III INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST`03

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2003
TRANSPORT z.51, nr kol. 1608

fail safe systems,
rail control and management systems

Andrzej LEWIŃSKI[1]
Marek SUMILA[2]

THE SEMI-FUNCTIONAL AND RELIABILITY MODELLING OF RAILWAY CONTROL SYSTEMS

The correct and reliable software, properly integrated with hardware, allows analysing the safety on the system integrity level using quantity measures determined corresponding to typical reliability and maintenance parameters. Paper presents that a safety related railway control system have to be described by several numbers of parameters. In the consequence it allows to determine system integrity level. An example presents a model of a safety railroad control system, which respect UE standards.

SEMI-FUNKCJONALNE I NIEZAWODNOŚCIOWE MODELOWANIE KOLEJOWYCH SYSTEMÓW STEROWANIA

Poprawne modelowanie kolejowych systemów sterowania wymaga uwzględnienia wielu parametrów mających wpływ na pracę systemu w warunkach bezpieczeństwa. Wymaga to analizy zarówno pod kątem urządzeń jak i oprogramowania takich systemów. W artykule za przykład posłużył model samoczynnej sygnalizacji przejazdowej, gdyż odpowiada on najwyższemu poziomowi bezpieczeństwa, tzw. *fail-safe*, wg międzynarodowych standardów CENELEC. Zakładając Markowski charakter procesów wyznaczono szereg zasadniczych parametrów tego systemu.

1. INTRODUCTION

Railway control system is an important part of any railway operations management system. Over the years, a number of different approaching to railway control systems have evolved in different countries (to perform requirements national railway administrations). These systems are incompatible and not interoperable with each other. Only a few are used in more than one country and in those cases where the same basic system has been adopted in different country [2].

One of the most important enterprises was unified and integration international standards of a railway control systems. This process is connected with specify common elements of reliability in each system. In order to establish international standardization of

[1] Faculty of Transport, Radom University of Technology, 26-600 Radom, lewinski@kiux.man.radom.pl
[2] The Division of Transport Telecommunication, Warsaw University of Technology, Koszykowa 79, 02-008 Warsaw, sumila@it.pw.edu.pl

control systems, the International Union of Railways (UIC) specifies the European Rail Traffic Management System (*ERTMS*). Other: European Rail Research Institute (ERRI), European Association for Railway Interoperability (AEIF), and European Committee for Electrotechnical Standardization (CENELEC) elaborate standards to those systems too [3][7][8][9].

The special feature of railway control systems is safety related to the whole process of system design including special assessment and approval procedures (system life cycle) [7]. Some methods are recommended for each stage of this process both for hardware and software level [8]. The integration of both levels allows to safety analysis on the system levels. For such analysis the estimation the quantitative measures of safety is required. Such criterion may be evaluated corresponding to the reliability theory [4]. Assuming the Markov character of processes modeling typical exploitation of railway control systems, the non safety may by related to the P, probability of catastrophic, dangerous failures.

CENELEC introduced "System Classification in Railway Control and Management" determined five safety integrity level (4 – very high, 0 – non-safety related). They suggest the following assumptions about reliability of computer systems applied in railway signalling and management.

In the paper we consider one of a part railway control system i.e. a railroad signaling system. Such systems are classified as safety related, assigned to the highest (fourth) integrity level responds to 10^{-9} h^{-1} failure rate.

2. MODELLING RAILROAD SIGNALLING GIVE CONSIDERATION TO OPERATING

We pay attention on a railroad signalling which prevent a train – a car collision. Function of a railroad signalling is generally known and we only remain that approaching a train to the level crossing cause closing gate arms until the train leaves it. In spite of simplicity of the system, it corresponds on highest fail-safe level (4). This concept is conformed to Polish Railway Standards of those systems [1].

2.1. HARDWARE SOLUTION OF THE RAILROAD SIGNALLING

Nowadays railroad signalling systems typically based on redundant hardware structures with self-testing. The duplex structures with independent channels (hardware separated) are required by CENELEC [7][9] standards and UIC recommendations. The double CAN bus connection assure the fail safe operation, with complex monitoring and fault recovery is realised in program way. Scheidt&Bachmann elaborate this solution to cross level protection system [5].

