Journal of ELECTRICAL ENGINEERING, VOL. 61, NO. 6, 2010, 350–356

SAFETY EVALUATION OF FAIL–SAFE FIELDBUS IN SAFETY RELATED CONTROL SYSTEM

Mária Franeková — Karol Rástočný *

The paper deals with the problem of modelling safety features of the safety Fieldbus transmission system used within safety related control systems. The basic principles of the modelling failures effect upon the safety of closed transmission system and standards used in the process of safety evaluation are summarized in the paper. The practical part is oriented to a description of a realized Markov model for determination of the random failures effect on the safety of a closed transmission system. The model reflects the safety analysis of failures effect caused by electromagnetic interference in the communication channel and random HW failures of the transmission system. In the paper the results of simulation of parameters of the transmission system are discussed, such as the probability of an undetected corrupted message.

K e y w o r d s: safety fieldbus, Markov model, safety analysis, random failures, Fieldbus transmission system

1 INTRODUCTION

A variety of characteristics within manufacturing processes in different industry sectors evoke the remaining requirements upon a flexible approach in the solution of the safety of control systems including communication networks.

Today, the industrial communication networks become a part of large measuring and control systems using modern information technologies.

Communication networks within the control systems present one of the essential but also vulnerable points, mainly when open systems based on Wi-Fi, Bluetooth and Zigbee are used [1]. To reach the safety goal within communications it is recommended to apply safety functions, which enforce safety and are executed by suitable safety mechanisms. Safety mechanisms can be implemented in SW (control access to system, using passwords, mechanisms based on cryptography, *etc*), in HW (cipher modules, authentication and identification cards), by physical means (safe deposit box, interlocks, *etc*) or by administration measures (norms, legislation, certification authority, *etc*). COTS (Commercial Off-The-Shelf) communication technologies are not essentially available (without supplementary technical measures) for transmission of safety-related data, although their transmission systems involve detection and correction methods for transmission assurance and eventually other protective mechanisms. Concerning the safety of the transmission, such systems are denoted as non-trusted. To decide which types of additional technical measures are necessary to apply depends on the risk analysis results (analysis of attacks and their effects) related to the controlled process and the acceptable risk.

Nowadays the number of vendors of safety-related communication technologies who guarantee besides standard communication, communication among safety-related equipment according to norm IEC 61 508 [2] is increasing. In the area of conventional industry networks Fieldbus technology [3], [4], is becoming a standard and many implementations appear in the safety-related applications [5], [6]. Nowadays, the standard IEC 61784-3 [7] deals with a definition of functional safety of industrial networks within a digital communication dedicated to use in the area of measuring and control systems in industry and defines safety profiles for CPF (Communication Profile Family) CPF2 (CIP Safety) [8], CPF3 (ProfiSafe) [9] and CPF6 (InterbusSafety) [10]. These safety profiles are recommended for using in safety-related systems with the Safety Integrity Level SIL 3 according to EN 61508 or the category 3 according to EN 954-1. It is assumed that the safety profiles development for the rest of the communication families defined by IEC 61158 will continue. For the industrial networks based on wireless technology it is necessary, besides a safety profile, to implement an additional, secure [11], which solves the requirements on secure communication in accordance with the new standard IEC 61784-4 [12].

The task of analysis and synthesis of a safety Fieldbus comes from the basic definitions valid for the area of railway transport control, presented in the standards [13] and [14].

Generally, four parameters of the system (the so called RAMS parameters) are recommended to monitor the life cycle of the system — R (Reliability), A (Amiability), M (Maintainable) and S (Safety) [15], [16].

