MODELLING OF DISTURBING EFFECTS WITHIN COMMUNICATION CHANNEL FOR SAFETY- RELATED COMMUNICATION SYSTEMS

M. Franeková, K. Rástočný

Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Univerzitná 1, 010 26 Žilina, tel.: +421 41 513 3346, mail: maria.franekova@fel.uniza.sk, tel.: +421 41 513 3320, mail: karol.rastocny@fel.uniza.sk

Summary The aim of the paper is using of modelling within development of safety–related communication systems presented in the areas where guaranty of safety integrity level is required. In the paper basic principles used in the process of safety evaluation in closed transmission systems are summarised. Dangerous states of system are mainly caused by random failures of HW within non-trusted transmission system, by electromagnetic interference caused with noise or interferences and by systematic failures within specification of system. Main part of paper describes the simulation of disturbing effects within communication channel via programme Matlab, relations for determination of probability of undetected errors of code words with using block codes and results of residual error rate for Hamming code.

1. INTRODUCTION

For achievement of safety goal within communication it is recommended the safety functions to apply, which support safety and perform with using seemly selected safety mechanisms. Safety mechanisms can be implemented in SW (control access to system, using of passwords, mechanisms on base of cryptography...), in HW (cipher modules, authentication and identification cart...), by physical means (safe deposit box, interlocks,...) or by administration measures (norms, legislations, certification authority,...) [1].

In many cases communication system is a component part of system which participates in control of safety-critical processes. Undetected corruption of data transmission (e.g. control commands) can cause considerable substantially damages within equipments, environments or demands on human health and this is the reason why system has to be designed to guarantee required *Safety Integrity Level* (SIL). COTS (*Commercial Off-The-Shelf*) communication technologies are essentially not available (without supplementary technical measures) for transmission safety-related data, although their transmission systems involve detection and correction methods for assurance of transmission, eventually other protective mechanisms. Concerning to safety of transmission, these systems are denoted as non-trusted. Which types of additional technical measures are necessary to apply depends on the risk analysis results (analysis of attacks and their effects) related with controlled process and on the acceptable risk.

Standard IEC 61508 [2] defines general principles valid for implementation of safety rules with the use *Electrical, Electronic, Programmable-Electronic* (E/E/PE) systems. In standard notices general requirements for achieving functional safety of safety-related system include communication part. Norms for area of control interlocking systems define communication safety within using closed ČSN EN 50159-1 [3] and open ČSN EN 50159-2 [4] transmission system. For railway applications the seven types of open transmission systems according to [4] are defined.

In area of conventional industry networks Fieldbus technology has been became the standard for area of safety-related application [5]. On the present the number of vendors of safety- related communications technologies is increased. Vendors guarantee without standard communication, communication between safety- related equipments according to [2]. At the present time proposal of standard IEC 61784-3 [6] is prepared, which deals in definition of functional safety for industry networks used in area of measuring and control systems.

Modelling fulfils very important tasks in the area of requirements specification to system, in process of structure design and production of communication system and also in process of its verification and validation. In some cases modelling may help to optimalize options or setting of parameters within existing communication systems so, those requirements to safety integrity level and availability, which are defined by customer or they are result of the risk analysis, would be accepted. Achievement of these tasks generally requires combinations of suitable modelling methods and tools. Generally in these cases an abstract model is creating which graphically or mathematically describes features of transmission system. It is advantageous when development of safety–related communication system is based on modelling methods using (for define phases of system development it is necessary). In principle safety-related features of communication system modelling are possible to separate into following parts:

- *Modelling of functional characteristics of communication protocol.*

In this case model on the base of semi-formal and formal methods forms (they are usually supported by SW tools), which consistent, explicit

and logical descriptions helps to create the functional possibilities of system. In this area can be used object oriented modelling (OOM). More suitable technique for this type of model design is unified modelling language (UML), which supports different modelling and visualisation elements [7].

- *Modelling of disturbing effects within communication channel.*

In this case model describes effects of *Electromagnetic Interference* (EMI) and failures occur in communication channel. Result of solution is choosing of criteria for selection of transmission and safety codes according to required SIL and calculation of residual error rate of decoders [8].

- *Modelling of failure effects in transmission system.*

In this case model for failure effects analysis, this can be realised on the base of quantitative and qualitative methods [9], [10].

Next part of this paper is devoted to the tasks of disturbing effects within communication channel modelling.

2. MODELLING OF DISTURBING EFFECTS WITHIN COMMUNICATION CHANNEL

On the Figure 1 structure of closed transmission system according to [3] is illustrated, in which safety-related equipments SRE1 and SRE2 are connected. These equipments communicate via safety-related messages. Safety-related equipments are created with two layers:

- layer of application process,
- layer of safety-related transmission.

