Computing and Informatics, Vol. 33, 2014, 343–368

QUANTITATIVE ASSESSMENT OF SAFETY INTEGRITY LEVEL OF MESSAGE TRANSMISSION BETWEEN SAFETY-RELATED EQUIPMENT

Karol Rástočný, Mária Franeková

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

Iveta Zolotová

Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9
042 00 Košice, Slovakia
e-mail: iveta.zolotova@tuke.sk

Karol Rástočný, Jr.

Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova
842 16 Bratislava, Slovakia
e-mail: karol.rastocny@stuba.sk

Abstract. This paper describes and analyses the possibilities of a quantitative assessment of message transmission between safety-related equipment for control and communication systems with a guarantee of a higher safety integrity level (SIL). The theoretical methods and standards recommended for industrial safety-related con-

trol, information and communication systems with SIL3 are described. The main part of the contribution covers theoretical methods and practical procedures used within a safety analysis of safety-related message transmission with the requirement of SIL4 for the area of railway interlocking systems. The theoretical analysis of these methods is compared with the knowledge and experience the authors gained within several safety verifications of such systems in practice in Slovakia as well as abroad. Also, based on a case study in the mentioned application area, the authors proposed their own quantitative mathematical model for assessing the safety integrity level of message transmission within a closed transmission system with the failure tree analysis (FTA) and Markov's analysis (MA). The designed model, which evaluates the effect of electromagnetic interferences (EMI) and random hardware failures of a safety-related communication system (SRComS) to its safety, was realised and verified. The verification in available conditions confirmed the contribution of the model to the process of objectification of the safety assessment of message transmission via SRComS.

Keywords: Safety-related systems and equipment, interlocking systems, transmission of safety-related messages, safety integrity level, safety assessment, safety code

Mathematics Subject Classification 2010: 60J27 (Continuous-time Markov processes on discrete state spaces)

1 INTRODUCTION

During the process of developing a safety-related control system (SRCS), the fact that the realisation of required safety functions is connected with message transmission inside the SRCS and with message transmission between the considered control system and co-operating systems or equipment must not be forgotten. Because of this, the safety of the applied communications, the so-called communication safety, which might affect RAMS (Reliability, Availability, Maintainability, Safety) parameters significantly, has to be considered. In general, communication safety may be characterised as the ability of a communication to assure:

- confidentiality of transmitted messages (only authorised objects/subjects have access to the transmitted messages);
- integrity of transmitted messages (the transmitted messages can only be modified by authorised subjects and the origin of each message is verifiable);
- availability of transmitted messages (the transmitted messages are accessible by authorised objects/subjects for a certain period of time).

The Commercial Off-The-Shelf (COTS) communication technologies are not essentially suitable (without additional technical safety measures) for transmission of safety-related messages even though they include detection and correction methods

for transmission assurance and other protective mechanisms, too. In terms of transmission safety, such systems are described as non-safety-related. What types of additional technical measures are needed to be applied to a COTS communication system depends on the risk analysis results (analysis of attacks and their effects) and the effect of the communication system to the required safety integrity level (SIL) of the SRCS which comprises the communication system.

Nowadays, the number of vendors of safety-related communication technologies who guarantee not only standard communication, but also communication among safety-related equipment in compliance with IEC 61508 [1] is increasing. For industrial communication systems, the standard IEC 61784-3 [2], which defines the procedure of designing safety profiles with regards to preserving functional safety for families of industrial networks used within measure and control systems on the technological control level [3], is valid.

It is a fact that safety is becoming an inseparable part of not only the lowest control levels, but also of the SCADA/HMI level [4, 5], and of the information level of a distributed system control [6, 7], where the interconnection of safety and security profiles as defined in IEC 61784-4 is concerned [8]. Over the last few years, the additional safety profiles CPF (Communication Profile Families) CPF1 (Safety Foundation Fieldbus), CPF2 (CIP Safety), CPF3 (ProfiSafe) and CPF16 (Open Safety) have been certified for SIL3 applications.

In practice (e.g. in railway transport), applications of SRCSs which require that message transmission is realised with SIL4 [9] can be seen. Since communication systems with such a property are not standardly available on the market, vendors of SRCSs with SIL4 incline to the development of their own safety-related communication systems if necessary. For the area of railway applications, the norm EN50159 [10], which includes general recommendations on how to proceed in the development of a SRComS, is valid. It is necessary that a trustworthy demonstration of the required safety facilities of a SRComS is included in its development. In the informative part of the norm [10], basic information on how to demonstrate the safety facilities of a communication system is introduced. However, this information is not always unambiguous, which creates space for a subjective approach to the safety assessment.

2 GOALS OF THE CONTRIBUTION

In this paper, the authors set their goal to be a comparison of the procedures used for a safety assessment of a SRComS presented in the informative part of the norm EN 50159 to their own method, based on which the model of a safety integrity level assessment of message transmission in a closed transmission system was realised. The authors' method is based on theoretical procedures for identification and quantitative evaluation of the factors effecting the transmission safety of data, as well as on a theoretical calculation of the probability of the occurrence of an undetected corruption within a corrupted message. The practical calculations were

realised for a specific SRComS used in railway applications and the obtained results were confronted with the results produced by the procedures mentioned in the norm EN50159. Achieving the main goal required the following particular tasks, which will be analysed and described in the following chapters, to be dealt with:

- Identification of the risk factors and the mechanisms of their effect to the safety of a considered SRComS.
- Quantitative evaluation of the parameters of the risk factors.
- Identification of protective measures and mechanisms of their effect to the safety of a considered SRComS.
- Quantitative evaluation of the parameters of the protective measures.
- A realisation of a state model describing the transition from a reliable functional state to a dangerous state.
- A verification (by a partial verification in available, real conditions) of the realised model.

3 MODEL OF A SAFETY-RELATED COMMUNICATION SYSTEM

The considerations present in this paper are linked to the simple model of a SRComS shown in Figure 1. The SRComS consists of safety- related equipment (SRE1) and (SRE2), interfaces (INT) located on the boundary between SRE and a non-safety-related transmission system, and the non-safety-related transmission system itself. The equipments SRE1 and SRE2 contain an additional safety layer which safeguards the safety-related functions of transmission and also contains a safety coder (SC) and a safety decoder (SD). The safety layer is an extension of the transmission system layers (transmission sender/transmission receiver). On the level of the link layer, a transmission coder (TC) and a transmission decoder (TD) are components of the safety layer. A safety-related message generated from the safety message source (part SRE1) is transferred across a communication channel (transmission media) and received in the safety message sink (part SRE2), whose task is to detect corrupted messages and to react appropriately to failures in transmission. The transferred messages are (or may be) affected by EMI (caused by noises, interferences or the fading effect) and failures of the SRComS, too.

During a transmission of safety-related messages, the following type of communication errors are expected:

- message repetition;
- message deletion;
- message insertion;
- re-sequences of a message;
- delay of a message;
- masquerade of a message.

