4th INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'04

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 200
TRANSPORT z.55, nr kol. 165

rail control systems,
fail safe systems,
safety computer networks

Andrzej LEWIŃSKI[1]
Tomasz PERZYŃSKI[2]

THE MODELLING OF COMPUTER NETWORKS FOR RAILWAY CONTROL AND MANAGEMENT

The paper deals with configuration of computers applied in railway systems: interlocking and dispatcher monitoring. Examples from the EU railways: specialised three computer interlocking SELMIS, dispatcher system WSKR, remote control of Warsaw Underground and GSM-R based ERTMS structure for train monitoring are analysed and modelled with respect to typical net parameters such as probability of the correct connection and delay time. The applied Markov process and temporal Petri net modeling allows to estimate necessary safety criteria, both time and probabilistic.

MODELOWANIE SIECI KOMPUTEROWYCH STOSOWANYCH W SYSTEMACH ZARZĄDZANIA I STEROWANIA RUCHEM KOLEJOWYM

Praca dotyczy konfiguracji komputerów w systemach zależnościowych i dyspozytorskich. Przykłady systemów stosowanych na kolejach europejskich: trzykomputerowy system zależnościowy SELMIS, system kontroli dyspozytorskiej WSKR, system zdalnego sterowania w Warszawskim Metrze i przyszłościowy system nadzorowania pociągu ERTMS/GSM-R są analizowane względem typowych parametrów sieci takich jak prawdopodobieństwo poprawnego przełączenia i czas opóźnienia. Zastosowane modele procesów Markowa i czasowych sieci Petriego pozwalają oszacować typowe kryteria bezpieczeństwa, zarówno probabilistyczne jak i czasowe.

1. INTRODUCTION

These computer network used for railway transport management and control apply different transmission methods based both on radio and cable standards. The rules of integration such networked systems are defined in ERTMS/ETCS project elaborated by organisation of European railways UIC. The main aim of this work is safety characteristics of such systems assuming typical computer network approach. Computer networks are efficient realisation of safety systems. The safety analysis related to reliability and functional

[1] Faculty of Transport, Technical University of Radom, Malczewskiego 29, 26-600 Radom, alewinski@pr.radom.net
[2] Faculty of Transport, Technical University of Radom, Malczewskiego 29, 26-600 Radom, tperzynski@pr.radom.net

parameters corresponds to Markov process modelling the exploitation of multicomputer systems. The natural extension of Markov process is temporal Petri net model with respect to additional conditions for passing the transition with assumed delay.

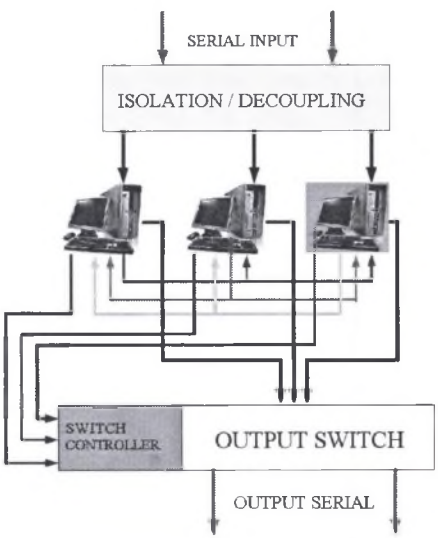
In the paper the modelling of typical network systems using Markov processes and extension towards temporal Petri nets is presented. Such network approach corresponds to typical computer network applications: three coupled processor structure of ESTW interlocking computer, ring topology dispatcher system WSKR, remote control system for Warsaw Underground and future wireless GSM-R railway control system corresponding to ERTMS/ETCS. The proposed approach give possibility of simulation for simple estimation of probabilistic and time parameters necessary for safety analysis.

