Karol Rastocny – Maria Franekova *

MODELLING IN DEVELOPMENT OF SAFETY-RELATED COMMUNICATION SYSTEMS

The aim of the paper is the use of modelling within development of safety-related communication systems presented in the areas where guaranty of a safety integrity level is required. The basic principles and standards used in the process of safety evaluation in closed transmission systems are summarised in the paper. Dangerous states of the system are mainly caused by systematic failures within a specification of the system, electromagnetic disturbance and random failures the HW effects. The main part of the paper describes the safety analysis process on the example of the end to end closed transmission system with the use of the fault tree and Markov's chain.

Key words: Integrity, safety, SIL, code, communication system.

1. Introduction

A variety of characteristics within manufacturing processes in different industry sectors evoke remaining requirements to flexible approach in the solution of safety of control systems including communication systems.

In many cases the communication system is a component part of the system which participates in control of safety-critical processes. Undetected corruption of data transmission (e.g. control commands) can cause considerable substantial damage within equipment, environment and demands on human health. This is the reason why the system has to be designed to guarantee the required safety integrity level (SIL).

COTS (Commercial Off-The-Shelf) communication technologies are not essentially available (without supplementary technical measures) for transmission of safety-related data, although their transmission systems involve detection and correction methods for transmission assurance or other protective mechanisms. Concerning the safety of the transmission, such systems are denoted as non-trusted. To decide 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.

Nowadays the number of vendors of the safety-related communication technologies who guarantee besides standard communication, communication among safety-related equipment according to [1] is increasing. In the present time the standard proposal [2] is prepared, which deals with a definition of functional safety for industry networks within digital communications used in the measuring area and the control systems in industry. Among the first manufacturers who have begun to use safety principles in development of their products there are the vendors of CAN technologies and products developed within the international organisation ODVA (Open Device Net's Vendor Association). The new network standard CIP Safety [3], published by ODVA, makes it possible to join standard and safety-related equipment across the same communication link. The vendors of Profibus and Profinet technology belong to the next important leaders in the area of industry Fieldbus. They develop a concept based on the integration standard and safety-related techniques that have been using the same communication tools for several years. This solution is signed as ProfiSafe and together with ProfiDrive profile it was approved and prepared for using in both types of industry networks Profibus and ProfiNet. In the present time the buses with communication profiles CIP Safety and ProfiSafe are recommended for using in safety-related systems with the safety integrity level 3 according to EN 61508 or the category 3 according to EN 954-1. The area of analysis and synthesis of safety-related communication systems assigned for control of the railway transport is presented in the norms [5] (for closed transmission systems) and [6] (for open transmission systems).

Modelling fulfils a very important task when specifying the requirements, in the process of structure design and the production of the communication system and also in the process of its verification and validation. In some cases modelling may help to optimize options, in other words, the setting of parameters within the existing communication system so that the requirements to safety integrity level and availability, which are defined by a customer or they are the result of the risk analysis, are accepted. In order to achieve these tasks it is generally required to combine suitable modelling methods and tools. Generally, in these cases an abstract model which graphically or mathematically describes features of transmission system is created.

* **Karol Rastocny, Maria Franekova**
Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Slovakia,
E-mail: karol.rastocny@fel.uniza.sk

2. Modelling of safety characteristics of the communication system

Think of the communication system on the level of the end to end (Fig. 1). The communication system consists of the safety-related equipment SE 1, SE 2 and trusted transmission system, which realises safety-related functions within transmission in compliance with [5]. The base of the trusted transmission system includes a non-trusted transmission system (COTS system), which insures transmission messages by the transmission code (TC). To achieve the required safety level of transmission, transmission messages have to be ensured by the safety code (SC). It is necessary to realise the encoder and decoder of the safety code on the fail-safe principle. The component part of the transmission system is the communication channel, which is influenced by electromagnetic interference (EMI) only. The authors assume the closed transmission system and the independence of encoders/decoders of safety and transmission codes only.

