https://doi.org/10.26552/com.C.2010.3A.93-97



Jan Rofar – Maria Franekova – Peter Holecko *

# MODELLING OF SAFETY CHARACTERISTICS OF REDUNDANT SAFETY – RELATED TRANSMISSION SYSTEM VIA MARKOV'S ANALYSIS

*The paper deals with problems of safety features modelling using a safety-related redundant transmission system as part of a safety –critical control system. The main part of the paper is oriented to the Markov model description which was realised for a 1oo2 redundant transmission system. The results of quantitative safety analyses are valid for the fail safe redundant transmission system – Profibus DP with a ProfiSafe safety profile.*

*Keywords: safety-related transmission system, industrial application, modelling, quantitative analysis, Markov model, safety code, transmission code, SHARPE*

## 1. Introduction

In control safety-critical processes in industrial applications safety-relevant industrial communication systems are being used for transmission of safety-relevant data, which are characterised by a high resistibility against hazardous failures. The consequences of failures on a communication system's operation can be examined directly on the original system or by the system's operation simulation using a proper constructed model or by theoretical considerations and calculations. It is necessary to point out that in most cases the strict safety requirements on a safety-relevant industrial communication system cannot be proved only by tests or practical results because the dangerous state percent occurrence of a communication system is very low. Therefore the value of mean time between hazardous failures many times exceeds the operational time of system. During safety analyses it is necessary to provide a proof that the resultant risk is acceptable and the safety requirements are met.

The goal of the analysis of failures consequences on an industrial communication system is to construct a model which enables to identify the system's transition process from a safe state to a hazardous state and allows calculating the probability of hazardous system state occurrence as a result of failures effects on the system's operation. An industrial communication system consists of terminal equipment and a transmission system. In most cases the vendors of safety-relevant devices indicate the resulting SIL (Safety Integrity Level) so only characteristics of the transmission system have to be examined.

The transmission system usually does not operate isolated but is a part of another superior system providing service for it. Therefore, the starting point of building a safety model is an exact definition of the interface between the transmission system and the superior system for the purpose to enable a complete hazard identification which has to be considered during the transmission system safety analysis. It is also necessary to explicitly define the event on the transmission system's output which is considered unwanted (hazardous) in respect to safety properties of the transmission system. An unwanted event usually includes an undetected data transmission corruption and the next data manipulation is considered to be correct.

The knowledge of a transmission system failure and error attributes create basic assumptions for realising measures not only for failure prevention but also for failure detection and failure consequences negation. It is necessary to know where, when and what failures occur in systems, what are their reasons and consequences on the system. From this point of view the considered failures can be in principle classified in [1]: random failures of the transmission system's hardware part, failures caused by EMI (*Electromagnetic Interferences*) and systematic failures of the transmission system.

Industrial communication systems with a higher safety integrity level often involve compound safety techniques in failure states based on a redundant multichannel structure. Then the execution of a safety-relevant function is realised independently by at least two functional units. The compound safety systems utilise several forms of redundancy for achieving the required safety integrity level [1].

The article presents a model of a 1 out-of 2 (1oo2) system.

* **Jan Rofar, Maria Franekova, Peter Holecko**
Faculty of Electrical Engineering, University of Zilina, Slovakia, E-mail: jan.rofar@fel.uniza.sk

## 2. The Sense of Safety-Relevant Industrial Communication System Modelling

Usually when modelling a safety-relevant industrial communication system several system parameters are being observed, which are a part of the system's technical quality care. Among these are reliability, safety, operational life, availability, no-failure operation and maintainability [2]. The generic standard IEC 61508 [3] recommends focusing on four parameters within the system lifetime: Reliability, Availability, Maintainability, Safety (RAMS), as illustrated in Fig. 1, which provides a more global view of the system safety. The defined system attributes can be fulfilled only with the use of additional safety measures (so-called Fault prevention, Fault tolerant or Fault forecast system) by which the effects of failures or failure states can be eliminated. In case it is not possible to exclude an unauthorised access to the industrial communication system besides RAMS parameters it is necessary to watch security attributes such as confidentiality, integrity and availability.

