Mechanics
Transport
Communications

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 13, issue 3/2, 2015

Academic journal http://www.mtc-aj.com article № 1213

MODELLING OF FAILURE EFFECTS WITHIN SAFETY- RELATED COMMUNICATIONS WITH SAFETY CODE FOR RAILWAY APPLICATIONS

Mária Franeková, Peter Lüley
maria.franekova@fel.uniza.sk, peter.luley@fel.uniza.sk

University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 010 26 Žilina
SLOVAK REPUBLIC

Key words: *Safety integrity level, railway applications, safety-related communications, safety code, CRC, Matlab, modeling*

Abstract: *The number of applications with higher SIL (Safety Integrity Level) for which is necessary to provide evidence of safety not only for hardware parts and software parts but also for the communication system is growing. The authors are in this papers dealing with the issue of safety-related communication and types of failures that may occur during transmission of safety-related messages. We focused on the requirements for the safety code according to standard EN 50159 with special attention to the cyclic code on the CRC principle. According to requirements of the standard it is necessary to demonstrate that transmission via real communication channel with safety code meets the required safety integrity level. Modeling has a significant role in this process, by mean of which, in particular for the case of time simulations of safety transmission is necessary to obtain parameters necessary for safety analysis. The main part is describing models of transmission system with cyclic redundancy in software tool Matlab with the support of Simulink to provide data for safety analyses and for the determination of the intensity of dangerous failure caused by the electromagnetic interference.*

INTRODUCTION

If the safety-related electronic system transfers information between different entities then the communication system is also part of a safety-related system and must be demonstrated that the transfer between end terminals is safe and in compliance with standard EN 50159 [1]. Safety-related communication system performs and fulfils safety functions with defined level of safety. Such a system includes a safety-related communication layer which contains all necessary mechanisms to ensure safety-related transfer of data [2]. Selection and use of a safety code and other recommended techniques depends on whether is the possible unauthorized access to the system or not. This fact is very significant because in case of possible unauthorized access (malicious attacks) it is necessary to use cryptographic techniques with secret key. If there is no possibility of unauthorized access to the transmission system it is used non-cryptographic safety code (type A0). If the unauthorized access is possible we can achieve the safety by the transmission functions related with safety with the use of cryptographic mechanisms (type A1). Further is for this case used term cryptographic safety code. In case of possible unauthorized access can be used separate access protection layer (type B0 or B1).

Corruption of the message during transmission can be caused by the network user, by the failure of transmission medium, by the interference of messages or by electromagnetic noise. Errors of this type are categorized as unintentional attacks. They can be detected by the CRC (Cyclic Redundancy Check) or by the CS (Check Sum). Evidence of safety with respect to the safety integrity level and the nature of the safety-related process must demonstrate appropriateness of:

- probability of the detection of random error types,
- ability to detect all types of expected message corruption systematic types.

Safety code must be independent of the transmission code what can be achieved in two ways. One is to use different encryption algorithms and the second is to use different configuration parameters of the same algorithm. To meet the required safety integrity level must be the probability of undetected errors below specified limit. Safety code must be able to detect transmission faults (e.g. impact of EMI) and systematic faults in untrusted transmission system caused by hardware failures. Safety code must also be able to detect these typical faults of transmission system:

- interrupted transmission line,
- all bits in logical 0,
- all bits in logical 1,
- negation of messages,
- loss of synchronization in case of serial transmission,
- random errors,
- systematic errors,
- combination of aforementioned errors.

In the paper we work with the message type A0 because we do not expect unauthorized access to the transmission system. Each message will be secured with non-cryptographic safety code CRC-r.

SAFETY ANALYSIS OF CRC CODE

Cyclic code is the most used code that can detect several multiple burst of errors. This code is one of the linear codes (n, k), for which is applicable the linearity property and also property that cyclic shift of code word creates again code word belonging to the code [3]. This feature is used in the construction of encoders, mainly by the use of linear shift register with feedback. From the group of cyclic codes in most communication protocols are used block systematic CRC codes marked CRC-r (where r is the number of redundant bits in the code word with length of n bits). For mathematical description of encoding, decoding, error detection and error correction is used algebra of polynomials [4].

If is used the safety code in transmission system it is necessary to demonstrate probability of undetected error during transmission below the limit defined by particular application or standard to ensure the required safety level. Therefore it is necessary to calculate the maximum value of probability of undetected error of code word in the transmission system for every safety code. In case of syndrome detecting techniques we look for event when syndrome is zero (error was not detected) but during the transmission of the code word occurred error. This case is mathematically expressed by probability of code word error p_{undet} depending on the error bit rate p_{b} of used channel. In the calculation is used statistical values of error bit rate of particular transmission speeds or if it is possible for particular application the channel is tested.