It is an advantage when the development of safety–related communication system is based on modelling methods usage (for the define phases of the system development it is necessary). In fact the safety-related features of communication system modelling can be divided into the following parts:

- *Modelling of functional characteristics of the communication protocol.* In this case the model is based on the semi-formal and formal methods (they are usually supported by SW tools), which helps to produce explicit and logical descriptions of the functional possibilities of the system. In this area the object oriented modelling (OOM) can be used. One of the most suitable techniques for a production of such model is the unified modelling language (UML), which supports different modelling and visualisation elements [8].
- *Modelling of disturbing effects within the communication channel.* In this case the model describes the effects of EMI and the failures occurred in the communication channel. The result of solution is choosing the criteria for transmission selection and safety codes according to required SIL and calculation of residual error rate of decoders [7].
- *Modelling of failure effects in the transmission system.* In this case the model reflects the analysis of the failure subsequence on the communication system, which can be realised on the base of quantitative and qualitative methods.

Next part of this paper is devoted to the tasks of failure effects modelling.

3. Modelling of failure effects within the closed transmission system

Safety-related systems are typically resistent against hazardous faults. The failure effects on the system can be directly determined by monitoring the original system installation, by a simulation of the system operation using its model, by computing and theoretical reasoning. It is necessary to remark that strictly safety requirements for the safety-related system are not possible to achieve only by tests or results from practice (the frequency of occurrence of a dangerous state is very low and the mean time among failures multiply exceeds the value of the useful lifetime of one safety-related system). It is important to provide the proof of the safety request performance and the resultant risk acceptability.

The aim of the failure effects analysis on the safety is to form a model which allows to identify 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 permits to calculate probability of the dangerous state occurrence of the system as a failure effect to the operating system.

The transmission system normally does not work isolated but it is a component part of another superior system for which it pro-

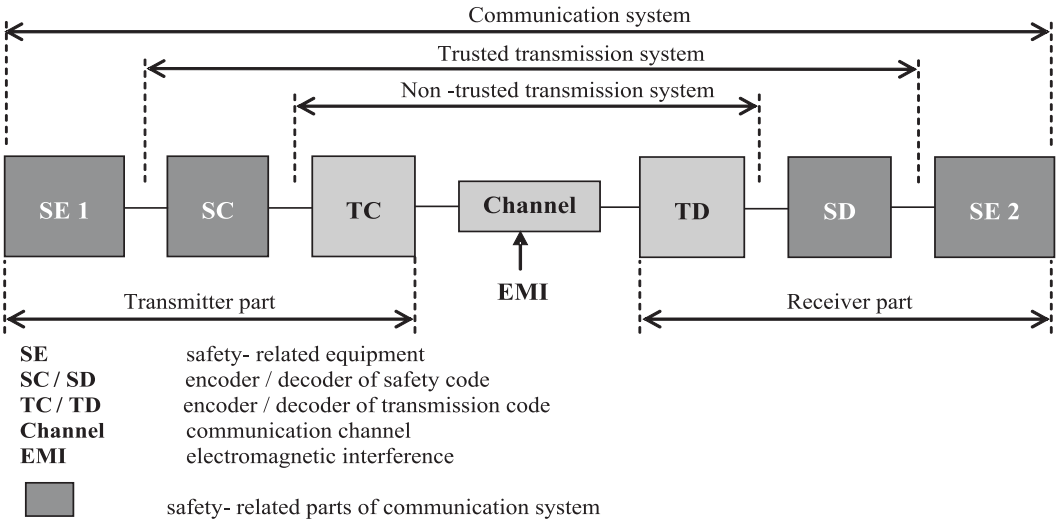

Fig. 1 The communication system on the level of the end to end

vides service. Therefore the starting moment of safety model generating is an exact definition of interface between the transmission system and the superior system with the aim to facilitate a total identity of treats with which it is necessary to consider in the process of analysis. Also it is necessary to define explicitly the event in the output of safety system which is considered as dangerous (undesirable) with regard to safety features of the transmission system. Generally, the undesirable event is considered to be such a violation of the transmission data which is not detected by the transmission system and further data are regarded as correct.