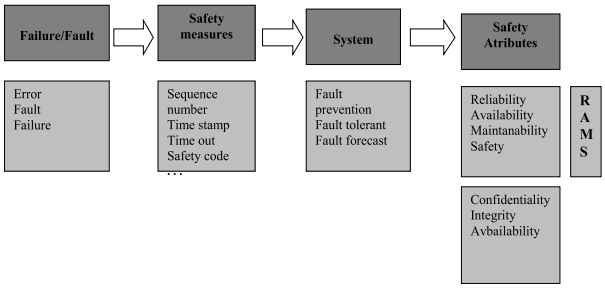


*Fig. 1 A more complex look on industrial communication system safety*

In praxis we encounter most frequently the following requirements related with the modelling of safety properties of an industrial communication system:

- Improvement of safety properties of an existing product or development of a new product, respectively.
  It is necessary to modify the safety layer and some algorithms of a communication protocol or to create a new protocol with the aim to increase the strength of safety mechanisms; when solving this type of tasks the Unified Modelling Language (UML) can be successfully utilised;

- Demonstration of safety properties of a new product
  It is necessary to demonstrate that the industrial communication system has a sufficient resistibility to attacks against transmitted messages by calculating the intensity of undetectable corruption of a transmitted message based on theoretical considerations (analysis of protocol safety properties, estimation of communication channel bit-error rate (BER), calculation of residual error rate of used codes, estimation of transmission system hardware failures intensity, ...) and also the results of the communication system testing in failure-free and failure operation; in this case we can use suitable combinations of modelling methods (RBD [4], FTA [5], FMEA [6], Markov model [7], Petri networks [8], ...) or software tools supporting these methods (e.g. BQR reliability engineering [9], RELEX software [10], ITEM software [11], Matlab – Communications Toolbox [12], OPNET Modeler [13]).

## 3. Makov Model Creation

A simultaneous influence of several factors on the transmission system safety can be well described by Markov model. Figure 2 shows a block scheme of a redundant channel structure $1_{00}2$ of a safety-relevant Profibus DP transmission system extended by a special ProfiSafe safety module [14]. A two channel structure is composed of two transmission channels connected in parallel, which perform the safety function of provisioning transmission integrity and eliminating the EMI influence with the use of implemented safety mechanisms in a form of safety code (SC) [15] and transmission-code TC [15] independently in both channels. This means that in case of a failure or system malfunction the hazardous failure had to occur in both channels.

The probability of undetected error pu with using a block linear channel ($n$, $k$) code (transmission or safety code) can be approximated by the relation

$$p_U \cong \frac{1}{2^{n-k}}\binom{n}{d_{\min}} p_b^{d_{\min}} (1 - p_b)^{n - d_{\min}} \qquad (1)$$

where the symbols represented:
$n$ codeword length,
$k$ information word length,
$d_{\min}$ minimal Hamming distance,
$p_b$ bir error rate of communication channel
Note: we assume model of BSC (*Binnary Symmetric Channel*)

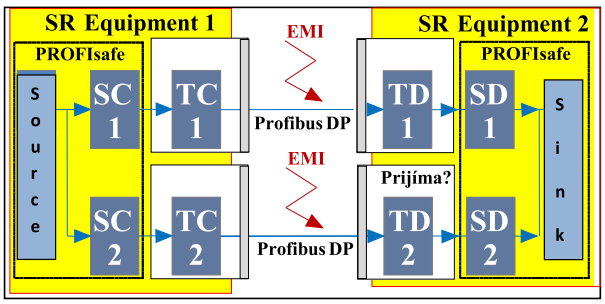


*Fig. 2 Two-channel redundant structure of a safety-relevant transmission fieldbus system*

Let's assume that any diagnostic testing can detect transmission errors only, not correct them. Furthermore, let's suppose that the individual transmission channels are of different hardware construction and that the safety mechanisms and the transmission mode have a cyclic character which is initialised by a master type transmission device.

