Computing and Informatics, Vol. 35, 2016, 470–496

MODELLING OF HAZARDS EFFECT ON SAFETY INTEGRITY OF OPEN TRANSMISSION SYSTEMS

Karol Rástočný, Mária Franeková, Peter Holečko

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

Abstract. The paper is concerned with safety appraisal of safety-related communication systems (SRComSs) with open transmission system, where except in addition to message transmission integrity also confidentiality is recommended to be provided. The authors focused on safety analysis of safety-related messages transmission secured using cryptographic and safety code mechanisms and on the possibilities of modelling safety-related industrial communication system, where a high safety integrity level SIL3 is required to be guaranteed. The paper features mathematical procedures to calculate the rate of hazardous transmission failure of safety-related messages in the result of electromagnetic interference (EMI) effects in the communication channel and by the presence of random hardware failures of SRComS. The theoretical techniques and safety analyses emerge from risk analysis and are compared with the knowledge gained by the authors during safety verifications of such systems for transportation applications. It is a little explored area, because the standards concerning safety-related control systems (SRCSs) did not support any cryptography-based methods. A quantitative safety integrity analysis

of SRComS is based on utilisation of Markov's processes. The proposed Markov's model is applied on an open transmission system built on the IEEE 802.11g standard, which is complemented by cryptographic and safety code. The calculations are performed using Mathematica software tool. The proposed base model is universal and can be modified (simplified) in dependence on the parameters of a specific SRComS.

Keywords: Safety-related communication system, open transmission system, industrial application, safety integrity level, encryption code, safety code, safety assessment, modelling, Markov model

1 INTRODUCTION

The problem related with the evaluation of safety-related communication (SRCom) for closed transmission systems is for several decades in focus of scientific teams of experts working in the area of SRCS and its components (sensors, actuators, ...), which typically use industrial buses (fieldbus) or some of the industrial Ethernet standards [1, 2, 3] for internal and external data transmission. Nowadays, for the industrial applications using closed transmission systems with SIL3 safety integrity level, "safety profiles" are certified for several families of CPF (Communication Profile Family), for example CIP Safety (CPF 2), ProfiSafe (CPF 3), openSafety (CPF 13), Foundation FieldBUS Safety (CPF 1), Interbus Safety (CPF 6). Manufacturers and users of these safety products from the field of industrial automation form associations, like Profibus and ProfiNet International [4], Open Device Vendor Associations (ODVA) [5], Ethernet Powerlink Standardisation Group (EPSG) [6].

The efforts for flexibility and cost reduction caused that the oncoming development of "safety profiles" heads to higher versions accepting also utilisation of open transmission systems for SRComS. More often, it is possible to practically encounter a SRComS utilising Commercial Off The Shelf (COTS) technologies, so called "security" principles from standard transmission systems, to support the "safety". For instance, producers of Profibus/ProfiNet technology developed a Scalance S security solution for the ProfiNet network based on VPN (Virtual Private Network) with the use of IPsec protocol tunnelling mode which uses cryptographic mechanisms [7]. We can say that the world of industrial communication, which was recently utilising proprietary solutions and generally did not support any cryptography-based methods, gradually proceeds to open solutions and is trying to catch up the ICT (Information and Communication Technology) world, even in the field of cryptography and the overall improvement of applications security management. The requirement to implement cryptographic mechanisms in industry emerged primarily from the growth of wireless technologies utilisation for the communication with remote workplaces via public networks [8]. Today it is obvious, that wireless communication systems have a great potential in the process control (not only in industry, but also

in other areas like transportation), as evidenced by (besides already exerted Wi-Fi, Bluetooth, ZigBee and other standards) the deployment of relatively new standards focusing on the process automation, specifically Wireless HART, WIA-PA and ISA 100.11a [9].

A standard SRCS can be generally decomposed to several basic components (blocks). One of these components is SRComS which can by its characteristics significantly influence the quality of safety functions performed by SRCS. Seeing that SRComS is just one of the components participating in the provisioning of safety function, it has to show a considerably lower probability of hazardous failure than the tolerable failure probability of safety function in activity in question. For example, in case the safety function has to be performed with SIL3, according to [10] the average frequency of dangerous failure of the safety function is $10^{-8} \leq$ up to $< 10^{-7}$ per hour for a high demand mode. Demonstration of appropriate safety properties of SRComS is a precondition for its practical utilisation.

In order to set a methodics for safety assessment of open communication systems with the cryptographic coder/decoder mechanism, it is necessary to go out from the definition of open communication system, from the analysis of attacks on messages during transmission through this system and from the current state of existing computationally secure security mechanisms from the cryptography field. Probably the most sophisticated specification of safety requirements on the communication between safety-related applications is stated in [11]. This specification is based on analysis of possible hazards and measures handling these hazards. The information part of standard [11] also introduces general recommendations on how to proceed when evaluating safety integrity of SRComS. However, these recommendations are primarily related to a closed SRComS, utilisation of which in railway applications has a long-term tradition. Many other standards related to industrial applications (for example [12]) are based on recommendations listed in [11]. According to [11], an open communication system can consist of an unknown number of users working on one hand with non-safety-related devices and on the other hand with safety-related equipment (SREs). When designing a communication system it is supposed, that the users are unknown and the transmission system transmits an unknown amount of data in an unknown format. The transmission media and its characteristics are unknown to users and the transmission system is routing and directing messages via routes from a single or several types of transmission media. In order to provide transmission of safety-related messages, an open communication system has to dispose of transmission functions that guarantee authenticity, integrity and recency of messages at the receiving end with the use of cryptography techniques.

2 PAPER CONTRIBUTIONS

The content of this paper is linked to the problem solved by the authors in [13] which was related to the assessment of safety integrity of a closed SRComS. The paper also builds on the results of mathematical modelling of cryptographic error

code probability for encrypted transmission of safety-related messages [14, 15] of variant length, which is disturbed by EMI and secured using a safety code.

The authors modified the method for assessment of SRComS safety integrity (published in [13]) so it respects the effect of random hardware failures of the evaluated SRComS and also considers attacks caused by an unauthorised person. These considerations focused on the choice of cryptographic code parameters in compliance with recommendations [11], with the goal to maintain computational and equivalent security of the chosen mechanisms in regard to cryptography utilisation specifics in a high safety integrity level applications.

The design of a generally valid method of quantitative assessment of safety integrity of an open SRComS can be considered genuine. It includes wireless technologies which are currently preferred in the industry for transmission of SR messages with the highest threat level (according to [11] transmission system category 3), where the masking thread type cannot be excluded.

The proposed state model has been applied to specific industrial SRComS utilising Wi-Fi IEEE 802.11g based transmission.

The main contribution of this paper is in the design of a quantitative method for evaluation of safety integrity of an open SRComS with open untrusted transmission system, where the core security mechanism is a cryptographic code. Achievement of this primary objective is connected with the following particular tasks:

- Analysis of hazards and its effects on safety integrity of the considered SRComS with a focus on wireless technologies standards recommended for use in industrial automation.
- Quantitative evaluation of risk factor parameters.
- Proposal of protection measures for elimination of risk factors with the focus on provisioning of integrity and confidentiality of SR messages transmission.
- Mathematical procedures for expression of the cryptographic decoder error probability (with the focus on modern computationally-secure symmetric block ciphers) in dependence on SR message length, cipher block size, in combination with the method of securing the transmitted messages using a safety code.
- Design of a base state model and its modification for the specific SRComS sample, assessment of its transitions between states with the goal to calculate the failure rate of its safety function.

The paper is not dedicated to methods and procedures providing a key for a symmetric cipher cryptographic code in SREs. It is supposed that the KMS (Key Management Systems) procedures from generation, distribution, archiving and alteration of keys is provided by a secure way in compliance with the recommendations [11].

The results of this analysis are applicable on a multipoint connection, because ultimately the preferred input methods in real-time (RT) communication enable transmission of SR messages of high priority between two nodes (for example a cyclic transmission in a master-slave mode).