Except the safety procedures analysis (the source of a message identification, check of the type of a message, check of the current of data, the analysis of safety codes characteristics, the analysis of safety reaction mechanism, etc) it is necessary, according to the norm [5], to evaluate quantitatively the intensity of undetected failures of the transmission system.

The knowledge of failures and faults attributes of the transmission system forms the basic assumptions related to the measures realisation 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 the reason of their occurrence and their effects to the system are. There are three ways in which a hazard may be created:

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

The occurrence of a systematic failure is bonded to a 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 a distribution and its parameters. Generally, we do not consider systematic faults in the process of a model realisation and we orientate to methods and techniques which are fixed to prevention of failures (e. g. formal specification, rigorous testing, etc). By a pursuant application of these methods we can assume that a systematic failure rates occurrence and consequently also their effects are negligible compared to random failure rates and failures involved in within a communication medium (it is caused mainly by influence effects in consequence of electromagnetic interference). Frequency of corrupted messages depends on a disturbance value. Because of the fact that the transmission system has to dispose with the required value of a safety level also in case of an unexpected reduction of the transmission line quality, in practical determination we generally issue from a very pessimistic assumption (each of the messages in the output of the transmission channel is corrupted).

The fault tree, which can cause undesirable event, is described in Fig. 2. Random failures can attack all parts of the transmission system. During the model realisation we accept the supposition that each of the messages in the input of the receiver is corrupted. This is the reason why we need not distinguish whether the corruption was caused by EMI or by a random failure of the receiver part of the transmission system or the communication channel. The random failures of a decoder of the transmission code create an important role in the failure effects analysis to safety of the transmission system. The failure of the transmission code's decoder can cause that all received messages are considered to be correct. It is also necessary to regard a situation in which a decoder of the transmission code checks the received message but consequently a message can be corrupted (during a transmission from a decoder of the transmission code to a decoder of the safety code). We do not consider a random failure of the decoder of the safety code

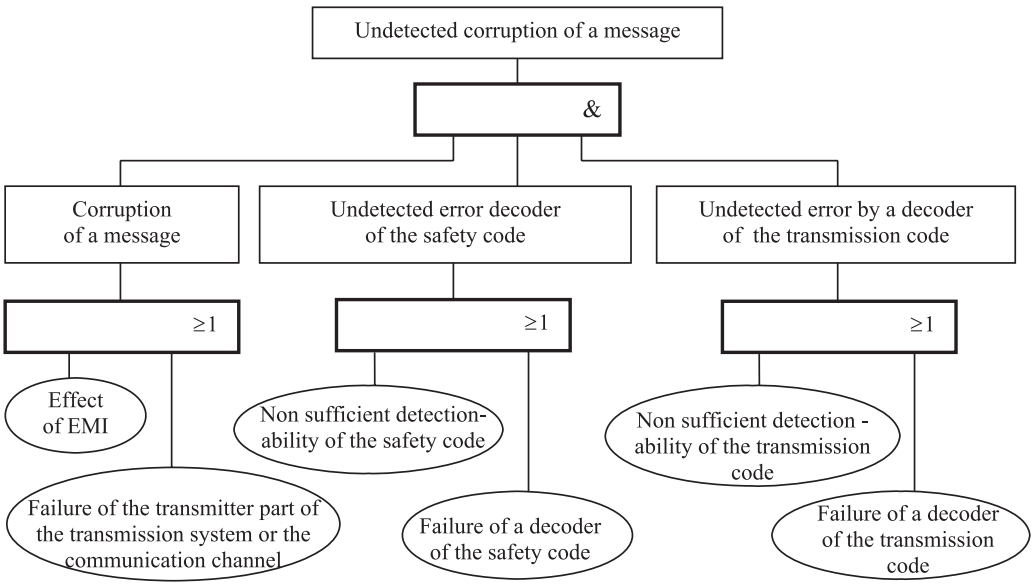

Fig. 2 Fault tree within the transmission system

because this type of a decoder is realised on the fail–safe principle (there are special technical measures applied for keeping required SIL). A safety code is not a component of the non-trusted transmission system.

