ANNALS of Faculty Engineering Hunedoara
International Journal of Engineering
ISSN: 1584 - 2665

EVALUATION OF SAFETY CODES USED IN SAFETY-RELATED INDUSTRIAL COMMUNICATION SYSTEMS

Mária FRANEKOVÁ

University of Žilina, Faculty of Electrical Engineering, Department of Control and Information Systems, Žilina, SLOVAKIA

ABSTRACT:
The paper deals with a methodology of safety codes evaluation used in safety-related industrial communication systems. The problems of determining the probability of undetected error of block detection codes used in practice are mentioned in comparison with theoretical knowledge. The main part is oriented to description of mathematical apparatus for determination of weight structure of safety codes and residual error probabilities and proposal of methodology and procedures for quantitative safety analysis of safety codes.
KEY WORDS:
industrial communication system, safety integrity level, safety code, probability of undetected error, weight structure, binary symmetric channel

1. INTRODUCTION

In the case if communication system is a component part of electronic system which participates in control of safety-critical processes (SCP), the system has to be designed to guarantee the required safety integrity level (SIL). Safety-related (SR) communication cannot be based on the principle of COTS (Commercial Off-The-Shelf) communication technology. For keeping off message integrity corruption in consequence of EMI (Electromagnetic Interferences) in transmission channel it is recommended to use without a transmission code (implemented in standard layer in communication protocol) a safety code, which is situated in the safety layer. Undetected corruption of data transmission (e.g. control commands in SCS) can cause considerable damages within equipments, environments or human health. In these applications it is necessary to perform the proof of system safety (in the phase of system development). Safety codes are one of very important techniques in SR applications. The first aim, which we regard within selection of safety code, is keeping of data integrity, but the safety code can be used for data authentication, too. In the process of quantitative analysis of a SR system it is necessary to determine the safety features of the code, mainly the failure probability of the code. Within the scope of communication system it is necessary to keep the proof of all safety functions operating in a concrete application during limited time (so called life time of system). The probability of SR function operation is represented by integrity of safety against random failures of system. In the case of using the SR system in continuous operation SIL defines the probability of failure per hour (PFH) related to one safety function, which is accepted in the SR system. Standard IEC 61508 [1] defines four levels of SIL from 4 to 1, whereby SIL 4 is the highest integrity level and SIL 1 the lowest level. A communication system with SIL 0 is safety – irrelevant.

2. RECOMMENDATIONS FOR USING SAFETY CODES IN INDUSTRIAL APPLICATIONS

The problem of SR communication systems analysis and synthesis is in detail described for the area of railway control systems. In this area the requirements on safety codes used in process of data transmission are described in norms EN 50159-1 [2] (for closed transmission systems), EN 50159-2 [3] (for open systems) and in norm EN 50128 [4] for assurance of SW integrity. Similar practice the norms for another resorts copy, where are required SR access, e. g. area of industrial automation. On the present increase of the number of the safety-related communication technologies vendors, who guarantee besides standard communication, communication among safety- related equipment according to [1]. The recommendations for using safety codes in SR industrial networks are described

in the IEC 61784-3 standard [5], which deals in definition of functional safety for industrial networks within digital communications used in the area of measuring and control systems in industry. Among first manufacturers that begin to use the safety principles in development of safety networks are vendors of Communication Profile Family CPF 1 (Safety Foundation), CPF 2 (CIP Safety), CPF 3 (ProfiSafe) a CPF 6 (Interbus Safety. The number of SR communication profiles will be increasing in the future. The model of SR message corresponding to the SR equipment used in industry is illustrated in the Figure 1.