Note: For open transmission system it is necessary to implement into safety- related equipment layer of safety- related access.

In the Figure 1 transmission between SRE1 and SRE 2 are realised across non-trusted (commercial) transmission system. For example within control system in industry or process automation can go about DeviceNet, Profibus or Ethernet. Non-trusted transmission system in the Figure 1 is understand in safety conception as black box, although in lower layers of communication protocol have to implement detection or correction mechanisms called as transmission code. Consequently the communication can be assured within layer of safety-related transmission by safety code, which detects all errors which were not detected in commercial transmission systems.

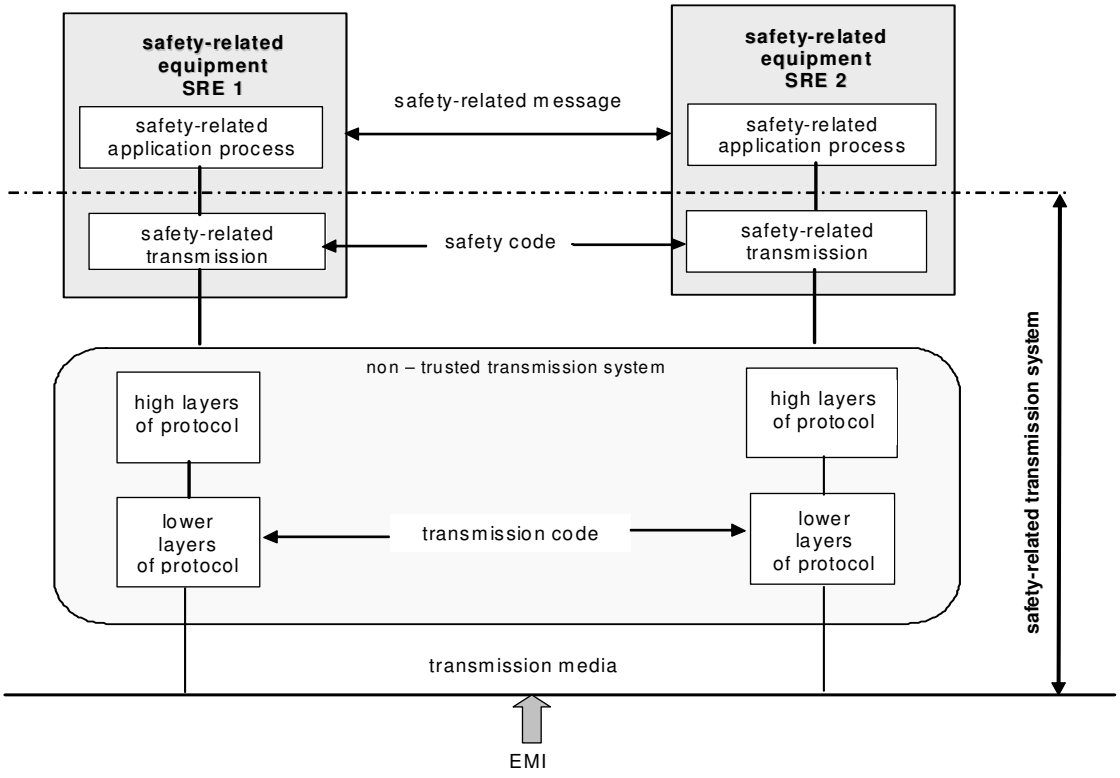

Fig. 1 Principle of safety- related transmission across closed transmission system

Communication channel affects transmission messages by noise, interferences or can cause fading of useful signal. These effects are generally marked as disturbance caused by *Electromagnetic Interference* (EMI) and they have strong effect to value of intensity of undetected (corrupted) messages. Effect of noise can have different form which depends mainly on physical characteristic of channel. Undesirable effect of EMI is possible eliminate with using safety and transmission code.

EMI causes in messages transmitted across communication channel errors of two types:

- replacing of one symbol within transmitted message another symbol;
- dropout of symbol, eventually filling up new symbol (failure of synchronisation).

EMI is result of variety different effects, which can not be described deterministically. This is way the models of communication channels are based on probabilistic characteristics.

Consequently effect of EMI depends on concrete type of disturbing within communication channel (simply – independent errors, burst of errors or combination errors) and on detection characteristic of transmission and safety code.