The coincident effect of several factors to safety of the transmission system can be demonstrated by using Markov's chain. The system transition from a functional safety state 1 to dangerous state 6 is illustrated in Fig. 3.

The meaning of particular symbols in the diagram in Fig. 3 is illustrated in Tab. 1. The characteristics of the particular states in Fig. 5 are described in Tab. 2 and Tab. 3.

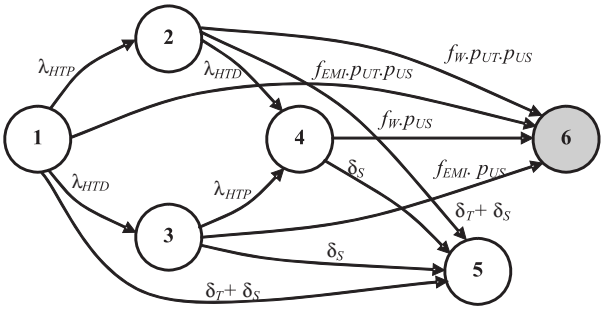

Fig. 3 Markov's chain of the transmission system

The meaning of symbols Table 1

Symbol	The meaning of a symbol
λ_{HTP}	HW failure rate of the transmitter part of the transmission system and the communication channel
λ_{HDT}	HW failure rate of a decoder of the transmission code
λ_{EMI}	The corruption rate of transmitted messages caused by EMI
p_{UT}	Probability of an undetected error of the transmission code
p_{US}	Probability of an undetected error of the safety code
f	Frequency of generating messages from a transmitter
f_{EMI}	Frequency of corrupted messages caused by EMI
f_{HTP}	Frequency of corrupted messages caused by HW failures of the transmitter part of the transmission system and the communication channel
f_W	Frequency of corrupted messages without the resolution of a corruption reason
T_T	Tolerance time of corrupted messages receiving in the non-trusted part of the transmission system
T_S	Tolerance time of corrupted messages receiving in the trusted part of the transmission system
δ_T	Intensity of the transition to permanent safety state caused by a failure of mechanisms operation for checking a number by a decoder of the transmission code
δ_S	Intensity of the transition to permanent safety state caused by a failure of the mechanisms operation for checking a number by a decoder of the safety code

Description of the diagram states Table 2

State	A description of the states
1	The transmission system is functional; transmission messages are corrupted by EMI
2	The transmission system state, when the transmitter part of the transmission system or some part of the communication channel are in failure
3	The transmission system state, when the decoder of transmission code is in failure
4	The transmission system state, when the transmitter part of the transmission system or some part of the communication channel and the decoder of the transmission code are in failure
5	Permanent interruption of transmission caused by a failure of mechanisms operation for checking of number of detected corrupted messages
6	The hazard state corrupted message was undetected

Transitions in the diagram

Table 3

Transition	A description of the transition	The meaning of transitions intensity
1 → 2	The transition is realised in consequence of the HW failure of the transmitter part of the transmission system or some part of the communication channel	λ_{HTP}
1 → 3	The transition is realised in consequence of the HW failure of a decoder of the transmission code	λ_{HDT}
1 → 5	The transition is realised in consequence of mechanisms operation for checking the number of detected corrupted messages by a decoder of the transmission code or the safety code	$\delta_T + \delta_S$
1 → 6	The transition is realised in consequence of the insufficient detection characteristic of the transmission and safety codes	$f_{EMI} \cdot p_{UT} \cdot p_{US}$
2 → 4	The transition is realised in consequence of the HW failure of a decoder of the transmission code	λ_{HDT}
2 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by decoder of transmission code or safety code	$\delta_T + \delta_S$
2 → 6	The transition is realised in consequence of the insufficient detection characteristic of the transmission and safe codes	$f_W \cdot p_{UT} \cdot p_{US}$
3 → 4	The transition is realised in consequence of the HW failure of the transmitter part of the transmission system or some part of the communication channel	λ_{HTS}
3 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code	δ_S
3 → 6	The transition is realised in consequence of the insufficient detection characteristic of the safety code	$f_{EMI} \cdot p_{US}$
4 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code	δ_S
4 → 6	The transition is realised in consequence of the insufficient detection characteristic of the safety code	$f_W \cdot p_{US}$

