II INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST`02

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2002
TRANSPORT z.45, nr kol. 1570

rail control systems,
fail safe systems,
safety computer networks

Andrzej LEWIŃSKI[1]
Tomasz PERZYŃSKI[2]

THE SAFETY PROBLEMS OF COMPUTER NETWORKS IN TRANSPORT APPLICATIONS

The paper deals with main safety aspects of safety related computer networks for railway control. The proposed model corresponding to real control systems (dispatcher centre, remote control, decentralised interlocking) and applying the homogenous and stationary Markov process allows to determine the necessary probabilistic and time parameters of redundant communicating control computers. This model may be extended towards another safety configurations connected with real requirements. Such approach is consistent with UIC recommendations and elaborated CENELEC standards for UE railways.

PROBLEMY BEZPIECZEŃSTWA SIECI KOMPUTEROWYCH W ZASTOSOWANIACH TRANSPORTOWYCH

W referacie przedstawiono główne aspekty bezpieczeństwa sieci komputerowych w konfiguracjach bezpiecznych dla zastosowań w sterowaniu ruchem kolejowym. Zastosowany model dostosowany do przykładowych konfiguracji (centrum dyspozytorskie, zdalne sterowanie, rozproszone sterowniki zależnościowe) i oparty na jednorodnych i stacjonarnych procesach Markowa pozwala określić istotne probabilistyczne i czasowe parametry komputerów nadmiarowych komunikujących się wzajemnie. Model może być z powodzeniem rozszerzony na inne konfiguracje bezpieczne, uwzględniając realne wymagania. Podejście takie jest zgodne z zaleceniami UIC oraz opracowanymi w UE standardami CENELEC.

1. INTRODUCTION

Computer networks are efficient realisation of safety systems. In transport control and management systems [1] two techniques of safety enforcement are used:

- Redundancy,
- Self-testing.

Both these methods, presented in intuitive way on the Fig.1, are applied together in the highest level (4) of system safety, especially in interlocking systems where system fault is connected with risk of human life lost. In system architecture designed by Siemens, Alcatel, two or three control computers communicate each other using fast bus interface standards. In the fail safe realisation of cross level protection controllers produced by Scheidt&Bachmann

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

or ABB Signal [2] two coupled computers are connected using serial transmission standards. Such networks related to fast rates and short distances are classified as μLAN, another applications connected with safety level 3 are typical LAN applications where computers may transmit messages up to hundred meters. These solutions are related to dispatcher centre computers or layers of centralised interlocking systems (ABB Signal, Alcatel). Level 2 corresponds to WAN, but these computer networks use special dedicated (not public) standards typical for remote control and information gathering

In all networks in railway control and management systems the safety transmission must satisfy the UIC requirements, CENELEC recommendations [3],[8],[9] and national standards [10]. Level 1 applications may apply public networks but with recommended cryptological data protection. (Level 0 is non safety related.)

There are two class of network computer systems [2]:

- System without repair (for implementation of level 4, 3, partially 2)
- System with repair (for implementation of level 0, 1, partially 2)

First systems are determined by reliability (or medium time to first failure), in the case of fault the emergency, fail safe procedure is initialled. The second systems assume the repair cycle after detected fault and is characterised by availability (or corresponding repair time and medium time between failures).

In the paper the modelling of both class of network systems using Markov processes is presented. This approach gives possibility of simple estimation of probabilistic and time parameters necessary for safety analysis.