3 APPROACHES PROMOTED WITHIN THE IMPLEMENTATION OF CRYPTOGRAPHY IN INDUSTRIAL SRCOMS

When utilising SRComS the transmitted and stored data have to be protected using cryptographic mechanisms, in case an intentional attack cannot be excluded. Regarding the required SIL of safety function utilising SRCom, a detailed safety analysis of transmission system and the utilised cryptographic protection has to be performed and prove the adequacy of:

- Technical choice of cryptographic techniques – related to selected encryption algorithm (e.g. symmetric or asymmetric), key characteristics (e.g. fixed or generated during connection – session keys), reasonability of selected key-length, frequency of key renewal, and physical key storage.
- Technical option of cryptographic architectures – related to the revision of correct functionality of chosen cryptographic mechanisms and cryptographic processes when implemented outside SRE.
- Cryptographic keys management activities – this part of safety analysis is related to generation, storage, distribution and cancellation of confidential keys, device management, revision process for the adequacy of cryptographic techniques in relation to risks emerging from malicious attacks.

In principle, approaches for application of cryptography within the communication between SREs can be divided into two solutions (see Figures 1 a), b)):

- Cryptographic technique is a part of security protections of an individual SRE (Assurance of unauthorised access layer in Figure 1 a)).
- Cryptographic technique is a part of security protections of several SREs communicating within an internal industrial network and is implemented into a separated assurance of unauthorised access layer (see Figure 1 b)). For instance, it is recommended to use firewall, though it has to be incorporated into the security policy of safety-related application. A firewall also utilises cryptographic mechanisms to perform security requirements. In addition to access protection, it can also provide other security services (for example confidentiality). Its primary task is to block unauthorised network traffic between an internal (protected) and external network for example by not allowing a direct connection between a node in the internet and a node in the industrial network. A firewall can be configured in a way allowing communication via specific protocols only, for example ProfiNet.

During the safety analysis of SRComS in the practical part of the paper, the authors came out from the approach described in Figure 1 a). As illustrated in Figure 1 a) and Figure 1 b), besides the assurance of unauthorised access layer, the assurance of data transmission level is always a part of SRE, which incorporates safety protections eliminating the effects of EMI in the transmission system. The

transmission system is often referred to as *"black channel"*, because its behaviour is partially or completely unknown.

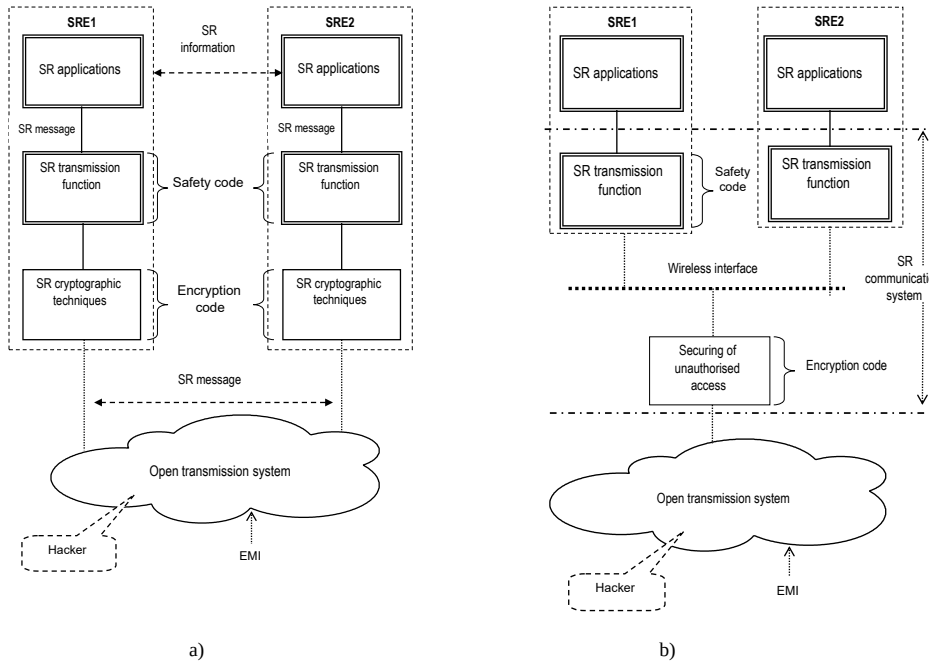

Figure 1. Approaches enforced when implementing cryptography in industrial SRComS

SRComS for industrial applications is in several cases composed of a certain number of nodes requiring real-time communication. Safety-related applications require a choice of cryptographic mechanisms parameters providing the highest possible safety integrity level, which considerably impacts time demandingness of operations and ultimately can cause a loss of real-time operation ability.

In case a SRComS utilises cryptography, following specifics have to be considered in addition to COTS technology:

- Limited computing performance of devices – in some applications (e.g. 8-bit architecture), the use of modern (primarily asymmetric) cryptography principles can be problematic, because it involves complex mathematical operations from theory of numbers and modular arithmetic.
- The required response during data transmission over the network in real-time (response speed) – performance of cryptographic operation has to be realised in real-time in order to meet the required response time.
- Effective cryptographic keys management – besides implementation of cryptographic algorithms, the key management has also to be performed in real-time

(a key is the biggest weakness of cryptographic protocols), cryptographic solutions are incomplete without key management. A key stored in a device is very vulnerable. It has to be frequently modified, the best way is to generate a new one for each new communication.

The most recommended cryptographic techniques for SRComS are encryption techniques and digital signature techniques. The following section of this section briefly introduces an overview of algorithms and operational modes recommended for the safety-related industrial applications area.

3.1 Encryption Techniques and Its Specifics

The encryption mechanisms in production enterprises are utilised for example for the concealment of production formulas, procedures and the overall enterprise "*know-how*". When using encryption on the technological control level in safety-related applications, in order to accelerate calculations, specialised modules are being used – security integrated circuits with high-speed processor [16], which performs encryption and key management separately, thereby relieving the application. In case of an unauthorised keys manipulation or unauthorised module intrusion detection, the keys are automatically destroyed.

Verified block cipher standards are recommended for SRComS; the use of stream ciphers is not recommended, due to a much lower security. From the block ciphers set, cryptographic measures utilising a single key can be preferred. These are symmetric encryption systems having several advantages for the use in industrial applications – they enable high-speed data encryption, utilise relatively short keylengths, are based on a more simple mathematical principles (substitutions, permutations) and besides safety integrity, they also provide confidentiality and data source authorisation (the communicating entities share a secret key on which they agreed or obtained in a secure way). In addition, the safety integrity can be improved by combining with a suitable operational mode. Safety-related applications are not recommended to utilise the ECB (*Electronic Code Book*) mode, but in order to improve safety integrity the CBC (*Cipher Block Chaining*) mode is enforced, exerting a feed-back mechanism before encryption and decryption, thereby eliminating some types of attacks, e.g. block replay [17]. Currently, computationally secure symmetric cipher algorithms are considered to be some modifications of DES (*Data Encryption Standard*) algorithm, primarily the 3-DES with three keys, for which (also in respect on existing cryptanalytic attacks) the effective keylength is 112 bits. A more enforced cryptographic standard is AES (*Advanced Encryption Standard*) [18] in AES-128, AES-192 and AES-256 versions, currently applied in all communication areas or data storage, programming languages and platforms, and is considered to be a computationally secure cipher.