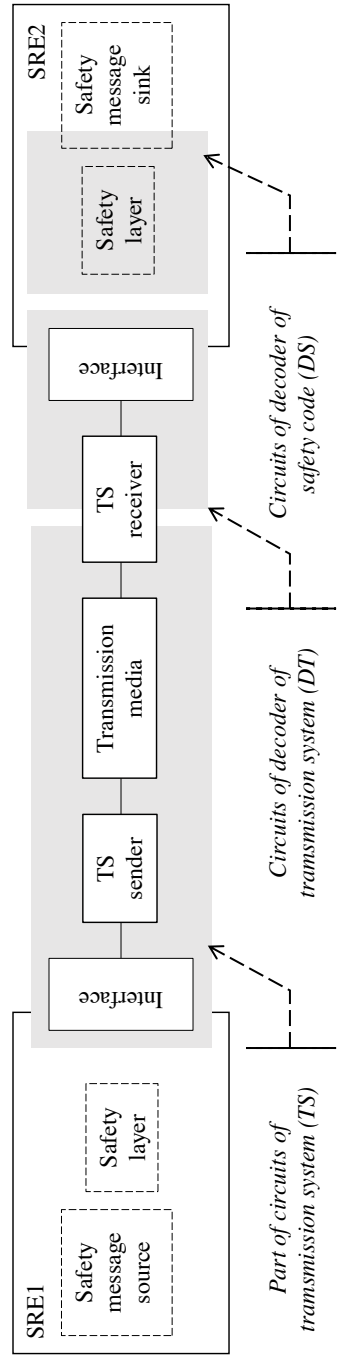

Figure 1. Model of a SRComS with a safety layer

At the receiver's side, the correctness of a transmitted message is evaluated on two levels. The correctness of a transmitted message is standardly evaluated by the decoder of the transmission code in a non-safety-related transmission system on the first level, and by the decoder of the safety code on the second level. The decoder of the safety code is a part of SRE2 and is realised on multiple channels [11] (in Figure 2, a two-channel decoding via decoders of the safety codes DS_R and DS_L is shown). Consequently, if the decoder of the transmission code interprets an incoming message as correct, the message from the decoder of the transmission code (still secured by the safety code) is sent to both the decoder DS_R and the decoder DS_L. These two decoders independently evaluate the correctness of the incoming message (and the correctness of application data too). The received message is considered to be correct if both of the decoders produce identical results. The comparison of the results from the decoders is a part of the safety mechanisms within SRE2. If both of the decoders produce the result that the received message may be considered to be correct, the received data is provided for further processing in each channel; if one of the decoders evaluates the received message as incorrect, the message is rejected and a safety procedure is called. Such a solution enables the required safety level in the event of random hardware failures of the decoder (decoders) of the safety code to be achieved.

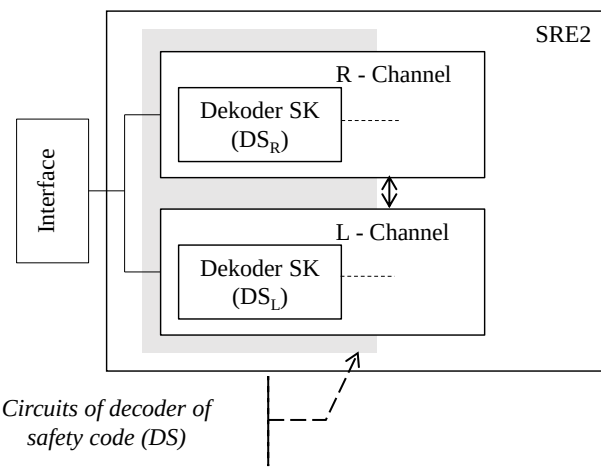

Figure 2. Block scheme of a SRComS – part located in SRE2

4 RISK FACTORS AFFECTING THE SAFETY INTEGRITY OF A SAFETY-RELATED COMMUNICATION SYSTEM

Failures of safety-related communication systems belong to the most important risk factors which affect the safety integrity of a system. Such failures can lead to a loss

of operational capability and can result in a health risk, life danger, environmental hazard or cause large substantial damage.

Detailed specifications of these failures and their interpretations are introduced e.g. in [12]. The causes of a corruption in a transmitted message can be SRComS (its failures). In this case, mainly the following has to be considered:

- systematic failures, which may be caused primarily by failures in the SRComS development, or by failures caused by insufficient maintenance of the SRComS;
- HW failures of the SRComS;
- the operational environment; in this case, mainly electromagnetic influences (EMI: noise, interference, fading) need to be considered.

From a quantitative evaluation of the safety integrity from SRComS point of view, it is necessary to be concerned only with failures that can be evaluated quantitatively, namely the following:

- random hardware failures;
- failures caused by the operational environment.

The effect of systematic failures on the safety integrity of a SRComS cannot be evaluated quantitatively because mathematical modelling of the occurrence of systematic failures is very problematic since it requires to know the type of the distribution of the systematic failures and the parameters of this distribution [13]. It can only be evaluated qualitatively, mainly by tests and demonstrations of suitable measures applied to prevent failures and errors on both the hardware and the software level.

4.1 Random Failures of SRComS Hardware

Since a SRComS is an electronic system, it is justifiable to assume that the occurrence of random failures of a SRComS can be described by the exponential probability distribution. From a safety assessment point of view, a SRComS may be decomposed to the following parts (see Figure 1):

- The part of a transmitter that is a component of SRE1. This is a non-safety-related part of a SRComS because SRE1 is fully responsible for the correctness of generated messages. SRE1 is designed according to the procedures in compliance with SIL4 as defined in [10].
- The part of the circuits of the transmission system, consisting of the interface between SRE1, the transmitter of a non-safety-related transmission system, the hardware of the communication channel and the receiver of a non-safety-related transmission system, and of a part of the circuits of the transmission code decoder. This part basically covers the parts of a non-safety-related transmission system whose failures result in corrupting a transmitted message (analogy

to corrupting a transmitted message by EMI). The failure rate of this part of a SRComS is later referred to as R_{TS}.

- The circuits of the transmission code decoder – the part of the decoder's circuits of the transmission code which take part in decoding the received message and in transmitting the decoded SRE2 message (without the redundant part of the transmission code). A failure of these circuits may cause an occurrence of a corrupted message at the entry of SRE2. The corruption may be caused either by the transmission of the message or by the processing within the circuits of the transmission code decoder. The failure rate of this part of a SRComS is later referred to as R_{DT}.

- The circuits of the safety code decoder – part of the circuits within SRE2 (see Figure 2). SRE2 is designed according to the procedures corresponding with SIL4, and its circuits (including the circuits of the safety code decoder) comply with the safety assessment as defined in [10]. In this case, the dangerous failure rate of a decoder of a safety code can be directly considered and expressed by the equation:

$$R_{DS}^{H} = 2\, R_{DSL} \cdot R_{DSR} \cdot T_S, \tag{1}$$

where R_{DS}^{H} is the dangerous failure rate of the decoder of the safety code, R_{DSL} is the failure rate of the decoder of the safety code in the left channel, R_{DSR} is the failure rate of the decoder of the safety code in the right channel and T_S is the time of the tolerance of receiving the corrupted message by the safety-related part of a transmission system.

4.2 Failures Caused by the Effect of the Operational Environment

Since safety-related messages are transmitted over a real communication channel, it is necessary to expect the effect of the noise or interference pattern to transmitted messages, which has significant impact to the frequency of corrupted messages. Electromagnetic interference is a result of a wide range of various influences which are indescribable deterministically. Therefore the models of communication channels are also based on probabilistic characteristics. For the safety analysis of communications based on binary transmission, the norm [10] recommends using the model of a binary symmetric channel (BSC) for the bit error rate of a communication channel from the interval $\langle 0; 0.5\rangle$. This model assumes that the errors occurred during binary transmissions are random and independent. If the BSC model is used for transmission of binary messages with the bit error rate p_e, the probability of a message of the length n containing exactly j errors is given by the equation:

$$p_j = p_e^j (1 - p_e)^{n-j}. \tag{2}$$

5 SAFETY MECHANISMS AND THEIR PARAMETERS

The protection against undesirable consequences of EMI is using a safety code from the group of channel codes. Because of the possibility of the failure masking effect, utilisation of the correction abilities of channel codes in a SRComS is not recommended for railway applications at all. It is recommended to apply detection block (n, k) codes or correcting codes with a modified decoding algorithm, which is finished by the process of message detection (n is length of code word, k is length of the information part of code word). Simple random errors in a SRComS are usually detected within a non-safety-related transmission system with a transmission code. If an error is detected by the safety code, there are usually more corrupted bits in a safety-related message.

