COMPUTER AIDED SAFETY ANALYSIS OF RAILWAY CONTROL SYSTEMS

KOMPUTEROWE WSPOMAGANIE ANALIZY BEZPIECZEŃSTWA W SYSTEMACH STEROWANIA RUCHEM KOLEJOWYM

Andrzej Lewiński, Tomasz Perzyński, Lucyna Bester

Kazimierz Pulaski University of Technology and Humanities in Radom

e-mail: a.lewinski@uthrad.pl

Abstract: *The paper deals with computer support of safety analysis of railway control system corresponding to each stage of its life cycle, especially design, testing and maintenance. It is related to the reliability estimation of actually designed, manufactured or exploited from several years railway control systems. But is possible to analyze with computer support the occurrence of critical situations using FTA method, estimation of probability connected with such situations and verification of obtained results using simulation methods. The paper is final report of research works realized in Electronics&Diagnostics Department in Faculty of Transport and Electrical Engineering UTH in Radom.*

Keywords: *safety of railway systems, computer analysis of safety*

Streszczenie: *W pracy przedstawiono komputerowe wspomaganie analizy bezpieczeństwa na każdym etapie życia systemu sterowania ruchem kolejowym: projektowania, testowania i eksploatacji. Dotyczy to szacowania niezawodności systemów nowoprojektowanych, aktualnie produkowanych oraz tych eksploatowanych od co najmniej kilku lat. Pokazano możliwość stosowania komputerowego wspomaganie analizy wystąpienia sytuacji krytycznych metodą FTA, szacowanie prawdopodobieństwa takich zdarzeń, czy weryfikację oszacowanych wartości metodą symulacji komputerowej. Artykuł jest podsumowaniem prac naukowo badawczych prowadzonych w Zakładzie Elektroniki i Diagnostyki na Wydziale Transportu i Elektrotechniki UTH w Radomiu*

Słowa kluczowe: *bezpieczne systemy srk, komputerowe wspomaganie analizy bezpieczeństwa*

1. Introduction

Polish accession to the EU in 2004 caused mandatory application of standards related to the design, testing, implementation and maintenance of safety systems of rail automation. The standards: PN-EN 50126 [10], PN-EN 50128 [11], PN-EN 50129 [12] and PN-EN 50159 [15] have become in force. In these standards identified, among other things, reliability, availability, maintainability, safety, [10], procedures and technical requirements for software design safety electronic system for the control and protection in railway application [11]. In addition, the standards defined the requirements for the design, testing, acceptance and approval of electronic systems, subsystems, devices signaling [12] and safety of open and closed transmission [15]. Currently, the basic numerical measure of safety of the system is the Tolerable Hazard Rate (THR) [16]. Determination of numerical values of THR is not the only way to assess the risk of signaling railway systems. There are other methods identified in standards such as the analysis using Markov processes and Fault Tree Analysis (FTA) [7]. In the safety analysis of the railway systems very helpful is computer simulation (used as a method of verification the parameters assumed in mathematical analysis). The analysis presented in the paper shows how the obligatory methods and recommended standards of the EU may be assisted by a professional and useful software developed for specific applications (e.g. determination of the failure intensity of the systems with complex series-parallel structure). In the paper the RASP cross level protection system is analysed. It is a typical example of realization “2from2” redundant structure, [8], [16], [22].

Fig. 1 Cross level protection system RASP-4 a) view of inside container, b) structure of the system (based on Kombud S.A.) [22]

2. Estimation and verification THR rate as a method of safety analysis

Concept of safety computer systems used in the railway systems assumes a very low intensity of faults, which with the total independence of processing channels ensures low probability of double or multiple failure - deciding on catastrophic failure (critical). The basis of analysis is the acceptable level of risk presented on the formula (the safety of the system depends not only on the intensity of the failure, but also depends on the time of single or double failure detection), [16]:

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

where:

- λ_i – failure rate,
- $t_{d_i}^{-1}$ – safe down rate.

The acceptable values THR for SIL-4 (Safety Integrity Level) are in the range $10^{-9} \leq THR \leq 10^{-8}$. The systems classified to the SIL-4 is combined with the time of single failure:

$$T_{sf} = \frac{k}{1000 \cdot \lambda} \quad (2)$$

and double failure:

$$T_{2sf} = \frac{2}{\lambda} \quad (3)$$

where:

- k – redundant rate (=1 for „2from2” and =0.5 for „2from3”),
- λ – a sum of middle failure intensity of elements which failure in the same time can cause dangerous situation.

