III INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'03

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

rail control systems,
fail safe systems,
safety computer networks

Andrzej LEWIŃSKI[1]
Tomasz PERZYŃSKI[2]

THE SAFETY OF MULTI- COMPUTER SYSTEMS FOR RAILWAY TRANSPORT MANAGEMENT AND CONTROL

The main aim of this work is safety characteristics of hierarchical, decomposed into several layers railway management and control systems based on ERTMS/ETCS requirements and configured from dissipated computers connected by network standards. The safety analysis related to reliability and functional parameters corresponds to Markov process modelling the exploitation of multicomputer systems composed from assumed number of coupled computers.

BEZPIECZEŃSTWO WIELOKOMPUTEROWYCH SYSTEMÓW NADZORU I STEROWANIA STOSOWANYCH W TRANSPORCIE KOLEJOWYM

Celem referatu jest charakterystyka bezpieczeństwa złożonego, wielokomputerowego systemu zarządzania i sterowania ruchem kolejowym opartego na wymaganiach ERTMS/ETCS i skonfigurowanego z rozproszonych systemów komputerowych połączonych za pośrednictwem sieci. Analiza bezpieczeństwa odnosząca się do niezawodności i parametrów funkcjonalnych koresponduje z procesem Markowa modelującym pracę systemów wielokomputerowych złożonych z przyjętej liczby połączonych komputerów.

1. THE SAFETY COMPUTER NETWORK FOR RAILWAY TRANSPORT MANAGEMENT AND CONTROL

The problems of coupled computers in the duplex systems applied in railway control have been presented in the [8]. The problem of safety defined with respect to two computers structure may be easy extended towards multi-computer structures, treated both as systems with repair and systems without repair.

The standardisation committee CENELEC suggests the following assumptions about reliability of computer systems applied in railway signalling and management. Corresponding

[1] Faculty of Transport, Radom University of Technology, 26-600 Radom, lewinski@kiux.man.radom.pl
[2] Faculty of Transport, Radom University of Technology, 26-600 Radom, perzynski@kiux.man.radom.pl

to assumption that the ratio between safety integrity levels may be as 100:1, the common failure rates (regarding system level including transmission) for subsystems are:

- System Integrity Level 4 - 10^{-9} h^{-1}
- System Integrity Level 3 - 10^{-7} h^{-1}
- System Integrity Level 2 - 10^{-5} h^{-1}
- System Integrity Level 1 - 10^{-3} h^{-1}

Table 1

Classification of computer systems in railway transport classification (CENELEC)

	Required integrity of safety	Consequences of system fault	Characteristics of system	Type of system
4	Very high	Lost of human life	To prevent the train collision and derailment	Fail-safe system
3	High	Injuries or illness	To identify the train integrity or characteristics	High integrity system
2	Medium	Environmental pollution	To manage the railway traffic	Safety involved system
1	Low	Loss or damage of property	To inform the passenger	Low integrity system
0	Non-safety related	Loss of non-safety related information	To manage the railway	Non-safety related system

Safety critical systems Safety essential) systems

These typical reliability parameters presented by producers of computer controllers and confirmed by maintenance records together with known time characteristics of designed systems give possibility of safety evaluation [3].

2. SAFETY AND RELIABILITY PARAMETERS OF COMMUNICATED NETWORKED COMPUTERS

For computer networks with greater number of communicating computers (both with repair and without repair approach) this approach may be extended in the way presented in the Fig. 1.

In the model with repair of dispatcher system [4] (Fig. 5.a) the failure for both computers may be assumed as an identical, $\lambda_M = \lambda_R = \lambda$ (typical value is less than $10^{-5}h^{-1}$), similarly the repair rates $\mu_M = \mu_R = \mu$. (typical value of repair time equal to μ^{-1} is less than $10^{-5}h^{-1}$), and probability of correct switch p (typical value is equal to $1 - 10^{-6}$).