5.1 Transmission Code

Even though only safety mechanisms located within the safety layer are relevantly important from a safety point of view, the check mechanisms used in the standard layer of non-safety-related transmission are significant for increasing the safety of a SRComS. The transmission code is part of these mechanisms too. In COTS technology, the transmission code often uses cyclic code working on the principle of CRC (Cyclic Redundancy Check). Especially when using cyclic code, the selection of the generator polynomial required special attention. The selection of the generator polynomial of cyclic code should be effected by the error patterns that occur in the considered connection most frequently. In safety-related applications, the independence of a transmission and a safety code is required, which for a safety code based on CRC means the inability to use commonly standardised types of generator polynomials within the COTS systems. It is also necessary to note that the most commonly used detection code in practice does not detect a negation of a message nor corrupted messages with all bits having the value of logical 1 or all bits having the value of logical 0.

5.2 Safety Code

A safety code with a broad detection coverage and a quick detecting algorithm is fundamental for safety-related applications. The requirements for the selection of parameters of a safety code depend on the required safety characteristics of a SRComS (especially on the rate or the probability of an undetected error). If both safety-related and non-safety-related messages are transmitted via a SRComS, then they have to have different structures.

The following practical problems need to be solved during the selection of the parameters of a safety code:

- Length of the code – it is usually required that a single code can be used for messages with different lengths, while most of the theoretical information on

codes is connected with specific recommended construction lengths of codes, which is not generally observed in practice (shortened or extended codes are used). It is necessary to note that codes of different lengths have different safety characteristic.

- Redundancy of a code – the dominant opinion is that the more the redundant bits, the higher the safety. The requirement for a higher number of redundant bits is not always justifiable (e.g. CRC-64 – ISO with 64 redundant bits has worse detection properties than a well-chosen code with 32 redundant bits) [14, 15].
- Minimum Hamming distance – $d_{\min}$ is bound to the requirement that the code needs to detect errors with a certain maximum length most of the codes detect simple (independent errors) as well as j-multiple errors (dependent errors – bursts). In practical application, the $d_{\min}$ of a code is not always known. If it is, then it is valid for a code of a given construction length. If the length is shortened, $d_{\min}$ can sharply decrease. To calculate $d_{\min}$, Gilbert-Varshamov bound [16] can be used.
- Detection of selected error patterns – some types of errors can occur frequently and therefore it is required of a code to detect them (e.g. repeated bursts of a certain length, all logical 1 bits, all logical 0 bits, negation of a message). However, the probability of the occurrence of error patterns is usually unknown.

5.3 Determination of the Probability of an Undetected Error

According to [10], the determination of the probability of an undetected error of a code p_U in a model of a BSC is obligatory. It is necessary to prove that the required value of p_U is valid for every length of safety-related messages. The probability of an undetected error p_U with applying linear binary block (n, k) codes expresses the event that the message (code word of length n) was sending and another message is receiving. It must be noted that the majority of methods of calculating p_U is connected with a certain class or group of codes (e.g. Hamming codes, Reed-Solomon codes) for which a quantitative analysis of a failure of a decoder is valid only for very simplified conditions, which is not entirely usable for practical applications.

To calculate p_U, the basic characteristic of the communication channel, the bit error rate p_e must be known. In practice, in most cases it is not possible to find the value of p_e by measuring and the statistical values of p_e known for certain communication channels have to be relied on. However, these values do not always characterise a specific application.

For all groups of linear binary block codes in a BSC model, the probability of an undetected error can be expressed in the form

$$p_U = \sum_{i=\| \frac{d_{\min}+1}{2} \|}^{n} A_i^n \, p_e (1 - p_e)^{n-i}, \tag{3}$$

where $d_{\min}$ is the minimal Hamming distance of the code, A_i^n is the weighted distribution of the binary (n, k) code, p_e is the bit error rate of the communication channel, i is the integral part of $\frac{d_{\min}+1}{2}$ and n is length of code word.

In order to calculate p_U according to (3), it is necessary to know the $d_{\min}$ of a code, even though in some sources, the bottom bound in the Equation (3) is $i = 1$. The vector of the weighted distribution of the binary (n, k) code needs to be calculated, too. For calculation of the weighted distribution, it is necessary to know the weighted polynomial $P_w(x, n, A_i^n)$ which describes the weight of code words according to:

$$P_w(x, n, A_i^n) = \sum_{i=1}^{n} A_i^n \, x^i. \tag{4}$$

Nowadays, the following approaches to calculating the weighted distribution of binary A_i^n codes (n, k) are known:

- A direct calculation of the weighting distribution – it is needed to gradually generate all code words with a generator matrix or a generator polynomial. However, this approach is time-consuming for long code words and therefore unusable for real-time safety-related message transmission.
- The determination of the weighted distribution with the MacWilliams identity – based on the fact that every linear binary (n, k) code – can be converted to a dual code for which there is the Equation (5) between $P_w(x, n, A_i^n)$ of the primary binary code and $P_w(x, n, B_i^n)$ of the dual code:

$$P_w(x, n, B_i^n) = \frac{1}{2^k}(1 + x)^n \, P_w\left(\frac{1 - x}{1 + x}, n, A_i^n\right). \tag{5}$$

  The advantage of this calculation method is that the dual code has much fewer code words than the primary code and the calculation of the weighted distribution is faster and easier. It should not be forgotten that for some linear binary (or character) block codes, their weighting functions are known but are only applicable for the constructive length of the codes n, which is not usually observed in practical applications. As an example, the weighted function of perfect Hamming codes [16] is provided:

$$P_w(x, n, A_i^n) = \frac{1}{n + 1}\left[(1 + x)^n + n(1 + x)^{(n-1)/2} \cdot (1 - x)^{(n+1)/2}\right]. \tag{6}$$

  For cyclic codes, working on the CRC principle can be used within the weighting distribution of the dual code procedures, which are described e.g. in [17] for the primitive generation polynomial $g(x)$ or for the polynomial $g(x)$, which is the product of the several irreducible polynomials. Such an approach is described as a method of two LFSR (Linear Feedback Shift Register) [18].