When specifying the requirements, in the process of structure design and the production of the communication system and also in the process of its verification and validation modelling fulfils a very important task. In some cases modelling may help to optimize options in other words the setting of parameters within the existing communication system, so that the requirements to the safety

* Department of Control and Information Systems, Faculty of Electrical Engineering, the University of Žilina, Univerzitná 8215/1, SK-010 26 Žilina, Slovakia, maria.franekova@fel.uniza.sk, karol.rastocny@fel.uniza.sk

DOI: 10.2478/v10187-010-0054-z, ISSN 1335-3632

integrity level and availability, which are defined either by a customer or are the result of the risk analysis, are accepted. In order to achieve these tasks it generally requires to combine suitable modelling methods and tools.

2 MODELLING OF SAFETY PROPERTIES OF TRANSMISSION SYSTEM

It is advantageous if the development of a safety-related communication system is based on the utilization of modeling methods (for particular phases of a systems development it is necessary). Basically, the point is that:

- Modelling of functional characteristics of safety mechanisms within SCL (Safety Communication Layer). In this case the model is based on the semi-formal and formal methods (they are usually supported by SW tools), which helps to produce explicit and logical descriptions of the functional possibilities of the system. In this area the object oriented modelling (OOM) can be used. One of the most suitable techniques for a production of such a model is the unified modelling language (UML), which supports different modelling and visualization elements [17].
- Modelling of disturbing effects within transmission media. In this case the model describes effects of Electromagnetic Interference (EMI) and the failures which occur in transmission media.
- Modelling of HW failure effects in the transmission system. In this case, the model reflects the analysis of a subsequent failure of the communication system, which can be realized on the bases of quantitative and qualitative methods.

The next part of this paper is devoted to the tasks of modeling the effect of failure in the Fieldbus transmission system.

2.1 Modelling of failure effects to safety of the closed transmission Fieldbus system

For safety-related systems it is necessary to prove that safety requirements are fulfilled and the consequential risk is acceptable [18]. It is necessary to remark that strict safety requirements for a safety-related system are not possible to achieve only by tests or results from practice (the frequency of occurrence of a dangerous state is very low and the mean time between multiple failures exceeds the value of the useful lifetime of one safety-related system).

The aim of the failure effects analysis on the safety of the system is to form a model, which allows identification of the transition process of the system from a safety state (it may not be necessarily a failure — a free state) to a dangerous state and permits one to calculate the probability of the dangerous state occurrence of the system as a failure effect to the operating system.

The transmission system normally does not work in isolation but as a component part of another, superior system, for which service is provided. Therefore, the start moment of a safety model generating is an exact definition of the interface between the transmission system and the superior system with the aim to facilitate a total identification of threats, which must be taken into consideration in the process of analysis. Also, it is necessary to define explicitly an event in the output of the safety system, which is considered as dangerous (undesirable) with regard to safety features of the transmission system. Generally, the undesirable event is considered to be a violation of the transmission data, which is not detected by the transmission system and further data are regarded as correct.

Except for the safety procedures analysis (the source of a message identification, the check of the type of message, the check of the current data, the analysis of safety codes characteristics, the analysis of safety reaction mechanism, *etc*) it is necessary, according to the norm [2], to evaluate quantitatively the intensity of undetected failures of the transmission system.

The knowledge of failures and faults attributed to the transmission system forms the basic assumptions related to the measures implemented which are not only used to avoid failures but also for the fault detection and negation of the failure effects within their occurrence.

It is important to know where, when, and what types of failures occur in the system, for what reasons they occur and what their effects are on the system. There are three ways in which errors can be divided:

- random failures of the transmission system HW;
- failures caused by EMI;
- systematic failures of the transmission system.

The effect of noise can have different forms which depend mainly on the physical characteristic of the transmission channel. The undesirable effect of EMI is possible to eliminate using both safety and transmission code.

In the messages transmitted across transmission channel EMI causes two types of errors:

- replacing one symbol within a transmitted message with another symbol;
- dropout of a symbol, eventually being replaced by a new symbol (failure of synchronisation).

Because of the fact that the transmission system has to dispose of the required value of a safety level in the case of an unexpected reduction of the transmission line quality, in practical terms we generally make a very pessimistic assumption (each of the messages in the output of the transmission channel is corrupted).