In case the computational performance of a safety-related application allows it, for the encryption of small data volumes cryptographic measures with a key pair can be implemented. These are asymmetric cryptographic systems eliminating the prob-

lem of secure channel needed for key transmission (in contrast to symmetric encryption systems) and based on operational conditions, the key pair can be utilised without modification for a longer period. Nowadays, the RSA (*Rivest Shamir Adleman*) algorithms are considered to be computationally secure and mostly used. According to preliminary estimations, a secure length of RSA parameters (the module N as a product of two prime numbers) exceeds the boundary of module $N > 2\,000$ (corresponding to a 300 or 600-digit number, respectively). This implies the recommendation not to utilise RSA with the length of N lower than 2 048 bits, and for a long-term use an implementation with the length of 8 192 bits is in preparation. The opinions of experts on the increase of cryptographic module N size vary, some cryptologists in the field of asymmetric cryptography recommend to switch as soon as possible to ECC (*Elliptic Curve Cryptography*), a new perspective trend in modern asymmetric cryptography [19].

The security of cryptographic algorithms can be expressed using equivalent security, which indicates a relation between keylength (in bits) in correlation with currently known cryptanalytic attacks on the algorithm [20].

3.2 Digital Signature Techniques and Its Specifics

Digital signature mechanisms are reasonable in safety-related applications where credibility of information incoming from (or outgoing to) remote nodes has to be verified. Other application areas are for example verification of a software update before its deployment, verification of hardware configuration changes and other.

Currently the most recognised digital signature schemes using asymmetric cryptography are the following:

- RSA digital signature scheme – security is based on the difficulty of large numbers factorisation (size of module N).
- DSA digital signature scheme (with modified El Gamal algorithm) – security is based on the complexity of discrete logarithms calculation.
- ECDSA digital signature scheme with elliptic curves algorithm – security is based on the complexity of discrete logarithms calculation referred to as ECDLP (*Elliptic Curve Discrete Logarithm Problem*) [21].

In addition, all digital signature schemes are based on the security of the employed hash function [22].

4 MODELLING OF HAZARDS EFFECT ON SAFETY INTEGRITY OF SAFETY-RELATED COMMUNICATION SYSTEM (SRCOMS) WITH CRYPTOGRAPHY CODE

Let there be a SRComS with the open transmission system enabling transmission of safety-related messages between two nodes (Figure 2).

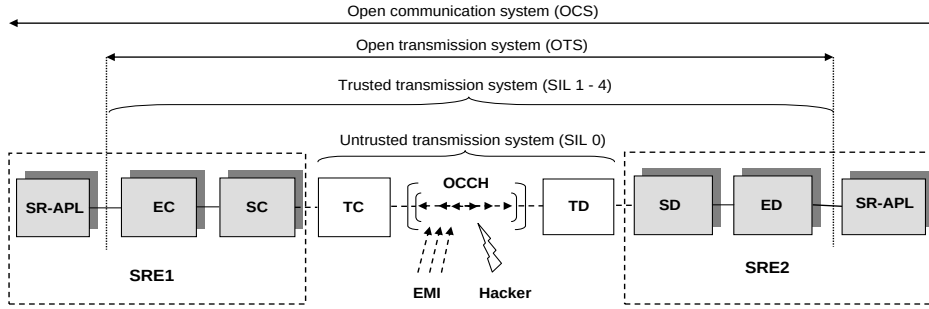

Figure 2. SRComS with cryptographic and safety codes

The SRComS under consideration (Figure 2) consists of two safety-related equipment SRE1 and SRE2 and an open untrusted transmission system. In order to provide trustworthiness of message transmission with a guaranteed safety integrity level, the transmission system has to incorporate proper transmission functions and has to prevent unauthorised access to a safety-related message. For a defined safety-related application (SR-APL), these functions are physically performed using a pair – *encryption coder/decoder* (EC/ED) and *safety coder/decoder* (SC/SD) and are a part of SRE. The mentioned safety functions are an extension of *transmission coder/decoder* (TC/TD) of the untrusted transmission system. A part of the untrusted transmission system is an *open communication channel* (OCC), which is affected by the electromagnetic interference and by attacks conducted by an unauthorised individual, which cannot be excluded in case of an open transmission system [14]. The safety analysis of SRComS presented in this paper is based on the assumption, that the message is bit-oriented and the communication channel can be modelled as a BSC (*Binary Symmetric Channel*). The function of cryptographic coder is to encrypt the message into an incomprehensible form, i.e. to ensure its confidentiality. As already mentioned before, SRComS are recommended to use a cryptographic code [11] operating with a secret key, therefore the safety analysis is realised for the EC/ED pair working with a cryptographic code from the block ciphers set. The probabilities of encrypted message error are influenced by the type of interference in the communication channel (bit error rate of a single element – bit in BSC) and its residual error rate in a great measure depends on the matter of securing using a chosen safety code. The introduced facts imply that during quantitative evaluation of cryptographic decoder error caused by EMI, the SC/SD pair cannot be omitted. From this perspective, the security extension in a form of EC/ED and SC/SD in SRE has to be understood as a combined coding system which algorithm operates with two block codes, with the difference that the EC/ED pair needs a variable element for its operation – a key.

4.1 Main Factors Affecting SRComS Safety

During transmission of a message its corruption has to be considered. Message corruption is an undesirable event, which can ultimately lead to a dangerous failure of safety function, on which the SRComS participates. The events which can cause message corruption can be categorised into:

- intentional – caused by a targeted activity of a person with the aim to gather, modify, insert or remove transmitted information
- unintentional – caused by a transmission system failure or its improper operation and maintenance or caused by the effects of the operational environment.

The main hazard in a safety-related communication is considered to be a situation, when a message generated by the application part of SRE1 is modified during its transmission through the transmission system in such a way, that it alters its information content and the application part of SRE2 considers it correct (not corrupted).

4.1.1 Attacks Caused by an Intentional Activity of Unauthorised Individual

The attacks by an unauthorised person cannot be evaluated quantitatively. The effect of these attacks on the safety of transmitted messages has to be considered within the risk analysis and based on this analysis to choose a suitable computationally secure cryptographic mechanism, in accordance with the development of modern cryptographic means.

4.1.2 Failures Caused by the Effect of the Operational Environment and Elimination Options

Seeing that safety-related messages are transmitted via a real communication channel, it is necessary to consider the influence of noise or interferences on the transmitted messages, which significantly affects the frequency of corrupted messages. The electromagnetic interference is a result of a number of various effects (noises, reflections, fading effect), which cannot be described in a deterministic way, therefore the models of communication channels are also based on probability characteristics. The standard [11] recommends for the safety analysis of communication based on binary transmission to use the binary symmetric channel model without memory for the bit error rate of the communication channel p_b within the interval 0 to 0.5. This model supposes that the errors during binary message transmission are random and mutually independent. In case a BSC model is considered at the transmission of binary messages with an error rate of one bit (element) p_b, then the probability, that a message of length m bits contains exactly i errors, is given by the relation [23]

$$p_i = (p_b)^i.(1 - p_b)^{m-i}. \tag{1}$$

If the bit error rate of BSC is over 0.5, it is probable, that the receiver (SRE2) inverts binary values, i.e. interprets 0 as 1 and 1 as 0. In this case there are no practically usable models available, therefore [11] recommends not to consider a value $p_b > 0.5$ within safety analyses.

A safety code with a high detection coverage and fast detection algorithm has fundamental significance for safety-related applications. The requirements on the choice of safety code parameters depend on the required safety properties of SRComS (mainly on the tolerable probability or error intensity of corrupted messages).

In order to choose a safety code, practical problems related to proper code parameters have to be solved [24]. These have to be considered, primarily:

- Code length. Typically, there is a requirement to be able to secure messages of variable length with a single code, while most of theoretical knowledge on codes is constrained on certain recommended construction code lengths, which is practically mostly not met (shortened or extended codes are used). It is necessary to keep in mind that a code of different length has different safety properties.
- Code redundancy. A dominating opinion is that the more redundant bits are used, the higher the safety is. The requirement for a higher number of redundant bits is not always legitimate (e.g. CRC-64 – ISO with 64 redundant bits has worse safety properties than a well-chosen code with 32 redundant bits) [25].
- Minimal Hamming distance d_{min}. Minimal Hamming distance is coupled on the requirement to detect or correct errors until a certain multiplicity. Most codes detect and subsequently correct single (independent) errors and errors of i – multiplicity (dependent errors – bursts), too.
- Detection of chosen error patterns. Some types of errors can occur more frequently. Therefore it is required to detect them by the code (e.g. repeated bursts of a certain length, all bits of the message have the significance of 1 or 0, message negation). But in most cases we do not know the probability of the error patterns occurrence.