  The above approach for calculating the probability of an undetected error can be simplified, if A_i^n in Equation (3) is approximated according to Equation (7),

which on the one hand brings larger deviation into the safety analysis, which can be caused by an unnecessary increase of the required redundant elements during the selection of the safety code, but on the other hand, the calculation is simplified:

$$A_i^n \cong \frac{1}{2^{n-k}} \binom{n}{i}. \tag{7}$$

Then, Equation (3) can be modified to:

$$p_U \cong \frac{1}{2^{n-k}} \sum_{i=1}^{n} \binom{n}{i} p_e^i (1-p_e)^{n-i}. \tag{8}$$

If the product $n \cdot p_e$ is much smaller than $(n \cdot p_e \ll 1)$, the sum in Equation (8) can be approximated as the first member of the sum:

$$p_U \cong \frac{1}{2^{n-k}} \binom{n}{d_{\min}} p_e^{d_{\min}} (1-p_e)^{n-d_{\min}}. \tag{9}$$

The calculation of a rough estimate of the probability of an undetected error is obtained with the assumption of the value of the bit error rate $p_e = 1/2$ as (10), where r is a redundant part of the code word.

$$p_U = \sum_{i=1}^{n} A_i^n \frac{1}{2^i} \left(\frac{1}{2}\right)^{n-i} = \left(\frac{1}{2}\right)^n \cdot 2^{k-1} = 2^{n-k} = 2^{-r}. \tag{10}$$

However, this is described as the most pessimistic estimation of the probability of an undetected message. This upper bound is not dependent on neither the weighted distribution nor the length of a code word n.

It must be noted that the value 2^{-r} does not need to be a maximum for different values of p_e. Therefore it is required to prove that on the interval $\langle 0; 0{,}5\rangle$ for the probability of an undetected error, the following holds: $p_U < 2^{-(n-k)}$.

Then according to [10], the safety code called "good code" is used.

Nowadays, new fast and effective methods for the calculation of the weighted distribution and the probability of an undetected error in a BSC model on the interval $\langle 0; 0{,}5\rangle$ are searched for [18].

5.4 Determination of the Failure Rate Caused by the Effect of EMI

Undetected errors caused by a corruption of a message integrity due to EMI during transmission occur in the case of a failure of both channel coders: the transmission coder (in a non-safety-related transmission system) and the safety coder (in the safety layer). If we know the probabilities of an undetected error of the transmission and safety codes, then the failure rate caused by the EMI effect R_{EMI}^H can be expressed as:

$$R_{EMI}^{H} = p_{UT} \cdot p_{US} \cdot f_{EMI}, \tag{11}$$

where p_{UT} is the probability of an undetected error of the transmission code, p_{US} is the probability of an undetected error of the safety code and f_{EMI} is the frequency of occurrences of corrupted messages caused by EMI per hour.

If a transmission system does not contain a channel coder/decoder of a transmission code, then $p_{UT} = 1$.

For the calculation of the probability of an undetected error of the transmission and the safety codes, some of the formulas defined by Equations (3), (8), (9) or (10) can be used. It is necessary to note that for the probability of an undetected error of the safety code, according to [10], it is necessary to verify that the function p_{US} is monotonous on the interval $\langle 0; 0,5 \rangle$, which involves a complex computation problem for long messages [19]. If function p_{US} satisfies the requirement, the safety code has the "proper code" attribute. Proper codes are always "good", but good codes are not always proper [10].

The frequency of the occurrence of an incorrect message per hour can be easily determined for cyclic message transmission. In other cases, it is necessary to implement a counter of corrupted messages, or the value of f_{EMI} is estimated, or the worst case is used (i.e. all generated messages from the source are corrupted).

In practice, in railway interlocking systems if a corrupted message is received, the receiver of SRE has to react by going to a predefined safe state (message is regarded as invalid and is ignored). In order to meet the requirement of availability of the systems, there is a set limit of corrupted messages within all received messages per a defined time interval and only having reached the limit, certain technical measures will take place to guarantee the required safety level of transmitted messages (e.g. a decrease of the transmission rate or a permanent interruption of message transmission). The specified calculation of the tolerance value of corrupted messages per a certain time interval depends on the error rate of the used communication channel. Within the safety assessments, the probability of l consecutive corrupted messages can be determined by Bernoulli's law (Equation (12)), where the number of observed independent results of an event v denotes the number of generated safety-related messages from a safety message source and p_m is the probability of one corrupted m-bit message:

$$p_v(l) = \frac{v!}{l!(v-l)!} \cdot p_m^l \cdot (1 - p_m)^{v-l}. \tag{12}$$

6 REALISATION OF MODELS OF SAFETY-RELATED COMMUNICATION SYSTEM

Within the safety analysis of a SRComS (illustrated in Figure 1), two stages were important: creating the model and substituting real data to the model. It was necessary to create a model that could simulate the effect of several simultaneous factors effecting the safety of a SRComS. Since the occurrence of corrupted messages

can be considered to be a Markov process, the authors of this paper decided to use a Markov model based on a CTMC (Continuous Time Markov Chain) for modelling the safety of a SRComS (the probability or the failure rate of an undetected corrupted message). Markov chain models are efficient tools for representing stochastic discrete event processes with wide applications in decision and control. A novel approach to fuzzy-Petri-net reasoning generated solution to initial or another state in Markov-chain models is proposed e.g. in [20].

A very important step of creating a final version of the model was identification of hazards (events) that can cause a failure of detecting a corruption of a message. The identification of these hazards was realised with a fault tree model.

In order to create a model that recognises the effects of individual factors effecting the safety of a SRComS, and a concrete evaluation of the model's transitions, it is necessary to clearly know the properties of the SRComS and its behaviour in various operational situations. This means a model that could be used for different SRComSs cannot be created. However, it is a fact that essentially the basics of models are always equivalent.

Since a SRComS has to work in all operational situations and guarantee the required SIL, while modelling the monitored safety parameters, it is necessary to suppose the worst situations that can occur in operation. This means that with a SRComS, it must be assumed that all transmitted messages are corrupted because of either EMI or a failure of its HW. Besides, it is needed to count with the failure of individual safety measures of a SRComS.

6.1 Realisation of the Fault Tree Model of SRComS

A fault tree model of the SRComS (Figure 3) that illustrates which basic events or combinations thereof can create an undesirable (top) event being an undetected corruption message of SRComS (Figure 1) was made. The term "undetected corrupted message" denotes the situation when a transmitted message is considered to be correct (without errors) even though it became corrupted (transmission data was changed) during its transmission. From the point of a quantitative assessment of safety integrity, it is required to calculate the probability of the occurrence of an undesirable (top) event. Since basic events must be considered to be independent, a simple logic function (Boolean function) can describe the relations between a top event and basic events. If the probabilities of the occurrences of basic events are known, then this is regarded as a simple matter from a mathematical point of view.

Even though the fault tree in Figure 3 is clear and very easy to design, it is not crucially important from the point of view of quantitative assessment of the safety integrity of a SRComS, because it is unable to consider changes of the operational state of a SRComS that occurred as a consequence of safety measures (for example a change of the transmission rate, a repetition of a message, etc.).