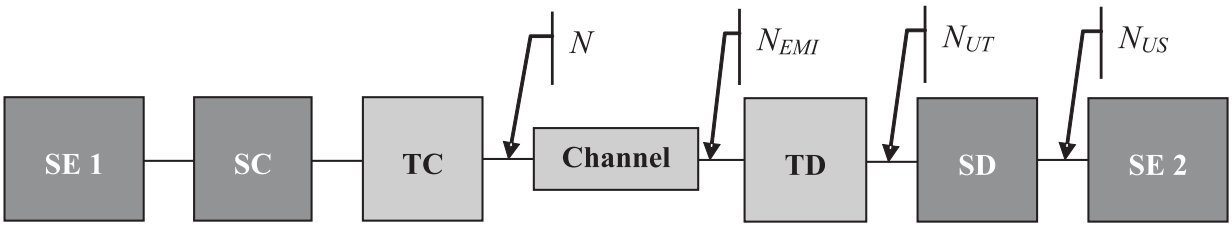

Fig. 4 Localities of number's determination of corrupted messages in the communication system

During the model designing it is necessary to know the number of corrupted messages (during a define time unit) in the parts of the communication system, which is important for the safety analysis (Fig. 4).

The meaning of the number of messages in Fig. 4 and their mathematical expression providing that the communication system is in a failure-free state:

- N is number of messages generated from a transmitter during time T, i. e. $N = f.T$.
- N_{EMI} is a number of corrupted messages in input TD during time T, i. e. $N_{EMI} = f_{EMI}.T$.
- N_{UT} is a number of corrupted messages in output of TD during time T, i. e. $N_{UT} = f_{EMI}.p_{UT}.T$.
- N_{US} is a number of corrupted messages in output of SD during time T, i. e. $N_{US} = f_{EMI}.p_{UT}.p_{US}.T$.

Similarly we can determine the number of corrupted messages which are detected by a decoder of the transmission code (N_{DT}) or by a decoder of the safety code (N_{DS}) during time T, i. e.:

$$N_{DT} = f_{EMI}.(1 - p_{UT}).T,$$

$$N_{DS} = f_{EMI}.p_{UT}.(1 - p_{US}).T. \quad (1)$$

The diagram in Fig. 3 can be simplified if we suppose that the failure of a decoder of the transmission code occurs so then there is no reason to consider some effects from other parts of the non-

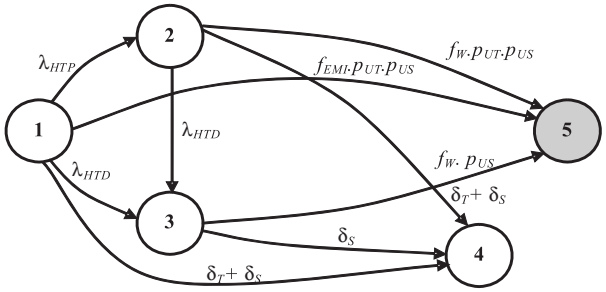

Fig. 5 Simplified Markov's chain

trusted transmission system on frequency of a corrupted data (Fig. 5).

Markov's chain can be mathematically described with the set of differential equations and by a vector of initial probabilities. The set of differential equations:

$$\frac{dP(t)}{dt} = P(t).A, \tag{2}$$

where $P(t) = \{p_1(t), p_2(t), \ldots p_n(t)\}$ is a vector of absolute probabilities and A is a matrix of intensity of transitions. The vector of initial probabilities is $P(t = 0) = \{1, 0, \ldots, 0\}$.