For system composed with two main computers plus one "reserve" computer the probability of dangerous failures is more difficult to calculate, but we can estimate that

$$P_2 = P_{21} + P_{22} \approx \frac{(1-p)\lambda}{\mu} + \frac{2(1-p)\lambda}{\mu} = \frac{3(1-p)\lambda}{\mu} \tag{1}$$

We can show, that for system with n active computers and one "reserve" computer the total probability of dangerous failures P_2 is approximately equal to

$$P_2 = \sum_{i=1}^{n} P_{2i} \approx \sum_{i=1}^{n} \frac{i(1-p)\lambda}{\mu} = \frac{n(n+1)}{2} \frac{(1-p)\lambda}{\mu} \approx \frac{n^2(1-p)\lambda}{2\mu} \tag{2}$$

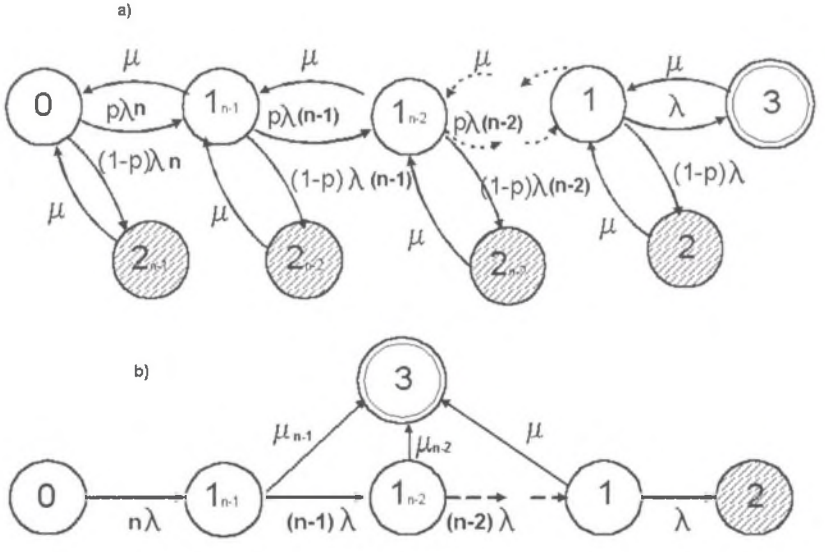

Fig. 1 Modelling of multicomputer structures a) systems with repair b) systems without repair

This approach for systems without repair may be extended in the way presented in the Fig. 6.b. System with three parallel computer ("2 from 3") has the probability of dangerous failures equal to

$$P_2 = \lim_{t\to\infty} P_2(t) = \frac{\lambda}{\lambda+\mu}\,\frac{2\lambda}{2\lambda+\mu} \approx \frac{2\lambda^2}{\mu^2}\Big|_{\mu >> \lambda} \tag{3}$$

For computer networks with greater number of communicating computers without repair this result may be extended in the way:

$$P_2 = \lim_{t\to\infty} P_2(t) = \frac{\lambda}{\lambda+\mu}\,\frac{2\lambda}{2\lambda+\mu}\,\ldots\,\frac{(n-1)\lambda}{(n-1)\lambda+\mu} = \prod_{i=1}^{n-1}\frac{(i\lambda)}{(i\lambda+\mu)} \approx (n-1)!\,\frac{\lambda^{n-1}}{\mu^{n-1}}\Big|_{\mu >> \lambda} \tag{4}$$

It is obvious that for increasing n the structure with repair the probability of P_2 will be greater (and safety measure $S = 1 - P_2$ will be worse) than for one active plus one reserve computers).