We can suppose that the safety properties of the SRComS under consideration will be in a great measure dependent on the properties of cryptographic block code and safety block code. These codes are used in combination, thereby positively affecting safety integrity of SRComS even in the case of variable length messages and variable error rate in BSC model.

In case a channel linear block code is used as a safety code, then the probability of undetected error of code word during the transmission via binary symmetric channel is [26]

$$p_U \leq \sum_{i=\left\|\frac{d_{min}+1}{2}\right\|}^{n} A_i.(p_b)^i.(1-p_b)^{n-i}, \tag{2}$$

where p_b is the probability of error of a single bit, n is length of code word, d_{min} is minimal Hamming distance of the code, A_i is the overall number of code words with weight i and $\|x\|$ means integer value of x.

A more detailed procedure recommended for safety analyses of block codes within communication systems with only a safety code is introduced in [27, 28].

4.1.3 Estimation of EMI Caused Failures Rate

Let the safety-related messages of length m bits transmitted from SRE1 be divided into blocks of length k bits (*plain text blocks*) before entering EC and let output blocks of length k bits (*encryption blocks*) from EC. Most of the commercially utilised block ciphers have the same plain text and encrypted text blocks. For instance the 3-DES block cipher has a block length of the processed plain text of 64 bits, the commercial AES cipher has the block length of 128 bits. In the next processing in the transmission chain according to Figure 2, r redundant bits are added to blocks of length k in SC because of EMI influence detection. The SC outputs binary blocks of length n. Let us assume that the TC/TD pair, which is not a part of safety-related transmission system also operates with a block channel code. Each bit inputting the communication channel represented by a BSC model is influenced by the p_b error rate. We can say that the encrypted message cw (*cipher words*) on the output of ED is evaluated as corrupted when at least one block of this message has been evaluated as corrupted using the detection codes techniques (mostly working in the receiving part on the principle of syndrome techniques).

If we assume independence of corrupt blocks on the input of ED, then the probability of whole message corruption p_{cw} is dependent on communication channel bit error rate p_b and is defined as [29]

$$p_{cw} = p\,(w/be)\,.\,[1-(1-p_b)^m]\,, \tag{3}$$

where $p\,(w/be)$ is the conditional probability of output unencrypted message w (word) corruption, if there is a corrupted block on the input of cryptographic decoder. If $p\,(w/be) = 1$, then

$$p_{cw} \leq 1-(1-p_b)^m \leq m.p_b. \tag{4}$$

According to [26], by repeating the analysis for a sufficient number of input m-bit messages, we can conclude, that for k bits in a simple encrypted block the average probability of its corruption on the output (if there is a corrupted block on the input) is given by the relation

$$p\,(w/be) = 1-\prod_{i=1}^{k}\frac{2^{m-1}-1}{2^{m+1-i}-1} = \frac{1-2^{-k}}{1-2^{-m}}. \tag{5}$$

Based on Relations (3) and (5) the average set probability of cryptographic message corruption for a block cipher can be expressed by the relation

$$\overline{p_{cw}} = \frac{1-2^{-k}}{1-2^{-m}}.\left[1-(1-p_b)^m\right]. \tag{6}$$

In case a proper safety code with error detection is used to increase the safety integrity of SRComS with probability of unencrypted message error p_w, then the Relation (6), under the conditions in [29], can be modified to

$$\overline{p_{cw}} = \frac{1-2^{-k}}{1-2^{-m}}.\left[1-(1-p_w)^{m/k}\right], \tag{7}$$

where p_w is probability of unencrypted message error and the ratio m/k is number of blocks created in the message.

If

$$p_b \ll 2.(m-1)^{-1}, \tag{8}$$

then after expansion of (7) into Taylor series we can accept that

$$\overline{p_{cw}} \approx \frac{1-2^{-k}}{1-2^{-m}}.\frac{m}{k}.\ P_w. \tag{9}$$

Let p_{US} be a probability of undetected error of safety code and p_{UT} a probability of undetected error of transmission code. Providing that both codes are independent, the probability of corruption of input unencrypted code word (in block) $p_w = p_{US}.p_{UT}$ and the resulting average probability of encrypted message corruption on the output of ED is

$$\overline{p_{cw}} = \frac{1-2^{-k}}{1-2^{-m}}.\left[1-(1-p_{US}.p_{UT})^{m/k}\right]. \tag{10}$$

The message failure rate MFR_{EMI} on the output of SRComS, which integrity has been impaired by EMI during transmission, can be expressed by the relation

$$MFR_{EMI} = \overline{p_{cw}}.f_{EMI}, \tag{11}$$

where f_{EMI} is frequency of corrupted messages in time (mostly per 1 hour) because of EMI.

Two message formats are typically supported in industrial safety-related applications – short format (e.g. 2 kB length) and long format (e.g. 256 kB length), which are mostly secured using transmission and safety code based on the principle of CRC (Cyclic Redundancy Check). In this paper, the values of p_{UT} were calculated with the assumption of CRC-16 cyclic code utilisation and p_{US} of CRC-32 cyclic code for both message formats.

Table 1 shows values of $\overline{p_{cw}}$ and MFR_{EMI} calculated using Relations (10) and (11) for typical parameters of SRComSs with Wi-Fi transmission according

to IEEE 802.11.g (physical transfer rate 54 Mb/s). From the perspective of transmission mode we suppose cyclic message transmission with transmission acknowledgement between master and the individual slave nodes in the network so that with a two-point connection (master–slave) a transmission occurs once in 50 ms (72 000 messages per hour). The calculated values (Table 1) are not time-dependent, because extreme (often practically the most adverse) values of p_{UT}, p_{US} are considered in regard to the time parameter. The most adverse scenario is supposed even when determining the frequency of corrupt messages f_{EMI}, i.e. it is expected that all messages on the input of receiver of the transmission system are corrupted. A message is considered to be corrupted in case when at least one message block is corrupted.

Short format of SR message $m = 2\,\mathrm{kB}$				Long format of SR message $m = 256\,\mathrm{kB}$		
k [b]	$\overline{p_{cw}}$ [-]	f_{EMI} [h^{-1}]	MFR_{EMI} [h^{-1}]	$\overline{p_{cw}}$ [–]	f_{EMI} [h^{-1}]	MFR_{EMI} [h^{-1}]
64	$0.888.10^{-12}$	72 000	$6.394.10^{-8}$	$113.686.10^{-12}$	72 000	$8.185.10^{-6}$
128	$0.444.10^{-12}$	72 000	$3.197.10^{-8}$	$56.843.10^{-12}$	72 000	$4.092.10^{-6}$

Table 1. MFR_{EMI} in dependence on block size k

However, the Relation (11) does not respect the effect of other risk factors (undesirable events) on the safety of transmitted messages (for example the effect of transmission system errors). Though, it is well suited for a "rapid" estimation of correct choice of transmission and safety code in combination with the used cryptographic code.

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

4.1.4 Failures of the Individual SRComS Components

A transmission system consists of components operation of which can be affected by:

- systematic failures
- random failures
- aging.

A source of systematic failures are primarily human errors caused during system development (erroneous firmware), its implementation (faulty configuration) or maintenance (improper servicing intervention). Systematic failures can be very effectively prevented by applying proper measures in all life-cycle stages of SRComS. Quantitative assessment of systematic failures effects on SRComS safety integrity is not performed, but it has to be proved that such measures were met, so that the effect of systematic failures on safety integrity can be neglected.

Electronic components of SRComS are subject to random failures and failures caused by aging. During the service life of SRComs it is not necessary to consider failures caused by aging; only the incidence of random failures is assumed [10].