The matrix A for the diagram in Fig. 5 is

$$A = \begin{pmatrix} -(\lambda_{HPT} + \lambda_{HTD} + f_{EMI}.p_{UT}.p_{US}) & \lambda_{HPT} & \lambda_{HTD} & 0 & f_{EMI}.p_{UT}.p_{US} \\ 0 & -(\lambda_{HTD} + \delta_T + \delta_S + f_W.p_{UT}.p_{US}) & \lambda_{HTD} & \delta_T + \delta_S & f_W.p_{UT}.p_{US} \\ 0 & 0 & -(\delta_S + f_W.p_{US}) & \delta_S & f_W.p_{US} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{3}$$

The relation of probability of particular states occurrence in the diagram according to the parameters of a model can be exactly formulated by an analytical solution. The solution for more complex diagrams is very difficult; hence in praxis we are satisfied only with a numerical resolution. The calculation precision depends on a suitable selection of a calculation method and on a numerical precision of computing techniques. In the present time there are several SW products which support a solution with the use Markov's diagram (e. g. BQR reliability engineering [9], RELEX software [10], ITEM software [11], etc).

Such a model is based on a supposition that if the detection of a corrupted message occurs then the system will go to the previously defined safety state. Otherwise this solution contributes to the increase of the integrity level of the system but, on the other hand, significantly decreases availability of the system, which negatively affects the secondary safety. Generally, it is necessary to choose a suitable compromise between availability and on the level of safety integrity requirements. The system availability increased by using the channel correction techniques is problematic due to a masquerade of HW failures of the transmission system. For availability increase it is necessary to create such a mechanism which according to strictly defined criteria evaluates the number of received and corrupted messages and permits the communication system to remain in operation after receiving this message too. It is obvious that in this case a corrupted message must be discarded for next processing. The solution of this problem can be based on using a timer counter, which is activated in time of the corrupted message receiving. If during the specified time interval the defined number of corrupted messages is received, then the system will go to a safety state. An alternative method uses so-called ratio criteria, which is based on the evaluation of the positive and negative ratio results of the correctness control of a received message. In fact the base of this method uses a time counter, which counts in a defined range <I; M> and by start it sets an initial value I (e. g. 0). The actual value of the time counter changes according to the result of the correctness control of a received message. In case of a positive result the state of counter is decremented by P (as far of the initial value) and in case of a negative result the state of the counter is incremented by value N. The condition N>P must be fulfilled. When the counter achieves or overruns the boundary value M, the safety reaction and transition of the system to the safety state occurs.

In case this mechanism is applied it is necessary to respect this fact within the model creation and consecutive calculations.

4. Conclusion

The process of a dangerous failure rate determination, which is described in the informative part in the norm [5], is simplified and it can not be mechanically applicable within the analysis of the safety communication system. Every concrete solution of the communication system has its own specific characteristic which is to be respected within the analysis. In case of using the open transmission system the possibility of intentional corruptions or destruction of a message must be regarded.

This work has been supported by the scientific grant agency VEGA, grant No. VEGA 1/004/08 "Mathematic-graphical modelling of safety attributes of safety-critical control system.

References

[1] EN 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems,* 1998

[2] IEC 61784-3: *Digital data communications for measurement and control, Part 3: Profiles for functional safety communications in industrial networks,* CDV 2007

[3] NAIR, S., VASKO, D.: DeviceNet Safety: *Safety networking for the future*, 9th CAN conference, Munich, 2003

[4] ProfiSafe: *Test Specification for Safety-Related Profibus DP Slaves,* draft version 0.82, PNO Order No 2.242, 2003

[5] EN 50 159-1: Railway applications: Communication, signalling, and processing systems, Part 1: *Safety-related communication in closed transmission systems*, 2001

[6] EN 50159-2: Railway applications: Communication, signalling and processing systems, Part 2: *Safety-related communication in open transmission systems*, 2001

[7] FRANEKOVA, M.: *Mathematical Apparatus For Error Probability Determination of Block Code Decoders*, Scientific Journal Communications, 4/2001, pp. 59-63, ISSN 1335-4205

[8] Unified Modeling Language Version 2.1.1. http://www.uml.org

[9] BQR Reliability Engineering. http://www.bqr.com

[10] Relex Software Continental Europe. http://www.relexsoftware.de

[11] Item Software. http://www.itemuk.com.