2. THE SAFETY COMPUTER NETWORK IN RAILWAY TRANSPORT

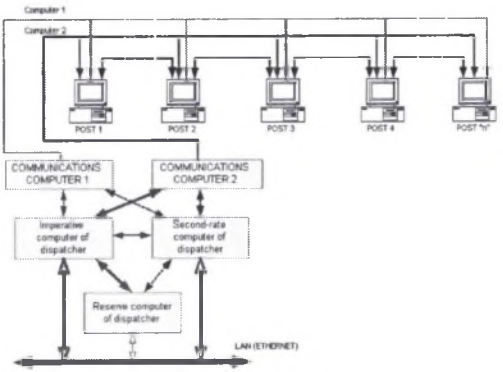
From historical point of view the first computer networks in railway control applications are configured for safety purposes [1], [4] such SIMIS (Siemens) or EBILOCK (ABB Signal) applying the special solutions of bus interfaces. Next we can observe introduction of industrial net standards such RS 232 or PROFIBUS into local systems such coupled controllers in Level Control Systems, or modem transmission into remote control or dispatcher systems. Now railway computer systems may use the radio transmission based on previous loop or beacon standards or new GSM-R recommendations elaborated specially to efficient railway traffic management.

Some examples of computer network in railway control is shown on the Fig 1. The bus connections in triple self-checking structure is presented on the Fig.1a . The special bus connection assure the fail safe operation, with complex monitoring and fault recovery is realised in program way. This solution SELMIS [3], [4] is elaborated by ALCATEL for centralised interlocking ESTW system. The implementation assures the checking of all bus signals, synchronisation and diagnostics of faulty modules.

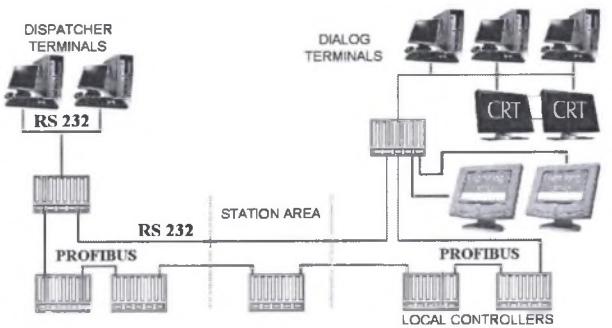
a)



b)



c)



d)

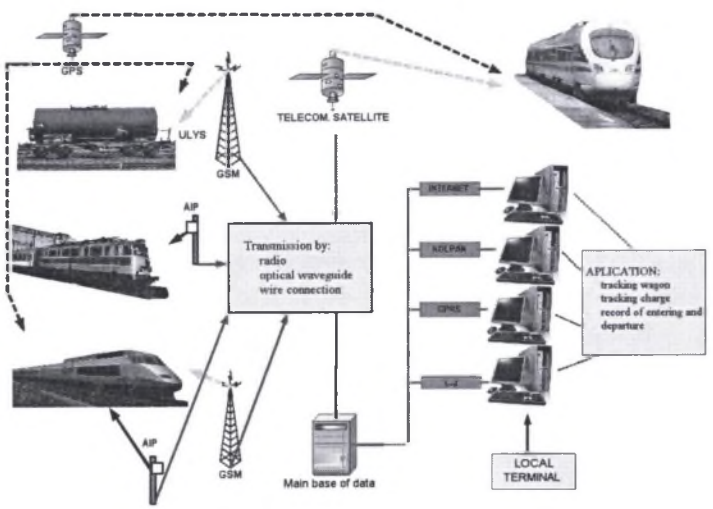


Fig.1. Computer networks in Polish railways a) Bus connections in specialised SELMIS computer for centralised interlocking system (ALCATEL) b) Dispatcher system WSKR, c) Remote control of Warsaw Underground (METRO), d) GSM-R connected ERTMS structure for train monitoring

The dispatcher system WSKR [1], [4] for local management has been installed in Kraków Tarnów line in the form from Fig.1b. The communication subsystem applies single ring topology, the duplex structure in the centre is based on main computer and hot stand-by computer. From technical point of view both computers have the same actual data sets and restart after switch caused by main computer fault has no influence on dispatcher work.