Seeing that for electronic systems it is principally impossible to construct a list of possible failures and analyse the effects of individual failures on the safety integrity of SRComS (e.g. using FMEA (Fault Modes and Effects Analysis) [31]), the safety analysis has to be based on probability principle and use the knowledge of random failures rate and its distribution. A generally accepted statement says, that the occurrence of random failures of electronic objects can be described by the exponential distribution law, hence the rate of random failures occurrence of these objects is constant. Under these assumptions, the effect of failures on the safety integrity of SRComS can be considered to be a homogenous Markov process with continuous time.

Generally we can suppose, that not all object failures affect the safety integrity of the object under consideration and following holds:

$$\lambda_T^O = \lambda_H^O + \lambda_S^O, \tag{12}$$

where λ_T^O is the total rate of random failures of an object, λ_H^O is the rate of random failures of an object affecting the safety integrity of an object; λ_S^O is the rate of random failures of an object not affecting the safety integrity of an object. Because it is very problematic to determine which part of random failures rate affects the safety integrity of an object, a pessimistic assumption is mostly used during safety analysis (primarily if a very high safety integrity is considered), that each failure of object affects its safety integrity.

When designing SRComS components which are parts of SREs (SC, EC, SD, ED), special techniques are being used to achieve the required SIL [18], assuring that the rate of hazardous failures of these parts is significantly smaller than the total rate of failures.

5 SRCOMS MODEL REALISATION

Figure 3 shows a state model of SRComS describing transition of SRComS from state 1 (a state when the system is operational and the transmitted messages are corrupted only by EMI influence) into a hazardous state 8 (message corruption has not been detected and the message has been evaluated as correct by the receiver). A transition from state 1 into state 8 can be realised as a result of:

- incidence of random failures of individual SRComS components
- insufficient detection properties of transmission code and safety code in combination with cryptographic code utilisation
- by EMI influence.

However, the introduced model does not respect the effects of systematic failures (e.g. software failures) nor the effect of attacks caused by an undesirable and intentional activity of an unauthorised person.

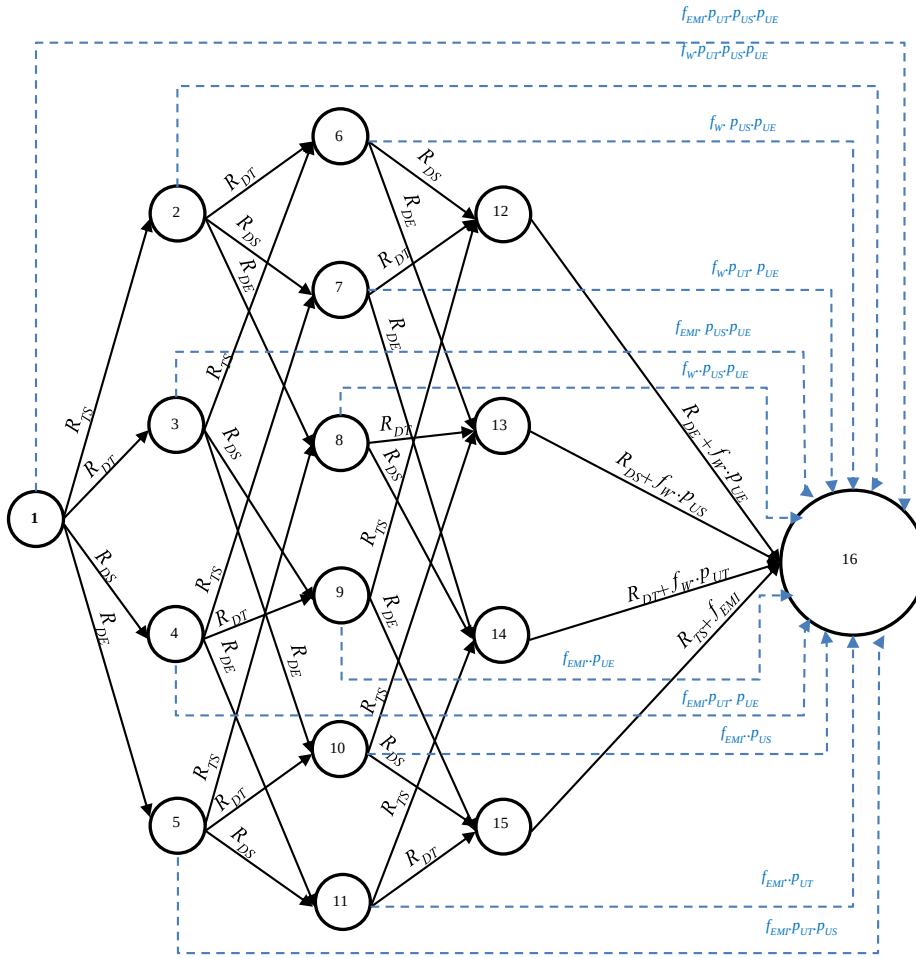

Figure 3. SRComS base model

The meaning of symbols used in Figure 3 is listed in Table 2.

The probability of achieving state 8 (or the rate of transition from state 1 into state 8) depends, besides the stated risk factors, on the frequency of transmitted messages and on the time between two functionality checks of SRComS (proof test interval).

When determining the frequency of messages corrupted because of EMI during a defined time unit (mostly 1 hour), we can consider a message transmission mode preferred in industrial applications, which is cyclic message transmission. In case the message is divided into blocks and each block is secured by a transmission and safety code, then the model has to consider message blocks (Figure 4). From the

Symbol	Description
R_{TS}	Rate of random hardware failures of transmission system part (transmitter, communication channel and receiver part)
R_{DT}	Rate of random hardware failures of transmission code decoder
R_{DS}	Rate of random hardware failures of safety code decoder
R_{DE}	Rate of random hardware failures of cryptographic code decoder
p_{UT}	Probability of error undetected by transmission code
p_{US}	Probability of error undetected by safety code
p_{UE}	Probability of error undetected by encryption code
f	Frequency of messages generated by transmitter
f_{EMI}	Frequency of messages on receiver input corrupted by EMI influence
f_W	Frequency of corrupted messages on receiver input without specification of corruption cause

Table 2. Meaning of symbols in the model shown in Figure 3

safety perspective, a positive fact is that a message corruption is detected if leastwise corruption of a single message block is detected.

However, many untrusted transmission systems implement a mechanism inspecting the quality of transmission path of the communication channel and if the bit error rate passes a threshold value, the transmission speed is decreased, thereby increasing system's availability, but can negatively affect the information delay time, primarily in real-time process control. Generally, the positive effect of this mechanism is not considered in the safety analysis of SRCS, because often the most adverse case is taken into account, i.e. the messages are transmitted at the highest data transmission rate and all messages on the receiver's input are corrupted.

A similar approach can be applied on the SRE2 side and suppose, that the receiver works in such a way, that all messages received are evaluated by the transmission code decoder as correct (e.g. as a result of its failure) and only safety properties of the safety code decoder are followed or a strategy is used, when we primarily rely on the transmission code and the safety code decoder performs a function of a supervisor. After detecting the first corrupted message (a message which has been evaluated as correct by the transmission code decoder), the safety code decoder responds by causing a permanent interruption of message transmission and provides such data to SRE2 logics, that SRE2 passes into a safe state – a state which does not threaten safety of the controlled process. However, this solution significantly affects the availability of SRCS, even while having a very positive effect on its safety integrity, therefore several compromise solutions are opted out practically. Typically, the following measures are applied at the safety code decoder level (individually or in combination):

- checking of number of messages marked by the safety code decoder as corrupted and if the tolerable number of corrupted messages in a defined time unit is exceeded, a safe reaction is concluded;
- use of a ratio counter.

