MODELLING OF SAFETY FIELDBUS SYSTEM VIA SW TOOL SHARPE

J. Rofár, M. Franeková

Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina
Univerzitná 1, 010 26 Zilina, tel.: +421 41 513 3337, mail: jan.rofar@fel.utc.sk

Summary Paper deals with the modelling of the safety-related Fieldbus communication system, which has to guaranty Safety Integrity Level (SIL) according to standard IEC 61508. There are methods of safety analysis for the closed safety Fieldbus transmission system summarized. The mainly part the modeling SW tool SHARPE describes. The realized models are based on Fault Tree Analysis (FTA) and Markov analysis.

1. INTRODUCTION

Nowadays the number of vendors of the safety – related communication technologies who guarantee besides the standard communication, the communication among the safety – related equipment according to IEC 61508 [1] is increasing. Also the number of safety – related products is increasing, e. g. safety Fieldbus, safety PLC, safety curtains, safety laser scanners, safety buttons, safety relays and other. The buses with the communication profiles CIP Safety, ProfiSafe [2] are recommended for using in the safety – related systems with the safety integrity level 3 according to IEC 61508 or the category 4 according to EN 954-1.

Modelling fulfils a very important task in process of analysis and synthesis of the safety – related communication systems within their lifetime. Within modelling the several parameters of system are controlled, which are the component part of the technical quality of a system. Between markers of the quality of systems belong: reliability, safety, lifetime, availability, no-failure operation, maintenance and assurance of maintenance [3]. Norm EN 50129 valid for interlocking systems [4] recommends to control within lifetime of system four parameters reliability, availability, maintainability and safety, signed as RAMS parameters.

Choices of the suitable modelling method or technique depend on the type of Fieldbus system.

Models are very often used in the process of structure design (production of new product) and also in the case of the setting of parameters after invasion to existing communication system, e.g. reparation of system or addition of safety function to system for reason of increasing safety integrity level of system (SIL). In order to achieve these tasks it is generally required to combine suitable modelling methods and tools on the base of the quantitative and the qualitative methods. The qualitative modelling method FTA (Failure/Fault Tree Analysis) is based on the deductive access (process from above to down) [3]. The goal of safety analysis on the based of fault tree is identification of failures types of system, which can cause the total failure of system. All reasons or the types of failures are determined for the top event or critical failure to next function level of the system. Accordance with [1] the quantitative method on the base of Markov analysis and Markov models is recommended for monitoring of RAMS parameters. The promulgation of IEC standard 61508 has significantly re-vitalized Markov analysis by requiring the analysis of various disparate failure modes from a safety perspective. The methods also are receiving more attention because today‘s software tools make computationally complex Markov analyses easier to perform than in the past [9].

2. MODELLING OF FAILURE EFFECTS WITHIN SAFETY FIELDBUS SYSTEM

Assume the digital industrial bus (Fieldbus) according to standard IEC 61158 [5]. Across this Fieldbus can communicate safety-non-related equipment (SNRE) as well as safety-related equipment (SRE). Analysis is focused just on the communications between the safety-related equipment (Fig. 1), which can fulfill the required safety integrity level (for safety industrial applications is sufficient the value SIL 3).

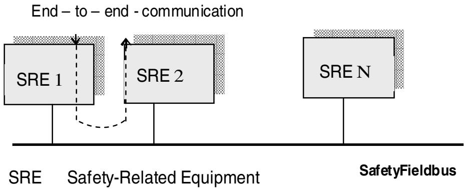

Fig.1 Communication between the safety-related equipment within the safety Fieldbus

Analysis of the communication is done on the level of the end to end connection (Fig. 2). The communication system consists of the safety-related equipments (SRE1, SRE2) and the trusted transmission system, which executes the safety-related functions within transmission according to [6]. Beneath the trusted transmission system is untrusted transmission system, which ensures the transmission messages by the transmission code. To achieve the required safety level of transmission, the transmission messages have to be ensured by the safety code, which is located into safety–related communication layer (SCL). Encoder and decoder of the safety code have to be realized on the fail-safe principle. The component part of the transmission system is the communication channel, which is influenced by electromagnetic interference only (EMI). The authors assume the closed transmission system and independence of encoders/decoders of the safety and transmission code.