Figure 3 represents a model of a two-channel redundant structure of a closed safety-relevant Profibus DP transmission system

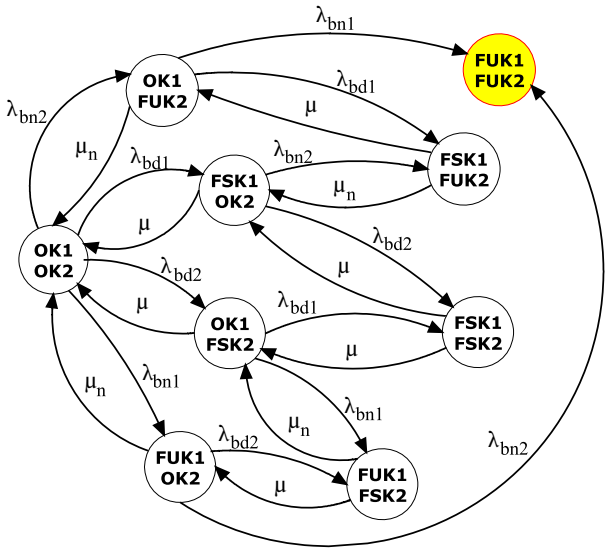


*Fig. 3 Markov diagram of a redundant two-channel 1oo2 structure of a transmission structure*

at a two-point connection level which is realised using Markov analysis. The meaning of individual states and transitions is characterised in Table 1.

At the beginning the redundant industrial safety-relevant system is in operating state in both transmission channels OK1 and OK2. On the occurrence and detection of a transmission error the system passes in both channels to the state of defined failure reaction, a so-called Fail Safe state: FSK1 and FSK2 with the intensity $\lambda_{bd}$ and subsequently requests a repeated message sending, i.e. the system returns to operating states OK1 a OK2 with intensity μ. In case the transmission error remains undetected (Fail Unsafe state) the system passes to FUK1 and FUK2 states with intensity $\lambda_{bn}$. If the states FUK1 and FUK2 don't occur at once, the discrepancy between transmission channels is detected based on diagnostic testing and the system switches again to operating states OK1 or OK2 with diagnostic testing recovery intensity $\mu_n$. In case that both these states FUK1 and FUK2 occur at the same time the system ends up in a hazardous state of undetected transmission error.

## 4. Results

The safety analysis of the model depicted in Fig. 3 was realised with the use of a transmission and safety code in form of cyclic block CRC (Cyclic Redundancy Check) codes (specifically CRC-16 and CRC-8) whereby the independence of generating polynomials is emphasised. As the input parameters for calculation of safety attributes: intensity of hazardous (critical) failures $\lambda_{kr}$ [$h^{-1}$], mean time to failure $MTTF_{kr}$ [h] statistical values of BER [-] were used, for the physical Profibus DP bus layer RS 485 (transmission rate 9,6kbit/s) for which the probabilities of undetected hazardous transmission code error in both channels $p_{u\_bk1}$ [-] and $p_{u\_bk2}$ [-]

States and transitions for the diagram in Figure 3 Table 1

| State | State description |
|---|---|
| OK1 | Transmission of uncorrupted messages between devices. Channel 1 operational state. |
| OK2 | Transmission of uncorrupted messages between devices. Channel 2 operational state. |
| FSK1 | Channel 1 safety decoder detected a corrupted message. It is a safe failure state of transmission channel 1. |
| FSK2 | Channel 2 safety decoder detected a corrupted message. It is a safe failure state of transmission channel 2. |
| FUK1 | Channel 1 safety decoder did not detect a corrupted message. It is a hazardous failure state of transmission channel 1. |
| FUK2 | Channel 2 safety decoder did not detect a corrupted message. It is a hazardous failure state of transmission channel 2. |
| **Transition** | **Transition description** |
| OK1→FSK1 | The transition occurs in dependence on transmission channel 1 message error, which is consequently detected by channel 1 safety code. |
| OK1→FUK1 | The transition occurs in dependence on transmission channel 1 message error, which is not detected by channel 1 safety code. |
| FSK1→OK1 | The transition occurs in dependence on failure handling mechanism and the repeated transition to transmission channel 1 operational state. In most cases on operator confirmation. |
| FUK1→OK1 | The transition occurs in dependence on diagnostic testing mechanism of both transmission channels and the repeated transition to transmission channel 1 operational state. In most cases on operator confirmation. |
| OK2→FSK2 | The transition occurs in dependence on transmission channel 2 message error, which is consequently detected by channel 2 safety code. |
| OK2→FUK2 | The transition occurs in dependence on transmission channel 2 message error, which is not detected by channel 2 safety code. |
| FSK2→OK2 | The transition occurs in dependence on failure handling mechanism and the repeated transition to transmission channel 2 operational state. In most cases on operator confirmation. |
| FUK2→OK2 | The transition occurs in dependence on diagnostic testing mechanism of both transmission channels and the repeated transition to transmission channel 2 operational state. In most cases on operator confirmation. |