Nowadays there is a lot of channel coding [19]. Within safety-related communication systems block and systematic (n, k) codes are frequently used. By standards it is recommended to use detection codes or correction codes with a modified algorithm for decoding, which finishes the decoding process with detection. The methods for determination of undetected errors in a code word (residual error rate of decoders) are very often derived providing that the mathematical model of either BSC (Binary Symmetric Channel) or AWGN (Additive White Gaussian Noise)

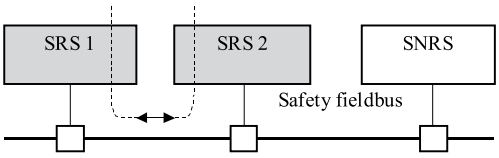

Fig. 1. Communications between SRSs across Safety Fieldbus

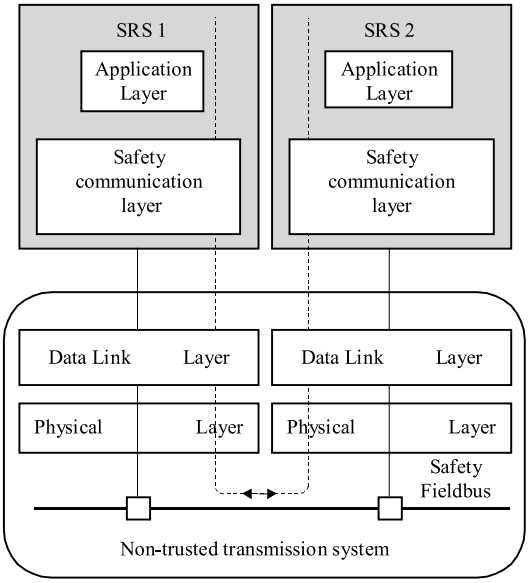

Fig. 2. Layers model of safety related transmission

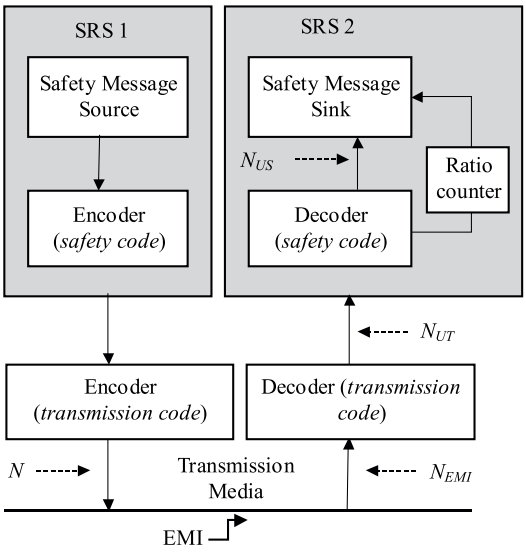

Fig. 3. Safety message transmission from SRS 1 to SRS 2

is used. During the determination of a residual error rate of a block code we can use the statistical results of Bit Error Rates (BER) of typical communication channels. In many cases we prefer to use the channel test (if an application enables it) or to predict the result of BER by simulation of a transmission with the help of a properly selected model of transmission channel.

In the technologies, COTS and also in the safety related layer, a systematic cyclic code is mostly preferred, which works on the principle of CRC (Cyclic Redundancy Check), for which we can determine the probability of an undetected error of the code word p_U according to

$$P_u \cong \frac{1}{2^{n-k}} \sum_{i=d_{\min}}^{n} \binom{n}{i} p_b^i (1-p_b)^{n-i} \tag{1}$$

where $d_{\min}$ is a minimal Hamming distance of code, n is a code word length, k is the length of an information word and p_b is a bit error rate of the channel.