On the present many techniques of channel coding exist [11], [12]. Within safety-related communication systems block systematic (*n*,*k*) codes are frequently used. In norms are recommended using of detection codes or correction codes with modified algorithm of decoding, which decoding process finish with detection. Relations for determination of undetected errors in code word (residual error rate of decoders) are very often derive providing that mathematically model of BSC (*Binary Symmetric Channel*) are used or AWGN (*Aditive White Gaussian Noise*) channel. During determination of residual error rate of block code can used statistical results of *Bit Error Rate* (BER) of typical communication channels, which are listed in tables. In many cases we prefer to realise the test of channel (if it application enables) or result of BER to predict by simulation of transmission with the used appropriated model of communication channel. On the Figure 2 model of determination of BER of communication channel (block *Error Meter*), which is realised via Matlab, Simulink, Communications Toolbox Lmtb-err (*Limited Binary Error Channel*) is illustrated [13]. Without basic characteristic BER (marked as p_b) via model Lmtb-err of channel we can simulate probability occurrence of i-multiply errors within transmission p_i (for pre i = 1,2,...,n), i. e. probability P, that i-multiply errors is occurred with value higher than h:

$$p_i = P(i > h) \tag{1}$$

On the Figure 3 error pattern of channel is illustrated for time interval from 750 to 1000 *s*. Vertical axle illustrates number of occurred i-multiply errors. During monitoring time interval is simulated transmission of 1, 2 and 3 – multiple errors, between which is minimal *Safety Interval* (SI), what is possible to express by random characteristic p_{SI}. Characteristic expresses that between two errors is number of fault received elements of signal $\overline{n_{ch}}$ higher than value x (2):

$$p_{SI} = P(\overline{n_{ch}} > x) \tag{2}$$

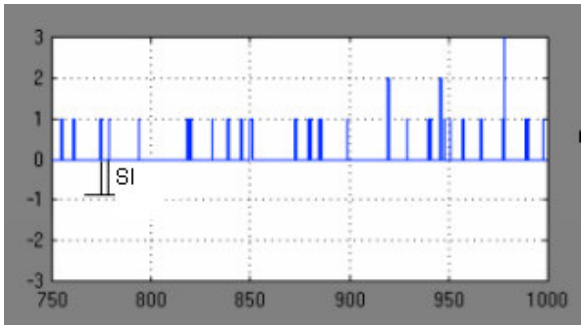

Fig. 3 Example of error pattern

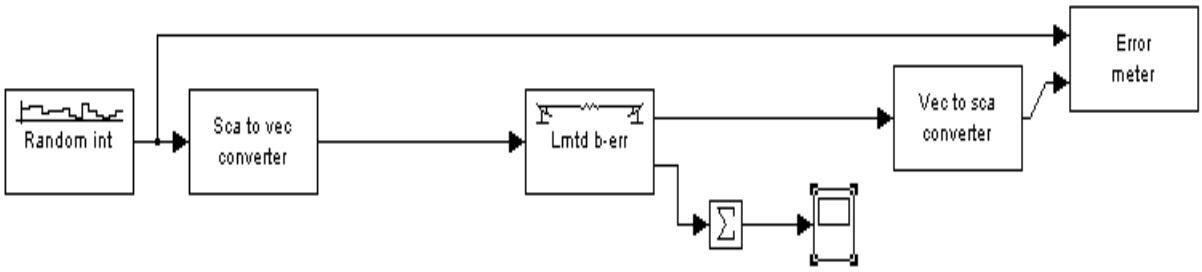

Fig. 2 Model for testing characteristics of BSC channel

Characteristic defined by relations (1), (2) are useful in process of safety block code (n, k) selection. Characteristic BER determines quality of communication channel, therefore tendency is within transmission chain to connect this type of channel coder/decoder, which eliminates number of occurred error to required value. Characteristics p_i a p_{SI} are used in praxis for determination of other important parameters of block code. On the base of value p_i we can determine number of redundant elements, which are necessary for error detection/correction and characteristic p_{SI} is used for determination of safety interval between errors, according to selected codeword length.

3. DETERMINATION OF RESIDUAL ERROR RATE OF BLOCK CODES

In relations of probability of undetected errors we assume errors, which are effect by EMI only, i.e. errors evoke the cross change of symbols. Father we assume that errors, which are effect by synchronisation's problem are solved by other safety mechanisms, for example in process of control transmitter and receiver within time signature. Effect of EMI manipulates the summary value of intensity of failures within transmission system.