When calculating the probability of undetected errors are considered only errors arising due to interactions that cause the interchange of symbols. Errors to the improper synchronization are resolved by other safety means. The probability of undetected error for codes with unknown weight function can be calculated by following equation [5]:

(1) $$p_{un\det} \cong \frac{1}{2^{n-k}} \cdot \sum_{i=d\min}^{n} \binom{n}{i} p_b{}^i . (1-p_b)^{n-i} .$$

If the conjunction of n and p_b is much smaller than one (np_b << 1) the sum can be approximated by the first number of the sum. The equation 1 can be adjusted to following:

(2) $$p_{un\det} = \frac{1}{2^{n-k}} \cdot \binom{n}{d_{\min}} p_b{}^{d_{\min}} . (1-p_b)^{n-d_{\min}} ,$$

where:

- n – total number of code bits,
- k – number of information part bits,
- d_{min} – minimum Hamming distance,
- p_b – error bit rate of the communication channel.

The minimum Hamming distance d_{min} and the length of code word n are the basis for the construction of block codes. The systematic block code (n, k) has the upper limit of achievable minimal Hamming distance given by Varshamov-Gilbert inequality. For odd values of d_{min} applies equation 3 and for even values of d_{min} applies equation 4. Codes where these two equations are equal are called perfect codes [6].

(3) $$2^k \sum_{i=0}^{(d_{\min}-1)/2} \binom{n}{i} \leq 2^n ,$$

(4) $$2^k \sum_{i=0}^{(d_{\min}-2)/2} \binom{n-1}{i} \leq 2^{n-1} .$$

Error probability calculated according to the equation 2 limits to the value $2^{-(n-k)} = 2^{-r}$, what is the highest residual error rate of the code (equation 5). This value is stated as maximum value of undetected error for CRC-r codes [1]. The probability of undetected error can be then calculated by the following equation:

(5) $$p_{un\det} = 2^{-r} ,$$

where:

- r – number of redundant bits.

If the error is not detected by transmission code nor safety code while the data integrity was corrupted by EMI during the transmission of the message the intensity of dangerous failure caused by EMI λ_{EMI} is calculated according to equation 6 [3]:

(6) $$\lambda_{EMI} = p_{SC} \cdot p_{TC} \cdot f_{cor} ,$$

where:

- p_{SC} is the probability of undetected failure of safety code,
- p_{TC} is the probability of undetected failure of transmission code, p_{TC}=1 if the transmission system does not include a channel encoder and channel decoder of transmission code,
- f_{cor} is the frequency of occurrence of corrupted messages. In case of cyclic transmission of messages can be easily determined. In case of non-cyclic transmission

of messages is this value estimated or set to the worst case scenario – all messages generated from the source are corrupted.

PRACTICAL PART

Realized model of safety-related communication system with transmission code and safety code is shown in Fig. 1. In the figure is the scheme composed of seven blocks. Communication system consists of transmission system and two terminal equipment's TE_1 and TE_2. Transmission system is composed of a communication channel CCH, encoder of transmission code E_{TC}, decoder of transmission code D_{TC}, encoder of safety code E_{SC} and decoder of safety code D_{SC}. The transmission system is untrusted if it contains only a communication channel and transmission code. The safety integrity level can be in this case defined as SIL 0. To achieve higher level of safety integrity SIL 1 to SIL 4 we have to add safety code for elimination of communication erros which are not detected via transmission code. The SIL level depends on the selected safety code.