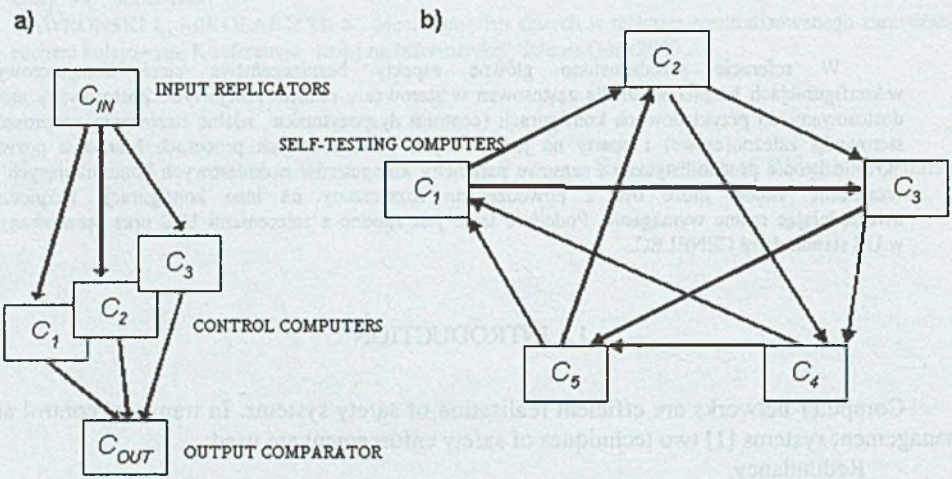

Fig.1. Redundancy, a) and self-testing, b) in computer networks

2. SAFETY RELATED COMPUTER NETWORKS

Typical computer networks applications in transport management and control is presented on the Fig.2. In the dispatcher centre presented on the Fig.2a [2],[4] both computers (main computer and hot stand-by computer) are connected using LAN standards. It is typical system with repair, after fault of main computer the stand-by computer is switched to work. After repair of permanent or reset of transient fault of faulty computer the two computers structure work is restarted. This system installed in Polish State Railways (PKP) has been successful exploited for ten years.

System without repair is μLAN solution of interlocking controller for industrial depot shows Fig.2b [1], [5], [7]. Both computers work in the parallel fail safe structure, after single fault system switches to emergency mode.

All multi-computer systems applied to railway control and management may be treated as systems of both presented classes.

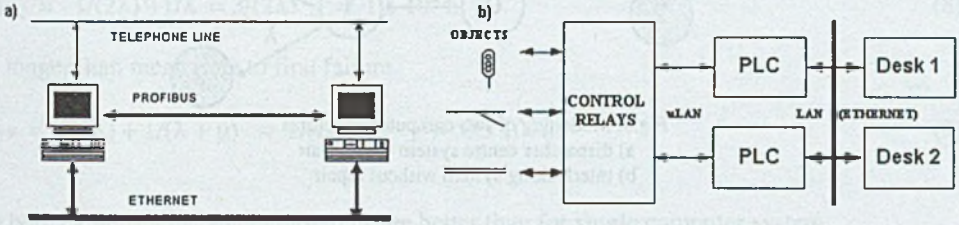

Fig.2. Computer networks in polish Railways
a) LAN computers in the dispatcher centre (system without repair)
b) μLAN computer controllers in industrial depot interlocking (system without repair)

3. SAFETY AND RELIABILRY PARAMETERS OF COUPLED NETWORKED COMPUTERS

The behaviour of multicomputer communicating systems may be modelled using Markov process model. Assuming exponential distribution of faults and stationary, homogenous and ergodic character of stochastic process [2], [4], [6] we can distinguish for two computers system 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

This state is introduced both for model without repair and model with repair presented on Fig.3.

In the model with repair of dispatcher system (Fig.3a) the failure rates and repair rates for both computers may be assumed as an identical, $\lambda_M = \lambda_R = \lambda = 10^{-5}h^{-1}$, $\mu_M^{-1} = \mu_R^{-1} = \mu^{-1} = 10^{-1}$ h , probability of correct switch (p) is equal to $1 - 10^{-6}$. The stationary values of probabilities P_2 and P_3 in this model are equal:

$$P_2 = \frac{(1-p)\lambda\mu}{\mu^2 + \lambda\mu + p\lambda^2} \quad , \quad P_3 = \frac{p\lambda^2}{\mu^2 + \lambda\mu + p\lambda^2} \tag{1}$$

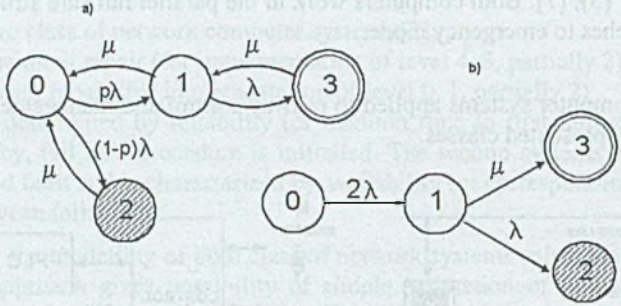

Fig.3. Modelling of two computer structures
a) dispatcher centre system with repair
b) interlocking system without repair