During determination of probability of undetected errors it is necessary to use relations for concrete transmission or safety code, e.g. Hamming, Reed-Solomon (if it application enables) and only in extreme situation to choice generally relations, which are applicable for all group of block (n, k,) codes. During determination certainly inaccuracy occur because in process of mathematical derive of probability of undetected error of code word is assumed that occurred errors are independent and their occurrence can be approximated by probability density according binomic distribution, what also may not be able in unify with analysed situation. The most used transmission and safety code in communication protocols of communication Technologies COTS and in safety related layer too is systematic cyclic code, which is worked on principle of CRC (*Cyclic Redundancy Check*), for which we can probability of undetected error of code word p_u determine according to:

$$p_U \cong \frac{1}{2^{n-k}} \sum_{i=d_{\min}}^{n} \binom{n}{i} p_b{}^i (1-p_b)^{n-i}, \tag{3}$$

where d_{min} is minimal Hamming distance of code, n is code word length, k is length of information word , p_b is bit error rate of channel.

If condition satisfies $n.p_b \ll 1$, than can approximate sum (3) by the first element of sum:

$$p_U \cong \frac{1}{2^{n-k}} \binom{n}{d_{\min}} p_b{}^{d_{\min}} (1-p_b)^{n-d_{\min}}. \tag{4}$$

In relation (4) it is necessary to know without parameters (n, k) also minimum Hamming distance of code words. If this value is unknown we can use for determination of $d_{\min}$ Gilbert's inequality according to (5) and (6).

$$2^k \sum_{i=0}^{(d_{min}-1)/2} \binom{n}{i} \le 2^n, \tag{5}$$

for $d_{\min}$ odd and

$$2^k \sum_{i=0}^{(d_{min}-2)/2} \binom{n-1}{i} \le 2^{n-1}, \tag{6}$$

for $d_{\min}$ even.

Selection of generate polynomial of cyclic code should be inspire by pattern errors, which are in concrete link very often occur. This is way it is necessary the first to test link and determine without basic characteristic p_b probability of i-multiply errors. Chosen degree of generate polynomial $r = (n-k)$ relates with requirement to length of burst detection. In safety-related application the requirement of independence of transmission and safety codes can be valid also, what in case of use CRC denote restriction of use standardised types of generative polynomials which are used in COST systems.

It is necessary to underline, that in group of block (n,k) codes exist family of codes, for which is not problem to determine number of code words A_i with weight i. In this group we can range for example Hamming codes or Reed - Solomon codes. If communication protocol uses this type of code, then the result of probability of undetected error of codeword determined by (7) is exactness.

$$p_U \le \sum_{i=\left\|\frac{d_{min}+1}{2}\right\|}^{n} A_i p_b{}^i (1-p_b)^{n-i}, \tag{7}$$

where A_i is number of code words with weight i and $\|x\|$ marked integer part from value x.

Consequential values of probability of undetected error for Hamming (128,120) code are illustrated in the Figure 4. Probability of error p_u is determined according to relation (7). Weight function of Hamming code (128, 120) according to (10) is determined via programme MATLAB.

$$A(x) = \frac{1}{n+1}\left[(1+x)^n + n(1+x)^{(n-1)/2}.(1-x)^{(n+1)/2}\right] \tag{8}$$

Coefficients of weight function of Hamming code (128, 120) are calculated with the use programme DERIVE. Curve on the Figure 4 is destined to value $p_U = 2^{-(n-k)} = 2^{-r}$, what is the highest residual error rate of code. This case to occur in assuming that bit error rate of binary data transmission is $p_b = 2^{-1}$. This value is mentioned in norm [4], as the worst case for block CRC-*r* codes. It is necessary to underline that this value is about several orders higher as in application when we can use strictly relations.

