MIECZYSŁAW KORNASZEWSKI*, ZBIGNIEW ŁUKASIK
Technical University of Radom
Faculty of Transport
Malczewskiego 29, 26–600 Radom, Poland
**Corresponding author*. E-mail: mkornasz@pr.radom.net

SAFE IMPLEMENTATION OF AUTOMATIC MICROPROCESSOR SYSTEMS OF LEVEL CROSSING ON THE EXAMPLE OF THE SPA-4 SYSTEM

Summary. Fulfilling high requirements of safety and reliability is an important question in devices of railway traffic control. Increased safety in computer systems is reached in the simplest way through redundancy of hardware and software, but also with other methods. A microprocessor system of automatic SPA-4 level crossing, manufactured by Bombardier Transportation Katowice (Poland), is a benchmark in the paper.

BEZPIECZNA REALIZACJA MIKROPROCESOROWYCH SYSTEMÓW SAMOCZYNNEJ SYGNALIZACJI PRZEJAZDOWEJ NA PRZYKŁADZIE SYSTEMU SPA-4

Streszczenie. Istotnym zagadnieniem w urządzeniach sterowania ruchem kolejowym jest spełnianie wysokich wymagań bezpieczeństwa i niezawodności. Zwiększenie bezpieczeństwa w systemach komputerowych osiąga się najprościej przez redundancję urządzeń i oprogramowania, ale także innymi sposobami. Punktem odniesienia w referacie jest mikroprocesorowy system samoczynnej sygnalizacji przejazdowej typu SPA-4 wyprodukowany przez Bombardier Transportation (ZWUS) Polska Sp. z o.o. Katowice.

1. INTRODUCTION

Because of the nature of tasks executed, traffic control systems have to meet special requirements referring to safe operation. Safe setups have to react to any interference with the signal or damage to the element in a safe way, which means to the composition of the railway crossing in case of application of devices stopping the traffic of cars.

As a rule, computer systems of railway traffic control should be executed as “fail-safe”, which means that a single damage (of equipment, software) or interference cannot cause a dangerous situation, assuming negligibly small probability of double (multiple) damage occurrence. Additionally, single errors are assumed to be detected in a relatively short time and the damage detected by an appropriate system’s response to the fact. The SIL 4 (Safety Integrity Levels) included in the norms of the European Committee of Normalization in CENELEC Electrotechnics is another important criterion. SIL 4 is the highest safety level and determines the damage intensity (the probability of damage occurrence in a unit time) for a single system element 10E-11.

A computer system of automatic SPA-4 type level crossing, manufactured by Bombardier Transportation Katowice, has been the subject of our investigations.

2. MAIN TRENDS PERMITTING REACHING OF A HIGH LEVEL OF RELIABILITY AND SAFETY IN COMPUTER SYSTEMS OF RAILWAY TRAFFIC CONTROL

For computer systems of railway traffic control it is necessary to consider issues of safety and reliability on two levels:

- of technical devices, creating the infrastructure of railway traffic control system;
- of system software.

To meet the requirements of safety the system has to consist of two computers linked together in a suitable structure, which at least performs appropriate data processing and mutual check-up possible, etc. There are also other systems, based on one unit. For obtaining required conditions of safety the other computer is utilized as an urgent reserve.

Appropriate software operations are executed for the safety of single-channel systems. They are relying on encoding and converting data through two programs in one unit which are testing each other. The best situation is when applications are written by different groups of programmers.

Multi-channel systems, most often two-channel or three-channel, are named “2 from 2” and “2 from 3” respectively, of which safety is ensured by redundancy of hardware and software. In solutions with two computers results are compared, and according to safe work condition of system “2 from 2” only full compatibility effects of all calculations are obtained on output of active channels. In the “2 from 3” system the negative result of comparison switches to action/operate the third computer, which result of converting is taking under consideration alike previously on two computers [1,4].

2.1. CONTROL SETUPS

Automatic SPA-4 system of level crossing was designed on the basis of Programmable Logic Controllers of the MINICONTROL type of Austrian manufacturer Bernecker & Rainer. The setup of the control contains two PLC drivers independently executing the control program. Drivers are linked with the use of a TTY interface, which also assures synchronization of two channels operation. Detection of the lack of parallelism is treated as a signalling failure.