One of the software used for forecasting and estimating parameters of reliability is SOBIN software [21]. This software consists of basic blocks: block input and block parameters for calculating of reliability. In the case of analytical solutions for the system composed of serial structure elements and assuming an exponential function of failure, the failure rates of the individual modules are summed:

$$\lambda_0 = \lambda_1 + \lambda_2 + \dots + \lambda_i = \sum_{i=1}^n \lambda_i \quad (4)$$

In the case of components working in parallel structure, there is a problem to estimate in a simple way the failure rate, and therefore a similar analysis can be based on calculation of the middle time to failure. For $n=2$ and $n=3$ (typical redundant in rail systems) it is shown in formula (5), [16]:

$$T_{MTF_{n=2}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} = \frac{3}{2\lambda} \Big|_{\lambda_1=\lambda_2=\lambda}$$

$$T_{MTF_{n=3}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \left(\frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_2 + \lambda_3} + \frac{1}{\lambda_1 + \lambda_3} \right) + \frac{1}{\lambda_1 + \lambda_2 + \lambda_3} = \frac{11}{6\lambda} \Big|_{\lambda_1=\lambda_2=\lambda_3=\lambda} \quad (5)$$

mean time to failure in module i equals:

$$T_{MTF_i} = \int_0^{\infty} R_i(t) dt = \int_0^{\infty} e^{-\lambda_i t} dt = \frac{1}{\lambda_i} \quad (6)$$

Figure 2 presents the window of software (SOBIN), in which the structure of channel in RASP-4 system is defined.

Nr	OK?	Nazwa podsystemu	Węz.pocz.	Węz.koń.	Lambda	MTTF
0	TAK	CALY SYSTEM	A	Z	4,78E-5	2,09E+4
1	TAK	NT/PS	A	B1	4,22E-5	2,37E+4
2	TAK	NT/PS	A	C1	4,22E-5	2,37E+4
3	TAK	CPU	B1	B2	1,52E-5	6,58E+4
4	TAK	CPU	C1	C2	1,52E-5	6,58E+4
5	TAK	PIFA	B2	B3	1,23E-6	8,13E+5
6	TAK	PIFA	C2	C3	1,23E-6	8,13E+5
7	TAK	E16A	B3	B4	8,40E-6	1,19E+5
8	TAK	E16A	C3	C4	8,40E-6	1,19E+5
9	TAK	A12B	B4	Z	4,60E-6	2,17E+5
10	TAK	A12B	C4	Z	4,60E-6	2,17E+5
11	NIE					
12	NIE					
13	NIE					
14	NIE					
15	NIE					
16	NIE					

Fig. 2 The window of SOBIN software (own study).

Estimation of THR based on producers data

For equipment used in RASP-4 system authors gave the following values MTBF (Mean Time Between Failures) based on producer data (Astor Kraków):

- main case IC695CHS012 – 761 000 [h],
- Power supply adapter AD IC695PSD140 – 1 092 000 [h],
- CPU IC695CPU310 – 638 000 [h],
- communication interface IC695ETM001 – 992 000 [h],
- In module IC694MDL660 – 6 393 000 [h],
- Out module IC694MDL754 – 553 000 [h].

Configuration of controllers contain different amounts of modules, which, assuming the worst case – serial structure, the MTBF value with different configuration is contained from 106 832.6186 [h] to 144 374.4267 [h]. Assuming short time of single detection and transition to the safety state, the THR rate equal $2.19\text{e-}13$ and is accordance with standard PN-EN 50129 for level SIL-4.

Forecasting estimation as a method of estimating the reliability of new systems

In the case of a system with unknown reliability characteristics of components it is possible to estimate failure rates by calculating the failure rate of the system based on the amount and reliability structure used discrete components and integrated circuits with different scale of integration. The general form for estimating operational reliability of discrete semiconductor is presented in formula, [8], [9], [16]:

$$\lambda_p = \lambda_b (\pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E) \quad (7)$$

where:

- λ_p - the part failure rate,
- λ_b - the base failure rate usually expressed by a model relating the influence of electrical and temperature stresses on the part,
- π_E - environmental factor,
- π_A - application factor,
- π_S - electrical stress factor,
- π_T - temperature factor,
- π_R - power rating factor, π_Q - quality factor,
- π_C - contact construction factor.