If the condition satisfies $np_b \ll 1$, then the sum (1) can be approximated by the first element of the sum

$$P_u \cong \frac{1}{2^{n-k}} \binom{n}{d_{\min}} p_b^{d_{\min}} (1-p_b)^{n-d_{\min}} . \tag{2}$$

If we do not have the parameters to relations (1) and (2) we can approximate p_u by the worst value of probability of an undetected error in the code word p_n, 2^{-r} (where r is a number of redundant symbols).

2.2 Object of modelling — closed transmission system (safety Fieldbus)

Think of the safety Fieldbus transmission system, which can also communicate between SRS (Safety Related Systems) and SNRS (Safety Non Related Systems) (Fig. 1).

Consider communications between two safety related systems, SRS 1 and SRS 2 on the level of the end to end, whose layer model is illustrated on the Fig. 2. To reach the required safety integrity level in the SCL (Safety Communication Layer) additional arrangements must be applied (*eg* time stamp, sequence number, source/destination address, *etc*) according to the recommendation in the norm [7]. The safety code has the most significant status among safety measures.

The safety code is used to assure integrity of the transmission which might be interfered with by the influence of electromagnetic interference and it is also used to increase safety features which are provided by a transmission code in a standard layer of communication protocol. It is one of the few safety mechanisms where it is possible, with the help of a mathematical mechanism for calculation residual error rate of the codes used, to determine failure intensity, which arises in the transmission system due to the effect of failures in the transmission channel.

The model in Fig. 3. illustrates one way communications can occur between the safety-related system SRS 1, and the safety-related system SRS 2.

A communication system (Fig. 3.) consists of the safety message source, safety message sink and trusted transmission system, which enforces safety-related functions within transmission in compliance with [13]. The

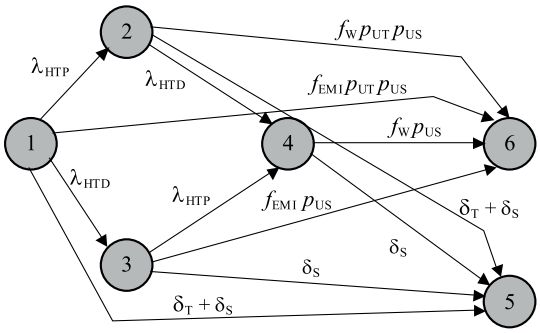

Fig. 4. Markov model of the transmission system

Table 1. The meaning of the symbols

λ_{HTP}	HW failure rate of the transmitter part of the transmission system and the transmission media.
λ_{HTD}	HW failure rate of a decoder of the transmission code.
λ_{EMI}	The corruption rate of transmitted messages caused by EMI.
P_{UT}	Probability of an undetected error of the transmission code.
P_{US}	Probability of an undetected error of the safety code.
F	Mean frequency of messages generated from a transmitter.
f_{EMI}	Mean frequency of corrupted messages caused by EMI.
f_{HTP}	Mean frequency of corrupted messages caused by HW failures of the transmitter part of the transmission system and the transmission media.
f_W	Mean frequency of corrupted messages in the input of transmission decoder without the corruption reason being resolved. Corruption of message is caused by un-trusted transmission system or by EMI.
T_T	Tolerance time of corrupted messages received in the non-trusted part of the transmission system. If within this interval a higher number of corrupted messages as defined number is detected by transmission decoder then permanent interruption of message transmission occurs.
T_S	Tolerance time of corrupted messages received in the trusted part of the transmission system. If within this interval a higher number of corrupted messages as defined number is detected by safety decoder then permanent interruption of message transmission occurs.
δ_T	The intensity of the transition to a permanent safety state caused by the failure of operation mechanisms for checking a number by a decoder of the transmission code. $\delta_T = 1/T_T$.
δ_S	The intensity of the transition to a permanent safety state caused by the failure of the operation mechanisms for checking a number by a decoder of the safety code. $\delta_S = 1/T_S$.

base of the trusted transmission system includes non-trusted transmission systems (COTS system), which ensures transmission messages by the transmission code (TC). To achieve the required safety level of a transmission, transmission messages have to be ensured by the safety code (SC). It is necessary for the encoder and decoder of the safety code to be implemented on the fail-safe principle. A component part of the transmission system is the transmission media, which is influenced by electromagnetic interference (EMI) only. The authors assume only a closed transmission system and the independence of the encoders/decoders of the safety and transmission codes. We do not assume unauthorized access to the system.