The safety and mean time to catastrophic failure are equal to

$$S = 1 - P_2 = 1 - \frac{(1-p)\lambda\mu}{\mu^2 + \lambda\mu + p\lambda^2} \approx 1 - (1-p)\frac{\lambda}{\mu}\Big|_{\mu \gg \lambda, p \to 1} \approx 1 - 10^{-12} \tag{2}$$

$$T_{FFC} = \frac{p\lambda^2 + p\lambda\mu + \mu^2}{(1-p)\lambda\mu^2} = \frac{1}{(1-p)\lambda}\left(1 + p\lambda\frac{\lambda+\mu}{\mu^2}\right) \approx \frac{1}{(1-p)\lambda}\Big|_{\mu \gg \lambda, p \to 1} \approx 10^{11}\,\text{h} \tag{3}$$

The availability and mean time to failure are equal to

$$A = 1 - (P_2 + P_3) = 1 - \frac{p\lambda^2 + (1-p)\lambda\mu}{\mu^2 + \lambda\mu + p\lambda^2} \approx 1 - \left(p\frac{\lambda^2}{\mu^2} + (1-p)\frac{\lambda}{\mu}\right)\Big|_{\mu \gg \lambda, p \to 1} \approx 1 - 2*10^{-12} \tag{4}$$

$$T_{FF} = \frac{\lambda + \mu + p\lambda}{\lambda^2 + (1-p)\lambda\mu} = \frac{1}{\lambda}\left(1 + \frac{p(\lambda+\mu)}{\lambda + (1-p)\mu}\right) \approx \frac{1}{\lambda}\frac{\mu}{\lambda + (1-p)\mu}\Big|_{\mu \gg \lambda, p \to 1} \approx 5*10^{10}\,\text{h} \tag{5}$$

Fig.3b shows model of interlocking control as a system without repair composed with two identical computer controllers (PLC), the outputs are compared by special fail-safe comparator. The failure rate of computer is $\lambda = 10^{-5}\ h^{-1}$ and $\mu^{-1} = t_R = 10^{-3}$ h is a time of comparator reaction after single computer fault. For this system the probabilities P_2 is evaluated as follows:

$$P_2 = \lim_{t\to\infty} P_2(t) = \frac{\lambda}{\lambda+\mu} \approx \frac{\lambda}{\mu}\Big|_{\mu \gg \lambda} \approx 10^{-8} \tag{6}$$

The safety is equal to

$$S = 1 - P_2 = 1 - \frac{\lambda}{\mu} \approx 1 - 10^{-8} \tag{7}$$

and depends on switch on time. The mean time to first catastrophic failure

$$T_{FFC} = 1/(2\lambda) + 1/\lambda = 3/(2\lambda)_{\lambda} \approx 1.5\ 10^5\ h \tag{8}$$

is longer than mean time to first failure

$$T_{FF} = 1/(2\lambda) + 1/(\lambda+\mu) \approx 1/(2\lambda)\Big|_{F} \approx 0.5\ 10^5\ h \tag{9}$$

In both examples the safety measures are better than for single computer system.

4. CONCLUSIONS

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.4.

