Archives of
Transport System
Telematics

Volume 6

Issue 1

February 2013

Semi-formal methods in safety railway control systems validation

J. MAGOTT[a], A. LEWIŃSKI[b], T. PERZYŃSKI[b]

[a] WROCŁAW UNIVERSITY OF TECHNOLOGY, Faculty of Electronics, Janiszewskiego 11/17, 50-371 Wrocław, Poland

[b] UNIVERSITY OF TECHNOLOGY AND HUMANITIES IN RADOM, Faculty of Transport and Electrical Engineering, Malczewskiego 29, 26-600 Radom, Poland

EMAIL: jan.magott@pwr.wroc.pl

ABSTRACT

The paper deals with extending the obligatory methods of safety proof of railway control and management computer systems towards more formalized methods based on mathematical apparatus. Such semi-formal methods are recommended by existing EU standards for the design, but also to demonstrate safe operation in accordance with the principle of the rail fail-safe rule, where no single error does not lead to catastrophic situations. The paper proposes an extension method of FTA (Fault Tree Analysis) method to FTTD (Fault Tree with Time Dependencies), and an analysis of THR method (Tolerable Hazard Rate) to the analysis of probability of catastrophic fault based on stationary Markov processes. Basic methods and their extension are shown on typical examples of rail automation systems: cross-level protection system and interlocking system.

KEYWORDS: safety analysis, railway control computer systems, THR, FTA, FTTD methods, Markov process analysis

1. Introduction

The papers deals with "state of art" in designing and implementation of computer railway control systems. From one side exist the UE recommendations and standards, but another side corresponds to engineering practice and maintenance of existing systems (not only computer control, but relay interlocking and hybrid systems related to computer-relay interfaces). The obligatory UE standards recommend semi-formal methods as a support for efficient safety analysis. The one of them is theory of Markov processes, the boundary probability of catastrophic failure in railway control system may be compared with THR (Tolerable Hazard Rate), but the mathematical model of the system may give detailed information about estimated time of catastrophic information and probabilistic and time parameters in states of controlled failures. The second case corresponds to semi-formal FTTD (Fault Tree with Time Dependencies) method – natural extension of obligatory FTA (Fault Tree Analysis) methods presenting the propagation of faults in the system.

2. Safety railway systems

The safety railway control system must satisfy the requirements of EU standards, recommendations and restrictions [9], [10], [12]. Concept of safety railway computer systems assume a very low intensity of failure. The Fig.1 shows the structure and realization of *fail-safe* control including the duplex structure of data processing (duplicated computer controllers with input/output signals).

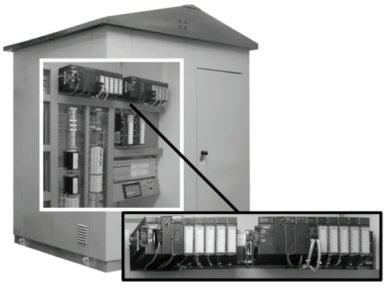

Fig. 1. The view of two channel structure of cross level protection system, type RASP-4

2.1 The closed transmission and safety criteria related to cross level protection system

railway control and management safety systems are mostly realized as a two channel redundant systems („2 from 2"). Implemented in each of the two channels PLC driver are based on two identical sets of built-in cassette form two independently working drivers with the mutual exchange of data and synchronization work through the Ethernet bus. In both channel different software is implemented (different operating systems and programs developed by independent teams of programmers). There is also secure standard ensured safety transmission (with integrity data code CRC32, detecting brake and appropriate authorization). Because cross level protection systems is produced for many years, it was possible to verify reliability parameters have a significant impact on safety (required by the standard THR level corresponds to small probabilities appearance of catastrophic situations). For systems currently in production have been proposed a method based on the producer's data, for exploited for many years systems - a method of statistical analysis of exploitation data, and for the new designed system - a method of forecasting reliability. The basis for the safe and reliable implementation of the railway signaling process is to ensure a safe of information between the systems involved in the process. The transmission of signaling systems is connected with the transmission between devices of control (commands, permission to ride) as well as confirmation of their implementation (reports, position reports). The safety data transmission in both closed and open transmission systems must meet the requirements and recommendations set out in the applicable standards [10]. The transmission system is considered a closed system in which: allowed only authorized access, is known to connect the maximum number of users, the transmission medium (usually copper wire or optical fiber) is a well-known and hard-wired devices to communicate. In this case, the probability of unauthorized access can be regarded as slight small although the network can operate both hardware protected and unprotected. The basic security of transmission is data integrity CRC code (Cyclic Redundancy Code) [2]. In addition, besides codes, the security increasing the transmission of safety level was introduced: diversity headers telegrams for channels A and B, and various locations of the telegram, variation in length and content of the various telegrams with excess information, time criterion causing the lack of a valid telegram in time about 1s is interpreted as a pause in transmission and causes the transition system to a safe state, failure the transmission cables, cards and power transmission, causing a break in the transmission and safe reaction of the system.