2.3 Markov model of the closed transmission system

The coincidental effect of several safety factors on the transmission system can be demonstrated by using Markov chain. The system transitions from a functional safety state 1 to a dangerous state 6 is illustrated in Fig. 4. In the model failures effect of safety decoder to safety features of the transmission system is not considered. Safety decoder is component part of SRS that is why the problems related to its safety are solving within SRS.

The meaning of particular symbols in the diagram in Fig. 4. is illustrated in Tab. 1. The characteristics of the particular states in the Fig. 5. are described in Tab. 2 and Tab. 3.

During the model designing it is necessary to know the number of corrupted messages (define time unit) in the parts of the communication system, which is important for the safety analysis.

The meaning of the number of messages according to Fig. 3. and their mathematical expression providing that the communication system is in a failure-free state:

- N is a number of messages generated from a transmitter during the time T, *ie* $N = fT$;
- N_{EMI} is the number of corrupted messages in input of TD during the time T, *ie* $N_{EMI} = f_{EMI}T$;
- N_{UT} is the number of corrupted messages in output of TD during the time T, *ie* $N_{UT} = f_{EMI}p_{UT}T$;
- N_{US} is the number of corrupted messages in output of SD during the time T, *ie* $N_{US} = f_{EMI}p_{UT}p_{US}T$.

Similarly we can determine the number of corrupted messages which is detected by a decoder of the transmission code N_{DT} or by a decoder of the safety code N_{DS} during the time T, *ie*

$$N_{DT} = f_{EMI}(1 - p_{UT})T\,, \tag{3}$$

$$N_{DS} = f_{EMI}p_{UT}(1 - p_{US})T\,. \tag{4}$$

The diagram in Fig. 3. can be simplified if we suppose that the failure of a decoder of the transmission code occurs, so then there is no reason to consider some effects from other parts of the non-trusted transmission system (the transmitter and transmission media) on frequency of a corrupted data (Fig. 5.). This case of safety can be characterized as pessimistic assumption, in which all received messages are corrupted and such failure of transmission decoder occurred that the transmission decoder considers

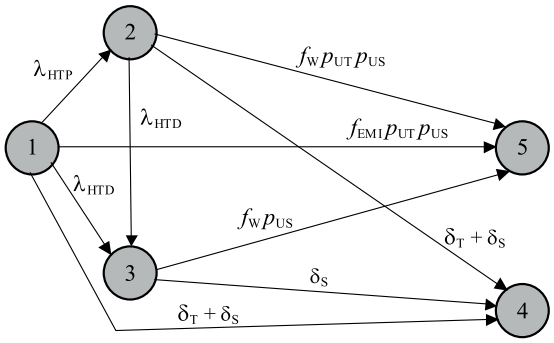

Fig. 5. Simplified Markov model of the transmission system

Table 2. The states in the diagram

State	A description of the states	$\mathbf{P}(t=0)$
1	The transmission system is functional; transmission messages are corrupted only by EMI.	1
2	The transmission system state, when the transmitter part of the transmission system or some part of the transmission channel is in random HW failure.	0
3	The transmission system state, when the decoder of transmission code is in random HW failure.	0
4	The transmission system state, when the transmitter part of the transmission system or some part of the transmission media and the decoder of the transmission code is in random HW failure.	0
5	Permanent interruption of transmission caused by the failure of operation mechanisms for checking of number of detected corrupted messages. Failures of the transmitter and transmission media are detected by the receiver.	0
6	The hazard state corrupted message was undetected.	0