The remote control system applying the RS 485 (PROFIBUS) standard is implemented in Warsaw Underground (Fig.1.c) [5]. It is realisation typical to distributed industrial systems. Both cable distances and transmission rates is sufficient for management of trains from one point of dispatcher centre.

The Fig.1.d shows the part of ERTMS/ETCS structure for train monitoring concerning several radio and cable transmission subsystems.

3. SAFETY COMPUTER SYSTEMS MODELLING

For safety analysis the estimation the quantitative (probabilistic and time) measures of safety is required. Such criterion may be evaluated corresponding to the reliability theory [4], [5], [7]. Assuming the Markov character of processes modelling typical exploitation of railway control systems, the non safety may by related to the P_F , probability of catastrophic, dangerous failures.

The basic concept of safety based on Christov model of railway control system has been introduced to safety analysis of many real systems [4]. It is a Markov model of system with repair presented on Fig.2. The transitions between states are described with respect to:

λ - failure rate,

μ_s , μ_d - repair rates from safe state and critical failure state,

$1/\lambda'$, $1/\mu'$, - time between messages and time of completing and processing messages from coupled computers,

p_{FS} - probability of fail-safe action (may be defined as a ratio $\lambda_s / (\lambda_d + \lambda_s)$ between safe failure rate and total failure rate).

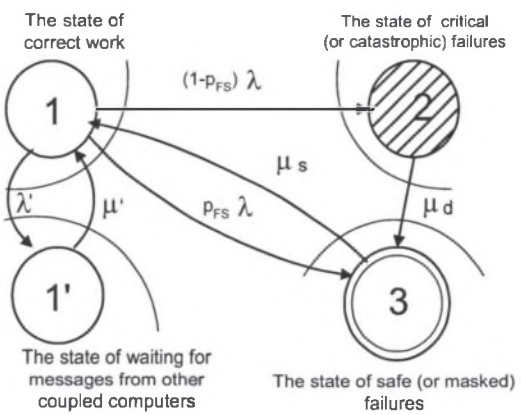


Fig.2. The model of safety railway system

The probabilities P_1 , P_1', P_2 , P_3 and mean time to transition to any set of failure states may be estimated using matrix method. For safety analysis (without network parameters λ' and μ') the stationary probability of P_2 is needed.

$$P_F = \lim_{t\to\infty} P_2(t) = \frac{\mu_s\lambda(1-p_{FS})}{\mu_s\mu_d + \lambda(\mu_d + \mu_s(1-p_{FS})} \approx \frac{\lambda(1-p_{FS})}{\mu_d} \tag{1}$$

In the practice, for $\lambda << \mu$, the mean time to first catastrophic failure T_{FFC} is determined

$$T_{FFC} = \frac{1}{(1-p_{FS})}\left(\frac{1}{\lambda} + \frac{p_{FS}}{\mu_S}\right) \approx \frac{1}{(1-p_{FS})\lambda} \tag{2}$$

The safety may be defined as follows

$$S = 1 - P_F \tag{3}$$

This measure may be applied both to the systems without repair and systems with repair. For computer networks with greater number of communicating this approach may be extended in the way presented in the Fig.3. [3], [4].

In both examples the safety measures are better than for single computer system. 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_F will be worse than for one active plus one reserve computers).

The problems of delays may be approximately estimated using extension of Markov model to mass service methods[9]. For $\lambda' << \mu'$ the mean number (N) of messages and mean time of delay (waiting for completing all messages) are equal to:

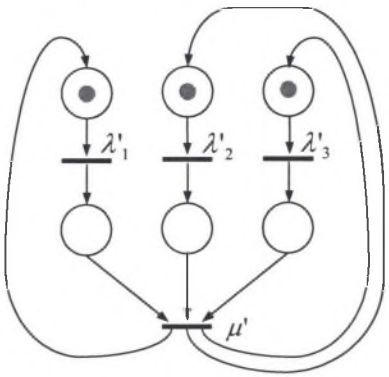
$$N = \frac{\lambda'/\mu'}{1-\lambda'/\mu'} = \frac{\lambda'}{\mu'-\lambda'} \quad , \qquad T_0 = N/\lambda' = \frac{1}{\mu'-\lambda'} \tag{4}$$

For computer networks the safety may be estimated with respect to estimated time T_0 , for example the efficient rate of service in systems without repair (typical fail-safe systems) may be a sum of delay time and reaction time ($1/\mu + T_O$) , in systems with repair the probability of correct switch of may be a function of failure rate and delay time $p(1/\lambda, T_O)$.