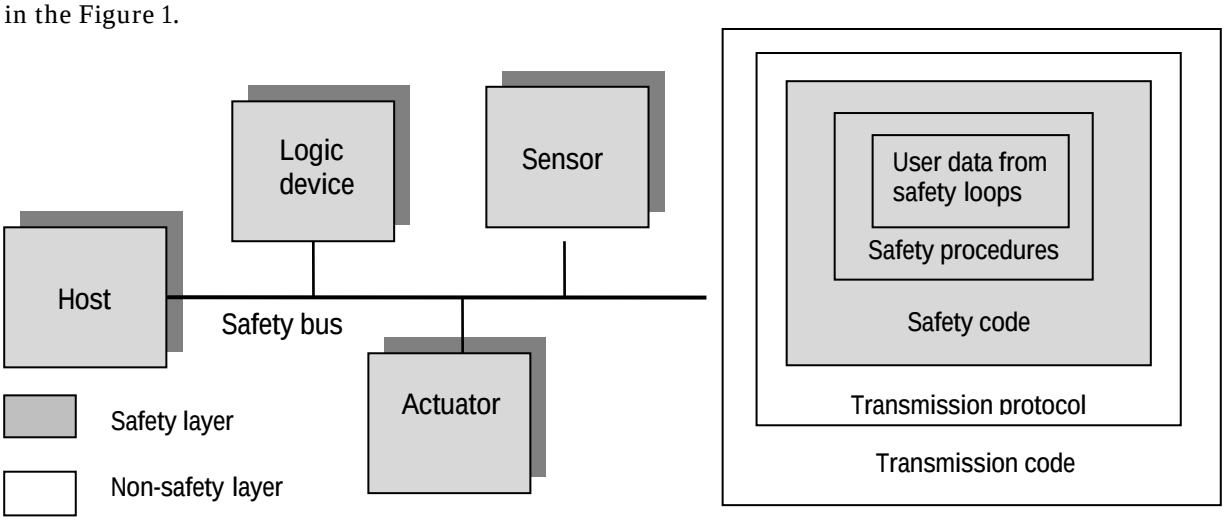

Figure 1. Model of a SR message with relation to the SR industrial equipment

In all referred examples of SR communication we must define the requirements on safety code, whereby the recommended are focused on detection channel techniques only. In the case of using safety code the following safety features of the code must be proofed: the possibility to detect random error, systematic error, burst of errors and combination pattern, possibility to detect all bits with log 1 and all bits with log 0 and inversion of message. The probability of undetected error of code must be under a guaranteed level. Hereby the independence of safety and transmission code must by keep.

3. PROBLEMS OF PROBABILITY OF UNDETECTED ERROR DETERMINATION IN PRACTICAL APPLICATIONS

In process of evaluation of safety properties of block detection codes in technical literature two parameters are used: minimal Hamming distance of code $d_{\min}$ and probability of undetected error of code words with the length n. Majority of presented results are connected to certain concrete class of codes (e. g. Hamming, RS codes) and results of decoder fault p_e are valid for certain situations and simplified conditions, which is not applicable in practice. The next problems are that presented theoretical proceedings are valid for a certain construction length of code, what is unusable in practice. The telegrams in communication protocols have exactly defined length of transmitted messages and in many cases it is necessary to verify the codes with short lengths, which have different safety properties as their original. This is why some relations for determination of p_e are very often unusable because of difficult calculation methods, too (especially for large code word length). For this case parallel processing methods and special computation tools are possible to use. This is why the safety analysis of safety codes used in practice is very often difficult and we must come out from pessimistic estimation of probability of corrupted messages only, a so called upper estimation. The probability of undetected error of code word p_e is depending on bit error rate p_b of used a transmission channel. In practise different types of transmission channel have different value of p_b and different behaviour of noise in concrete media. In many cases the transmission channel testing is not possible. The transmission channel can effect the transmitted messages by noise, interference or by fading of signal. These effects are generally referred to as EMI (Electromagnetic Interference) and they have significant influence on the value of intensity of corrupted messages.

EMI results from different influences, which cannot be described by deterministic relations. Relations for determination of probability of undetected error of code assume the occurrence of EMI (replacing of one symbol of transmitted message by another symbol) only. Within monitoring of EMI effects to all value of intensity of failure is tendency to maximally approximate the analysed situation by the mathematical expression. During the determination of p_e the statistical values of bit error rate

in typical transmission media are very often used.

When we know the value p_b (finding by testing in real conditions or as a statistical value) it is very important to determine p_e in dependence on p_b for all telegrams lengths used in communication protocol and to prove the monotonicity of function for p_b from 0 to 0,5. In many cases the function is not monotone, what can effect the hazard and the occurrence of dangerous states. For some types of telegrams lengths the value p_e very often exceeds the upper estimation.

The next problem within the real situations is determination of number of redundant bits in the safety code for keeping the required safety integrity level. Very often an idea is dominant the bigger number the better safety features while not keeping the other parameters and it is not true. In some applications very often another supplementary procedure increases the safety of transmission (e. g. double assurance of message in direct and inverse others of message symbols by two different codes).

4. EXAMPLES OF USING SAFETY CODES

The most widely used safety code in safety-related industrial communication systems is binary cyclic detection codes CRC (Cyclic Redundant Check), which ensures the integrity of all safety transfers. The safety CRCs serve as the primary measure to detect possible corruption of transmitted data. In safety-related industrial networks based on CIP Safety (CPF2) there are four safety CRCs used in the safety protocol:

- a 8-bit CRC-S1 or CRC-S2 - used for the data section connections containing up to two bytes of safety data and the time stamp,
- a 16-bit CRC-3 - used for data section for 3 to 250 bytes of data and for the time correction and time coordination messages,
- 32-bit CRC-S4 - used for connection establishment, configuration and the safety extension to the EDE file definition.