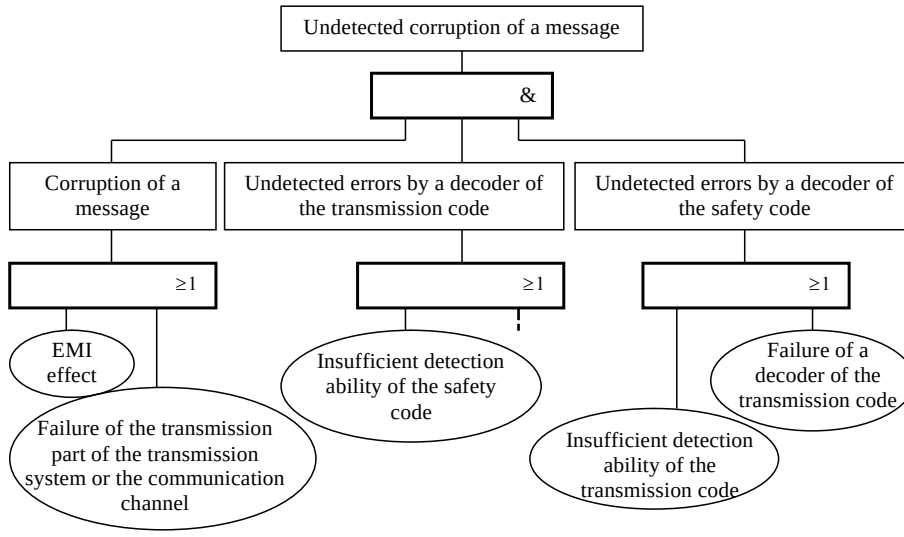

Figure 3. Fault tree of a SRComS

6.2 Safety Assessment of SRComS Using Realised Markov Models

A Markov model is more flexible than a fault tree and is able to count with the effect of several factors to the safety integrity of a SRComS. In Figure 4, a CTMC is illustrated. This chain describes the transitions of the SRComS (presented in Figure 1) from a functional, safe state (state **1**) to a dangerous state (state **8**). In addition to state **8**, the diagram has one more absorption state (state **7**) that is not primarily dangerous for a controlled process. A SRComS gets into this state if the safety mechanisms decide that continuing data transmission is inadequate from a safety point of view, and the data transmission is needed to be interrupted indefinitely (only operator can restart the transmission again). To make Figure 4 more readable, the transitions into state **8** (transitions done by the safety measures of the SRComS) are illustrated by dashed lines.

Each symbol used in Figure 4 is defined in Table 1. The characteristics of each state and transition in Figure 4 is described in Tables 2 and 3.

The diagram in Figure 4 can be described by a set of differential equations and a vector of the initial probabilities (13).

To solve the set of differential equations defined by Equations (13) and (14), the SW tool Wolfram Mathematica was used.

Since according to [10] the SIL of a SRComS can be evaluated as the rate of undetected a corrupted message, it is suitable to know overall failure rate of the SRComS transmission from state **1** to state **8** in Figure 4.

Symbol	Meaning
R_{TS}	HW failure rate of the transmission system part (the transmitter, the communication channel and parts of the receiver).
R_{DT}	HW failure rate of the decoder of the transmission code.
R_{DS}	HW failure rate of the decoder of the safety code.
p_{UT}	Probability of an undetected error of the transmission code.
p_{US}	Probability of an undetected error of the safety code.
f	Frequency of generated messages by the transmitter.
f_{EMI}	Frequency of corrupted messages caused by EMI.
f_{HTP}	Frequency of corrupted messages caused by HW failures of the transmitter part of the transmission system (the transmitter, the communication channel and parts of the receiver).
f_W	Frequency of corrupted messages without distinguishing the source of the corruption.
T_T	Tolerance time of receiving corrupted messages by the non-trusted part of the transmission system.
T_S	Tolerance time of receiving corrupted messages by the trusted part of the transmission system.
δ_T	Intensity of the transition to the permanently safe state caused by the mechanism for checking the number of received (detected) corrupted messages by the decoder of the transmission code.
δ_S	Intensity of the transition to the permanently safe state caused by the mechanism for checking the number of received (detected) corrupted messages by the decoder the safety code.

Table 1. Meaning of symbols

State	Description
1	The transmission system is functional; EMI corrupted transmitted messages.
2	A transmission system state, in which the transmitter part of the transmission system or a part of the communication channel have a failure.
3	A transmission system state, in which the decoder of the transmission code has a failure.
4	A transmission system state, in which the decoder of the safety code has a failure.
5	A transmission system state, in which the transmitter part of the transmission system or a part of the communication channel and the decoder of the transmission code have a failure.
6	A transmission system state, in which the transmitter part of the transmission system or a part of the communication channel and the decoder of the safety code have a failure.
7	Permanent interruption of transmission caused by safety mechanisms. A safe state.
8	A dangerous state, in which a corrupted message was undetected.

Table 2. Description of the states in Figure 4

Transition	Description	The meaning of symbols
$1 \to 2$ $3 \to 5$ $4 \to 6$	The transition is realised as a consequence of a HW failure of the transmitter part of the transmission system or a part of the communication channel.	R_{TS}
$1 \to 3$ $2 \to 5$	The transition is realised as a consequence of a HW failure of the decoder of the transmission code.	R_{DT}
$1 \to 4$ $2 \to 6$	The transition is realised as a consequence of a HW failure of the decoder of the safety code.	R_{DS}
$1 \to 8$	The transition is realised as a consequence of a message being corrupted by EMI and insufficient detection abilities of the transmission and safety codes.	$f_{EMI} \cdot p_{UT} \cdot p_{US}$
$1 \to 7$ $2 \to 7$	The transition is realised as a consequence of the operation of mechanisms for checking the number of detected corrupted messages by a decoder of the transmission code or the safety code.	$\delta_T + \delta_S$
$2 \to 8$	The transition is realised if a transmitted message is corrupted (as a consequence of the HW failure of the transmitter part of the transmission system or a part of the communication channel) and the transmission and safe codes have insufficient detection abilities.	$f_W \cdot p_{UT} \cdot p_{US}$
$3 \to 7$ $5 \to 7$	The transition is realised as a consequence of the operation of the mechanisms for checking the number of detected corrupted messages by the decoder of the safety code.	δ_S
$4 \to 7$ $6 \to 2$	The transition is realised in consequence of the operation of the mechanisms for checking the number of detected corrupted messages by the decoder of the transmission code.	δ_T
$3 \to 8$ $5 \to 8$	The transition is realised if the transmitted message is corrupted (by a HW failure) and the safe code has insufficient detection ability, or the decoder of the safety code has a failure.	$R_{DS} + f_W \cdot p_{US}$
$4 \to 8$ $6 \to 8$	The transition is realised if the transmitted message is corrupted (by a HW failure) and the safe code has insufficient detection ability, or the decoder of the transmission code has a failure.	$R_{DT} + f_W \cdot p_{UT}$