A ratio counter counts within a defined range from the initialisation value IV to the maximal value MV. During SRComS start the current value AV of ratio counter is set on the IV initialisation value. The current value of the counter is changing in dependence on the verification of the message received by the safety code decoder. In case the received message is marked as correct, the value of AV is decremented by the value PV (the IV value is a threshold value of decrementation). In case the received message is marked as corrupted, the value of AV is incremented by the value NV (while $NV > PV$). After reaching or exceeding the value MV, a safe reaction is concluded. An analysis of the ratio counter operation and the evaluation of its effect on SRComS safety integrity is presented in [30].

5.1 Modification of the SRComS Model

The base model (Figure 3) can be modified (simplified) in dependence on how significantly the individual risk factors influence the safety of messages transmission in a case of a concrete SRComS. For example, we can suppose that the cryptographic code has no effect on the identification of a message corrupted by hardware failure or by EMI ($p_{UE} = 1$). Accordingly, we can suppose that all message blocks incoming to the receiver are corrupted (the cause of corruption is not differentiated – corruption caused by EMI or corruption caused by transmitter failure, i.e. $f_{B\_W} = f_B$, where f_{B_W} is frequency of corrupted blocks on receiver input without corruption cause specified and f_B is frequency of blocks generated by the transmitter). A model modified according to these assumptions is shown in Figure 4. In this case, SRComS is in state 15_16 if the message block corruption has not been detected and the message block has been evaluated as correct by the receiver. In case all blocks on the input of transmission system receiver are corrupted, the message will be evaluated as correct (non-corrupted) when all corrupt message blocks will be evaluated as correct (non-corrupted) by the SRComS. Seeing that for the message corruption detection holds, that if a corruption of leastwise a single message block is detected, then message corruption is detected. Then

$$MFR \leq BFR.\frac{k}{m}, \tag{13}$$

where MFR is message failure rate, BFR is block failure rate, k is number of bits in a block and m is number of message bits.

Safety analysis can also be approached in an even more pessimistic way (what is reasonable in case of high demands on safety integrity level of the transmitted messages) by not considering safety properties of an untrusted transmission chain (as if it would not have positive, but negative effect on the transmission safety integrity) and only detection properties of safety code and potential random failures of safety and cryptographic decoder are taken into account. In other words – it is supposed that all messages incoming on the safety code decoder input are corrupted. Such a very pessimistic approach is positive to the intent that at the change of untrusted

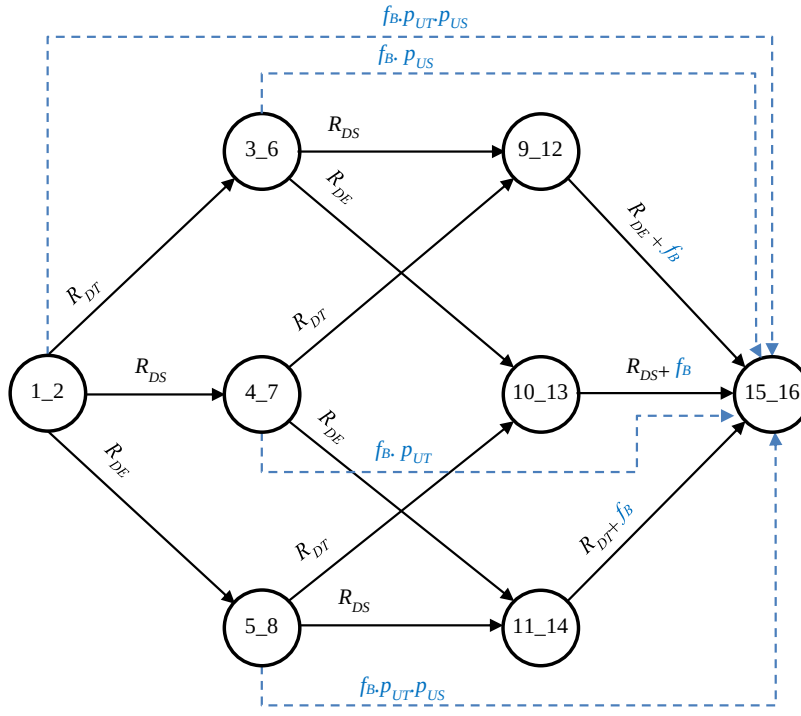

Figure 4. Modified SRComS model providing $p_{UE} = 1$ *and* $f_{B\_W} = f_B$

transmission system (a COTS system) or its components, there is no need to prove the safety properties of a trusted transmission system again.

6 OBTAINED RESULTS

Let us consider a SRComS according to Figure 2, for which the following technical and operational data is characteristic:

- rate of random hardware failures of transmission system components (transmitter, communication channel and receiver component) $R_{TS} = 5.3.10^{-5}h^{-1}$
- rate of random hardware failures of transmission code decoder $R_{DT} = 2.5.10^{-6}h^{-1}$
- rate of random hardware failures of safety code decoder $R_{DS} = 1.0.10^{-8}h^{-1}$
- rate of random hardware failures of cryptographic code decoder $R_{DE} = 1.0.10^{-8}h^{-1}$
- probability of error undetected by transmission code $p_{UT} = 2^{-16}$
- probability of error undetected by safety code $p_{US} = 2^{-32}$

- frequency of messages generated by the transmitter $f = 72\,000h^{-1}$
- short message length $m = 256\,\text{kB}$, or a long message length $m = 256\,\text{kB}$
- number of bits in a message block $k = 64\,\text{b}$, or $k = 128\,\text{b}$.

Let us assume, that all blocks on receiver input are corrupted. Then

$$f_{B\_W} = f_B = f.\frac{m}{k}. \tag{14}$$

Figures 5 to 8 show graphs of probability of undetected corrupted message block p_{B_H}, message failure rate *MFR* and block failure rate *BFR* in a message in SRComS for the created Markov model shown in Figure 4 and the considered technical and operational data of SRComS stated at the beginning of Section 5.2. The time dependencies p_{B_H}, *BFR* and *MFR* shown in Figures 5 to 7 are calculated for short message format of SR message $m = 2\,\text{kB}$ and cryptographic code blocks size $k = 64$ bits. For comparison, Figures 8 to 10 show the time course of the results of p_{B_H}, *BFR* and *MFR* for cryptographic code block size $k = 128$ bits.

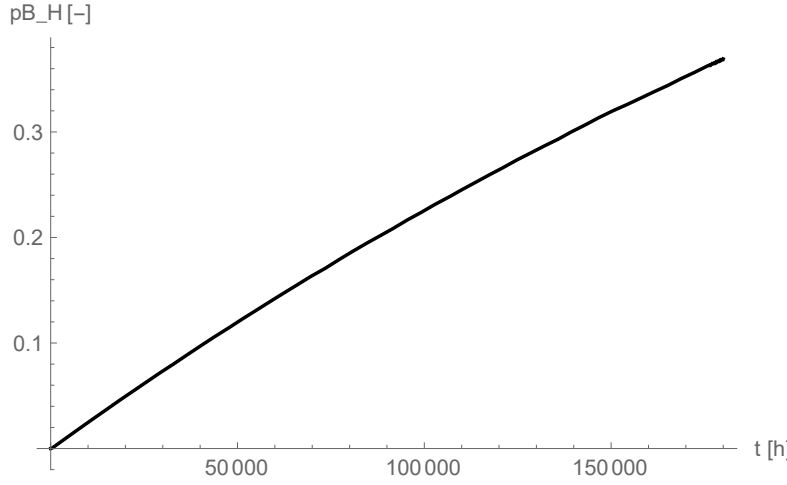

Figure 5. Time dependence of probability of the undetected corrupted message block for a short message format and cryptographic code block size $k = 64\,\text{b}$

The same way using the Markov model (Figure 4) we could generate graphical dependencies p_{B_H}, *BFR* and *MFR* for the long message format in dependence on block size k.