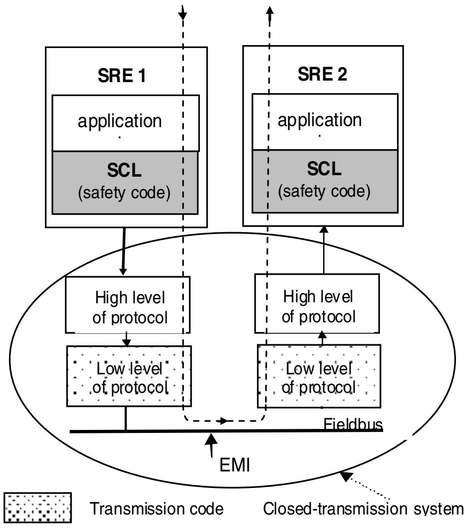

Fig.2 Communication within closed transmission system

The aim of the failure effects analysis on the safety is to form a model which allows to identify the transmission 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 systems as a failure effect to a operating system.

Fieldbus system normally does not work isolated but it is component part of another superior system for which it provides services. It means that initial point for safety evaluation model is to define the peripheries and borders of the transmission system and its superior control system with the aim to identify possible hazards of transmission system. Also it is necessary to define undesirable output events according to safety properties of the system. Undesirable events are usually undetected message integrity corruptions. Besides the analysis of safety functions it is necessary to make a quantitative evaluation of the undetected message rate of the transmission system according to [6].

The knowledge of faults attributes of the Fieldbus forms the basic assumptions related to the measures relation not only used to avoid failures but also for the fault detection and negation of the failure effects within their occurrence. From this vision the considered faults in the transmission system Fieldbus can be divided to the following types: random failures of the transmission system Fieldbus HW; failures caused by EMI and systematic failures of the transmission system.

The occurrence of a systematic failure is bonded to a concrete situation and a state of the Fieldbus transmission system. Mathematical modelling of this incidence is very problematic, because we have to know the type of distribution and its parameters.

Faults caused by effect of interferences are represented mainly by disturbing of communication channel in consequence in electromagnetic interference (EMI). Frequency of corrupted messages depends on a disturbance value. Because of the fact that the Fieldbus transmission system has to dispose with the required value of a safety level also in case of an unexpected reduction of transmission line quality, in practical determination we generally issue from a very pessimistic assumption (each of the messages in the output of the transmission is corrupted) [7].

3. REALIZATION OF FTA AND MARKOV MODEL

The safety analysis of communication via SW tool SHARPE is created for a closed Fieldbus communication system (without fixation to concrete type of the system and vendor). Assume the communication between two safety–related equipments (SRE1, SRE2) as it is shown Fig. 2. Component part of equipment SRE is encoder and decoder of safety code (safety code is located into safety communication layer). Assume that communication system is ensured also by transmission code of untrusted transmission system too. The top event within a transmission system is corruption of message in input of the receiver of Fieldbus transmission system. Message can be corrupted by the following aspects: failures in transmitter part of Fieldbus communication system, failures in the transmission system (HW failures) and failure in communication channel (failures caused by EMI).

The random failures of a decoder of the transmission code are the important part in the failure effects analysis for safety of the transmission system. The failure of the transmission code decoder can cause that all received messages are considered as correct. It is also necessary to take account a situation in which a decoder of the transmission code checks the received message but after that message can be corrupted during transmission from decoder of the transmission code to a decoder of the safety code. The fault tree, which can cause undesirable event, is illustrated in Fig. 3.

Top event (failure) in this model is "*undetected corruption of message*". Under this event followed by "AND" gate are three other events. The first is "*corruption of a message*", the second is "*undetected error of the safety code*" and the last one is "*undetected error of the transmission code*".

SHARPE let users to define every event with optional distributions and their parameters. In this model are events defined by exponential distribution and the failure rate. Distributions like Weibull, distribution, Erlang distribution and others distributions are also available [8]. In the Tab.1 descriptions of the events in the model are described.