On the basis of the technical documentation there was prepared a preliminary study of the safety analysis in order to estimate the failure rate λ and the THR coefficient. The results of estimation are as follows:

- sensors driver – $\lambda = 8,8\text{E-}05$,
- radio driver 1 – $\lambda = 4,09558\text{E-}05$,
- radio driver 2 – $\lambda = 1,50242\text{E-}05$,
- decision system – $\lambda = 2,54\text{E-}04$.

Result of estimation: $\lambda = 3,98\text{E-}04$, $t_d = 1,25\text{s}$, THR equals $1.1 \cdot 10^{-10}$.

The estimation of THR on the basis of forecasting

The value of failure rate is possible to be estimated on the basis of forecasting. Tests of compatibility are one of the ways of verification assumed hypothesis of failure rate. In the paper there was used the χ^2 Pearson test [16]. It is nonparametric test of verification. The χ^2 Pearson test is used in case, when n -time experience may possess k – different results. The statistics presents formula:

$$\chi^2_{emp} = \sum_{i=1}^k \frac{(n_i - n_i^t)^2}{n_i^t} \quad (8)$$

where:

$$n_i^t = N \cdot p_i^t; \quad N = \sum_{i=1}^k n_i; \quad p_i^t = P_F \{X - \text{assumed value of class } i\}.$$

If $\chi^2_{emp} > \chi^2(\alpha; k - r - 1)$ - assumed hypothesis H_0 is rejected (r – number of unknown parameters of the hypothesis distribution F). In the Table 1. there is presented a description of statistics. The Fig. 3 shows the lists of intensities of failures in RASP-4 cross level protection system (assumed time interval 2700h, each interval 4500h), [16]. To estimate the failure rate λ the Statistica software was used, [19]. Because the hypothesis was not rejected by the rejection of the assumptions for the exponential distribution, the calculated value of λ equals $7.40741 \cdot 10^{-5} \text{h}^{-1}$. For calculation of THR earlier data were used (assuming time of periodical testing $T = 500 \text{ms}$, negation time $NT_{in} = 1 \text{s}$, negation time $NT_{out} = 1 \text{s}$ and, $t_d = 1.25 \text{s}$), estimated THR equals $5,56 \cdot 10^{-12}$.

Table 1. Description of statistics

CLASS	NUMBER
$(-\infty, x_1)$	n_1
$\langle x_1, x_2 \rangle$	n_2
$\vdots$	$\vdots$
$\langle x_{k-2}, x_{k-1} \rangle$	n_{k-1}
$\langle x_{k-1}, \infty \rangle$	n_k

Fig. 3 Exploitation data, failure in time interval. (own study).

3. FTA analysis

The graphic description by Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) can be used for modeling of risk in railway control and management systems. On the basis of The Fault Tree Analysis it is possible to present factors which have an influence on safety. The FTA method requires detailed information which is necessary to analyse possible events carefully. The example of FTA is presented in the Fig. 4, [11].

Fig. 4 Example of FTA of railway system.
(own study on the basis of standard PN-EN 50159: 2010 [12])

In the case of FTA the possibility of the development of the initiating event is analyzed (in the FTA the barrier of safety is described and sequences of events are considered), [11].

For FTA analysis [14] the RAM Commander - ALD Company software was used [17]. The general assumption was: the top event, *Critical Fault*, and open transmission in system. The window of analysis is shown in the Fig. 5.

With regard to forecasting estimation data, the value of failure rate of each card was assumed:

- Input card 1.21e-05,
- Output card 9.45e-06,
- CPU 4.16e-05,
- Module of interface 2.62e-05,
- Error of transmission on the basis of formula [8]:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \quad (9)$$

The example report of analysis is presented in Fig. 5b. For such tree and assumed parameters, $Q(t)$ equals $1.09\text{e-}10$ (time of analysis 100 000h).

Fig. 5 Tree of FTA for railway level protection system of RASP-4
a) window of analysis, b) rapport of analysis. (own study)

4. Markov processes, probabilistic and time parameters in safety analysis

The railway control and management systems are safety that means that every single failure should be detected in short time. The system should initiate safety reaction and detected single failure can not cause a dangerous situation.