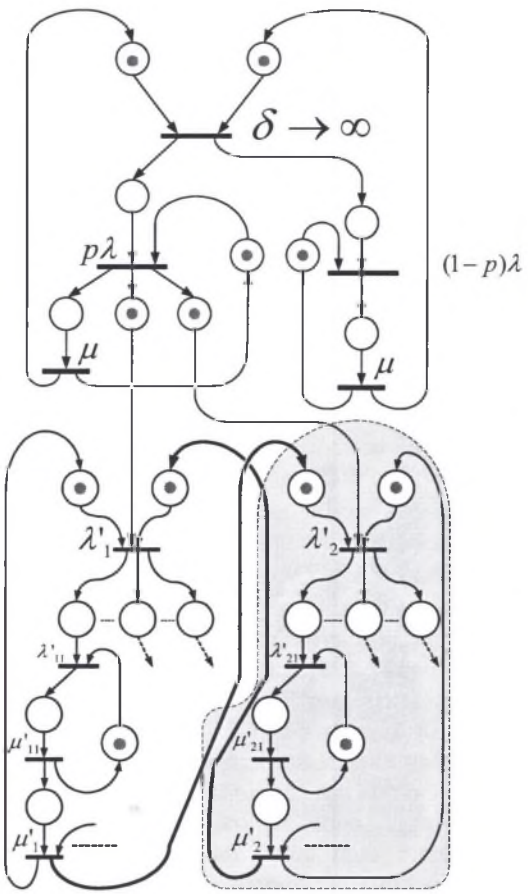
In real systems with many states the detailed description of Markov model and analytical solution of corresponding equations are rather sophisticated [8]. The system functional and reliability parameters may be different for each computer in the system and some of them may be difficult to estimate in the first months of exploitation. The natural extension of introduced Markov models are temporal Petri nets [2] presented on the Fig.3. These models concern delay and rate but additionally the transition in the graph is a result of conditions satisfying the input conniunction. The modelled processes may work simultaneously, may co-operate each other via common memory or special hardware input/output module. The probability of dangerous fault P_F and time to catastrophic failure T_{FFC} may be estimated using simulation, especially the Monte Carlo method.

The obtained results may be compared with theoretical solutions treated as a lower limit of assumed safety criteria.

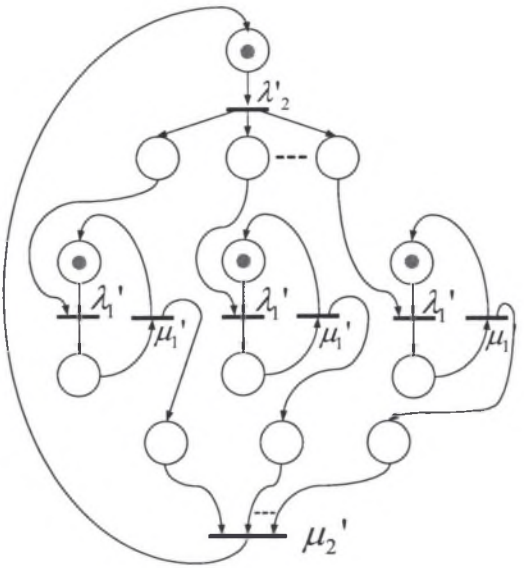
a)



b)



c)



d)