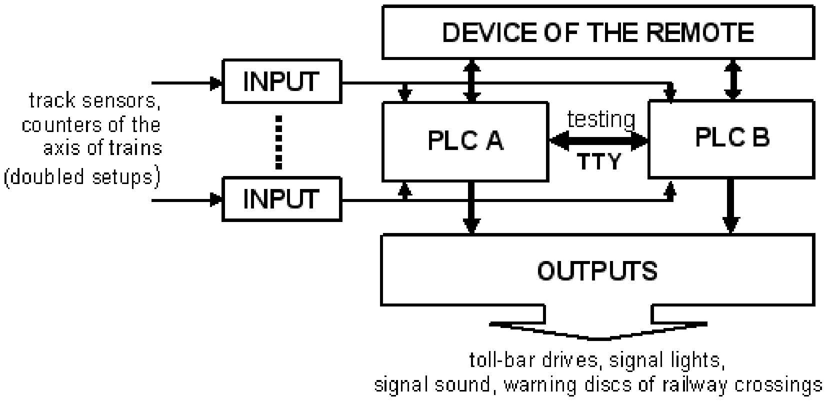

Fig. 1. Example of the configuration of PLC drivers in the automatic SPA-4 system of level crossing
Rys. 1. Przykład konfiguracji sterowników PLC w systemie samoczynnej sygnalizacji przejazdowej SPA-4

PLC drivers should generate, based on their current input signals, output signals that in turn control signalling and executive devices. Information about error occurrences or failure-free work of signalling and information about the state of signalling (switching on or stand-by) is sent to ERP-6 type remote control device by means of the transmission network. This information is generated independently in each of two signalling drivers [5,7].

2.2. CONTROL PROGRAMME

The redundancy of control programme is often the most encountered method of safety assurance in computer systems from the software point of view. A change to the emergency control programme of the control application is a method used in case of damage detection (both methods are operating on the system level, they respond to hardware and software errors themselves this way). In standard implementations it is possible to encounter two basic structures capable of redundant software detecting or of errors tolerating:

- n Version Programming (nVP) assumes n execution of similar programmes and selecting of the effect by a special comparing application;
- n Recovery Block (nRB) assumes replacing the damaged programme by the next equivalent programme (from the sequence) executed in the application at the moment after the error finding [2,8].

Control application of the level crossing signalling originates from the activation of PROSYS system supplied by the manufacturer of drivers. The programme is executed in the sequential mode. The cycle length is 15÷25ms dependent of the quantity of warning devices. The software was written on the level of processor 6303 assembler. In PLC drivers there is a possibility of automatic conversion from the level of the internal language to the level of logical diagrams [3].

For a specific application the modification of programmes consists of adding or removing software blocks executing the operation of each device without infringing the structure of the programme. This has essential meaning to relevance containing all elements of the system in standard configuration of software correctness tests which are carried out from the point of view of nominal quantities.

It is necessary because of software reliability to notice not detected errors of the project, casual errors of the use and defect of resistance to interferences also during operation. Indeed, for safe railway traffic control systems the software should be free from assumption, errors (semantic, syntactic, side effects of compilers, operating systems and utility programmes), however, the practice of using control computers and programmed drivers shows that states following e.g. incapacity result from hanging-up of the application or of the operating system [6,8].

3. FEATURES TOLERATING MAINTENANCE OF THE HIGH LEVEL OF SAFETY OF THE COMPUTER SPA-4 SYSTEM

3.1. EQUIPMENT REDUNDANCY

Two independently operating channels A and B exist in the setup of the SPA-4 system control: starting from the power supply, the battery of batteries, drivers, sensing devices, and ended in warning devices. An independent elaboration of output signals controlling each warning device follows on the basis of current values of actuating signals in each channel. Each channel has its independent source of actuating signals.

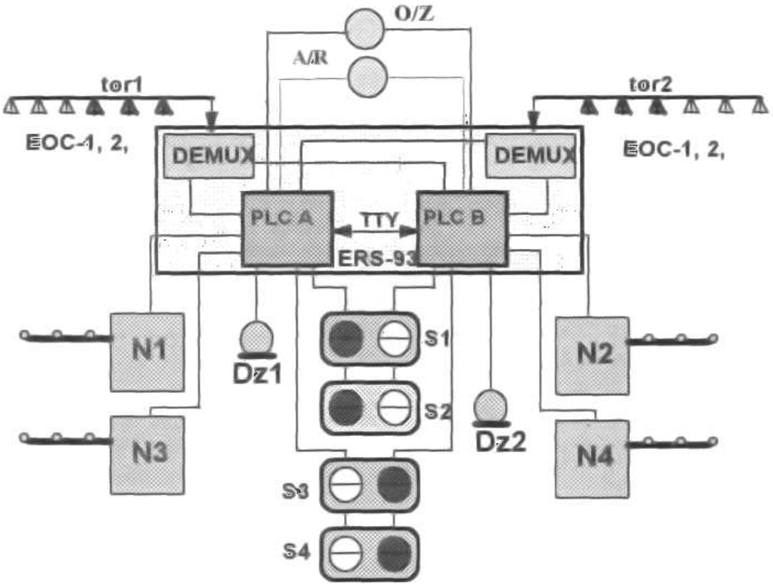

Fig. 2. Redundant structure of the SPA-4 system of level crossing automation
Rys. 2. Struktura redundantna systemu samoczynnej sygnalizacji przejazdowej SPA-4

Warning devices installed on the railway crossing are assigned to channels independent of their quantity and kind (A and B), so that in case of malfunction of one control channel the other channel ensures sufficient protection of the railway crossing when a train approaches [7].