If we take a look at the results of message failure rate *MFR* within the SRComS lifecycle and compare them for example for the time $t = 10\,000$ hours (which corresponds to SRComS operation of over 17 years), the message failure rate *MFR* is of order 10^{-8}, which satisfies the recommended values presented in [10],

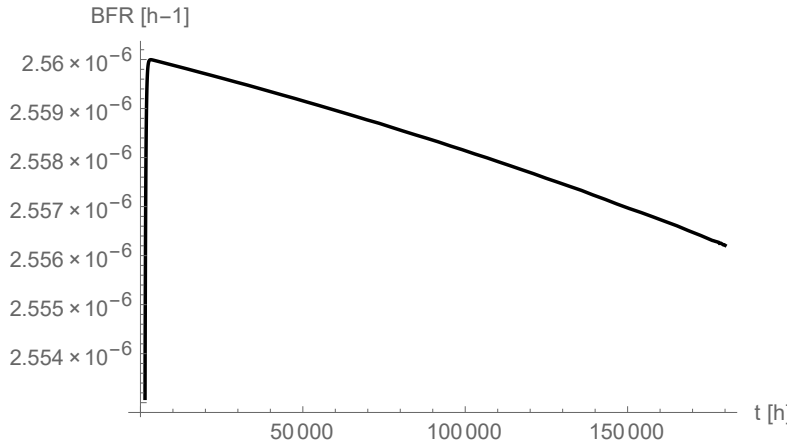

Figure 6. Time dependence of block failure rate for a short message format and cryptographic code block size $k = 64$ b

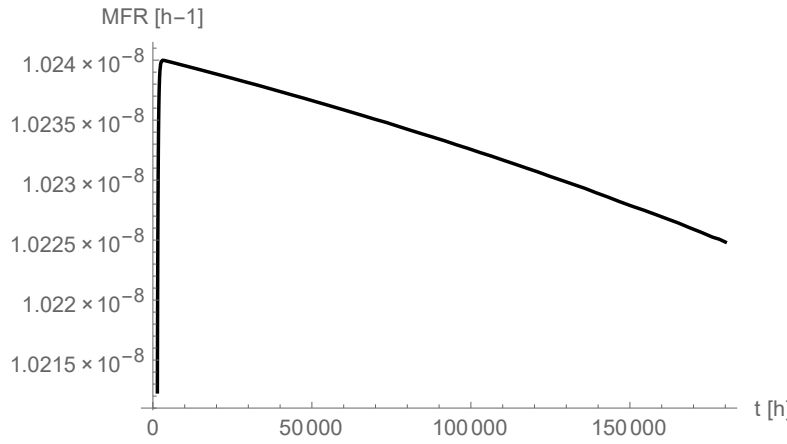

Figure 7. Time dependence of message failure rate for a short message format and cryptographic code block size $k = 64$ b

thereby corresponding to safety integrity level SIL3. The comparison of results presented in Figures 7 and 10 shows, that the results of rate of undetected corrupted messages of SRComS for a chosen block size k for the EC and ED pair are only slightly different and satisfy even the most pessimistic estimation we considered for the safety analysis of SRComS (according to Figure 2), the required safety integrity level SIL3, which is a sufficient tolerable intensity of hazardous failures for a SR industrial communication system with open transmission system.

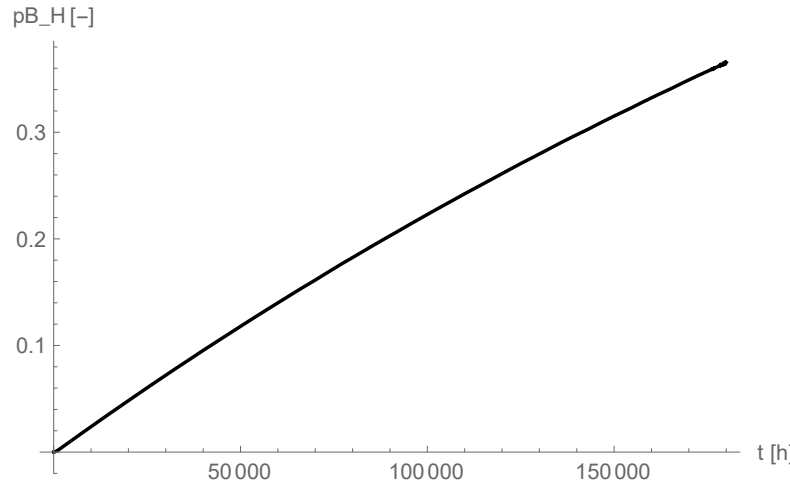

Figure 8. Time dependence of block failure rate for a short message format and cryptographic code block size $k = 128$ b

Using the realised model in Figure 4, the results of safety analysis of a SRComS could be easily generated for a different SRComS with different technical parameters of open transmission system.

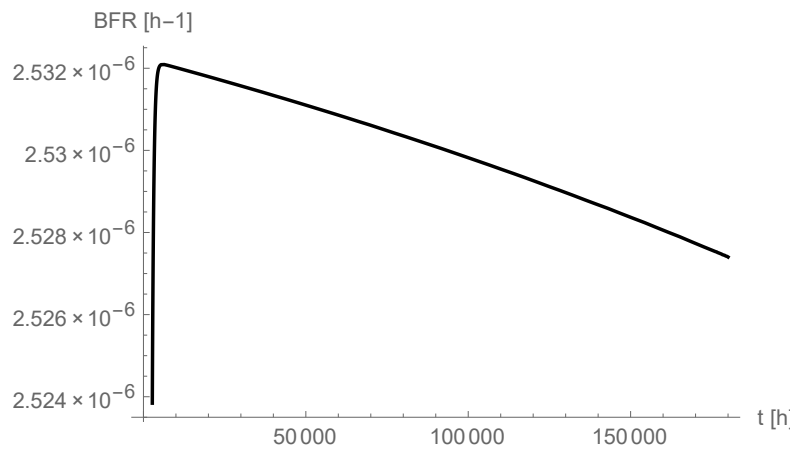

Figure 9. Time dependence of block failure rate for a short message format and cryptographic code block size $k = 128$ b

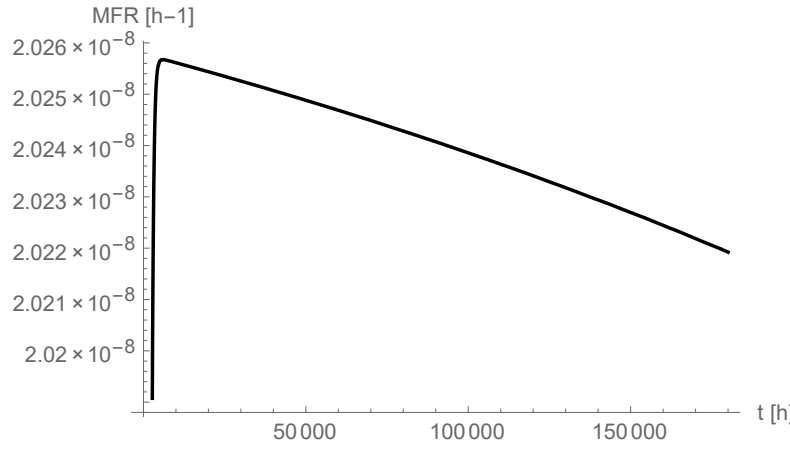

Figure 10. Time dependence of message failure rate for a short message format and cryptographic code block size $k = 128$ b

7 CONCLUSION

During safety analysis of SRComS the authors focused on the calculation of the most important safety attributes of SRComS – failure rate or probability of hazardous failures of SRComS, while building on the SIL3 safety integrity level, where quantitative proof is practically required for the development of industrial safety-related communication systems. The authors aimed at safety analysis of SRComS with open transmission system which is being increasingly used in industrial applications and not only in COTS applications, but also in the applications with elevated safety integrity level. Providing the use of open transmission system, it is necessary to suppose an intentional attack on the system, i.e. the transmitted SR messages have to be protected not only by the means of safety codes eliminating the effect of communication channel interference, but also by the means of cryptographic mechanisms. The contribution solves safety analysis of a combined SRComS (Figure 2) with safety and cryptography code, while assuming the cryptographic code providing confidentiality of the transmitted SR messages. According to the requirements based on standards for cryptographic code, in the Markov model as well as in the mathematical formulation of cryptographic code error probability (rate of non-detection of message by the SRComS), the authors focused on a cryptographic code belonging to the set of block symmetric cryptographic systems, while the block size k has been chosen in line with computationally secure standards from the block cipher set ($k = 64$ b – 3-DES algorithm, or $k = 128$ b – AES algorithm). Mathematical calculations of a message (or block) non-detection are derived with the assumption of a binary symmetric channel (BSC).