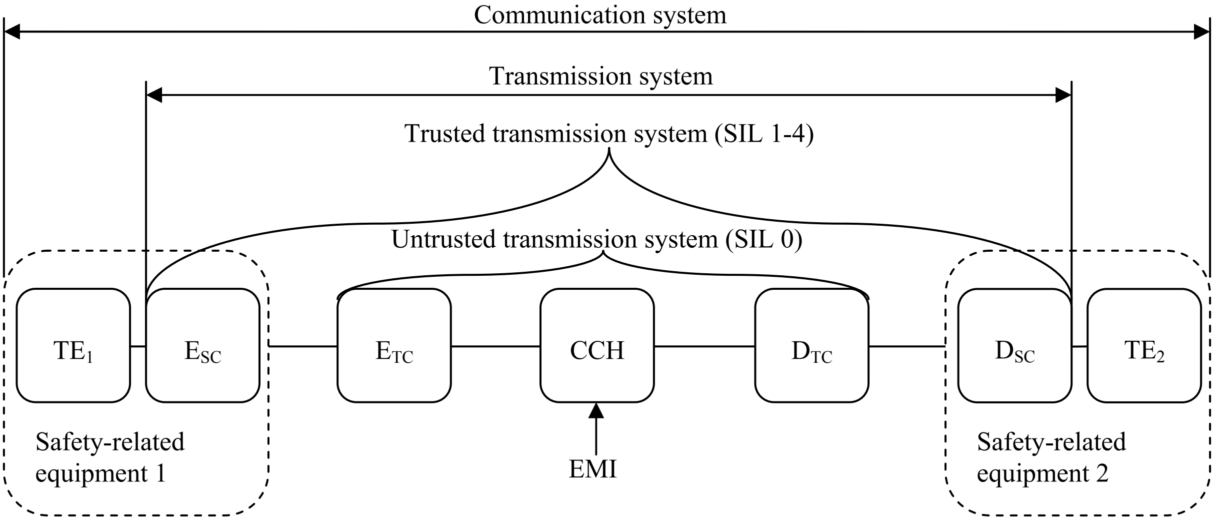
Communication system
Transmission system
Trusted transmission system (SIL 1-4)
Untrusted transmission system (SIL 0)
TE1
ESC
ETC
CCH
DTC
DSC
TE2
Safety-related equipment 1
EMI
Safety-related equipment 2

Fig. 1. Safety-related communication system for two-point connection

In Fig. 2 is shown the model simulating the transfer of *n* messages secured with safety code and transmission code which was constructed in software tool Matlab, version 7.10.0 (R2010a) and Communications System Toolbox library [7], [8].

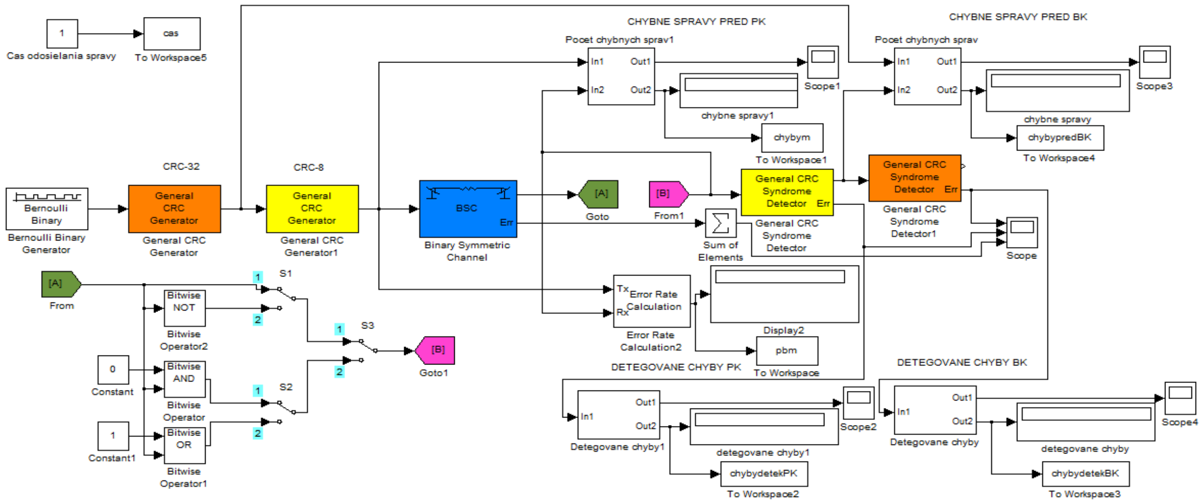

Fig. 2. Model with a safety code and transmission code realized in Matlab [7]

