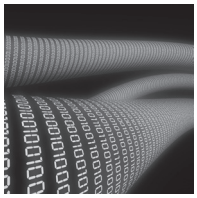

Archives of
Transport System
Telematics

Volume 4

Issue 2

May 2011

Safety mechanisms of Open Safety profile and their modelling

J. ĽUPTÁK[a], M. FRANEKOVÁ[a]

[a] Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia

EMAIL: juraj.luptak@fel.uniza.sk

ABSTRACT

Authors describe the solutions of safety industrial Ethernet with orientation to safety-related industrial control systems. Nowadays the numbers of safety solutions of industrial Ethernet are increasing (e. g. CIP Safety, ProfiSafe, Safety Interbus). Bernecker & Rainer is coming with the new solution - Open Safety, which was developed for technology Ethernet PowerLink (EPL), but open platform is compatible with the other types of industrial Ethernet too, e. g. Sercos, Ethernet/IP, Modbus, and Profinet. Mainly part of paper the safety analyses of Open Safety frame with orientation to safety codes used in two sub-frames are mentioned. Practical part is orientated to model realisation via Matlab, Simulink with the use of safety codes with possibility to demonstrate the detection capability of cyclic CRC codes dependence on characteristics of communications channel and generator polynomial selection.

KEYWORDS: safety industrial Ethernet, safety integrity level, safety profiles, Open Safety safety mechanisms, electromagnetic interferences, data integrity, safety code, Matlab, Simulink, model, time simulation

1. Introduction

Industrial communication systems are important elements of automation systems and they are used in wide variety of application, e. g. process manufacturing, electric power generation and distribution, gas and water supply, transportation and others. In many cases the industrial communication subsystem is part of safety -related control system, where undetected corruption of message can cause considerable substantially damages within equipment, environment or demands on human health and this is reason why the system has to be designed there is guarantee of required Safety Integrity Level (SIL). For this reason the safety - related devices must have implemented a number of safety mechanisms located into special safety profiles [1].

Nowadays the industrial Ethernet is becoming the communication standard used within all level of distributed control system with connection of industrial and office domains [2]. Developed additional safety profile within industrial Ethernet supports safety-related communication between safety-related devices generally

in safety integrity level (SIL) 3. Analysis of existing safety protocols within industrial Ethernet communications has shown that they are not suitable as a base for open and real time-capable Ethernet communication. Therefore Bernecker & Rainer is coming with new open solution - Open Safety profile, which is defined as a bus-independent, autonomous frame, which can in principle also be inserted into standard protocols other than Powerlink [3]. Basically the referenced standards for Open Safety devices are the generic standard IEC 61508 [4], IEC 61784-4 [5] or comparable standards. Open Safety has been designed so that standard data and safety data transfer is possible within the same network. The basic principle of implementation Open Safety profile is illustrated in the fig. 1.

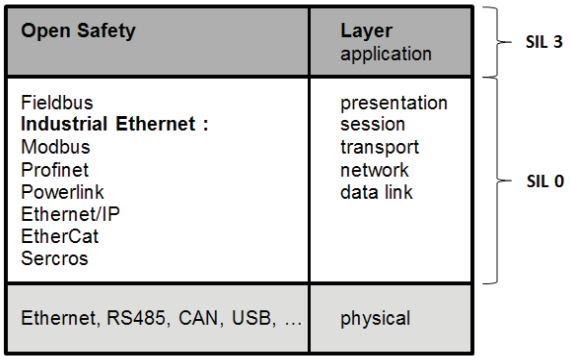

Fig.1. Principle of Open Safety implementation in RM OSI model

As we can see Open Safety profile is compatible without PowerLink with industrial Ethernet as Sercos, Ethernet/IP, Modbus, ProfiNet, EtherCat and in the future is able to be implemented in other types of industrial wire or wireless Ethernet.

Thanks to the very flexible construction of the frames, Open Safety can be adapted extremely well to various applications such as machines, installations or transport systems. The frame length is determined by the reference data needed by the application.

The basic advantages of the Open Safety solution can be characterized as the following [6]:

- there is guarantee of real time communication with data transfer time down to 100 μs,
- it fulfils the intensity rate up to SIL3 according to IEC 61508,
- standard and safety - related devices can be used in the same industrial network,
- from fieldbusses prefers CAN but supports complex lover architectures of RM OSI for network structures,
- there is independence of transport media,
- there is maximum of 1023 safety-related devices within one safety domain,
- is supports 1023 safety domains,
- it is compatible to Ethernet TCP/IP with Powerlink as the underlying communication layer.