Table 3. Transitions in Figure 4

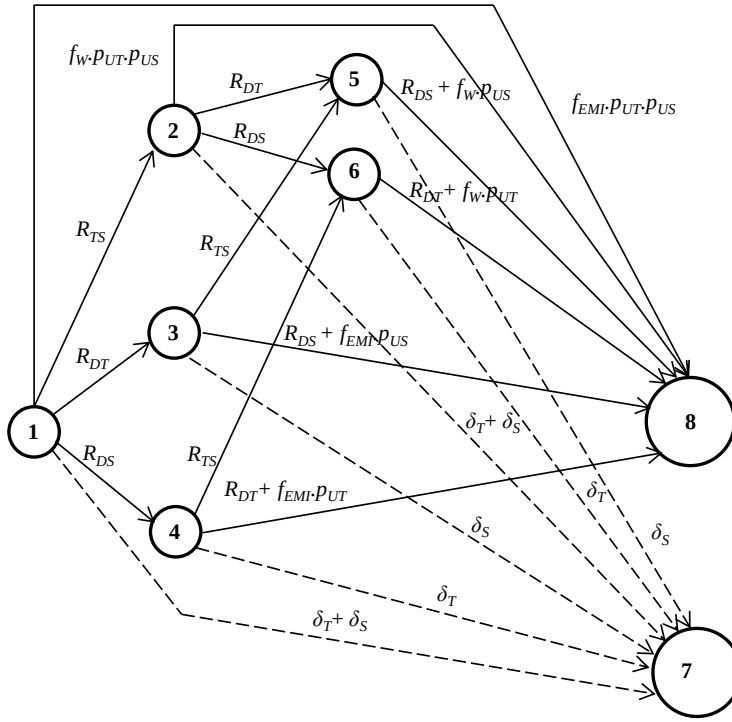

Figure 4. Markov model of a SRComS

$$
\begin{aligned}
\frac{\mathrm{d}p_1(t)}{\mathrm{d}t} &= -(R_{TS} + R_{DT} + R_{DS} + f_{EMI} \cdot p_{UT} \cdot p_{US} + \delta_T + \delta_S) \cdot p_1(t);\\
\frac{\mathrm{d}p_2(t)}{\mathrm{d}t} &= R_{TS} \cdot p_1(t) - (R_{DT} + R_{DS} + f_w \cdot p_{UT} \cdot p_{US} + \delta_T + \delta_S) \cdot p_2(t);\\
\frac{\mathrm{d}p_3(t)}{\mathrm{d}t} &= R_{DT} \cdot p_1(t) - (R_{TS} + R_{DS} + f_{EMI} \cdot p_{US} + \delta_S) \cdot p_3(t);\\
\frac{\mathrm{d}p_4(t)}{\mathrm{d}t} &= R_{DS} \cdot p_1(t) - (R_{TS} + R_{DT} + f_{EMI} \cdot p_{UT} + \delta_T) \cdot p_4(t);\\
\frac{\mathrm{d}p_5(t)}{\mathrm{d}t} &= R_{DT} \cdot p_2(t) + R_{TS} \cdot p_3(t) - (R_{DS} + f_w \cdot p_{US} + \delta_S) \cdot p_5(t);\\
\frac{\mathrm{d}p_6(t)}{\mathrm{d}t} &= R_{DS} \cdot p_2(t) + R_{TS} \cdot p_4(t) - (R_{DT} + f_w \cdot p_{UT} + \delta_T) \cdot p_6(t);\\
\frac{\mathrm{d}p_7(t)}{\mathrm{d}t} &= (\delta_T + \delta_S)[p_1(t) + p_2(t)] + \delta_S \cdot [p_3(t) + p_5(t)] + \delta_T \cdot [p_4(t) + p_6(t)];\\
\frac{\mathrm{d}p_8(t)}{\mathrm{d}t} &= p_{UT} \cdot p_{US} \cdot [f_{EMI} \cdot p_1(t) + f_w \cdot p_2(t)] + (R_{DS} + f_{EMI} \cdot p_{US}) \cdot p_3(t)\\
&\quad + (R_{DT} + f_{EMI} \cdot p_{UT}) \cdot p_4(t) + (R_{DS} + f_w \cdot p_{US}) \cdot p_5(t)\\
&\quad + (R_{DT} + f_w \cdot p_{UT}) \cdot p_6(t).
\end{aligned}
\tag{13}
$$

$$\vec{p}(0) = [p_1(0), p_2(0), p_3(0), p_4(0), p_5(0), p_6(0), p_7(0), p_8(0)] = [1, 0, 0, 0, 0, 0, 0, 0]. \tag{14}$$

According to [21] the rate of undetected corrupted message can be calculated using Equations (15), (16).

$$R^H(t) = \frac{\frac{\mathrm{d}p_A(t)}{\mathrm{d}t}}{1 - p_A(t)} \cdot \frac{p_8(t)}{p_A(t)}, \tag{15}$$

$$p_A(t) = p_7(t) + p_8(t). \tag{16}$$

It is possible to assume that the HW failure rate of the decoder of the safety code $R^H_{DS} \ll 1 \cdot 10^{-9}$ h^{-1} and therefore the following condition $R^H_{DS} \ll R_{TS}$, $R^H_{DS} \ll R_{DT}$ is met. Then the diagram illustrated in Figure 4 can be modified as shown in Figure 5. Because of the mentioned requirements, states **4** and **6** are irrelevant in the realised model, but remain in the model to keep it readable.

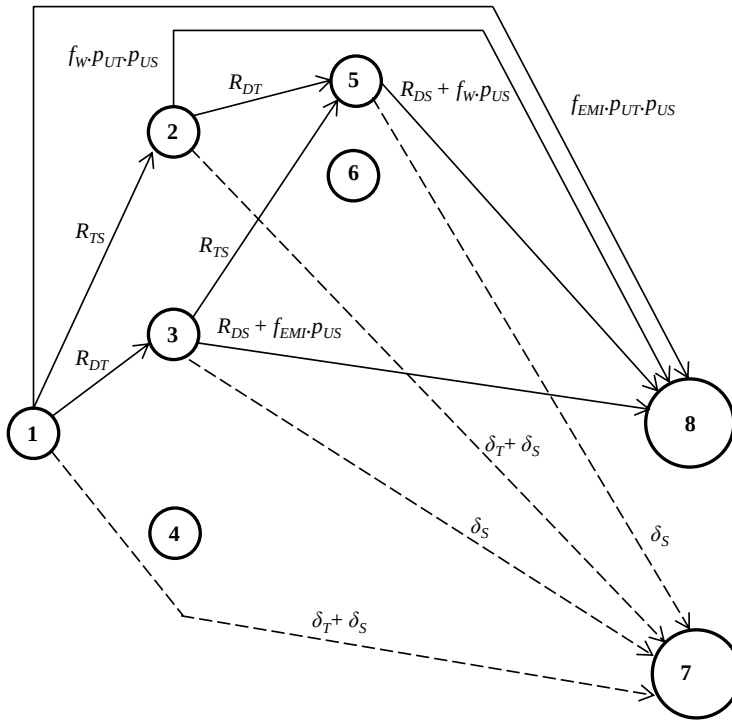

Figure 5. Modified Markov model of the SRComS

7 OBTAINED RESULTS AND THEIR VERIFICATION

The safety assessments of the SRComS illustrated in Figure 1 and described in Section 6 were based on the worst assumptions, as the norm [10] requires, and the transmission and safety codes were regarded as cyclic CRC block codes, namely CRC-16 (transmission code) and CRC-32 (safety code).

Input parameters for the calculation of the safety indicators: the rate (or the probability) of an undetected corruption in a message was determined based on the assumption that the frequency of generated safety-related messages from SRE1 is $f = 72\,000\,\mathrm{h}^{-1}$, i.e. the message transmission was assumed to be cyclic (cyclic time: one message per 50 ms). To determine of the probability of an undetected error of both codes, Equation (10) for the worst case of bit error rate of the communication channel was used.

Additional input parameters for the safety assessment of the SRComS were selected for a specific communication system used in railway transport [21]:

- HW failure rate of the transmitter part of the transmission system $R_{TS} = 5.3 \cdot 10^{-5}\ \mathrm{h}^{-1}$;
- HW failure rate of the decoder of the safety code $R_{DS} = 5.3 \cdot 10^{-5}\ \mathrm{h}^{-1}$;
- Probability of an undetected error by the transmission code $p_{UT} = 2^{-16}$;
- Probability of an undetected error by the safety code $p_{US} = 2^{-16}$.

During the safety assessment, the authors considered several operational situations. Let the SRComS have no safety measures for granting the safety integrity of message transmission except the transmission and safety codes. This means that if the decoders of the transmission or the safety code detect a corrupted message in the process of receiving, the corrupted message is rejected but no additional safety measures take place. If it is assumed that all received messages are corrupted (e.g. as a consequence of random HW failures), then from a safety point of view it is the worst case, i.e.

$$f_W = f_{EMI} = f = 72\,000\,\mathrm{h}^{-1}, \qquad \delta_T = \delta_S = 0\,\mathrm{h}^{-1}. \tag{17}$$

In Figure 6, the graphical relations of the probability and the rate of an occurrence of an undetected corrupted message for the model described in Figure 5 are illustrated.