The model is constructed to simulate the transmission of messages through safety-related communication system secured by transmission code and safety code for two-point connection. From the point of view of ensuring the transmission we are using the safety code and transmission code based on CRC-r. Length of information part of the message was set to 64 bits. In order to ensure the independence of both types of codes was the generating polynomial of transmission code selected from standardized polynomials. For safety analysis we used generating polynomial of 8th degree type G(x)= x^8+x^2+x+1, which is used for example in ATM link protocol. Safety code generating polynomial was also selected from standardized polynomials for safety-related applications. There was selected polynomial of 32nd grade G(x)=$x^{32}+x^{30}+x^{27}+x^{25}+x^{22}+x^{20}+x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^4+1$, which is used for example by the European Train Control System ETCS and if used separately it provides integrity level SIL 2. Model is designed so that we can simulate different error pattern. To trigger them we use three switches (S1, S2, S3). If we want to simulate transmission where the messages are affected only by functional block of binary symmetric channel (which generates random errors) S1 must be in position 1, on the position of S2 does not matter and S3 must be in position 1. If we want to simulate transmission where the messages are affected by functional block of binary symmetric channel and subsequently negated the position of switches is as follows: S1 – position 2, S2 – does not matter, S3 – position 1. If we want to simulate transmission where all bits are set to logical 0 the position of switches is as follows: S1 – does not matter, S2 – position 1, S3 – position 2. If we want to simulate transmission where all bits are set to logical 1 the position of switches is as follows: S1 – does not matter, S2 – position 2, S3 – position 2.

OBTAINED RESULTS

During the time simulations of safety-related messages we were changing the bit error rate (BER) of the binary symmetric channel (BSC) by changing of BER in the range 1.10^{-8} to 0,5 (values less than 10^{-8} has shown very low error rate). Time of the simulation was set to 100000 s for every error bit rate of binary symmetric channel to simulate transfer of 100000 messages with length 104 bits (64 bits of information part, safety code 32 bits and transmission code 8 bits). Each second was sent one message. Results of simulations are shown in Tab. 1. [7].

Tab. 1 Generated, detected a not-detected corrupted messages for realized model

Total number of transferred messages: 100000.							
p_b [-]	1,00E-02	1,00E-03	1,00E-04	1,00E-05	1,00E-06	1,00E-07	1,00E-08
Corrupted messages before PK decoder	64731	9917	989	94	4	1	0
Detected corrupted messages by PK	64719	9917	989	94	4	1	0
Not-detected corrupted messages by PK	12	0	0	0	0	0	0
Corrupted messages before BK decoder	61592	9144	902	81	4	1	0
Detected corrupted messages by BK	61592	9144	902	81	4	1	0
Not-detected corrupted messages by BK	0	0	0	0	0	0	0

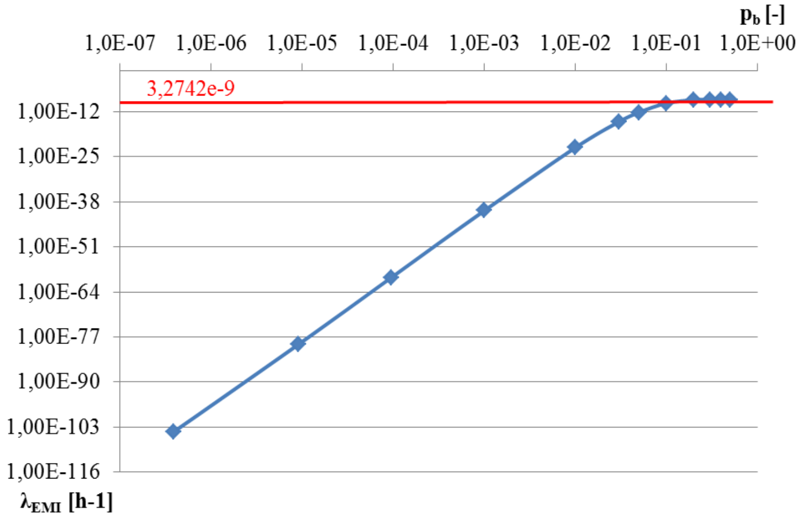

Fig. 4. Dependence of λ_{EMI} on p_b [5].

In the Fig. 2 is shown intensity of dangerous failures caused by EMI in closed transmission system which is assured by transmission and safety codes depending on the real BER of the communication channel. The value (3,2742e-9) is the worst intensity of dangerous failure. This is calculated as conjunction of the value of worst probability of transmission code (2^{-8}), value of worst probability of safety code and (2^{-32}) and the frequency of corrupted massages, when all messages are considered as corrupted (3600). This implies that such transmission system complies with requirements for the safety intensity level SIL 4 classified for all system with high demand ($10^{-9} \leq \text{THR} \leq 10^{-8}$).