Table1 shows the polynomials used in CIP Safety protocol.

Table 1: Generating polynomials used in CIP Safety protocol

CRC	Application	Generating polynomials G(x)
CRC-S1	Short data section (actual data) Time stamp section	$x^8+x^5+x^4+x^2+x+1$
CRC-S2	Short data section (inverse data)	$x^8+x^5+x^4+x^3+x+1$
CRC-S3	Long data section (actual and inverse data) Time correction and coordination sections	$x^{16}+x^{11}+x^3+x^2+x+1$
CRC-S4	Configuration of equipment and connection establishment	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

In the ProfiSafe safety profile developed for industrial network Profibus and ProfiNet within fail-safe PDU the safety CRCs are used too. Also the CRCs mechanism is used as an effective safety technique for signature determination (from data before transmission and from data during parameterisations and configuration of equipment).

Within ProfiSafe profile four types of CRCs is defined:

- CRC_s-0 - used for data integrity check of GSD in F-Device equipment,
- CRC_s-1 - used for calculation of the signature from F-parameters,
- CRC_s -2 - used for data integrity check in all F-PDU,
- CRC_s-3 - used for data integrity check of initial parameters of F-Device.

Mechanisms of calculation of CRC_s type in the CIP Safety protocol and the Profisafe profile are described in detail e. g. in [6].

5. PROPOSAL OF PROCEDURES FOR DETERMINATION OF PROBABILITY OF UNDETECTED ERROR OF SAFETY CODES

A manufacturer may choose various calculation methods for providing estimates for the data integrity mechanisms of industrial networks. The results of these calculations may lead to either more effort in the design of hardware and software to provide integrity or more effort in the calculation and proof of the reliability of the overall control system.

The determination of probability of undetected error in code word of length n (so called residual error rate) for CRC_s code can be calculated if we suppose a simplified communication error in transmission channel (noise, cross-talk) or burst interferences. The residual error rate is calculated from the residual error probability of the superimposed (safety) data integrity assurance mechanism

and the transmission rate of safety relevant messages. The relations are based on the simplifying assumption of an equal bit error probability p_b for the corrupted bits within a message worst case residual error probability.

Some approach of determination of residual error probability [7] needs to know all code words of code. Then the probability of undetected sequence error p_{e1} for Binary Symmetric Channel (BSC) can be calculated according to (1):

$$p_{e1} = \sum_{i=\left\| \frac{d_{\min}+1}{2} \right\|}^{n} A_i \, p_b^{\,i} (1 - p_b)^{n-i}, \tag{1}$$

where:

d_{min} is the minimal Hamming distance of code

A_i is the total number of sequences in the code words with weigh of i

p_b is the bit error rate of channel

A few classes of safety codes for which the complete weight function of code words $A(x)$ is known only, where $A(x)$ is the weight-enumerating function of a code:

$$A(x) = \sum_{i=0}^{n} A_i x^i \tag{2}$$

To this class belong e. g the binary linear Hamming perfect (n,k) codes, Reed - Solomon (RS) codes over Galois field GF(q).

The weight-enumerating function for the distance-3 Hamming codes of code words length $n=2^r-1$ (where, r is number of redundancy bits) is:

$$A(x) = \frac{1}{n+1}\left[(1+x)^n + n(1+x)^{(n-1)/2}.(1-x)^{(n-1)/2}\right] \tag{3}$$

The weight-enumerating function of Reed-Solomon codes with q symbols can be calculated:

$$A_0 = 1, A_i = 0 \qquad for \quad (1 \le i \le d_{\min}),$$

$$A_i = \binom{q-1}{i}(q-1)\sum_{j=0}^{i-d_{\min}}(-1)^j \binom{i-1}{j}\left[q^{\,i-d_{\min}-j}\right] \quad for \quad d_{\min} \le i \le n. \tag{4}$$

Both Hamming and RS codes are very often used in safety - communication protocol as safety codes. Hammning codes based on generating polynomials are equivalent with cyclic codes used generator polynomials. It is necessary to point out, that the relation (3) is valid for original construction length of Hamming code not for shortened codes. The Reed-Solomon codes are MDS (Maximum Distance Separable) codes in which the safety characteristic of shortened MDS code is the same as in code within original construction length.

The weight structure of non perfect safety codes can be determined by two ways:

- Direct calculation - for short code words length only.
- Calculation using dual codes (so called Mac Willams's identity [8]) - for code words of large length computational very difficult and very often needs to have efficient computational tools or parallel processing of data.