were calculated according to relation (1). The calculation was providing that the generation frequency of safety-relevant messages from source 1 and from source 2 is $f_{brs1} = f_{brs2} = 18\,000$ messages/h.

The resulting safety attributes values of a redundant two-channel structure can be found in Table 2. The graphs of safety function

$S(t)$ which represents the time dependence of the system getting into an undetected failure state while using a two-channel redundant structure FUK1 and FUK2 are shown in Fig. 4. The results were obtained using the SHARPE modelling tool [16].

The graphs in Fig. 4 represent results with the recommended type of CRC code used in the ProfiSafe profile in both cases the CRC-16 only with different generating polynomials.

The curve of function $S(t)$ 2 and 3 is a result of CRC codes combination, as stated in Table 2. From the results obtained it is obvious that the scheme with $1_{OO}2$ redundant structure fulfils the safety integrity level SIL3 requirements where the tolerated intensity of hazardous failures per hour is within the limits from $10^{-8}$ to $10^{-7}$.

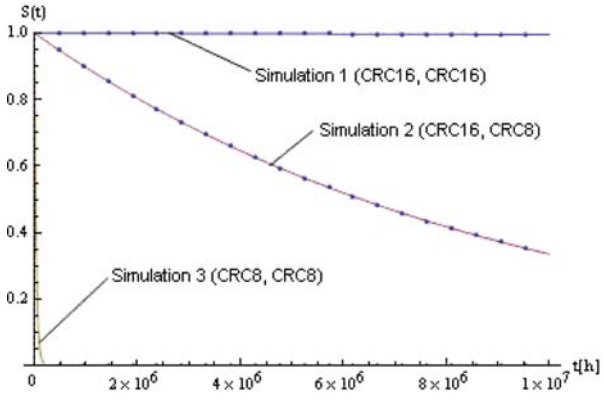


*Fig. 4 Graphs of S(t) safety function for Markov diagram in Fig. 3*

Input and output values for the diagram in Fig. 3 Table 2

| Denotation | Simulation 1 | Simulation 2 | Simulation 3 |
|---|---|---|---|
| | 9.6kbps, CRC 16, CRC 16 (O) | 9.6kbps, CRC 16, CRC 8 (O) | 9.6kbps, CRC 8, CRC 8 (O) |
| $f_{brs1}$ [$h^{-1}$] | 18000 | 18000 | 18000 |
| $f_{brs2}$ [$h^{-1}$] | 18000 | 18000 | 18000 |
| $p_{ned\_bk1}$ [-] | $1.52588.10^{-5}$ | $1.52588.10^{-5}$ | 0.00390625 |
| $p_{ned\_bk2}$ [-] | $1.52588.10^{-5}$ | 0.00390625 | 0.00390625 |
| $p_{brch1}$ [-] | 0.00127919 | 0.00127919 | 0.00127919 |
| $p_{brch2}$ [-] | 0.00127919 | 0.00127919 | 0.00127919 |
| $\lambda_b$ [$h^{-1}$] | 1 | 1 | 1 |
| $\lambda_d$ [$h^{-1}$] | 1 | 1 | 1 |
| $MTTF_{kr}$ [h] | $2.34.10^9$ | $9.17.10^6$ | $3.59.10^4$ |
| $\lambda_{kr}$ [$h^{-1}$] | $4.27691.10^{-10}$ | $1.09099.10^{-7}$ | $2.78311.10^{-5}$ |

## 5. Conclusions

Using the presented model it is also possible to realise a safety analysis of a two-channel redundant structure at the level of a two-point connection in case that both transmission channels use different transmission media or their transmission is ensured by different safety mechanisms.