CONCLUSION

The main part of the article was orientated to model realization that simulates transmission of safety-related messages via communication system with closed transmission system at the level of two-point connection. We simulated transfer of messages for various settings of bit error rate of communication channel (model BSC). We also simulated transfer of messages in extreme fault condition as inversion of the message, all bits in logical 0 and all bits in logical 1. We applied limited binary error channel to test the integrity of the transfer with CRC-r safety code and transmission code for various lengths of simulated burst of errors. To obtain information on the probability of undetected error in transmission code and safety code and on the intensity of dangerous failure from the motel we created program with graphical interface. To calculate the probability of undetected error for any block code (n, k) was created a supporting program that displays the probability of undetected error for selected interval of error bit rate. We can see from the measured and calculated values obtained by the simulation that with increasing error bit rate is increasing also intensity of dangerous failures. Transmission code did not detect all corrupted messages therefore it is necessary to use safety code independent on transmission code in safety-related applications. CRC is not able to detect errors if all bits are logical 0.

ACKNOWLEDGEMENTS

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) 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.

REFERENCES

[1] EN 50159: Railway applications – Communication, signalling and processing systems. Safety-related communications. CENELEC. 2010

[2] CHERNEVA G- E. DIMKINOVA: An Invariance of the Performance of Noise-Resistance of Spread Spectrum Signals. Proceedings of the 9th International Journal on Marine Navigation and Safety of Sea Transportation, vol.5,N 2, 2011. ISSN 2083-6473, Poland, p.183-186.

[3] FRANEKOVÁ, M.- PIRNÍK, R.- PEKÁR, Ľ: Modelling of data transmission via Matlab, Simulink, Communication Toolbox. Textbook. In: Slovak, University of Žilina, 2014, ISBN 978-80-554-0896-5

[4] MUZIKÁŘOVÁ, Ľ. – FRÁNEKOVÁ, M.: Theory of information and signals. Textbook. In: Slovak. University of Žilina, 2009, ISBN 978-80-554-0075-4.

[5] FRANEKOVÁ, M.- KÁLLAY, F.- PENIAK, P., VESTENICKÝ, P.: Safety communication of industrial networks. Monograph. In: Slovak, EDIS - ŽU Žilina, 2007, ISBN 978-80-8070-715-6

[6] CLARK, C. – G. CAIN, J. B.: Error – Correcting Codes for Digital Communications. Plenum Press, New York, 1988, ISBN 0-306-40615-2.

[7] CAUNER, R.: Models of transmission systems with cyclic code generation via SW tool Matlab for safety-related applications. In: Slovak. Diploma work, University of Žilina, 2015

[8] CHERNEVA G.- ANDONOV A.: Simulation and Examination of a Direct Sequence Spreed Spectrum System Using Matlab/Simulink. Proceedings of the XLIV International Scientific Conference Information, Communication and Energy Systems and Technologies ICEST 2009, 25-27.06.2009, p.619-622

МОДЕЛИРАНЕ НА РИСКОВИ СИТУАЦИИ, СВЪРЗАНИ С БЕЗОПАСНОСТТА НА ДВИЖЕНИЕТО – ПРИЛОЖЕНИЕ НА КОМУНИКАЦИОННИ ТЕХНОЛОГИИ С КОДОВЕ ЗА БЕЗОПАСНОСТ В ЖЕЛЕЗОПЪТНИЯ ТРАНСПОРТ

Mária Franeková, Peter Lüley
maria.franekova@fel.uniza.sk, peter.luley@fel.uniza.sk

Жилински Университет, Факултет по Електроенергетика, Жилина
СЛОВАКИЯ

Ключови думи: *ниво на безопасност, приложения в жп транспорт, комуникационни приложения за безопасност, код за безопасност, CRC, Matlab, моделиране.*

Резюме: *През последните години непрекъснато се увеличава броят на комункационните приложения с високо ниво на безопасност, като нараства необходимостта от създаване не само на хардуерни, но и софтуерни решения. Настоящата статия разглежда основните типове комуникационни приложения за безопасност, както и рисковете, които могат да възникват при предването на съобщения чрез тях. Вниманието е фокусирано върхи изискванията, на които трябва да отговарят тези кодове за безопасност съгласно стандарт EN 50159, като акцент се поставя върху цикличен код CRC. Според изискванията на стандарта, трябва да се докаже, че съобщението, което реално се пренася по комуникационния канал съответства на утвърденото ниво на безопасност. В тази връзка процесът на моделиране има ключова роля, тъй като служи за получаване на съответните параметри за безопасност при извършване на анализа. Основната цел на разработката е да представи модел на преносни системи за безопасност с циклични съкращения с помощта на софтуерните програми Matlab и Simulink, чрез които могат да се извършват анализи за определяне на опасните рискове от електромагнитни смущения в железопътния транспорт.*