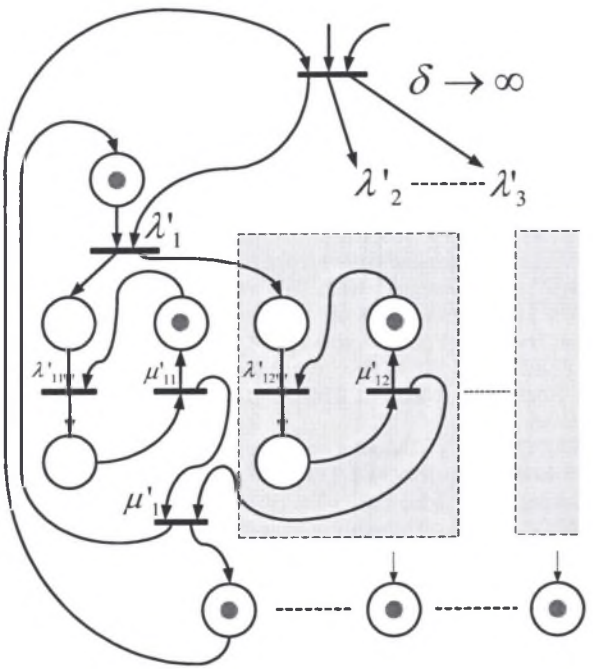


Fig.3. Temporal Petri Net modelling of multicomputer net structures:
a) SELMIS b) WSKR c) METRO d) ERTMS

4. CONCLUSIONS

The analysis of safety criteria (probabilistic or time measures) for real systems based on computer networks is more complicated. The estimation of rates μ and λ, necessary for evaluation is difficult because such parameters are rather unknown and may be determined with respect to tests elaborated during several years [4], [10]. (The estimation of μ_i in systems without repair composed with several computers is rather sophisticated with respect to characteristics of multiple switches.)

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 (European Railway Traffic Management System) 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] DĄBROWA-BAJON M., KONOPINSKI L., LEWIŃSKI A., „Wybrane komputerowe systemy sterowania ruchem kolejowym na tle europejskich zaleceń normalizacyjnych," Problemy Kolejnictwa, Zeszyt 116, 1994

[2] DUTUIT Y., SIGNORET J-P., „Dynamic systems modelling by using stochastic Petri Nets and Monte Carlo simulation", materiały Międzynarodowej Konferencji BEZPIECZEŃSTWO I NIEZAWODNOŚĆ SYSTEMÓW 'KONBIN2003', Gdynia, 2003

[3] KONOPINSKI L., LEWINSKI A., „The safety of decentralised computer systems for railway transport management and control", materiały Międzynarodowej Konferencji BEZPIECZEŃSTWO I NIEZAWODNOŚĆ SYSTEMÓW 'KONBIN2003', Gdynia, 2003

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

[5] LEWINSKI A., „The safety of decentralised computer systems for railway transport management and control" , Archiwum Transportu PAN, Warszawa, Nr 4, Vol. 14, 2003

[6] LEWINSKI A., PERZYŃSKI T., „New computer control systems in Polish State Railways", I Międzynarodowa Konferencja Naukowa TELEMATYKA SYSTEMÓW TRANSPORTOWYCH'TST 2002', Katowice-Ustroń, 2001

[7] LEWINSKI A., PERZYŃSKI T., „The safety problems of computer networks in transport applications", II Międzynarodowa Konferencja Naukowa TELEMATYKA SYSTEMÓW TRANSPORTOWYCH'TST 2002', Katowice-Ustroń, 2002

[8] LEWINSKI A., PERZYŃSKI T., „The safety of multi-computer systems for railway transport management and control", VII Konferencja Naukowa KOMPUTEROWE WSPOMAGANIE W TRANSPORCIE, NAUCE I PRZEMYŚLE 'TRAANSCOMP 2003', Katowice, 2003

[9] TANENBAUM A. S., „Sieci komputerowe", WNT 1995

[10] Railway applications: The specification of dependability, reliability, availability, maintability and safety (RAMS), Report on pre-standard EN 50126, CENELEC 1997

Reviewer: Ph. D. Jerzy Mikulski