all messages as correct. Markov chain can be mathematically described with the set of differential equations and by a vector of initial probabilities. The set of differential equations are the following

$$\frac{\mathrm{d}\mathbf{P}(t)}{\mathrm{d}t} = \mathbf{P}(t)\mathbf{A}\,, \tag{5}$$

where $\mathbf{P}(t) = \{p_1(t), p_2(t), \ldots, p_n(t)\}$ is a vector of absolute probabilities and $\mathbf{A}$ is a matrix of intensity of transitions. The vector of initial probabilities is $\mathbf{P}(t=0) = \{1, 0, \ldots, 0\}$.

The relation of probability of a particular states occurrence in the diagram, according to the parameters of a model, can be exactly formulated by an analytical solution. The solution for more complex diagrams is very difficult; hence in praxis we are satisfied only with a numerical resolution. The calculation precision depends on the suitable selection of a calculation method and on the numerical precision of computing techniques. In the present time there are several SW products which support a solution with the use of Markov model.

Such a model is based on the supposition that if the detection of a corrupted message occurs then the system will go to the previously defined safety state. Otherwise this solution contributes to the increase of the integrity level of the system but on the other hand significantly decreases availability of the system, which negatively affects the secondary safety.

Table 3. The transitions in the diagram

Transition	A description of the transition
$1 \to 2$ (λ_{HTP})	The transition is realized as a consequence of HW failure of the transmitter part of the transmission system or some part of the transmission media.
$1 \to 3$ (λ_{HTD})	The transition is realized as a consequence of HW failure of a decoder of the transmission code.
$1 \to 5$ $(\delta_T + \delta_S)$	The transition is realized as a consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the transmission code or the safety code.
$1 \to 6$ $(f_{EMI} p_{UT} p_{US})$	The transition is realized as a consequence of insufficient detection characteristic of the transmission and safety codes.
$2 \to 4$ (λ_{HTD})	The transition is realized as a consequence of HW failure of a decoder of the transmission code.
$2 \to 5$ $(\delta_T + \delta_S)$	The transition is realized as a consequence of the mechanisms operation for checking the number of detected corrupted messages by decoder of transmission code or safety code.
$2 \to 6$ $(f_{EMI} p_{UT} p_{US})$	The transition is realized as a consequence of insufficient detection characteristic of the transmission and safe codes.
$3 \to 4$ (λ_{HTS})	The transition is realized as a consequence of HW failure of the transmitter part of the transmission system or some part of the transmission media.
$3 \to 5$ (δ_S)	The transition is realized as a consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code.
$3 \to 6$ $(f_{EMI} p_{US})$	The transition is realized as a consequence of insufficient detection characteristic of the safety code.
$4 \to 5$ (δ_S)	The transition is realized as a consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code.
$4 \to 6$ $(f_{EMI} p_{US})$	The transition is realized as a consequence of insufficient detection characteristic of the safety code.

Generally, it is necessary to choose a suitable compromise between availability and the level of safety integrity requirements. The solution of this problem can be based on using the so-called ratio criteria, which is based on the evaluation of the positive and negative ratio results of the correctness control of a received message. In fact the base of this method uses the ratio counter (Fig. 3.), which counts in a defined range $\langle I; M \rangle$ and by start it

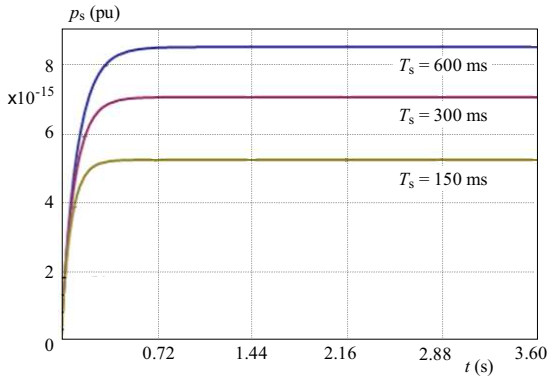

Fig. 6. The probability of undetection of a corrupted message (example 1)