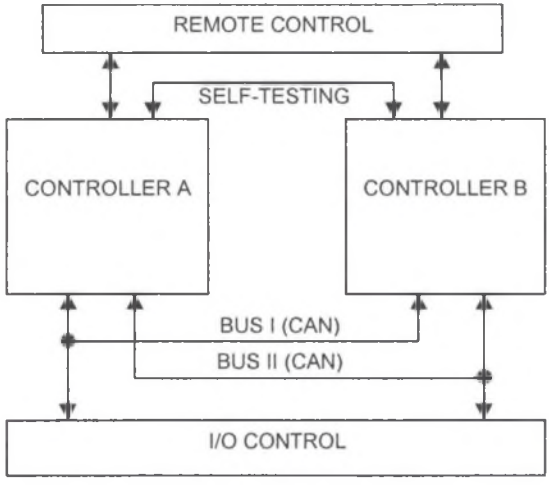

Fig.1. The railroad signalling system hardware configuration

Described by European Standards RAMS parameters[3] are determined and given by manufactures and suppliers of a system based on reliability of particular elements and exploitation experiences. A Christov model of railway control systems is a good way to analysis of many real systems and its parameters [6]. The Markov model (with repair) presented below is much more complicated to fully present estimated safety and reliability parameters.

2.2. THE MODEL OF THE SYSTEM SAFETY

Now we introduce a basic exploitation model of railroad signalling system as a state-space graph. In spite of that, our model has real complex indicators and transitions. The graph represents the status of the system with regard to its functioning and failure states. These states are represented by the nodes of the graph. In the model we consider four states: supervision (S_0), operating (S_1), fail-safe state (S_2), and non-critical fails (S_3). Diagram is given in figure 2. The transitions between the states are caused by various mechanisms and activities such as failures, repairs, replacements, and switching operations (we do not consider it in the article).

[3] RAMS: Reliability, Availability, Maintainability and Safety [7].

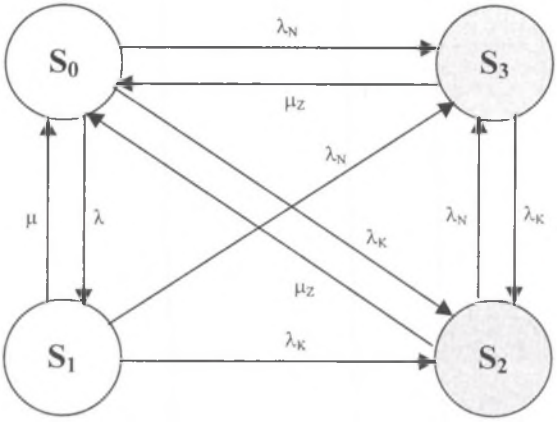

Fig.2. State-space diagram of the Railroad signalling system. S_0 – supervision, S_1 – operation, S_2 – fail-safe, S_3 – non-critical fail state, μ – trains exit rate, λ – train entry rate, λ_K – critical failure rate, λ_N – non-critical failure rate, μ_Z – repair rate

In normal operation, model is present in one of two states: supervision or operating. When any train approach to railway crossing system transits from supervision to operating state. System comes back to supervision state when last train (when it is more) leave controlled area by system. In the case when failure occurs, in any states, system goes into one of two others states: non-critical fail state or fail-safe state. It is regard to demand highest safe level for train control systems. We assumed that rates of normal work are equal:

- Train entry - $\lambda = 20\ h^{-1}$,
- Trains exit - $\mu = 20\ h^{-1}$;

Failure rates and repair rates are equal:

- Critical failure - $\lambda_K = 0.5 \cdot 10^{-5}\ h^{-1}$,
- Non-critical failure - $\lambda_N = 10^{-5}\ h^{-1}$,
- Repair - $\mu_Z^{-1} = 10^{-1}\ h$;

3. TRY TO DETERMINE PARAMETRES OF RELIABILITY

3.1. PROBABILITY OF THE FAILURE OF THE RAILWAY SIGNALLING (MARKOV PROCESSES)

In this paragraph we try to determine reliability parameters of the system with regards to the European Standards [3][5][7]. The Markov technique is suitable for modelling redundant systems in which the level of redundancy varies with time due to component failure or repair [4][8]. In probabilistic terms the Markov property is defined by

$$\begin{aligned} &P(X(t+v)=j \mid X(t)=i;\, X(u)=x(u);0\le u\le t) \\ &=P(X(t+v)=j \mid X(t)=i) \\ &\qquad\qquad \text{for all possible } x(u);\ 0\le u\le t \end{aligned} \tag{1}$$

Additional assuming, in our model the transition probability does not depend on the time t ($t \to \infty$) but only on the time interval v for the transition, the transition probabilities are said to be stationary

$$P(X(t+v)=j \mid X(t)=i)=P_{ij}(v) \quad \text{for } t,\ v>0; \quad i,j=0,1,2,\ldots,r \tag{2}$$

A Markov process with stationary (or steady state) transition probabilities is often called a process with *no memory*.