The Open Safety frame is independent from standard frames because is encapsulated with its safety mechanisms within the standard communication. The big advance of this communication is that any existing Ethernet and fieldbus communication protocol can be used. The resistance of communication with the used Open Safety profiles against unauthorized access caused intentionally by human factor or unintentionally by several attacks or viruses depends on the protection of the underlying communication layer.

The security of Open Safety is based on applying Open Safety domain (SD) and the Open Safety domain gateway (SDG) as it is we can see in the fig. 2 where we can see the connection of industrial (factory) zone

with office (company zone).

The number of safety devices within one Open Safety domain is limited to the number of safety devices connected to Ethernet. Open Safety domain gateway is a special device which is able to communicate with different Open Safety domains.

In the paper safety mechanisms used in safety profile Open Safety are analyzed with orientation mainly to integrity mechanisms based on safety codes used CRC principles.

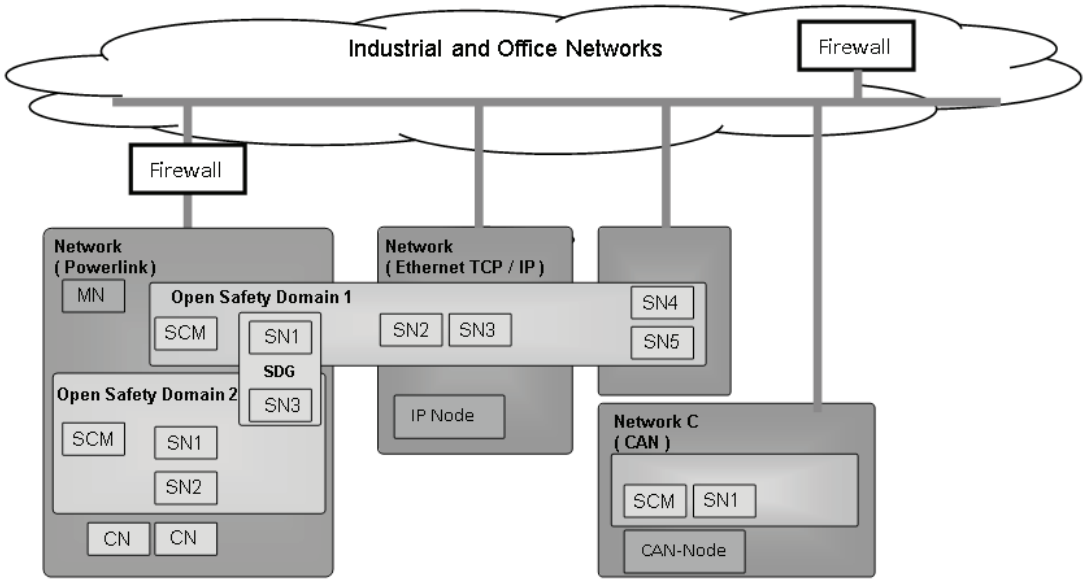

Fig.2. Integration of Open Safety into the IT infrastructure of end customer

2. Analyses of safety mechanisms used in Open Safety profile

Communication errors in black channel with the used Open Safety profile can be caused by EMI, failures in HW, SW or by human factor [7]. The task of Open Safety mechanisms is quick detection of errors and realization of adequate reaction to safety case. Philosophy of Open Safety profile is based on information redundancy. The frame of Open Safety profile consists of two sub frames (see fig. 3) in which the check is realised independently. Within the sub- frame we are able to transmit user data of several lengths (maximum to 254 bytes).

As we can see in the fig. 3 every sub-frame consists of the following fields: address field (ADR), frame identificator (ID), length field (LE), consecutive type field -CT(L), field of used data (DB_0,...DB_n) and CRC field.

Very important safety mechanism is the time stamp allocated in consecutive time field, which eliminates the communication errors: duplicity of data, re-sequences of delay of data. Time stamp consists of the actual time related to time clock of actual data transmitter. System does not use distributed clock but for this reason special procedure was created, which provides reliable source for synchronisation all microcontrollers clocks in every nodes. Mechanism of time stamp is used for error detection, e. g. loss of data or detection of large delay. This type of check is realised continually with monitoring of all nodes from which consumer requires the answer and then it has information about state of connection.

Identifier eliminates insertion of message. Open Safety frame allows the unique 8-bits or 16-bits identifier which is determined from address field, type of message field and type of frame field.

Data integrity check is realised with using safety cyclic code based on CRC (Cyclic Redundancy Check) determination on dependence on defined generic polynomials. The frame uses two kinds of CRCs depending on the length of the payload data. CRC is created for every sub-frame differently and check in the receiver parts. The second sub-frame transmits the same data (data is redundant) for this reason additionally the cross checking from safety codes in both sub-frames is realised.

Table 1 shows the structure of the basic Open Safety frame. The grey colored lines within table 1 describes sub frame two. Sub frame two frames SPDO (Open Safety Process Data Object) and SSDO (Open Safety Service Data Object) are additionally coded with the UDID (Unique Device Identification) of the SCM (Open Safety Configuration Manager) using a logical XOR operation.

Table 1. Structure of allocation of safety mechanisms in basic Open Safety frame

	Bit Offset							
Octet Offset	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	ADR (Bit 0 - 7)							
1	ID						ADR (8 , 9)	
2	LE							
3	CT (Bit 0 - 7)							
3 … n+3	DB 0 to DB n							
n+4 … n+4+o	CRC - 8 / CRC - 16							
n+5+o	ADR (Bit 0 - 7) XOR SDN (Bit 0 - 7)							
n+6+o	ID						ADR (8 , 9) XOR SDN (8, 9)	
n+7+o	CT (Bit 8 - 15)							
n+8+o	TADR (Bit 0 - 7)							
n+9+o	TR						TADR (8, 9)	
n+9+o … 2n+9+o	DB 0 to DB n							
2n+10+o …								
2n+10+2o	CRC - 8 / CRC - 16							

Note:
n is number of payload data in bytes $0 \le n \le 254$
o is CRC correction offset $0 \le n \le 8$, $o = 0$ (CRC8),
$9 \le n \le 254$ $o = 1$ (CRC16).

3. Analyses of safety codes used in Open Safety sub-frames

Basic requirement to safety codes used within safety - related communications in closed and open transmission systems are described in EN 50159 [8].

Open Safety uses for data integrity check safety code based on the principle CRC with defined primitive generator polynomials [9]. The type of generator polynomials depends on the value of length of data (LE) as it is illustrated in the Table 2. The receiver controls the syndromes after CRC determination not only in both sub-frames but realised cross

Table 2. Assignment of CRC codes according to LE

LE value [byte]	CRC - generator polynomial
0-8	CRC – 8 $g(x) = x^8 + x^5 + x^3 + x^2 + x + 1 \approx$ 12F hex
9-240	CRC – 16 $g(x) = x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^2 + 1 \approx$ 15935 hex
241-255	Reserved by producer