Therefore, stochastic processes in the form of Markov processes are convenient method of analysis for railway control systems. These systems are characterized by stochastic processes without repair. The model of cross level protection system with two computers (parallel structure) is presented in Fig. 6.

Fig. 6. Model of cross level protection system, without repair
(own study)

Assuming exponential distribution of failures and stationary, homogenous and ergodic character of stochastic process we can distinguish for two computers the following states:

- 0 - state of correct work with both computers,
- 1 - state of single (one computer) fault,
- 2 - state of catastrophic failure single computer fault without emergency reaction,
- 3 - state of fail-safe (controlled) failure initialising the emergency reaction.

The aim of the analysis of the mathematical model of the system is to determine the probability of a dangerous situation and time to achieve such dangerous state. To realize the aim authors used the Mathematica software by Wolfram Research Inc. This is a wide-ranging software for the implementation of symbolic and numerical calculations with high precision, which enables the visualization of the results. The window of Mathematica software for models from Fig. 6 is presented in Fig. 7 [16], [17].

Fig. 7 Window of Mathematica software for model from Fig. 6. (own study)

Solving the equation and using the inverse Laplace transform, the probability $P_2(t)$ was calculated:

$$P2(t) = \frac{\lambda((1 + e^{-2t\lambda} - 2e^{-t(\lambda+\mu)})\lambda + (-1 + e^{-2t\lambda})\mu)}{\lambda^2 - \mu^2} \quad (10)$$

Assuming typical rates $\lambda=0,00001\text{h}^{-1}$ and $\mu=1\text{h}^{-1}$ [16], the function of safety ($S=1-P2(t)$) is shown in Fig. 7.

It was also possible to calculate the probability of being in each state, assuming time of work $t \rightarrow \infty$. For model from Fig. 6 the final probability $P2$ was calculated:

$$P2(t) = \frac{\lambda}{\lambda + \mu} \quad (11)$$

Very interesting problem, from viewpoint of safety, is calculation of the probability of appearing the collision on cross level protection of category C (railway level with warning light without barrier). Model of such railway level is shown in Fig. 8 [1], [5].

Fig. 8 Model of safety for railway level of C category with warning lights.
(own study)

In the presented model (Fig. 8) we can distinguish:

- State 0 – safety state, without dangerous,
– appears rail, disappears the car,
- State 1 – the driver stopped before level, level system switch on,
- State P_k – dangerous state, collision car - rail, failure of level system.

The transitions between states describing:

- λ_1, λ_4 – intensity of transition to the state 1 and P_k ,
- μ_1, μ_4 – intensity of back to safety state „0”.

The probability of being in state $P_k(t \rightarrow \infty)$ is presented in Fig. 9. Assuming the value of parameters $\lambda_1=0,000000079$ [h⁻¹], $\lambda_4=0,0000015$ [h⁻¹] i $\mu_1=0,0016$ [h⁻¹], $\mu_4=0,3$ [h⁻¹], the probability of appearing of dangerous, catastrophic state equals $P_k = 4.98 \cdot 10^{-6}$, and $P_k(t)$ is a value, which is a measure of the quality of the system:

$$P_k(t) |_{t \rightarrow \infty} = \frac{(\lambda_1 + \mu_1)\mu_4}{\lambda_4\mu_1 + (\lambda_1 + \mu_1)\mu_4} \quad (12)$$

Fig. 9 The P_k probability profile (own study)

5. Simulation analysis of safety

From viewpoint of safety, verification of models of automation rail systems is very essential, especially parameters assumed in the models. In the chapter 2.3 the forecasting estimation results were presented on the basis of typical statistical methods. For designed systems and for systems without such research, the only method of verification are computers simulations. In the Fig. 10 there is shown the window of computer simulation. This is a simulation of model from Fig. 8, cross level protection category C. In order to make a simulation the authors used the MATLAB/SIMULINK software (with SimEvents module), [1], [5], [18].

As a result of simulation the limit probability of being in the state P_k was estimated, $P_k = 1,42 \cdot 10^{-6}$. The estimated result is consistent with result of mathematical analysis [5].

Fig. 10 The simulation of railway level of C category a) the structure of simulating models in SimEvents, b) the P_k probability of function profile. (own study)

6. Conclusions

The paper shows the modern computer-aided methods for safety analysis of control and management railway systems. Presented method can be obligatory, as THR and FTA, but also can be highly recommended as Markov process or computers simulations.