The constructed model represents a suitable tool for quantitative safety analysis of a safety-relevant Profibus DP-type transmission system which has a wide application within the frame of safety-critical processes control in industry. The described method is suitable for modelling of safety properties of dynamic systems where the occurrence of random failures (caused for example by aging, physical corruption of the transmission system's hardware components and unintentional EMI failures) is expected. It is created for the Profibus DP safety profile but with a change of input parameters or after a minor modification of the individual models it is also applicable for quantitative safety analyses of other safety fieldbus systems.

**Acknowledgement:**

This contribution is the result of the project implementation: **Centre of excellence for systems and services of intelligent transport,** ITMS 26220120028 supported by the Research & Development Operational Programme funded by the ERDF.


"Podporujeme vyskumne aktivity na Slovensku/Projekt je spolufinancovany zo zdrojov EU."

## References


[1] ZAHRADNIK, J., RASTOCNY, K., KUNHART, M.: *Bezpecnost zeleznicnych zabezpecovacich systemov* [Safety of Railway Control Systems], EDIS ZU, Zilina, 2004, ISBN 80-8070-296-9 (in Czech).

[2] MYKISKA, A.: *Bezpecnost a spolehlivost technickych systemu* [Safety and Reliability of Technical Systems], CVUT Praha, 2006, ISBN 80-01-02868-2, (in Czech).

[3] IEC 61508: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems,* 1998.

[4] BILLINTON, R., ALLAN, R. N.: R*eliability Evaluation of Engineering System - Second Edition,* Extension College ol Engineering University ol Saskatchewan Saskatoon : Saskatchewan : Canada. 2007.

[5] CICHOCKI, T., GORSKI, J.: Failure Mode and Effect Analysis for Safety-Critical Systems with Software Components, *Lecture Notes in Computer Science,* Springer Berlin : Heidelberg, ISSN 0302_9743 (Print) 1611-3349 (Online).

[6] JESTY, P. H., HOBLEY, K. M., EVANS, R., KENDALL, I., CARS, J.: *Safety Analysis of Vehicle-Based Systems,* In: www.scholar/google.sk.

[7] BUKOWSKI, J. V., GOBLE, W. M.: Using Markov Models for Safety Analysis of Programmable Electronic Systems, *ISA Transactions,* Vol. 34, 1995, pp. 193–198.

[8] LEE, W. J., KIM, H. N.: A Slicing-Based Approach to Enhance Petri Net Reachability Analysis, *Journal of Research and Practice in Information Technology,* Vol. 32, No 2, 2000, 131

[9] www.bqr.com

[10] www.relexsoftware.de

[11] www.itemuk.com

[12] FRANEKOVA, M.: *Modelovanie komunikacnych systemov v prostredi Matlab, Simulink a Communications Toolbox* [Communication Systems Modelling in Environment Matlab and Communications Toolbox], ZU, 2003, ISSN 80-8070-027-3 (in Slovak).

[13] www.opnet.com.

[14] MALIK, R., MUHLFELD, R.: A Case Study in Verification of UML Statecharts: the PROFIsafe Protocol, *Journal of Universal Computer Science,* Vol. 9, Issue 2p, pp. 138–151.

[15] EN 50 159 - 1: *Railway Applications: Communication, Signalling, and Processing Systems - Part 1: Safety-related Communication in Closed Transmission Systems,* CENELEC, 1999.

[16] SHARPE Manual, http://www.ee.duke.edu/˜chirel/MANUAL/manualSharpe.pdf.