For this reason we very often use a simplified relation for determination of residual error probability or maximal value of estimation 2^{-r}. For block safety codes (n, k) with code word of lengths n and with generating polynomial $g(x)$ the equation (1) can be modified by (5), in which the value of A_i is approximated by (6).

$$p_{e2} \cong \frac{1}{2^{n-k}} \sum_{i=d_{\min}}^{n} \binom{n}{i} p_b^{\,i} (1-p_b)^{n-i} \tag{5}$$

$$A_i \cong \frac{1}{2^{\,n-k}} \binom{n}{i} \tag{6}$$

If $np_b<<1$ in (5) then, the sum can be approximated by the first member of the sum (7):

$$p_{e3} \cong \frac{1}{2^{n-k}} \binom{n}{d_{\min}} p_b^{\,d_{\min}} (1-p_b)^{n-d_{\min}} \tag{7}$$

It is evident that in the expression (7) besides parameters of n, k it is necessary to known also the minimum Hamming distance of code words d_{min}. If this value is unknown the Gilbert's unequation for even length of code words (8) and for odd length of code words (9) can be used for determination of $d_{min.}$

$$2^{k} \sum_{i=0}^{(d_{\min}-1)/2} \binom{n}{i} \leq 2^{n} \tag{8}$$

$$2^{k} \sum_{i=0}^{(d_{\min}-2)/2} \binom{n-1}{i} \leq 2^{n-1} \tag{9}$$

The lowest number of redundant symbols r for concrete values of $d_{\min}$ and n it is illustrated in the Table 2. In the Table 3 the numerical results of the probability of undetected error p_{e1} ,according to relation (1) and p_{e2}, according to relation (5) for binary cyclic expanded Hamming code (128, 120) are calculated. The weight structure of code was determined via DERIVE program.

Table 2: Minimal number of redundant bits for concrete code words lengths

$d_{\min}$	$r \geq$	$n=10$	$n=100$	$n=1000$
2	1	1	1	1
3	$\log_2(1+n)$	3	7	10
4	$1+\log_2(n)$	3	8	11
5	$\log_2(1+n/2+n^2/2)$	5	13	20
6	$1+\log_2(1+n/2+n^2/2)$	6	14	21
7	$\log_2(1+5n/6+n^3/6)$	4	18	28

Table 3: Results of the probabilities of undetected error of cyclic Hamming code (128, 120)

p_b	2^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}	10^{-9}
p_{e1}	3,9 10^{-3}	2,58 10^{-3}	7,54 10^{-8}	8,42 10^{-12}	8,52 10^{-16}	8,53 10^{-20}	8,53 10^{-24}	8,53 10^{-28}	8,53 10^{-32}
p_{e2}	3,9 10^{-3}	1,57 10^{-4}	3,77 10^{-8}	4,12 10^{-12}	4,16 10^{-16}	4,16 10^{-20}	4,16 10^{-24}	4,16 10^{-28}	4,16 10^{-32}

6. CONCLUSIONS

The calculation of the probability of undetected error for the safety codes is an important part of system's safety analysis. For real code word length used in practise it is not as easy to evaluate as it is mentioned in the coding theory. Many types of shortened codes have different safety properties from codes in their construction length and therefore it is necessary to determinate the residual error probability in dependence on bit error rate for all telegram lengths via relations and procedures for weight function enumeration which the paper deals with and to proof the required safety integrity level (in majority of industry communication system the SIL 3is required).

Acknowledgements
This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0023/08 "Theoretical apparatus for risk analysis and risk evaluation of transport telematic systems".

REFERENCES

[1] *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1989*
[2] *EN 50159-1: Railway applications – Communication, signaling and processing systems. Part 1: Safety-related communication in closed transmission systems. 1998*

[3] *EN 50159-2: Railway applications – Communication, signaling and processing systems. Part 2: Safety-related communication in closed transmission systems. 1998*
[4] *EN 50128: Railway applications - Communication, signaling and processing systems. SW for interlocking systems. ČNI, Praha. 2003*
[5] *IEC 61794-3: Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. 2007*
[6] *FRANEKOVÁ, M. et al: Safety Communication of Industrial Networks. Monography (in Slovak), EDIS, ŽU Žilina, 2007, ISBN 978-80-8070-715-6*
[7] *KASAMI, T.- LIN, S.: On the probability of undetected error for the maximum distance separable codes. IEEE Transaction on Communication. COM 32, September 1994. N 9, p. 998-1006*
[8] *DODUNEKOVÁ, R.- DODUNEKOV, S.M.- Sufficient conditions for good and proper error correcting codes. IEEE Transaction on Information Theory 43 (November 1997), N 6, p. 2023-2026*

ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING