Archives of
Transport System Telematics

Volume 2

Issue 3

September 2009

Analyses of safety-related message transmission

K. RÁSTOČNÝ[a], M. FRANEKOVÁ[a]

[a]Faculty of Electrical Engineering, University of Zilina, Department of Control and Information Systems, Univerzitná 1, 01026 Žilina, Slovakia, ,

EMAIL:karol.rastocny@fel.uniza.sk, maria.franekova@fel.uniza.sk

ABSTRACT

The analyses were aimed at determination of failure effects in the transmission system, which allow identifying the transition process of the system from a safety state (it may not be necessarily a failure – a free state) to a dangerous state and permit to calculate probability of the dangerous state occurrence of the system as a failure effect to the operating system. Dangerous states of the safety Fieldbus system are mainly caused by systematic failures within a specification of the system, electromagnetic interferences (EMI) and random failures of the HW effects. The effects of electromagnetic interferences and random failures of HW can be described in the paper by the use of time table.

KEYWORDS: safety-critical applications, Safety Integrity Level, communication errors, closed transmission system, safety mechanisms, ratio counter, probability of undetected error

1. Introduction

To reach the safety goal within communication it is recommended to apply safety functions, which enforce safety and are executed by suitable safety mechanisms. Safety mechanisms can be implemented in SW (control of access to the system, using passwords, mechanisms based on cryptography, etc.), in HW (cipher modules, authentication and identification cards), by physical means (safe deposit box, interlocks, etc.) or by administration measures (standards, legislation, certification authority, etc.). COTS (Commercial Off-The-Shelf) communication technologies are not essentially available (without supplementary technical measures) for transmission of the safety-related data, although its transmission systems involve detection and correction methods for transmission assurance, or other protective mechanisms, if any. Concerning the transmission safety, such systems are denoted as non-trusted. The decision which types of additional technical measures are necessary to apply depends on the risk analysis results (analysis of attacks and their effects) related to the controlled process and the acceptable risk [3].

Nowadays, on the technological level, the Fieldbus technology is an acceptable standard, which is now widely used for transmission of non-safety related and safety-related control data, too. The specific utilization of the common function by the specific groups of participants is called a profile. Today the 79 IEC Fieldbus Standards are broken down into 15 Communication Profile Families (Table 1) [4].

As it is shown in Table 1, today only four communication profile families CPF have defined additional services and specified protocols based on the safety-related principles – CPF1 (Safety Foundation Fieldbus), CPF2 (CIP Safety), CPF3 (ProfiSafe) and CPF6 (Interbus Safety) [5]. These safety profiles are recommended for using in the safety-related systems with the Safety Integrity Level SIL 3 according to EN 61508 [6]. In industrial practice for all safety products the next years are assumed to see the highest

Table 1. Communication profiles families for Fieldbus technology

CPF	Technology name	Safety profile
CPF1	Foundation Fieldbus	Safety Foundation Fieldbus
CPF2	CIP	CIP Safety
CPF3	Profibus/Profinet	ProfiSafe
CPF4	P-Net	-
CPF5	World FIP	-
CPF6	INTERBUS	Interbus Safety
CPF7	SwiftNet	-
CPF8	CC Link	-
CPF9	Hard	-
CPF10	Vnet/IP	-
CPF11	TC/Net	-
CPF12	EtherCAT	-
CPF13	EtherNet Power Link	-
CPF14	EPA	-
CPF15	Modbus-TRPS	-

growth of market within the safety related network and the safety PLC (fig. 2), what is the result of the world survey published on www sites of safety products vendors [7].

It is assumed that the safety profiles development for the rest of the communication families CPF (summarised in Table 1) will continue.

Modelling and safety analyses fulfil a very important task in the process of analysis and synthesis of the safety-related Fieldbus systems within their lifetime. We can divide products (equipment, system) within their life time to five phases (fig. 2).

Within the process of modelling several parameters of the system are controlled, which are a component of the technical quality of the system (product). Markers of the systems include for example reliability, safety, lifetime, availability, no-failure operation, maintenance and assurance of maintenance. Standard EN 50129 valid for the interlocking systems [6] recommends controlling, within the life time of the system, four parameters: reliability, availability, maintainability, and safety, called RAMS parameters.

Choices of the suitable modelling methods or techniques depend on the type of the Fieldbus system. It is necessary to choose methods which make possible:

- to model and evaluate the problems in a wide range,
- to carry out systematic qualitative and quantitative analyses,
- to predict the numerical values (in the case if data is available).

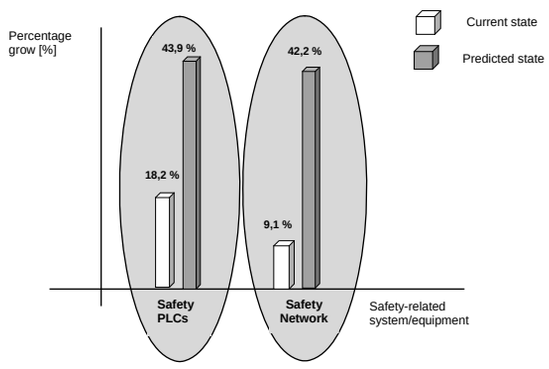

Fig.1. Prediction of needs of safety-related networks in industrial practice

2. Analyses of communication system for safety-related message transmission with the use of a ratio counter

Let us consider communication on the end to end level (fig. 3). The communication system includes the source SI and the receiver of information RI and a trusted transmission system, which performs the safety critical functions in transmission according to the standard [6]. The base of the trusted transmission system is a standard (untrusted) transmission system, which secures the transmission messages by a transmission code. To keep required Safety Integrity Level (SIL) the transmission messages must be secured by additional security measures, i.e. by a time stamp, security code, feedback message or cryptographic techniques.

Let the information transmission is secured by a transmission code and a security code (e.g. work on the CRC - Cyclic Redundancy Check principle), which are independent. Let the component of the transmission system is a communication channel, which is effected by Electromagnetic Interferences (EMI) only. We assume a closed transmission system.

The channel decoder of the transmission code and channel decoder of the security code are determined, if according to the transmission of information a the corruption occurs or not. In the case of information failure detection by the channel decoder of the transmission code TD or by the channel decoder of the security code SD the control system must stay in fail safe state.

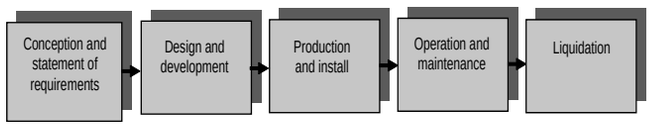

Fig.2. Classification of the life time of system

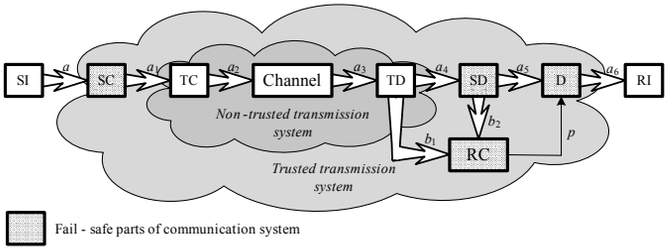

Fig.3. Closed transmission system with a ratio counter

It means that the received information (in the case of TD - a3 and in the case of SD - a4) is repudiated and the receiver must work with the last received message or must go to the defined safety state. The next task of the channel decoder of the transmission and of the security code is to inform the ratio counter RC (fig. 3), that the received message is considered as correct or incorrect. In the case of detection of a certain number of incorrect messages from all received messages the ratio counter must respond and the system must go to a defined permanent safety state. In our case the permanent safety state is the disconnection of the receiver of information RI from the trusted transmission system with the use of the disconnector D, which works on the basis of information p from ratio counter RC. This state can be changed by the specialized person only. It stands that the trusted part of the transmission system must be realized on the fail-safe principle. It this case certain problems with safety function of the ratio counter RC may occur, because RC depends on information b1, which is generated by the untrusted decoder of the transmission code TD.

For the closed transmission system with the ratio counter the safety reaction occurs when ARC ≥ MRC, where ARC is the actual value of ratio counter RC (ARC is function f(b1, b2)) and MRC is the boundary value of ratio counter RC).

3. The time tables of safety-related messages transmission

The relationships among various safety response times during transmission of messages may be presented via the time tables. The time table of normal operation of a safety function within transmission (without faults) is illustrated in fig. 4. fig. 5 illustrates the case of the fault detection in transmitted messages and the consecutive reaction of system to the detected fault (in our case the transition to safety state is performed after the first detection of fault).

The meaning of symbols used in fig. 4 and fig. 5 is the following:

- t_1 – time between the demand of a safety function and the sending of the corresponding safety message [s];
- t_2 – time between the ending of received message check and ending of request realisation [s];
- t_3 – time between detection of fault message and the transition of system to specified permanent safety state [s];
- t_4 – time between the detection of fault message and request of repetition of transmission [s];
- T_{MDT} – message detection time [s];
- T_{FDT} - fault detection time [s];
- T_{SRT} – reaction time of safety, where $T_{SRT} = T_{MDT} + T_{FDT}$ [s].

The knowledge of failures and faults attributes of the transmission system forms the basic assumptions related to the implementation of measures not only used to avoid failures but also for the fault detection and negation of the failure effects within their occurrence.

It is important to know where, when, and what types of failures occur in the system, what are the reasons of their occurrence and their effects to the system. There are three ways of hazard creating:

- random failures of the transmission system HW,
- failures caused by EMI,
- systematic failures of the transmission system.

The occurrence of a systematic failure is related to the concrete situation and a state of the transmission system. Mathematical modelling of this incidence is very problematic, because we have to know the type of distribution and its parameters. Generally, we do not consider systematic faults in the process of a model implementation and we orientate to methods and techniques which are used to prevent failures (e.g. formal specification, rigorous testing, etc.).

At appropriate application of these methods we can assume that a systematic failure rates occurrence and

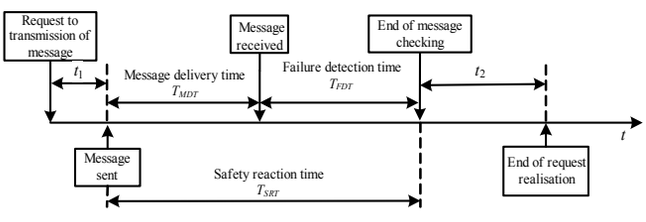

Fig.4. Normal operation of safety function using closed transmission system

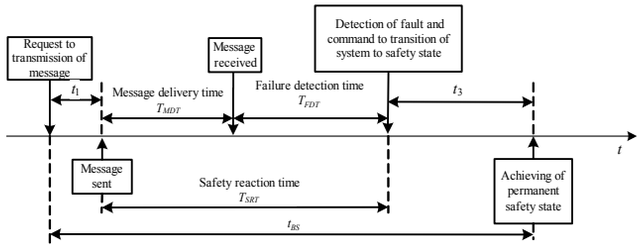

Fig.5. Operation of safety function in the event of the first detection of fault in the received message

consequently also their effects are negligible compared to random failure rates and failures involved within a communication medium (it is caused mainly by influence effects in consequence of electromagnetic interference). The effect of noise can have different forms, which depend mainly on physical characteristic of channel. The undesirable effect of EMI may be eliminated using both security and transmission code.

The effect of several factors coincidence on safety of the transmission system can be demonstrated using Markov's chain. For the transmission system with the ratio counter (illustrated in fig. 3) a Markov diagram was realized, which shows the system transition from a functional safety state to dangerous state and is described in detail in paper [9].

During determination of the transition of the system to the specified permanent safety state we can consider the following cases:

- all received messages are faults (the worst case),
- fault messages are coming randomly,
- all coming messages are correct (ideal case).

The results described in the paper are for the worst case within message transmission, that all generated messages from source are faults.

4. The results of safety analyses

Let us assume that all received messages are faults, the transition of transmission system (illustrated in fig. 3) to safety state occurs after the detection of x received fault messages. The value of the reaction time t_{BS} is proportional to the number of received fault messages x, which must be coming so that the actual value of the ratio counter A_{RCS} will achieve (or go over) a boundary value of the ratio counter M_{RCS}. Operating of communication and the transition of the system to the permanent safety state in the case of detection of x consecutive messages is illustrated by the time table in fig. 6.

In the case of cyclic transmission of messages (i.e. $T_{SRT}1 = T_{SRT2} = ... = T_{SRTn}$) the value of the time t_{BS} is

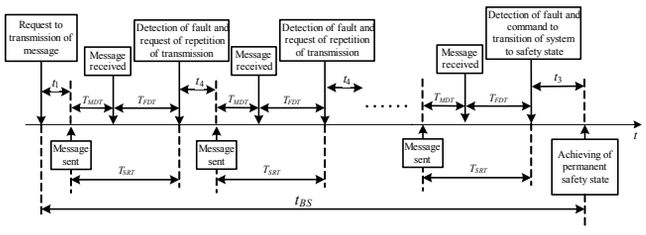

Fig.6. Time table of operating state and the transition of system to permanent safety state in the case of x faults detection in consecutive messages

determined by function $f(x, t_1, t_3, t_4, T_{SRT})$. The number of received fault messages x, which must come so that the actual value of the ratio counter A_{RCS} will achieve (or exceed) the boundary value M_{RCS}, may be determined by the following equation:

$$\|x\| = \frac{\left(M_{RCS} + \left(N_{RCS} - 1\right) - I_{RCS}\right)}{N_{RCS}}, \quad (1)$$

where ||x|| is the entire part of the relation and $x \in \langle n,\ n+1 \rangle,\ n \in Z$ must be valid, N_{RCS} is the value around which the actual value of RC will be increased (in the case of negative result) and I_{RCS} is the initial value of the ratio counter.

The value of failure rate of the communication part of the system $\lambda_{SL}(p_b)$ according to standard [5] is defined by:

$$\frac{\lambda_{SIL}}{100} > \lambda_{SL} \quad (2)$$

where λ_{SIL} is the failure rate of the all part of transmission system. The failure rate λ_{SL} is a function of bit error rate of the communication channel pb and according to standard [5] we can write the relation:

where $p_{ME}(p_b)$ is the probability of residual error rate of the transmission message using a detection mechanism (most commonly on the basis of CRC– cyclic redundancy check), f_W is the maximal number of the transmitted safety-related messages during one hour and m is the maximal number of receivers (for our case m = 1).

The probability of an undetected error in code words pus (one message) may be determined in detail using the relation published e. g. [10], [11], or by the relation for the worst case 2^{-r} (r-is number of redundant bits in the message). Then the maximal vale of the fault message, which is coming consecutively may be determined by [12]

$$\left\|x_{mamn1}\right\| \le \frac{\lambda_{SIL}}{100.p_{US}.m} \quad (4)$$

The number of fault messages x, which can come, that the actual value of the ratio counter ARCS keeping or increasing the boundary value a of the ratio counter, must be within the range $\langle 2, \|x_{mamn1}\| \rangle$.

In the case of cyclic communication we can determine the value of the reaction time by the following equation

$$t_{BS} = t_1 + t_3 + \left(\|x\|.\left(T_{MDT} + T_{FDT}\right)\right) + \left(\left(\|x\| - 1\right)t_4\right) \quad (5)$$

Graphical relations of the number of received fault messages x, which must come so that system goes to the safety state, are illustrated in fig. 7. These values depend on the boundary value of the ratio counter M_{RCS} and on the changed value of N_{RCS}. The initial value of ratio counter is $I_{RCS} = 0$.

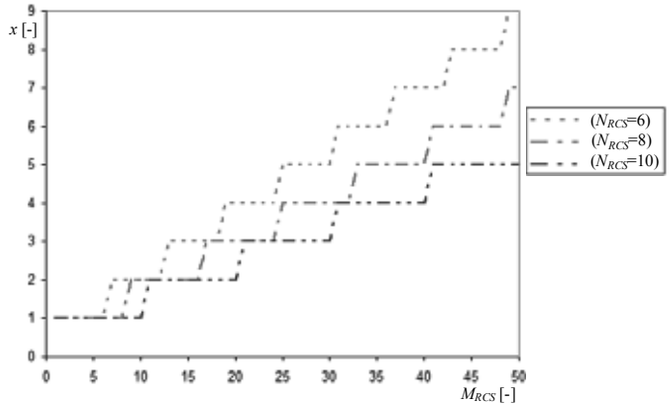

Fig.7. Graphical relations of number of fault messages in accordance with parameters of ratio counter

5. Conclusion

Within the application of the control system used in the safety-critical process control the safety characteristics are the most important, but not sufficient. The next important characteristic is the reliability of the system. The solution of the control system is a compromise between the safety and the reliability characteristics of system. The application of safety-related message transmission using the ratio counter can significantly and positively affect the reliability of the transmission system at the expense of the safety. That is why the selection of parameters of the ratio counter must be carried out very sensitively so that the value of the required safety integrity level must be fulfilled. Fulfilment of the safety integrity level must be accomplished not only by practical experiences but also by using a modelling method which allows modelling the effects of the risk factors on the safety of transmission systems. Among the risk factors we can arrange the parameters of the ratio counter described in the paper.

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 "Mathematic-graphical modelling of safety attributes of safety-critical control systems".

Bibliography

[1] EN 50159 – 1: Railway applications: Communication, signalling and processing systems - Part 1: Safety - related communication in closed transmission systems. 2002.
[2] EN 50159 – 2: Railway applications: Communication, signalling and processing systems - Part 2: Safety - related communication in open transmission systems.
[3] RÁSTOČNÝ K: Risk Analysis of a Railway Interlocking System. In Scientific Journal: Advances in Electrical and Electronic Engineering, No. 3 - 4 Vol. 2/2003, pp. 24 -29, ISSN 1336-1376, (in Slovak).
[4] www.iec.ch
[5] IEC 61784-3: Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks. 2007.
[6] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998.
[7] www.odva.org
[8] EN 50129: Railway application. Safety-related electronic systems for signalling. 2003.
[9] RÁSTOČNÝ K., FRANEKOVÁ M: Modelling of Safety Properties of Communication Systems. In Scientific Journal: Communications No. 1/2008, pp. 24-30, ISSN 1335-4205.
[10] FRANEKOVÁ M.: Mathematical Apparatus For Error Probability Determination of Block Code Decoders. In Scientific Journal: Communications No. 4/2008, pp. 59-63, ISSN 1335-4205.
[11] FRANEKOVÁ M., et al.: Communication Safety of Industrial Network. Monograph. EDIS, ŽU Žilina, 2007
[12] ZELENKA J.: A Reaction of a safety-critical control system to failure. Dissertation Work, University of Žilina, 2009