Property $P_{ij}(t+v)=\sum_{k=0}^{r} P_{ik}(t)\cdot P_{kj}(v)$, for $t,\ v>0$ is known as the Chapman-Kolmogorov equations and follows from the rule for total probability

$$\begin{aligned} P_0'(t) &= -(\lambda+\lambda_N+\lambda_K)P_0(t)+\mu P_1(t)+\mu_Z(P_2(t)+P_3(t)) \\ P_1'(t) &= -(\mu+\lambda_N+\lambda_K)P_1(t)+\lambda P_0(t) \\ P_2'(t) &= -(\mu_Z+\lambda_N)P_2(t)+\lambda_K(P_0(t)+P_1(t)+P_3(t)) \\ P_3'(t) &= -(\mu_Z+\lambda_K)P_3(t)+\lambda_N(P_0(t)+P_1(t)+P_2(t)) \end{aligned} \tag{3}$$

The general form of equations may be written as

$$\dot{P}(t)=A\cdot P(t) \tag{4}$$

The state equation (3) in general (4) can be written in matrix form

$$\begin{bmatrix} \dot{P}_0(t) \\ \dot{P}_1(t) \\ \dot{P}_2(t) \\ \dot{P}_3(t) \end{bmatrix} = \begin{bmatrix} 0 & a_{01} & a_{02} & a_{03} \\ a_{10} & 0 & a_{12} & a_{13} \\ a_{20} & 0 & 0 & a_{23} \\ a_{30} & 0 & a_{32} & 0 \end{bmatrix} \cdot \begin{bmatrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \end{bmatrix} \tag{5}$$

The state equations (5) are seen to be a set of linear, first-order differential equations. The easiest and most widely used method to solve such equations is by Laplace transforms. Additional we assume that state S_0 is an initial state. This can be expressed as

$$P_i(0) = P(X(0) = i) = 1$$
$$P_k(0) = P(X(0) = k) = 0 \quad \text{for } k \neq i. \tag{6}$$

Another assumption concern of the sum of probability and is given below

$$\sum_{j=0}^{r} P_j(t) = 1 \tag{7}$$

Finally we achieve solution of the stationary values of probabilities present in P_2 and P_3 (failure states) are equal:

$$P_2 = \frac{\lambda_K}{\lambda_N + \mu_Z + \lambda_K}; \quad P_3 = \frac{\lambda_N}{\lambda_N + \mu_Z + \lambda_K} \tag{8}$$
$$P_2 \approx 5 \cdot 10^{-7}; \quad P_3 \approx 1 \cdot 10^{-6}$$

We can see that the probability of failure not depend on frequency normal work of the system but depend on failure rates and reaction times in the emergency, safety procedure. The estimation of safety measures is necessary and obligatory for safety proof but we do not give consideration to proper work indicators.

3.2. SAFETY AND RELIABILITY PARAMETERS OF THE SYSTEM

Now we may consider several reliability parameters [4].

Mean Time to Failure

The mean time to failure ($MTTF_s$) is defined as the inverse of failure rate of the component/system ($1/\lambda$).

$$MTTF = \frac{1}{\sum \lambda} = \frac{1}{\lambda_N + \lambda_K} = 6{,}6(6) \cdot 10^4 \tag{9}$$

Mean Time to Repair

The mean time to repair ($MTTR_s$) is equal to the inverse of repair rate of the system ($1/\mu$).

$$MTTR = \frac{1}{\sum \mu} = \frac{1}{\mu_Z} = 0{,}1 \tag{10}$$

System Availability

Let $S = \{0, 1, 2, 3\}$ be the set of all possible states of the system. Some of these states represent system functioning according to some specified criteria. Let B denote the subset of states in which the system is functioning, and let $F = S - B$ denote the states in which the system is failed (see fig. 2). The average, or long-term, availability of the system is the mean proportion of time when the system is functioning; that is, its state is a member of B. The average system availability A_s is thus defined as

$$A_s = \sum_{j \in B} P_j = P_0 + P_1 \tag{11}$$

in the following we will omit term average and call A_s the system availability. The system unavailability $1 - A_s$ is then

$$1 - A_s = \sum_{j \in F} P_j$$

$$A_s = P_2 + P_3 = \frac{\lambda_K + \lambda_N}{\lambda_K + \mu_Z + \lambda_N} \approx 1{,}5 \cdot 10^{-6} \tag{12}$$

The unavailability $1 - A_s$ of the system is the mean proportion of time when the system is in a fail state. We can also write that

$$A_s = P_i = \frac{MTTF_i}{MTTF_i + MTTR_i}; \quad \text{and } 1 - A_s = P_j = \frac{MTTR_j}{MTTF_j + MTTR_j} \tag{13}$$

Frequency of System Failures

The frequency ω_F of system failures is defined as the expected numbers of visits to a fail states (j in F) per unit time, computed over a long period of time.

