61508 standard for functional safety. *Reliability Engineering and System Safety*. 1999, vol. 66, iss. 2, pp. 171–175. ISSN 0951-8320. DOI: 10.1016/S0951-8320(99)00034-4.

[6] SLOVAK, R. *Metodische Modellierung und Analyse von Sicherungsystemen des Eisenbahnverkehrs*. Braunschweig, 2006. Dissertation work. Technische Universitat Braunschweig.

[7] RASTOCNY, K. and J. ILAVSKY. Effects of Recovery on the Safety of a Safety-related Control System. In: *International Conference on Applied Electronics (AE), 2011*. Pilsen: IEEE, 2011, pp. 1–4. ISBN 978-1-4577-0315-7. ISSN 1803-7232.

[8] KLAPKA, S. *Detekcni kody v zabezpecovaci technice*. Prague, 2009. Habilitation work. Czech Technical University in Prague.

[9] RASTOCNY, K. and J. ILAVSKY. What Is Concealed Behind the Hazardous Failure Rate of a System? In: *Modern transport telematics: 11th international conference on transport systems telematics, TST 2011*. Berlin Heidelberg: Springer-Verlag, 2011, pp. 372–381. ISBN 978-3-642-24659-3. ISSN 1865-0929.

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

[11] EN 50129. *Railway applications: Safety-related electronic systems*. Brussels: CENELEC, 2003.

[12] RASTOCNY, K. and J. ILAVSKY. A Markov model of technical safety of a control system. *Journal of Information, Control and Management Systems*. 2010, vol. 8, no. 5, pp. 559–568. ISSN 1336-1716.

About Authors

Juraj ILAVSKY was born in 1985 in Hybe, Slovak Republic. In 2012 he received his Ph.D. from University in Zilina, in the field of Automation - Process control. His professional focus lays in the safety assessment of safety-related control systems, mainly in railway applications, which is closely related to his research activities that cover mathematical models of safety attributes of control systems.

Karol RASTOCNY born in 1958 in Setechov, Slovak Republic. He received his Prof. in 2009 in the field of "Control Engineering". His professional orientation covers solving problems of functional and technical safety, hazard analysis and risk analysis of safety-related applications, preferably oriented to railway domain.

Juraj ZDANSKY was born in 1980 in Nova Bana, Slovak Republic. He received Ph.D. in 2007 in the field of "Control Engineering". His professional orientation covers programming and design of the control and visualization systems, especially in the field of Safety-PLC controlled systems.