2.2 New generation of cross level protection system with open transmission

The very good example of introduction of open transmission standard instead existing cable connection is innovative system of cross level protection [4]. Because λ_{OTS} is quantity 10^{-12} about reliability of the system decided hardware ($\lambda \sim 10^{-05}$). The applied B0 type transmission with duplex structure of radio-connection ("2from2") satisfies SIL4 requirements.

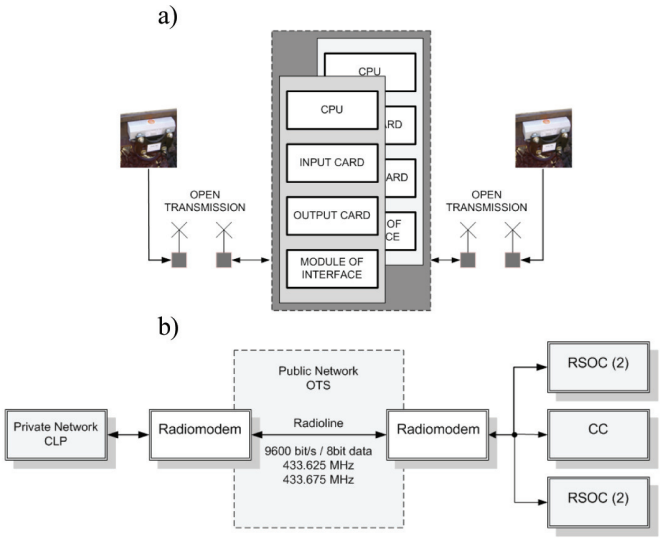

Fig. 2. a) example structure of cross level protection system with OTS, b) the experimental structure of railway management with OTS

The another application of OTS is experimental system of railway management and area control ESTER [1] with basic structure presented on Fig.2b. The following subsystems may be distinguish: Cross Level Protection System (CLP), Station Control System (CC), Rail Section Occupancy Control System (RSOC).

3. THR and Markov processes

the idea of safety computer systems in railway control application, defined in EU standards EN 50129 [9] assumes the significantly low level of failures and redundant channel architecture ("2 from 2" or "2 from 3"). Such assumptions lead to very small value of probability of critical (catastrophic) fault related to multiple failures in independent processing channels. The base of safety analysis is Tolerable Hazard Rate (THR) - measure defined with respect to failure rate (λ_i) in channel "i" and connected time of system reaction (t_d) after failure in this channel [8]:

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \quad (1)$$

For the system, in which the testing is holding periodically, the safe down rate equals:

$$t_d = \frac{T}{2} + NT \quad (2)$$

where: T – time of periodical testing, NT – negation time.

The time of failure diagnostics (t_d) in railway control computer systems assigned to SIL4 level must satisfy the following relations:

- for single failure:

$$T_{sf} = \frac{k}{1000 \cdot \lambda} \quad (3)$$

• for multiple failures:

$$T_{2sf} = \frac{2}{\lambda} \tag{4}$$

where k is redundancy coefficient equal to 1 for "2 from 2" systems and equal to 0.5 for "2 from 3" systems, and λ is a sum of mean intensities of elements leading to catastrophic situation.

3.1 Tolerable hazard rate calculations

In order to estimate the THR it is necessary data of failure rate of individual components and cards. In designer phase the only way to calculate characteristic rates is forecasting estimation. On the basis of forecasting estimation the THR for the system presented on Fig. 1 was calculated [7], [8]. Assuming T = 500ms (time of periodical testing), negation time NTin = 1s, negation time NTout = 1s and because time $NT_{IN} = NT_{OUT}$, t_d = 1.25s, estimated THR equal:

$$THR = 2,46678 \cdot 10^{-12} \tag{5}$$

For the system presented on Fig. 2a, assuming value of failure rate and time t_d published in [8] and open transmission characteristics [5], the estimated THR value equals:

$$THR = 5,56 \cdot 10^{-12} \tag{6}$$

This THR value is similar to existing cable realization of cross level protection systems.