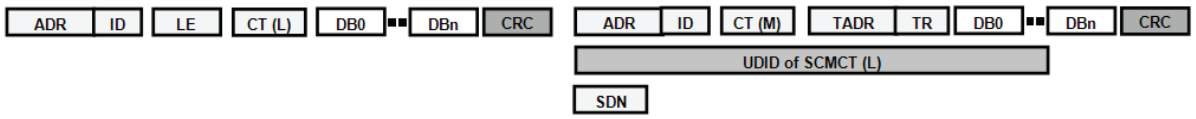

Fig.3. Data format of basic sub-frames of Open Safety profile

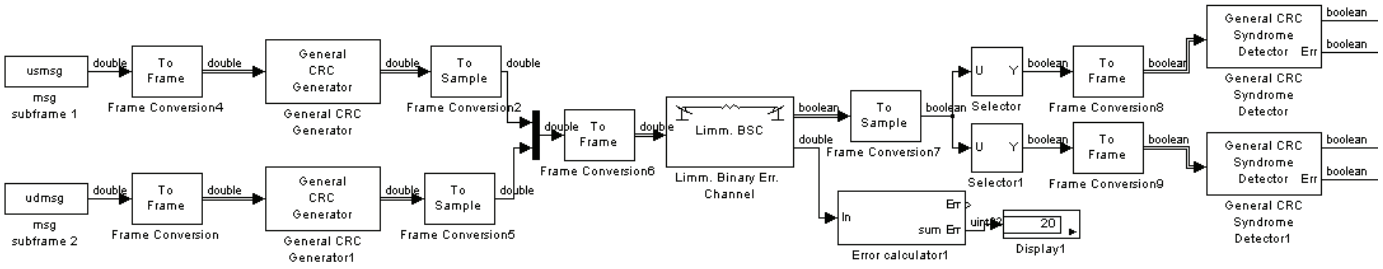

Fig.4. Model of sub-frames of Open Safety profile

Note: R - number of real simulated errors, D - number of detected errors

checking mechanisms whereby the safety of communication is increasing. Characteristics of cyclic CRC codes used in Open Safety profile are illustrated in table 3.

Detection possibilities of cyclic CRC codes are illustrated in the Table 3.

4. Results of practical part

The model which simulated the operation of safety codes used in Open Safety sub-frames was realised via SW Matlab [10]. The functional blocks were constructed with aim to suggest the detection possibilities of cyclic detection codes based on CRC principle with using recommended generator polynomials in Open Safety frames (see Table 2) for short and long format of data dependence in noise characteristic of communication channel. Realised model is illustrated in the fig. 4. Model was created with support of toolboxes: Simulink, Communication blockset, Signal processing blockset and own created blocks.

Transmitted and receiver parts of model content:

- generator of messages,
- functional blocks describing two sub-frames of Open Safety profile with orientation to CRC mechanism,
- model of binary communication channel,
- sink,
- graphical unit (scope).

Table 3. Characteristics of cyclic coded with CRC polynomials used in Open Safety frames

CRC polynomials [hex]	Detection possibilities
12F Frames to 8 bytes	HD 4 to 119 bits
15935 Frames from 9 to 240 bytes	HD 5 to 241 bits HD 4 to 2048 bits
11EDC6F41 Data to 4k bits for one block	HD 8 to 128 bits HD 6 to 4k bits HD 4 to 64k bits

Note: HD (Hamming Distance)

Table 4. Vector of generated messages

Type of message	Vector representation
S1	$s(i) = 1, i = 1, 2,\ldots,n$
S2	$s = s_1(i)+s_2(i); s_1(i) = 1; s_2(i) = 0, i =1,2\ldots,n/2$
S3	$s(i) = 0, i = 1, 2,\ldots,n$

Table 5. Results of detection possibilities of safety code according to simulated different error pattern

safety code	CRC- 8					generator polynomial: $g(x) = x^8 + x^5 + x^3 + x^2 + x + 1$														
p_b [-]	10^{-3}					10^{-2}					10^{-1}					0,5				
***i*-fold error**	2	4	8	9	10	2	4	8	9	10	2	4	8	9	10	2	4	8	9	10
subframe1 (D)	0	0	0	0	0	5	7	7	7	8	72	92	97	96	105	384	461	529	488	517
subframe1 (R)	0	0	0	0	0	5	7	7	7	8	72	92	97	97	106	384	461	530	489	520
subframe2 (D)	0	0	0	0	0	6	7	8	8	9	77	99	98	98	106	389	472	533	487	521
subframe2 (R)	0	0	0	0	0	6	7	8	8	9	77	99	98	99	107	389	472	533	490	521

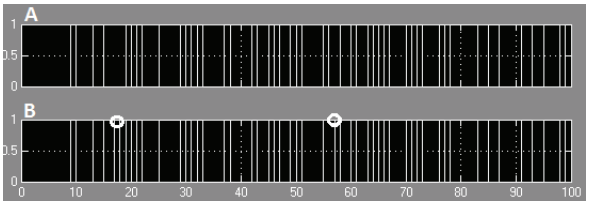

Fig.5. View of time simulation of transmitted messages effected by EMI

For safety code - CRC realisation in the transmitted and received part of model the following functional blocks were used from Communication blockset:

- general CRC generator,
- general CRC syndrome detector.

The block general CRC generator creates on the base of valid rules for cyclic detection code [9] and selected generator polynomial types the redundant bits which are added to each transmitted message. On the received part the block general CRC syndrome detector according to syndrome technique realisation [10] determined the syndrome and check the integrity of received message and detect the corrupted message to the degree of selected generator polynomial. As model of communication channel own type of functional block Limited Binary Symmetric Channel was created in which different type of error pattern (single error, burst of errors) are possible to generate [11], [12].