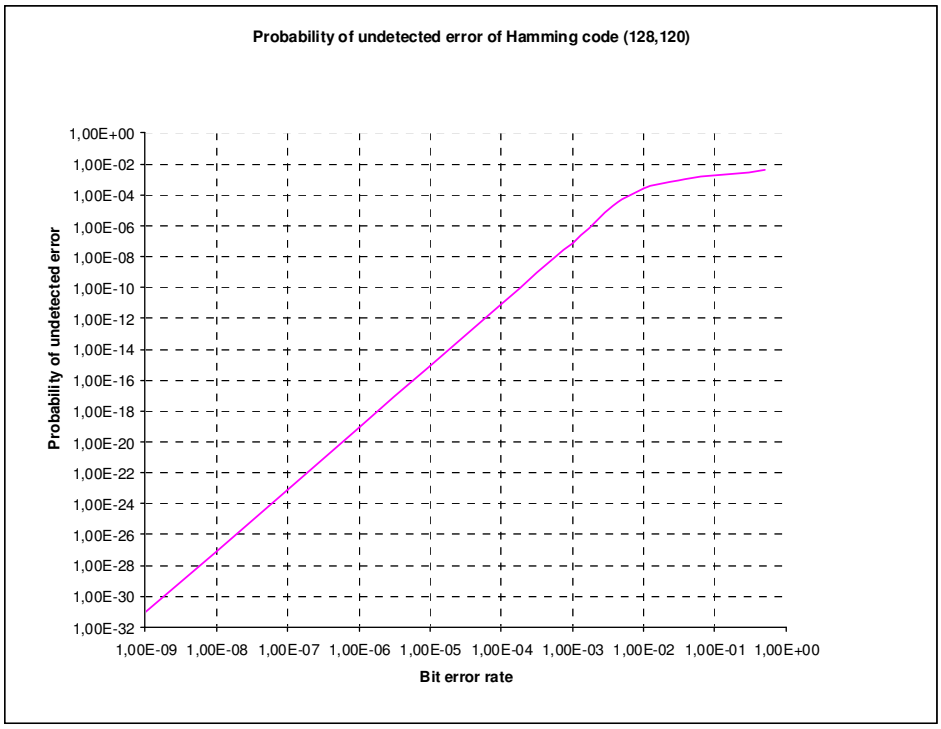

Fig.4 Results of probability of undetected errors of Hamming code (128,120)

4. CONCLUSION

Generally value $p_u = 2^{-r}$ is mentioned within majority safety analyses of transmission systems. Thereby requirement that during all life time of communication system not allow be bit error rate higher as was considered within certificate of safety is automatically fulfil. In theory of channel code the weight functions are known for reduced group of block codes so called perfect codes, in which are validated couples of (*n*, *k*). In praxes we must very often to choice another codeword length *n*, i. e. the use not valid couples (*n*, *k*). Then is necessary to determine values of probability of errors for all used length of safety code *n* and to verify, if satisfy requirement to demand SIL.

For open transmission system it is necessary to implement into safety-related equipment communication layer of safety access, which is generally based on the principles and methods of cryptography [14].

This paper was supported by grant of Slovak Research and Development Agency, Number: APVV - 20-P00705: "General-purpose inteligent controller for road traffic control" and Culture and Educational Grant Agency of Slovak Republic, Number: K-057-06-00:"Innovation of methods of laboratory education on the base of modelling and simulation via Matlab in combination of education models within area of e-learning".

REFERENCES

[1] LEVICKÝ, D.: *Kryptografia v informačnej bezpečnosti*. Elfa Košice, 2005, ISBN 80-8086-022

[2] EN 61508: *Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems*. 1998

[3] EN 50 159 - 1: *Railway applications: Communication, signalling, and processing systems - Part 1: Safety-related communication in closed transmission systems.*

[4] EN 50159 - 2: *Railway applications: Communication, signalling and processing systems - Part 2: Safety - related communication in open transmission systems.*

[5] MAHALIK, N. P.: *Fieldbus technology, Industrial network standard for Real-Time Distributed Control*. Springer, 2003

[6] IEC 61784-3: *Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks*. Draft 2006

[7] RASTOČNÝ, K., JANOTA, A., ZAHRADNÍK, J.: *The Use of Development of a Railway Interlocking Integration of Software Specification Techniques for Applications in Engineering*. Springer-Verlag Heidelberg, 2004, ISBN 3-540-23135-8

[8] FRANEKOVÁ, M: *Modelovanie komunikačných systémov v prostredí Matlab, Communications Toolbox a Simulink. Žilinská univerzita*. 2003, ISBN 80-8070-027-3

[9] RÁSTOČNÝ, K.: *Modelling of Failure Effects to Integrity of System*. AEEE No. 2 Vol.3/2004, ŽU v Žiline, pp. 91-94, ISSN 1336-1376

[10] ZAHRADNÍK, J., RÁSTOČNÝ, K., KUNHART, M.: *Bezpečnosť železničných zabezpečovacích systémov*. EDIS, ŽU v Žiline, 2006, ISBN 80-8070-546-1

[11] CLARC, C. C., CAIN, J. B.: *Error - Correcting Codes for Digital Communications*. Plenum Press New York, 1988, ISBN

[12] FARKAŠ, P.: *Kódovanie a modulácie*. STU Bratislava, 1993

[13] MATLAB, *Communications Blockset, User's Guide*. version 6.0 Release12, The Math Works, 2000

[14] STALLINGS, W.: *Cryptography and Network Security*. PrenticeHall, New Jersey, 2003