3.2. DIVERSIFICATION OF PROGRAMMES CONTROLLING CHANNELS A AND B

Programmes for PLC drivers in channel A and B have been developed by independent teams of programmers. Diversity of programming languages and tools (compilers) was also taken into consideration.

Diversity of programmes takes into consideration among other things:

- two independent source programs;
- diversification of the structure;
- using various areas for two separate drivers by RAMs resulting from the application;
- various methods of the same execution functions.

Programmable Logic Controllers in channels A and B work combined with a serial TTY interface, through which an information exchange occurs between them to determine compatibility through the decision layer of the system which switching on or off signalling in both channels.

3.3. TESTING THE CORRECTNESS OF SYSTEM MODULES AND DEVICES WORK UP-TO-DATE

Controlling programmes contain procedures testing the correctness of work of feeding setups, moreover apart from procedures executing each function of the automatic system of level crossing devices, of warning and selected modules devices as well as the procedure and mechanisms of self-testing of controlling setups.

It is taken by testing devices of automatic system of SPA-4 level crossing from the application work in time, in particular:

- state control of traffic signalling lights lamps and warning discs on railway crossings;
- position of barrier drives and continuity of barrier poles on railway crossings;

- presence of signals from track sensors on modules for input drivers;
- communication of every PLC driver with organization of remote ERP-6 check-up;
- efficiency of signal transfer from sensing devices of optoisolators in track sensors to drivers A and B;
- existence of the supply voltage and of appropriate value of batteries' voltage;
- communication between channels A and B.

Communication between drivers in channels A and B allows comparing the value of the switch on signal in both channels, synchronization of the control of signal light lamps and the information exchange to switch on in both channels. If values of switching on signals in channel A and B are differing during the time exceeding 5s, the lack of synchronization error is detected.

3.4. TESTING THE CONTROLLING PROGRAMME UP-TO-DATE

The controlling programme, beyond procedures executing each function of the system, contains also procedures verifying correct execution, verifying every software cycle and the procedure ,correctness of current values of automatic system of the level crossing parameters (e.g. train counters).

The integrity of the controlling programme algorithm is tested in each cycle of the programme. The type applied to the SPA-4 system driver possesses reliable self-testing mechanisms [3].

4. CONCLUSIONS

In practical solutions of railway traffic control computer systems, an increase in safety is reached most often through redundancy (excess). The simplest solution is executed through the two-channel construction of setups, consisting in the application of two, working in parallel, functional channels and in comparing of their work, and through two independent programmes written by various teams of programmers. The setup is the safest, the more diversified are both functional channels. It is related to larger complexity and at the same time to lower reliability of the setup and to heavy expenses.

Safety of the automatic system of the SPA-4 type level crossing results from the type of applications of modern technologies (of programmable drivers), is based on two control channels, diversity of applications in channel A and B, possibilities of immediate faults detection in devices and applications (self-testing), and also on the possibility to carry out monitoring of the work system by both registration of all events and of failures.

Computer systems of the railway traffic control should be realized and configurated using equipment fulfilling specific requirements: high level of reliability, possibility to enter safety conditions (errors analysis and detecting and the proper reaction), modularity, possibility to link in the network, simplicity of creating various configurations (flexibility), possibility to link the external infrastructure to different elements, possibility to connect many devices used and many external devices, possibility of work in specific, severe conditions (temperature, dampness, vibration).

Literature

1. Bergiel K., Karbowiak H.: *Automatyzacja prowadzenia pociągu*. Wydawnictwo EMI-PRESS, Łódź 2005.
2. Dąbrowa-Bajon M.: *Podstawy sterowania ruchem kolejowym. Funkcje, wymagania, zarys techniki*. Oficyna wydawnicza Politechniki Warszawskiej, Warszawa 2002.
3. DOKUMENTACJA TECHNICZNO-RUCHOWA: *Samoczynna sygnalizacja przejazdowa typu SPA-4*, ADTranz Zwus Sp. z o.o., Katowice 1997.

4. Dyduch J., Kornaszewski M.: *Analiza bezpieczeństwa systemów automatyki przejazdowej.* XI Konferencja „Drogi kolejowe 01”. Wrocław-Żmigród 2001.
5. Dyduch J., Kornaszewski M.: *Systemy sterowania ruchem kolejowym.* Wydawnictwo Politechniki Radomskiej, Radom 2003.
6. Kornaszewski M.*: Analiza niezawodności samoczynnej sygnalizacji przejazdowej typu SPA-4.* Transport. Prace Naukowe Politechniki Radomskiej nr 11. Radom 2000.
7. Kornaszewski M.: *Charakterystyka wybranych mikroprocesorowych systemów samoczynnej sygnalizacji przejazdowej*. Międzynarodowa Konferencja Naukowa TRANSPORT XXI WIEKU, Warszawa 2004.
8. Lewiński A.: *Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego*. Wydawnictwo Politechniki Radomskiej, Radom 2001.