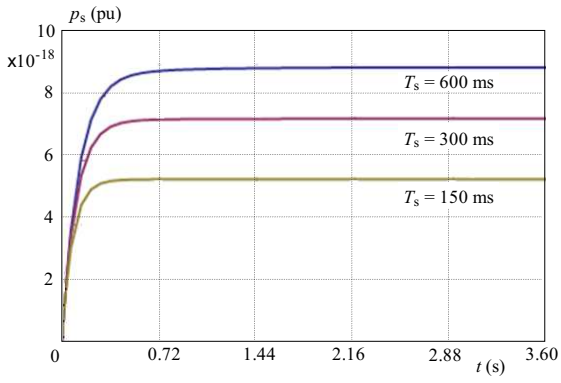

Fig. 7. The probability of undetection of a corrupted message (example 2)

sets an initial value I (*eg.* 0). The actual value of the ratio counter changes according to the result of the correctness control of a received message. In case of a positive result the state of the counter is decremented by P (as far of the initial value) and in case of a negative result the state of the counter is incremented by the value N. The condition $N > P$ must be fulfilled. When the counter achieves or overruns the boundary value M, the safety reaction and transition of system to safety state occurs.

In case of this mechanism application it is necessary to respect this fact within the model creation and consecutive calculations.

3 OBTAINED RESULTS

In practice the application of the model in Fig. 5 runs into trouble at a high rate of indefiniteness of parameters of the model.

In practical calculations it is possible to solve this problem using a pessimistic approach in the selection of values of parameters of the model.

Consider the following parameters of a closed transmission fieldbus system, which was described in Fig. 5:

- $\lambda_{HTP} = 5.3 \times 10^{-5}\mathrm{h}^{-1}$;
- $\lambda_{HTD} 2.5 \times 10^{-6}\mathrm{h}^{-1}$;
- $f_W = 72000\,\mathrm{h}^{-1}$ (messages are transmitted periodically every 50 ms; we assume that all messages are corrupted);
- $f_{EMI} = 72000\,\mathrm{h}^{-1}$ (messages are transmitted periodically every 50 ms; we assume that all messages are corrupted in the effect of EMI);
- $T_T = 150$ ms (the transmission system is configured so that if three consecutively received messages are false then the connection is interrupted);
- $p_{UT} = 2^{-16}$; according to norm [13] the probability of an undetected error by a transmission code, we can estimate by $p_{UT} = 2^{-r}$ (CRC-16);
- $p_{US} = 2^{-32}$ (CRC-32).

The result of the probability of undetection of a corrupted message p_5, (state 5 in the model) depending on the uptime of the operating system and the tolerated time of the corrupted messages received in the trusted part of transmission system, is illustrated in Fig. 6.

It stands to reson that by increasing the quality of transmission channel there is a change of safety features of the transmission system. In Fig. 7 the graphical results of probability of undetected corrupted messages are illustrated if the parameter $f_{EMI} = 72\,\mathrm{h}^{-1}$ (in simulated example each thousandth message is corrupted).

From the graph it stands to reason that the result of the probability of undetected corrupted message is markedly affected by the setting of tolerated time of the corrupted messages received in the trusted part of transmission system T_S *ie* by suitable selection of ratio criteria.

4 CONCLUSIONS

In the paper the results of safety analysis of EMI and random failures effects of transmission system safety Fieldbus are mentioned. We assumed permanent types of failures only. Effects of fail-silent and transient failures were not considered in the paper by reason that quantitative evaluation of occupance rate is problematic. For evaluation of effects of fail-silent and transient failures the qualitative methods are used [2].

The presented advancement of the calculation of probability of undetected error was applied within the verification and validation of the safety of electronic interlocking systems which are used in the operation of the railways of The Slovak Republic.