3.2 Markov processes

Another recommended method for analysis and modeling of railway traffic are Markov processes [3], [8]. Markov processes belong to a group of stationary stochastic processes, that is, probabilistic properties of which do not change during the conversion of the time axis. Markov processes with continuous time closely correlated with the Poisson process. If the transition from one state to another due to a jet stream of events is Poisson stream, the random process running on the system is a Markov process with an abrupt and continuous time. The transition of the system from the state S_i to the state S_j is a function $\lambda_{ij}(t)$, where λ is failure rate or the intensity of transitions. Matrix describing the graph corresponds to a chain that can be written in the form of differential equations. The differential equation for the *i* state is shown in the formula:

$$\frac{dP_i(t)}{dt} = -P_i(t)\sum_{i=1}^{n}\lambda_{ij}(t) + P_j(t)\sum_{j=1}^{n}P_i(t)\lambda_{ji}(t) \tag{7}$$

where *i = 1, 2, 3, ..., n,* $P_i(t)$ – probability distributions of individual states. To solve this equation must be set the initial conditions:

$$P_i(0) = P_i \tag{8}$$

where i = 1, 2, 3, ..., n.

On the Fig. 5a the model of *2from2* (cross level protection system) system is presented [8]. It is a system without repair, used in many systems of railway automation. Solving the equations, and using the inverse Laplace transform, it was received the equation:

$$P2(t) = \frac{\lambda\left(\left(1 + e^{-2t\lambda} - 2e^{-t(\lambda+\mu)}\right)\lambda + \left(-1 + e^{-2t\lambda}\right)\mu\right)}{\lambda^2 - \mu^2} \tag{9}$$

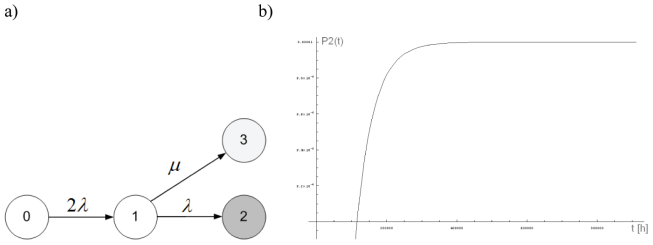

Fig. 5. a) model of system *2from2*, b) function P2(t)

Estimated probability of P2 (catastrophic, dangerous state) for the model from Fig. 5a is expressed by the formula:

$$P2 = \frac{\lambda}{\lambda + \mu} \tag{10}$$

Based on Mathematica software and assuming rates ($\lambda = 0{,}00001h^{-1}$, $\mu = 1h^{-1}$) the function of P2(t) is presented on Fig. 5b.

4. FTA and FTTD methods

In relation to the railway standards, another obligatory method of safety analysis is *Fault Tree Analysis* (FTA). The FTA method [2], [5], [11] requires detailed information about events and time dependences between them. In classical description in the FTA analysis there is no dependence on time between individual events, but for testing time dependence in FTA there can be used Petri Nets methods. The new method, proposed in the paper is natural extension of FTA towards FTTD (Fault Tree with Time Dependencies). This method is a type of dynamic analysis, some faults may be catastrophic after assumed time [6].

4.1 The typical FTA analysis

The Fig. 6 shows the scheme of FTA analysis of cross level protection systems with additional event - *Transmission Error* (Fig. 6a) and with closed transmission (Fig. 6b). The top event is a *Critical Fault*. To carry out the FTA analysis (Fig. 6a), with regard to data from forecasting estimation [8], the values of failure rate of each card was assumed [2]: input card - 1.21e-05h^{-1}, output card - 9.45e-06 h^{-1}, CPU - 4.16e-05 h^{-1}, module of interface - 2.62e-05 h^{-1}, error of transmission on the basis of formula:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \tag{11}$$

On the basis of FTA trees diagram it fallows that for such assumption and type of the tree, probability of failure at a given time point – 100 000h for both systems amounts 0.99986.

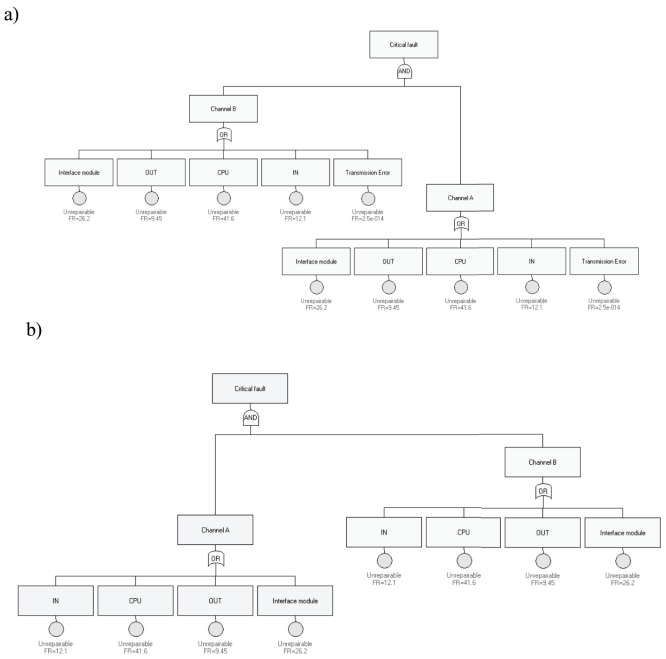

Fig. 6. a) FTA analysis of cross level protection system with open transmission error, b) FTA analysis system with closed transmission

4.2 FTTD

The Fault Tree with Time Dependencies Analysis (FTTD) allows, additionally, for analysis of timing relationships between events [6]. To avoid ambiguity, a notation of events and gates in Fault Tree with Time Dependencies (FTTD) was formalized.