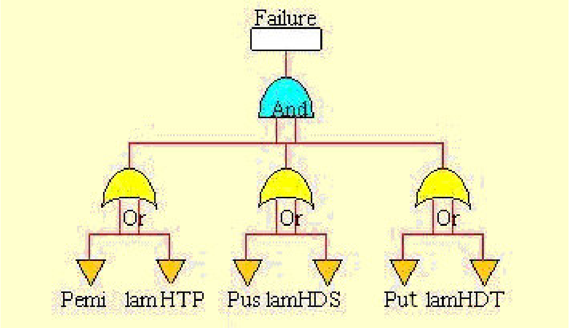

Fig.3 FTA model of safety Fieldbus via SHARPE

Tab.1 The root events of the FTA model

Event	Value	Description
Pemi	1.10^{-5}	Effect of EMI
lamHTP	1.10^{-4}	Failure of the transmitter part of the transmission system or the communication channel
Pus	2^{-32} (2^{-16})	Non sufficient detection ability of the safety code
lamHDS	1.10^{-6}	Failure of a decoder of the safety code
Put	2^{-8}	Non sufficient detection ability of the transmission code
lamHDT	1.10^{-6}	Failure of a decoder of the transmission code

During the analysis users could select one or more outputs. Each modelling method in SHARPE has got its own outputs. Outputs of FTA are divided into two main parts: models with or without repeat events and models only with repeat events. In the first group are outputs like cumulative distribution function CDF, mean time to failure MTTF etc. If the function assigned to each component is the CDF of its failure time it gives the system failure time CDF. If the function assigned to each component is the instantaneous or steady-state availability it gives the instantaneous or steady-state system. Mean time to failure gives the mean of the exponential polynomial. In the second group are outputs such a minimal cuts. Output from the model could be also reliability (safety) graph. For instance graph from realized example of models with safety codes CRC16 and CRC32 are in the Fig. 4. Time values in the graph are in seconds. Unreliability for curve 2 which describes the transmission with safety code CRC 32 is limiting the number 1 after 2.10^{10} s.

The advantage of using non-state-space models (fault trees) is that they are efficient to specify and analyze.

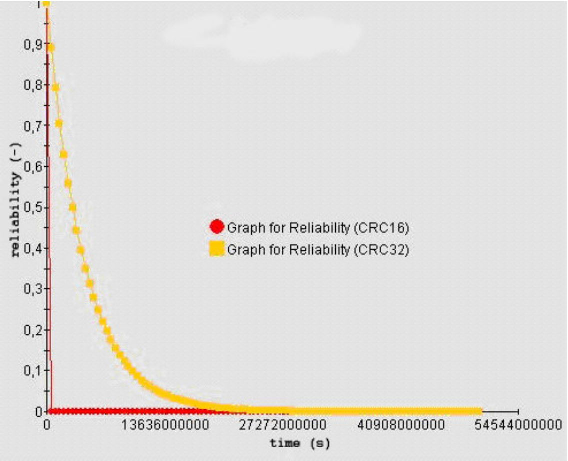

Fig.4 Reliability graph of the FTA model

However, the analysis of these models assumes the components are independent. For instance fault-tree components must be completely independent of one another in their failure and repair behavior. A failure in one component cannot affect the operation of another component, and components cannot share a repair facility.

Nowadays, one of the most commonly used techniques for the modelling of gracefully degradable systems is the Markov model. Markov analysis looks at a sequence of event and analyzes the tendency of one event to be followed by another. Using this analysis, we can generate a new sequence of random but related events, which appear similar to the original.

The Markov model assumes that the future is independent of the past given the present. When using Markov the random variable is indexed in time, which can be either discrete or continuous.