The future works in this area can be orientated to realization of model modification on the assumption of open transmission system.

Acknowledgment

The paper is supported by the scientific grant agency No. VEGA-1/0040/08, Mathematical and graphical modelling of safety attributes of safety — critical control system.

References

[1] MALM, T.—HÉRARD, J.—BØEGH, J.—KIVIPURO, M.: Validation of SafetyRelated Wireless Machine Control Systems, TR605, Approved 2007-03, Nordic Innovation Centre, Oslo, Norway.

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

[3] MAHALIK, N. P.: Fieldbus Technology, Industrial Network Standard for Real-Time Distributed Control, SpringerVerlag, Berlin, 2003.

[4] THOMESSE, J. P.: Fieldbus Technology in Industrial Automation, Proceedings of the IEEE **93** No. 6 (June 2005), 1073–1101.

[5] KANAMARU, H.—HARIMA, T.: Safety Field Network Technology and its Implementation, SICE Annual Conference, Tokyo, August 2008, pp. 1487–1490.

[6] FRANEKOVÁ, M. *et al*: Safety Communications of Industrial Networks, EDIS, Žilina, Slovakia, 2007. (in Slovak)

[7] IEC 61784-3: Digital Data Communications for Measurement and Control. Part 3: Profiles for Functional Safety Communications in Industrial Networks, 2007.

[8] VASKO, D. A.: DeviceNet Safety: Safety Networking for Today and Beyond. PUB 00110R0. ODVA 2005.

[9] Evaluation report No: PK55299T, Profibus Specifications, PROFIsafe - Profiles for Failsafe Technology, TÜV Product Service GmbH, München, May 2007.

[10] KARSTEN, M. G.: Solution for Safety Technology using Interbus Safety, Control Engineering Europe. Covering control, Instrumentation and Automation System (June 2002).

[11] DZUNG, D.—NAEDELE, M.—Von HOFF, T. P.—CREVATIN, M.: Security for Industrial Communication System, Proceeding of the IEEE **93** No. 6 (June 2005).

[12] IEC 61784-4: Digital Data Communications for Measurement and Control. Part 4: Profiles for Secure Communications in Industrial Network, 2007.

[13] EN 501 59-1: Railway Applications: Communication, Signalling, and Processing Systems. Part 1: Safety-Related Communication in Closed Transmission Systems, 2001.

[14] EN 501 59-2: Railway Applications: Communication, Signalling, and Processing Systems. Part 2: Safety-Related Communication in Open Transmission Systems.

[15] SARASWAT, S.—YADAVA, G. S.: An Overview on Reliability, Availability, Maintainability and Supportability (RAMS) Engineering, International J. of Quality & Reliability Management **25** No. 3 (2008), Emerald Group Publishing Limited 0265-671X.

[16] CAUFFRIEZ, L.—BERNARD, V.—RENAUX, D.: A New Formalism for Designing and Specifying RAMS Parameters for Complex Distributed Control Systems: The Safe-SADT Formalism, IEEE Transaction on Reliability **55** No. 3 (Sep 2006), 397–410.

[17] MÜHLHAUSE, M.—DIEDRICH, C.—RIEDL, M.—SCHMIDT, D.: Formalized Specification of a Test Tool for Safety Related Communication, Emerging Technologies and.

[18] RÁSTOČNÝ, K.: Risk Analysis of Safety-Critical Control Systems, Advances in Electrical and Electronic Engineering No. 1-2 (2008), 277–230.

[19] CLARK, C.—CAIN, J. B.: Error-Correcting Codes for Digital Communications, Plenum Press, New York, 1988.

Received 12 March 2010

Mária Franeková (1961) received her Associated Professor in 2004 in the filed of Information and Safety-related Systems. Her research interests include safety data transmission, analysis of safety communication on the base of coding and cryptography tools within safety related applications.

Karol Rástočný (1958) received his Professorship 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.