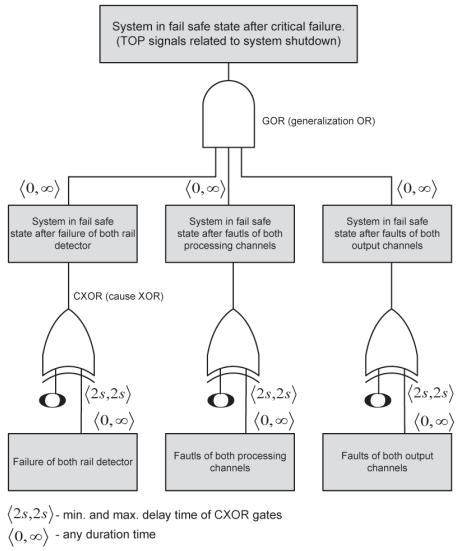

Fig. 7. FTTD analysis of cross level protection system corresponding to FTA analysis from Fig. 4

More information about FTTD and FTTDA can be found in [4]. The assumptions in FTTD analysis include the reaction time corresponding to (2), and does not include the dynamic of he train and its context with other trains and emergency breaking procedure. The main information is related to signaling TOP lights for train driver without signals about barriers and signals for car divers. Of course the open transmission is only one part replacing the existing cable transmission, but the safety level corresponding to SIL4 is the same.

5. Conclusion

The main idea of the paper is an extension of obligatory methods used in safety proving of railway control systems to more scientific methods of safety systems analysis recommended in UE standards.

The THR as a safety measure has a form of critical failure intensity, independent of exploitation time and environment conditions. Of course is minimal standard required for safety system, but Markov (or semi Markov) process analysis may show how the probability of catastrophic failure may change in time. (The more sophisticated models may regard the human factor or transmission parameters.)

The obligatory FTA method is typical static analysis, the final catastrophic situation is a composition of signals evaluated using logical operations (AND, OR gates) In real railway control systems time parameters (delays, reaction times or lost of transmission) have a great influence for faulty accident. The proposed FTTD method may regard the time coincidences in each FTA branch, including the appearance of top event – catastrophic failure.

The paper shows the another question – the computer support of safety analysis. The basic, the methods such THR, FTA or FTTD may be done using specialized software, Markov process may be analyzed using typical academic package such MATHEMATICA or MATLAB.

Bibliography

[1] KOMBUD S.A. Technical Documentation
[2] LEWIŃSKI A, PERZYŃSKI T., TORUŃ A.: Risk Analysis as a Basic Method of Safety Transmission System Certification. CCIS vol. 239. Springer 2011'.
[3] LEWIŃSKI A., PERZYŃSKI T., TORUŃ A: The Analysis of Open Transmission Standards in Railway Control and Management. In J. Mikulski (Ed.): TST 2012, CCIS vol. 329, pp. 10–17, Springer, Heidelberg (2012)
[4] LEWIŃSKI A., PERZYŃSKI T.: The reliability and safety of railway control systems based on new information technologies. In J. Mikulski (Ed.): TST 2010, CCIS vol. 104, pp. 427-433, Springer, Heidelberg (2010)
[5] LEWIŃSKI, A., PERZYŃSKI, T., TORUŃ A.: The risk analysis as a basic designed methods of safety open network transmission applied in railway control systems. Logistyka 03/2011, (in Polish)
[6] MAGOTT J., LEWIŃSKI A., SKROBANEK P., TORUŃ A.: The FTTD method application to the safety analysis of Changeable Block Distance System, In J. Mikulski (Ed.): TST 2012, CCIS vol. 329, pp. 267–275, Springer, Heidelberg (2012)

[7] Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defence (1991)
[8] PERZYŃSKI, T.: The problems of safety of computer nets applied in the railway control. PhD dissertation – Technical University of Radom, Faculty of Electric Engineering and Transport, Radom (2009), (in Polish)
[9] Standard PN-EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling
[10] Standard PN-EN 50159 – 2010. Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems.
[11] Standard PN-IEC 1025:1994 – Fault tree analysis (FTA).
[12] Standards PN-EN 50126 - "Railway application – The specification and Demonstration of Reliability, Availability, Maintainability and Safety RAMS".