With respect to the fact that the occurrence of corrupted messages can be in great measure considered to be a Markov process, the authors of the paper decided to

make use of a CTMC-based model to model the safety attributes of SRComS (probability of non-detection of corrupted message, rate of non-detection of corrupted message).

In order to create a model respecting the effect of the individual factors influencing the safety of SRComS with a specific evaluation of its transitions, it is necessary to know the characteristics of SRComS and its behaviour in various operational situations. This means it is not possible to create a model which would be universally applicable for different SRComS, however the fact is, that the foundations of the model remain basically always the same.

Because the SRComS has to operate under all operational situations, in order to guarantee the required SIL when modelling the monitored safety parameters, it is necessary to consider the worst situations that can possibly occur during the operation. That means, that in case of SRComS we suppose, that all transmitted messages are corrupted by either EMI, or because of hardware failure. It is also necessary to consider the failure of the individual protection mechanisms dispatched within the SRComS. In our case, it is an operational situation for which the calculated results are shown in Figures 5 to 10. The practical calculations were realised for a specific SRComS utilised within industrial applications with Wi-Fi transmission and they confirmed, that the SRComS under consideration satisfies the SIL3 requirements according to [10]. To solve the system of differential equations, Wolfram Mathematica software tool has been used.

The presented model and the results obtained do not respect the fact that other protection mechanisms exist (time-stamp, ...), which also significantly decreases the probability of an improper message interpretation by the application part of the receiver.

The verification of the model for evaluation of safety properties of a SRComS is greatly problematic, cannot be assessed and cannot be performed by a practical verification (very small values of probability of undetected corrupted messages). The verification can only be performed based on statements of experts engaged in the problem or by comparing the results obtained using different models.

Acknowledgement

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) projects number 008ŽU-4/2015 Innovation of HW and SW tools and methods of laboratory education focused on safety aspects of ICT within safety critical applications of processes control (70 %) and number 001TUKE-4/2015 CyberLabTrainSystem – demonstrational and training of information control systems – innovation (30 %).

REFERENCES

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

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

[3] Zolotová, I.—Landryová, L.: Knowledge Model Integrated in SCADA HMI System for Failure Process Prediction. WSEAS Transactions on Circuits and Systems, Vol. 4, 2005, No. 4, pp. 309–318.

[4] www.profibus.com/technology/profisafe.

[5] www.odva.org.

[6] www.ethernet/powerlink.org.

[7] PROFILE System Description – Safety Technology and Applications. Profibus Nützerorganisation e.V., November 2010. www.profibus.com.

[8] Candian, A.: ProfiSafe and ProfiNet via Industrial Wireless LAN. Siemens, PICC Meeting 2008, Brescia, Italy.

[9] Alcaraz, C.—Lopez, J.: Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. 40, 2010, No. 4, pp. 419–428.

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

[11] EN 50159: Railway Applications. Communication, Signalling and Processing Systems. Safety-Related Communication in Transmission Systems, 2010.

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

[13] Rástočný, K.—Franeková, M.—Zolotová, I.—Rástočný, K. Jr.: Quantitative Assessment of Safety Integrity Level of Message Transmission Between Safety-Related Equipment. Computing and Informatics, Vol. 33, 2014, No. 2, pp. 343–368

[14] Franeková, M.—Lüley, P.—Ondrašina, T.: Modelling of Failures Effect of Open Transmission System for Safety Critical Applications with Intention of Safety. Elektronika ir Elektrotechnika, Vol. 20, 2014, No. 1, pp. 19–24.

[15] Franeková, M.—Výrostko, M.—Lüley, P.: Determination of Error Probability of Cryptography and Safety Codes for Safety-Related Railway Applications. Advances in Electrical and Electronic Engineering, Vol. 11, 2013, No. 2, pp. 94–99. ISSN 1804-3119. Available on: http://advances.utc.sk/index.php/AEEE/article/view/762.

[16] Tremlet, Ch.: Industrial Systems Need Supplementary Protection by Safety Integrated Circuits. ATP Journal, 2013, No. 1. ISSN 1335-2237 (in Czech).

[17] NIST – Special Publication SP80-38a: Block Cipher Modes of Operation. http://csrs.nist.gov/publications/fips/fips197/fips197.pdf. Accessed March 2010.

[18] FIPS 197 AES Standard. http://csrs.nist.gov/publications/fips/fips197/fips197.pdf. Accessed March 2010.

[19] Stallings, W.: Cryptography and Network Security. Principles and Practice. Prentice Hall, 2011. ISBN 978-0-13-609-704-4.

[20] Levický, D.: Cryptography in Information and Network Security. Monograph. Elfa, 2010. ISBN 9788080861636 (in Slovak).

[21] Gaudry, P.: Index Calculations for Abelian Varieties of Small Dimension and the Elliptic Curve Discrete Logarithm Problem. Journal of Symbolic Computations, Vol. 44, 2009, No. 12, pp. 1690–1702. ISSN 0947-7171.

[22] Aumasson, J. P. et al.: Information Security and Cryptography. The Hash Function Blake. Springer-Verlag Berlin Heidelberg, 2014. ISBN 978-3-662-44757-4.

[23] Franeková, M.: Mathematical Apparatus for Safety Evaluation of Cryptography and Safety Codes Used in Safety-Related Communication System. Modern Transport Telematics: 11th International Conference on Transport Systems Telematics (TST 2011), Katowice-Ustrón, Poland, October 2011. Springer-Verlag Berlin Heidelberg, Communications in Computer and Information Science, Vol. 239, 2011, pp. 126–135. ISBN 978-3-642-24659-3.

[24] Klapka, Š.: Detection Codes in Interlocking Systems. Inaugural Dissertation Work. ČVUT Prague, 2009, 99 p. (in Czech).

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

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

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

[28] Karná, L.—Klapka, Š.: Message Doubling and Error Detection in the BSC Model. 23rd International Symposium EURO-ŽEL 2015 – Recent Challenges for European Railways – Symposium Proceedings. Žilina, Tribun EU, 2015, pp. 52–57. ISBN 978-80-263-0936-9.

[29] Torrieri, J.: Principles of Secure Communication Systems. Artech House, Norwood, MA, USA, 1992. ISBN 0-89006-555-1.

[30] Zelenka, J.—Rástočný, K.—Holečko, P.—Franeková, M.: Ratio Counter – Solution of Relation Between Safety and Availability of Communication System. IEEE International Conference on Applied Electronics, Pilsen, 2010, pp. 383–386. ISSN 1803-7232, ISBN 978-80-7043-865-7.

[31] EN 60812: Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA). 2006.

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 his Ph.D. in the field of safety analysis in 1995. Since 2008 he has been working as Professor in the Department of Control and Information Systems at the Faculty of Electrical Engineering, University of Žilina. His professional orientation covers solving problems in 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 Professor in 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 the control of safety-critical processes in transport (railway and road) and in industry.

Peter Holečko graduated at the Department of Information and Safety Systems of the Faculty of Electrical Engineering, University of Žilina in 2004. He received his Ph.D. degree at the University of Žilina in 2012 in the field of automation and specialisation on sensor networks. Currently he is working as an assistant at the Department of Control and Information Systems at the Faculty of Electrical Engineering, University of Žilina and his research interests include security of information systems and sensor networks.

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 Professor in 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.