The software presented in the paper, in addition to specific results, can also generate appropriate documentation which confirms functional assumptions, particularly reliability parameters. The paper shows the analysis of one of many cross level protections systems [2], [3].

The data confirmed both the high reliability of the equipment and also an adequate level of safety (SIL-4) for such type of equipment.

7. References

- [1] Bester L. „Analiza zintegrowanego systemu bezpieczeństwa w transporcie lądowym na przykładzie przejazdów kolejowych” Rozprawa doktorska, Wydział Transportu i Elektrotechniki Politechniki Radomskiej, Radom 2012
- [2] Dyduch J., Kornaszewski M.: „Problemy bezpieczeństwa samoczynnych sygnalizacji przejazdowych stosowanych na PKP”, Transport Zeszyt 11 WPR Radom 2000
- [3] Dyduch J., Kornaszewski M.: „Systemy sterowania ruchem kolejowym”, Wydawnictwo Politechniki Radomskiej, Radom 2003

- [4] Lewiński A., Bester L.: "The dependability and safety of new wireless systems in railway control and management" ADVANCES IN TRANSPORT SYSTEMS TELEMATICS – 2007 (monograph), Katowice – Ustroń 2007
- [5] Lewiński A., Bester L.: "Additional warning system for cross level". Communications in Computer and information Science (104), Springer-Verlag Berlin Heidelberg 2010.
- [6] Lewiński A., Perzyński T. „Modelowanie bezpiecznych systemów w sterowaniu ruchem kolejowym”, Materiały Konferencji Naukowej TRANSCOMP 2005, Zakopane 2005
- [7] Lewiński A., Perzyński T., Toruń A., „Risk Analysis as a Basic Method of Safety Transmission System Certification”. Communications in Computer and Information Science 239), Springer-Verlag Berlin Heidelberg 2011
- [8] Lewiński A., Perzyński T.: The reliability and safety of railway control systems based on new information technologies. Communications In Computer and Information Science 104. Springer 2010'. Transport Systems Telematics.
- [9] Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defense (1991).
- [10] Norma PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikowanie i wykazywanie Nieuszkodzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS). Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia.
- [11] Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.
- [12] Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.
- [13] Norma PN-EN 60812:2009 Techniki analizy nieuszkodzalności systemów. Porcedura analizy rodzajów i skutków uszkodzeń (FMEA),
- [14] Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA),
- [15] Norma PN-EN 50159: 2010. Zastosowania kolejowe. Systemy łączności, sterowania ruchem i przetwarzania danych -- Łączność bezpieczna w systemach transmisyjnych
- [16] Perzyński T.: „Problemy bezpieczeństwa sieci komputerowych stosowanych w sterowaniu ruchem kolejowym”. Rozprawa doktorska, Wydział Transportu i Elektrotechniki Politechniki Radomskiej, Radom 2009
- [17] Wolfram S.: „Mathematica”, version 4, Wolfram Media – Cambridge University Press 1999
- [18] Oprogramowanie MATLAB/SIMULINK
- [19] Oprogramowanie STATISTICA

- [20] Oprogramowanie RAM Commander - ALD Company
- [21] Program do szacowania THR (SNOS-SOBIN)
- [22] Materiały firmy KOMBUD S.A. w Radomiu

Prof. PhD. Eng. Andrzej Lewiński. Graduate Warsaw University of Technology, Faculty of Electronics. Head of the Electronics & Diagnostics Department in Faculty of Transport and Electrical Engineering, Kazimierz Pulaski University of Technology and Humanities in Radom. Author's scientific interests are connected with designing and modeling of safety computer systems for railway applications, especially with reliability and correct software for such systems.

PhD. Eng. Tomasz Perzyński. Graduate Technical University of Radom, Faculty of Transport and Electrotechnical. Lecturer of Electronics & Diagnostics Department in Faculty of Transport and Electrical Engineering, Kazimierz Pulaski University of Technology and Humanities in Radom. Author's scientific interests are connected with modeling of safety computer systems for railway applications.

PhD. Eng. Lucyna Bester. Graduate Technical University of Radom, Faculty of Transport and Electrotechnical. Lecturer of Electronics & Diagnostics Department in Faculty of Transport and Electrical Engineering, Kazimierz Pulaski University of and Humanities Technology in Radom. Author's scientific interests are connected with modeling of safety computer systems for railway applications.