Detection possibilities testing were realised for three types of messages generated from generator source with rate 1 message per second:

- S1 - all bits logical 1,
- S2 - half to half bits of logical 1 and logical 0,
- S3 - all bits of log 0.

The vector representation of generated messages is illustrated in the Table 4. Each simulation consisted of 1000 messages from which the statistical results were determined. The result of detection possibilities accordance with bit error rate of communication channel is illustrated in the Table 5, where the number of corrupted messages within sub-frame 1 and sub-frame 2 were counted. The results are illustrated for two value of bit error rate $p_b = 10^{-3}$, $p_b = 10^{-2}$, $p_b = 10^{-1}$, $p_b = 0{,}5$. Simulation of messages across noise channel was realised in the worst condition of noise for generated burst of several lengths.

In the Figure 5 time simulation of corrupted messages in sub- frame 1 in the output of Limited Binary Erroris illustrated.

Channel Figure 5a) and time simulation of detected messages in general CRC syndrome detector Figure 5 b) are illustrated. By mark "o" is signed the message (in time) in which was not detected error.

5. Conclusion

Nowadays the trend within safety-related industrial communication system is applying some type of industrial Ethernet in which the requirements to safety is solved by additional safety profile. In the last decade several number of safety communication profiles valid for safety industrial Ethernet were developed and certificated with safety integrity level 3. The disadvantage of these solutions is that the safety profiles are not compatible with large scale of safety devices from different vendors. The safety solution developed by B & R company (Open Safety) based on open access negates these disadvantages. For safety mechanisms which are implemented must be safety case determined for every concrete application and required requests. The safety code is one very important mechanism used for data integrity keeping. Safety code can assure not only transmitted data but other safety mechanisms and parameters which are not transmitted (implicit data) too. This is way we must in detail the selection of parameter of safety code determined via model. In the paper the model of Open Safety frames was realized with orientation to analyses of detection possibilities of cyclic detection code (CRC) dependence on noise conditions in communication channel and parameters of CRC code (generator polynomial, length of transmitted messages). Several error patterns within model communication channel were generated and the detection possibilities of safety codes recommended to use within Open Safety profile were tested. The model is usable as a universal tool which we can use in process of optimalisation of parameters of safety code based on CRC principles for different types of generator polynomials degree. The model can be expanded about transmission code used in untrusted transmission system and about other tools related with problem of CRC codes, e. g. generating the all primitive polynomials of defined degree, testing of irreducibility of generator polynomial and determination and graphical presentation of probability of undetected errors in the side of decoder.

Acknowledgement

This work was supported by project Centre of excellence for systems and services of intelligent transport,
ITMS 26220120028, University of Žilina, Žilina, Slovak republic

Bibliography

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

[2] STRÉMY, M., et. all: Introduction to programmable logical controller. In: Slovak. Slovak Technical University Bratislava. Published in Detached place of work MTF Trnava, 2011
[3] B&R, B&R-Automation. In B&R [online]. 2011 http://www.br-automation.com
[4] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1989
[5] IEC 61784-4: Digital data communications for measurement and control. Part 3: Profiles for secure communications in industrial network. 2006
[6] EPSG Working Draft Proposal: Open Safety. Safety Profile Specification 3. Version 1.1.3. Ethernet POWERLINK Standardisation Group. 2010
[7] ZAHRADNÍK, J.- RÁSTOČNÝ, K.- KUNHART, M.: Safety of interlocking system. EDIS ŽU Žilina, 2004. In Slovak. ISBN 80-8070-296-9
[8] EN 50159: Railway applications - Communication, signalling and processing systems - Safety - related communication in transmission systems. Cenelec 2010
[9] MUZIKÁŘOVÁ, Ľ.- FRANEKOVÁ, M.: Theory of information and signal. EDIS, ŽU Žilina, 2009. In Slovak. ISBN 978-80-554-0075-4
[10] FRANEKOVÁ, M.: Moddeling of communications systems via Matlab, Simulink and communications toolbox. Edis, ŽU ŽU Žilina, 2003. In Slovak. ISBN 80-8070-0273
[11] MathWorks – Matlab Documentacion. In English, [online]. 2011 http://www.mathworks.com/help
[12] Communications Blockset - Communications Blocks. In English [online]. 2011 http://www.kxcad.net/cae_MATLAB/toolbox/