The relations given in Figure 6 imply that during the lifetime of the SRComS (approximately 20 years), the rate of an undetected corrupted message will only be on SIL1.

It is a fact that this is an operationally unrealistic case, because the decoder of the safety code is a component of SRE2 and is realised with two channels with a comparison of the decoding results. Therefore in further considerations it is assumed that all transmitted messages are corrupted and if the decoder of the safety code detects that a received message is corrupted, then the received message is rejected

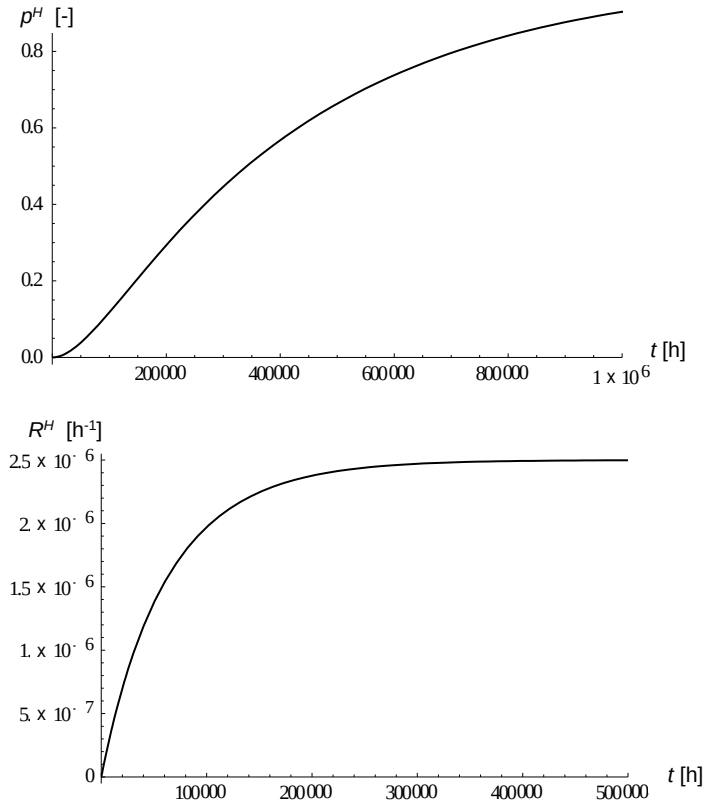

Figure 6. The probability and the rate of an occurrence of an undetected corrupted message with the parameters $f_W = 72\,000\,\mathrm{h}^{-1}$ a $\delta_T = \delta_S = 0\,\mathrm{h}^{-1}$

and the transmission interrupted indefinitely. If the decoder of the transmission code detects a corrupted message, then the received message is rejected, but no additional safety measures are carried out, i.e.

$$f_W = f_{EMI} = f = 72\,000\,\mathrm{h}^{-1}, \qquad \delta_T = 0\,\mathrm{h}^{-1}, \qquad \delta_S = 36\,000\,\mathrm{h}^{-1}. \tag{18}$$

In Figure 7, the graphical relations of the probability and the rate of an occurrence of an undetected corrupted message for the model described in Figure 5 and parameter calculated in (18) are illustrated.

The graphical relations in Figure 7 imply that during the lifetime of the SRComS, the rate of an undetected message occurrence will be $R_H < 3 \cdot 10^{-10}\ \mathrm{h}^{-1}$, which markedly exceeds the requirement for SIL4.

If we assume that all transmitted messages are corrupted and the decoder of the safety code detects that a received message is corrupted, then the message is rejected and the transmission is interrupted indefinitely. If the decoder of the transmission

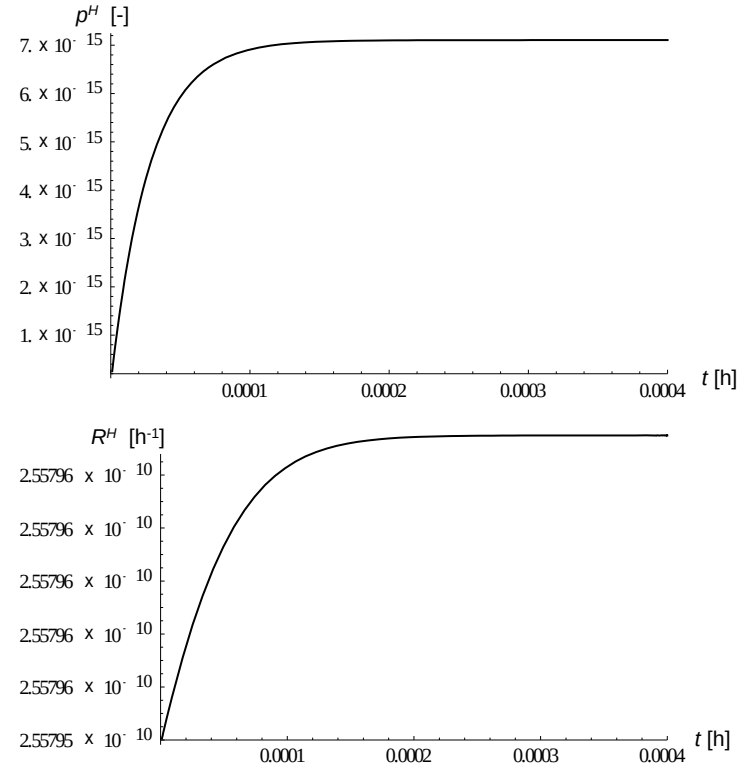

Figure 7. The probability and the rate of an occurrence of an undetected corrupted message with the parameters $f_W = 72\,000\,\mathrm{h}^{-1}$, $\delta_T = 0\,\mathrm{h}^{-1}$ a $\delta_S = 36\,000\,\mathrm{h}^{-1}$

code detects three consecutive corrupted messages, not only the received messages are rejected but the transmission is interrupted indefinitely too, i.e.

$$f_W = f_{EMI} = f = 72\,000\,\mathrm{h}^{-1}, \qquad \delta_T = 18\,000\,\mathrm{h}^{-1}, \qquad \delta_S = 36\,000\,\mathrm{h}^{-1}. \tag{19}$$

The calculation of the probability of receiving consecutive corrupted messages was realised according to Equation (12). The results of modelling the operational scenario according to the selected parameters in Equation (19) are illustrated in Figure 8.