$$\omega_F = \sum_{j \in F} P_j \left(\sum_{\substack{k=0 \\ k \neq j}}^{r} a_{jk} + \sum_{\substack{k=0 \\ k \neq j}}^{r} a_{kj} \right); \quad \text{or } \omega_F (1 - A_s) \sum_{i=1}^{r} \mu_i \tag{14}$$

Hence

$$\omega_F = \frac{\lambda_K^2}{\lambda_N + \mu_Z + \lambda_K} + \frac{\lambda_N^2}{\lambda_N + \mu_Z + \lambda_K} \approx 1{,}25 \cdot 10^{-11} \tag{15}$$

Mean Duration of a System Failure

The mean duration θ_F of the system failure is defined as the mean time from the system enters into a fail state (F) until it is repaired/restored and brought back into a functioning state (B). It is obvious that the system unavailability is equal to the frequency of system failures multiplied by the mean duration of a system failure.

$$1 - A_s = \omega_F \cdot \theta_F$$
$$\theta_F = \frac{1 - A_s}{\omega_F} \tag{16}$$

Thus

$$\theta_F = \frac{\lambda_K + \lambda_N}{\lambda_K^2 + \lambda_N^2} = 1{,}2 \cdot 10^5 \tag{17}$$

Mean Time Between Failures

The mean time between system failures $MTBF_s$ is the mean time between consecutive transitions from a functioning state (B) into a failed state (F). The $MTBF_s$ may be computed from the frequency of system failures by

$$MTBF_s = \frac{1}{\omega_F} = \frac{\lambda_N + \mu_Z + \lambda_K}{\lambda_K^2 + \lambda_N^2} \approx 8 \cdot 10^{10} \tag{18}$$

Mean Functioning Time until System Failure

The mean functioning time (up-time) until system failure $E(U)$ is the mean time from a transition from a failed state (F) into a functioning state (B) until the first transition back to a failed state (F). Its is obvious that

$$MTBF_s = E(U)_s + \theta_F$$
$$E(U)_s = MTBF_s - \theta_F = 7{,}99 \cdot 10^{10} \tag{19}$$

4. CONCLUSION

The railway control systems demand special deal with considers to safety and reliability procedures. The safety systems design with respect recommended the safety integrated level for railway management systems need a method requires to proof the safety level. Presented methodology permits to verification of real and designed systems by estimation its parameters. In the case of new-designed systems methodology can help to choose optimal solution.

Presented in the paper model of the safety railroad signalling system consists real safety behaviour of that system. Assumed indicators come from information of manufactures and we do not change it. We determined various parameters to provide proof of system integrity level. The results of the estimation probability present in failure states P_2, P_3 are not responding to request integrity level.

Our approaching gives more precise results of estimation of safety level by specified indicators and shows that probability present in states of failure (P_2, P_3) is independent from work frequency (see (8)). It is show that assumed failure rates and repair rates are not responds to failure rate of the highest (fourth) integrity level.

In the future research, we will test potential possibility presented methodology with using CASE tools. It should provide opportunity to review and simulate modelling systems [10].

BIBLIOGRAPHY

[1] Bezpieczeństwo systemów sterowania ruchem kolejowym, Polska norma ZN-91/MTiGM-CBP-12, 1991.
[2] CICHOCKI T., GÓRSKI J.: Safety assessment of computerized railway signalling equipment, Münich – Germany 1999.
[3] DĄBROWA-BAJON M., KONOPIŃSKI L., LEWIŃSKI A.: Wybrane komputerowe systemy sterowania ruchem kolejowym na tle europejskich zaleceń normalizujących, Problemy kolejnictwa, Zeszyt 116, 1994.
[4] HØYLAND A., RAUSAND M.: System Reliability Theory. Models and Statistical Methods, JOHN WILEY & SONS, INC. Toronto, New York 1994.
[5] KONOPIŃSKI L., LEWIŃSKI A.: System wspomagający ocenę niezawodności komputerowych systemów sterowania ruchem kolejowym, materiały konferencyjne KONBIN, Szczyrk 2001.
[6] LEWIŃSKI A.: Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego, Seria Monografie Nr 49, Wydawnictwo Politechniki Radomskiej, Radom, 2001.
[7] Railway Application: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), European Standard EN 50126, CENELEC September 1999.
[8] Railway Applications: Communication, signaling and processing systems – Software for railway control and protection systems, European Standard EN 50128, CENELEC March 2001.
[9] Railway applications: Safety Related Electronic Railway Control and Protection Systems, report on the standard EN 50129, CENELEC 1997.
[10] SUMIŁA M.: Próba realizacji oprogramowania bezpiecznego SRK z wykorzystaniem technik obiektowych, VII konferencji „TRANSCOMP". Zakopane 2003.

Reviewer: Ph. D. Jerzy Mikulski