3. CONCLUSIONS

This result emphases the sense of redundancy. The fundamental rule of fail safe introduced in the [4]:

$$P_2 \approx (1-p_{FS})\,\frac{\lambda}{\mu_d} \tag{5}$$

where p_{FS} is prbability of fail safe failures (corresponding to the CENELEC requirenments the p_{FS} value must be better than $1 - 10^{-3}$, it means that one failure for thousand failures occurred may be critical). Corresponding to (2) for systems with repair

$$p_{FS} \approx p_{FS} \approx 1 - \frac{n^2(1-p)}{2} \qquad \text{for } n \geq 2 \tag{6}$$

and for systems without repair (4)

$$p_{FS} \approx 1 - (n-1)! (\lambda / \mu)^{n-2} \qquad \text{for } n \geq 2 \tag{7}$$

The main conclusion confirm the well-known rule that parallel system without repair is better for safety applications than system with reserve and reconfiguration (without repair). The analysis of safety criteria (probabilistic or time measures) for real systems based on computer networks is more complicated. The estimation of rates λ and μ, necessary for evaluation is difficult because such parameters are rather unknown and may be determined with respect to tests elaborated during several years [3]. (The estimation of μ_i in systems without repair composed with several computers is rather sophisticated with respect to characteristics of multiple switches). The repair rate may be estimated during special safety tests.

The railway management system may be treated as a large computer network integrating typical computer controllers dedicated to different functions on the distinguished levels corresponding to hierarchical multilevel approach. Such techniques combine different net technologies and transmission techniques: copper cables, fibre optics and radio transmission (GSM-R). The computer network may be treated as an approach to ERTMS project, where all systems are integrated in the form of one hierarchical system of European railway, where the co-operation of many computer systems is assumed.

BIBLIOGRAPHY

[1] Railway Application: The specification of dependability, reliability, availability, maintainability and safety (RAMS), Report on the EN 50126 standard, CENELEC 1997.

[2] DĄBROWA-BAJON M., KONOPIŃSKI L., LEWIŃSKI A., „Wybrane komputerowe systemy sterowania ruchem kolejowym na tle europejskich zaleceń normalizacyjnych", Problemy Kolejnictwa, Zeszyt 116, 1994.

[3] KONOPIŃSKI L., LEWIŃSKI A., „System wspomagający ocenę niezawodności komputerowych systemów sterowania ruchem kolejowym", Materiały Międzynarodowej Konferencji BEZPIECZEŃSTWO I NIEZAWODNOŚĆ SYSTEMÓW 'KONBIN2001', Szczyrk, 2001.

[4] LEWIŃSKI A., „Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego", Seria Monografie Nr 49, Wydawnictwo Politechniki Radomskiej, Radom, 2001

[5] LEWIŃSKI A., KONOPIŃSKI L., „Computer network systems for railway transport control and management", II Międzynarodowa Konferencja TELEMATYKA SYSTEMÓW TRANSPORTOWYCH, Katowice-Ustroń, 2002.

[6] LEWIŃSKI A., PERZYŃSKI T., „Nowe rozwiązania komputerów sterujących w systemach sterowania ruchem kolejowym na przykładzie systemów ssp", prace konferencji TRANSPORT W XXI WIEKU, Wydział Transportu Politechniki Warszawskiej, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2001.

[7] LEWIŃSKI A., PERZYŃSKI T., „New computer control systems in Polish State Railways", I Międzynarodowa Konferencja Naukowa TELEMATYKA SYSTEMÓW TRANSPORTOWYCH, Katowice-Ustroń, 2001.

[8] LEWIŃSKI A., PERZYŃSKI T., „The safety problems of computer networks in transport applications", II Międzynarodowa Konferencja TELEMATYKA SYSTEMÓW TRANSPORTOWYCH, Katowice-Ustroń, 2002.

[9] LEWIŃSKI A., KONOPIŃSKI L., „The safety of decentralised computer system for railway transport management and control", prace Międzynarodowej Konferencji KONBIN 2003, Gdynia 2003, TRANSPORT W XXI WIEKU, Wydział Transportu Politechniki Warszawskiej, Wydawnictwa Instytutu Technicznego Wojsk Lotniczych, Nr 1 /2003.

Reviewer: Ph. D. Jerzy Mikulski