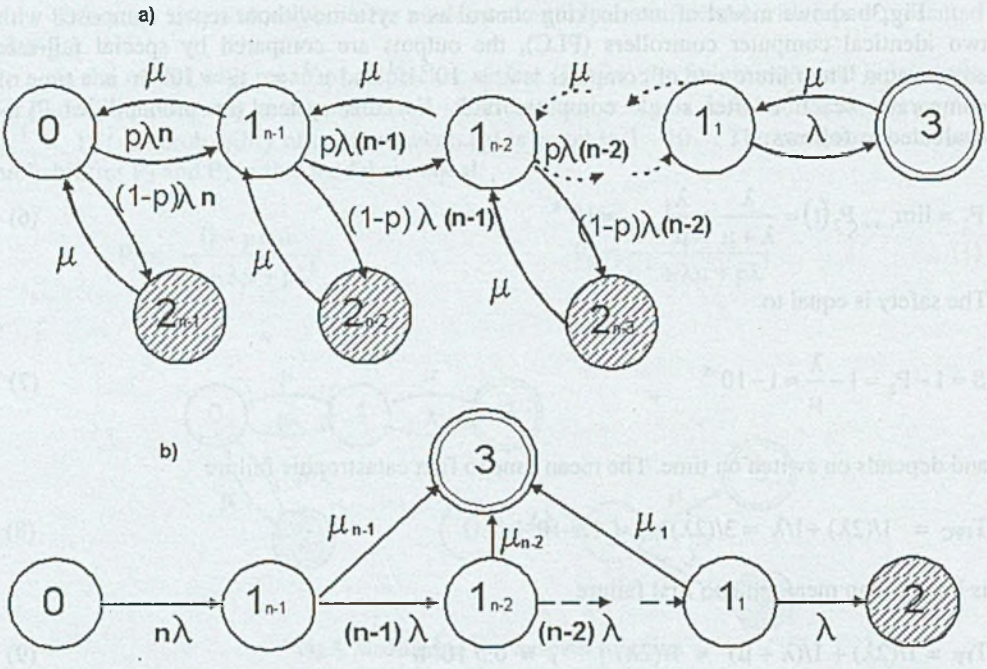

Fig.4. Modelling of multicomputer structures a) systems with repair b) systems without repair

The analysis of safety criteria (probabilistic or time measures) for real systems based on computer networks is more complicated, the matrix description both for system with repair and for system without repair is rather sophisticated and solutions require the computer support. 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. (The estimation of μ_i in systems without repair composed with several computers is rather sophisticated with respect to characteristics of multiple switches). The failure rate for computer controllers installed at Polish State Railways guaranteed by producers (Siemens, PEP Modular Computers Inc.) is better than $10^{-5}\,h^{-1}$. The repair rates may be estimated during special safety tests. The system level analysis must regard both software and hardware coincidences, some hardware faults are masked by software methods, software faults sometimes require additional hardware. The obtained results have rather qualitative aspect and are an optimisation criteria for system structure. Another aspect is related to comparison of functionally consistent systems (validation of several cross level signalling systems applied the presented interlocking computer structure).

BIBLIOGRAPHY

[1] LEWIŃSKI A., PERZYŃSKI T., New computer control systems in polish state railways, I Międzynarodowa Konferencja Naukowa TELEMATYKA SYSTEMÓW TRANSPORTOWYCH, Katowice-Ustroń 2001

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

[3] LEWIŃSKI A., The design of correct software for safety related railway control systems according to UE standards, requirements and recommendations, Archiwum Transportu PAN, Warszawa, Nr 2, 2001

[4] LEWIŃSKI A., KONOPIŃSKI L., Szacowanie niezawodności i bezpieczeństwa komputerowych systemów sterowania ruchem kolejowym, Przegląd Kolejowy, Nr 8, Warszawa 2000

[5] 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

[6] LEWIŃSKI A., SIERGIEJCZYK M., Problemy szacowania bezpieczeństwa i niezawodności mikroprocesorowych systemów sterowania ruchem, Prace Konferencji BEZPIECZEŃSTWO SYSTEMÓW, Zakopane 1998, Wydawnictwa Instytutu Technicznego Wojsk Lotniczych, Nr 7, 1998

[7] LEWIŃSKI A., PERZYŃSKI T., Zastosowanie sterowników PLC w bezpiecznych systemach sterowania dla potrzeb systemów sterowania ruchem kolejowym, prace konferencji Wydziału Transportu Politechniki Radomskiej TRANSCOMP 2001, Zakopane 2001

[8] Railway applications: Safety Related Electronic Railway Control and Protection Systems, report on the standard EN 50129, CENELEC 1997.

[9] Railway Application: The specification of dependability, reliability, availability, maintability and safety (RAMS), report on the standard EN 50126, CENELEC 1997

[10] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym, opracowanie Centrum Naukowo-Technicznego Kolejnictwa, Zakład Sterowania Ruchem i Zasilania, zadanie Nr 1060/23, Warszawa 1997

Reviewer: Ph. D. Jerzy Mikulski