8 CONCLUSIONS AND FUTURE WORK

During the verification of the results, the authors focused on the calculation of the most important indicators of a SRComS's safety – the rate (or the probability) of dangerous failures of the SRComS, stemming from the requirement for SIL4, whose

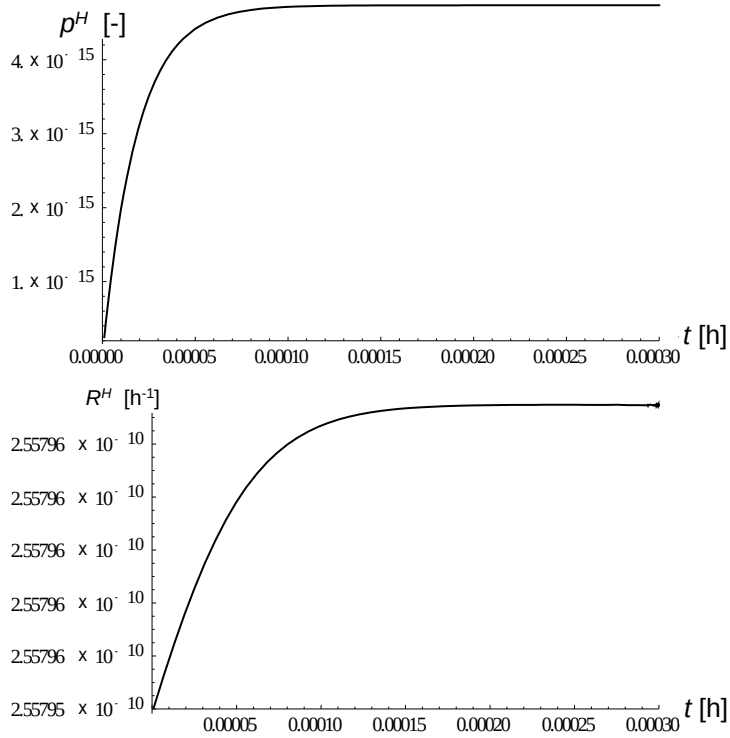

Figure 8. The probability and the rate of an occurrence of an undetected corrupted message with the parameters $f_W = 72\,000\,\mathrm{h}^{-1}$, $\delta_T = 18\,000\,\mathrm{h}^{-1}$ a $\delta_S = 36\,000\,\mathrm{h}^{-1}$

quantitative proof is required in practice during the development of interlocking and communication systems in railway applications.

The practical calculations were implemented for the particular SRComS, which is used in railway applications and the results confirmed that the considered SRComS meets the SIL4 requirements according to [10].

The designed model can be used for assessments of ordinary operational situations, too. In such a case, it is necessary to consider that transmitted messages are only effected by EMI. However, to calculate the transition rate of the SRComS to the safe state (state **7** in Figure 4 or Figure 5), it is needed to evaluate the probability of an occurrence of l consecutive corrupted messages. If l consecutive corrupted messages occur, the SRComS goes to the safe state (state **7** in Figure 4 or Figure 5), while the transition rate (the rate of an occurrence of an undetected corrupted message) depend on the message length and on the bit error rate of the communication channel. In practice, in most cases two formats (a short format, usually with up to 2 bytes, and a long format, usually with up to 256 bytes) are used for the length of safety-related messages. A verification of a model for the

assessment of safety characteristics of a SRComS is very problematic and cannot be realised by practical measuring (because of very small values of the probability of an undetected corrupted message). A verification can only be carried out based on opinions of experts in this area, or by a comparison of results obtained with other models. The results obtained via suggested model correspond with the results obtained by using the procedure described in the informative part of the norm [10], which is simplified and cannot be applied mechanically within a safety assessment. Against an advancement which is mentioned in the norm [10] the designed model decreases the subjective effect of an assessor on the final result.

Currently, the authors are focusing on:

- additional verifications of the designed model;
- a modification of the model, so that it could take into consideration other mechanisms of quality control of the transmission part (different to those used in the designed model);
- creating a model for a safety assessment of message transmission in open transmission systems, where in addition to assessing the safety code, it is necessary to evaluate the effect of a failure of the cryptography code [22].

Acknowledgement

This work was supported by the VEGA scientific grant agency, grant No. VEGA-1/0388/12: Quantitative safety integrity level evaluation of control systems in railway applications (80 %) and cultural and KEGA education grant agency, grant No. KEGA-021TUKE-4/2012: CyberLabTrainSystem – Demonstrator and Trainer of Information-Control Systems (10 %) and No. KEGA-024ŽU-4/2012: Modernisation of educational technologies and methods with focus on cryptography for safety-related applications (10 %).

REFERENCES

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

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

[3] Franeková, M. et al.: Safety Communications of Industrial Networks. In: Monograph, EDIS Žilina, Slovakia, 2007, ISBN 978-80-8070-715-6 (in Slovak).

[4] Zolotová, I.—Landryová, L.: Knowledge Model Integrated in SCADAHMI System for Failure Process Prediction. In: WSEAS Transactions on Circuits and Systems. Vol. 4, 2005, No. 4, pp. 309–318, ISSN 1109-2734.

[5] Zolotová, I.—Hošák, R.—Pavlík, M.: Supervisory Control Sustainability of Technological Processes After the Network Failure. In: Electronics and Electrical Engineering. Vol. 18, 2012, No. 9, pp. 3–6, ISSN 1392-1215.

[6] Ligušová, J.—Liguš, J.—Horanský, K.: Design and Configuration of the Network Control System 2006. In: Kybernetika a informatika. STU Bratislava, 2006, ISBN 8022724319 (in Slovak).

[7] Sarnovský, J.—Hladký, V.—Jadlovská, A.: Control of Complex Systems. Elfa – Košice, 2005 (in Slovak).

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

[9] Franeková, M.—Rástočný, K.: Safety Evaluation of Fail-Safe Fieldbus in Safety Related Control System. In: Journal of Electrical Engineering. Vol. 61, 2010, No. 6, pp. 1–7, ISSN 1335-2547.

[10] EN 50159: Railway applications: Communication, Signaling, and Processing Systems. Safety-related communication in transmission systems, 2010.

[11] EN 50129: Railway Application. Safety-related electronic systems for signalling, 2003.

[12] ISO IEC 50-191: International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service, 1990.

[13] Zahradník, J.—Rástočný, K.—Kunhart, M.: Safety of Interlocking Systems. In: Monograph, EDIS Žilina, Slovakia, 2004, ISBN 80-8070-296-9 (in Slovak).

[14] Castangoli, G.—Bräuer, S.—Herrmann, M.: Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits. IEEE Transactions on Communications 1993.

[15] Koopman, P.: Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks. Preprint: The International Conference on Dependable Systems and Networks, DSN-2004.

[16] Clarc, C. C.—Cain, J. B.: Error-Correcting Codes for Digital Communications. Plenum Press, New York 1988, ISBN 0-306 40615-2.

[17] Maganiello, F.: Computation of the Weight Distribution of CRC Codes. University of Zurich 2008.

[18] Harlenderová, M.: Solution of Safety Analysis of Detection Possibilities of Safety Codes within Binary Symmetric Channel. Dissertation thesis, ČVUT Prague, 2011 (in Czech).

[19] Klapka, Š.—Harlenderová, M.: Quantitative Assessment of Safety Code. Symposium FORMS/FORMAT, Budapest 2008.

[20] Dimirovski, G. M.: Fuzzy-Petri-Net Reasoning Supervisory Controller and Estimating States of Markov Chain Models. In: Computing and Informatics, Vol. 24, 2005, No. 6, pp. 563–576, ISSN 1335-9150.

[21] Rástočný, K.: Safety Assessment Report. System NEXUS – Generic Product. Client C-Modul Slušovice, document: NEXUS_SARepot_KRIS_V01_01, 2011-03-20 (assessor: Rástočný, K.).

[22] Franeková, M.: Mathematical Apparatus for Safety Evaluation of Cryptography and Safety Codes Used in Safety Related Communication System. In: Modern Transport Telematics, 11th International Conference on Transport Systems Telematics, CCIS 104, 2011, pp. 126–135, ISBN 978-3-642-24659-3.

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

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

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

Karol Rástočný, Jr. graduated at the Institute of Informatics and Software Engineering of the Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava in 2011. Since 2011 he has been post-graduate student and researcher at the Institute of Informatics and Software Engineering. His professional orientation covers metadata management and maintenance of large information systems (e.g., the Web) and designing software systems.