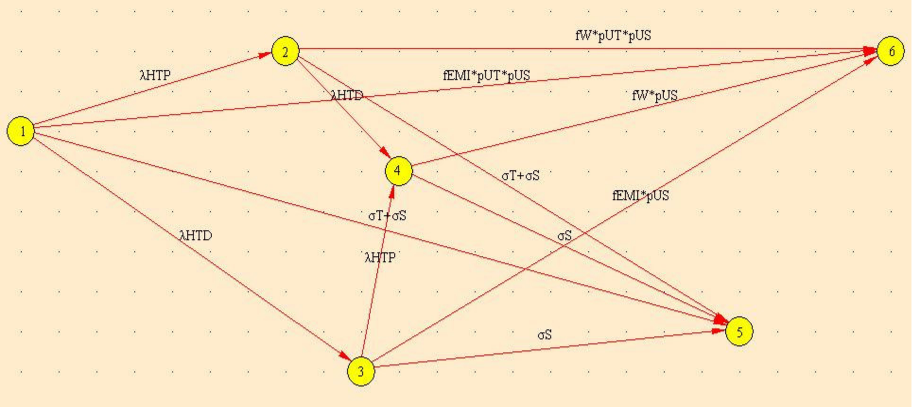

Fig. 5 Markov model of safety Fieldbus system via SHARPE

Markov model used for evaluation of safety of the Fieldbus transmission system between SRE1 and SRE2 created in a SW SHARPE is shown in Fig. 5.

Tab. 2 Description of the diagram state

State	A description of the state
1	The transmission system is functional; transmission message 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

Tab. 3 The meaning of symbols

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
f_{EMI}	Frequency of the corrupted messages caused by EMI
f_W	Frequency of the corrupted messages without the resolution of a corruption reason
p_{US}	Probability of an undetected error of the safety code
p_{UT}	Probability of an undetected error of the transmission code
σ_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
σ_S	Intensity of the transition to permanent safety state caused by a failure of mechanisms operation for checking a number by a decoder of the safety code

The system could be during a time in 6 states. Each of the states is defined in a Tab 2. System is at beginning of the simulation defined by initial probabilities. Probability to be in state 1 at the start is Pst(1) =1, it means that simulation always starts in the state 1. Transitions between states are shown in a Fig. 5 and meanings of the symbols are in the Tab 3.

Markov model analysis in SHARPE has got also several possible outputs like cumulative distribution function CDF, steady state probability, state probability at the absorption, probability to be in the state at the defined time, mean time to failure etc. Users could also use a reliability/safety graph. Among most important outputs for this model belong CDF and absorbing state probability. Given state is called absorbing when it is impossible to leave it. There are two absorbing states in this model (state 6 and state 5). Hazard state where the corrupted message was undetected (dangerous state) is 6th state. State 5 is a safety state of permanent interruption of transmission.

4. CONCLUSION

Markov models may be used to analyze smaller Fieldbus systems (as subsystem part of the total system) with strong dependencies requiring accurate evaluation. Then other analysis techniques, such as FTA, may be used to evaluate the total system using simpler probabilistic calculation techniques. Large systems, which exhibit strong component dependencies in isolated and critical parts of the system, may thus be analyzed using combination of Markov analysis and simpler quantitative models.

Acknowledgement

This work has been supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 “Mathematic-graphical modelling of safety attributes of safety-critical control systems” and particularly by grant No. KEGA- 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] IEC 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. 2007

[3] MYKISKA, A.: Bezpečnost a spolehlivost technických systémů. ČVUT Praha, 2006, ISBN 80-01-02868-2

[4] ČSN EN 50129: Drážní zařízení- Sdělovací a zabezpečovací systémy a systémy spracování

dát – Elektronické zabezpečovací systémy. 2003

[5] IEC 61158: Digital data communications for measurement and control – Fieldbus for use in industrial control systems. 2003

[6] IEC622280-2: Railway applications. Communication, signalling and processing systems, Part 1: Safety-related communication in closed transmission. 2000

[7] FRANEKOVÁ, M.- KÁLLAY, F.- PENIAK, P. VESTENICKÝ, P.: Komunikačná bezpečnosť priemyselných sietí. ŽU Žilina, 2007, ISBN 978-80-8070-715-6

[8] SHARPE Interface – user manual, version 1.01

[9] ZAHRADNÍK, J.- RÁSTOČNÝ, K.- KUNHART, M.: Bezpečnosť zabezpečovacích systémov. EDIS ŽU. 2004, ISBN 80-8070-296-9