Methods of the Safe Assurance of Functioning of the Computer System of Automatic of the Level Crossing of the SPA-4 Type

M. Kornaszewski[1], Z. Łukasik[2]
Technical University of Radom, Poland
E-mail :[1]mkornasz@pr.radom.net, [2]z.lukasik@pr.radom.pl

Abstract:
He is a substantive question in devices of the control of the rail traffic fulfilling of high requirements of safety and reliability. In computer systems upsizing of safety is reaching himself/herself through redundancy of devices and software in the most simple way, but with also other methods. A microprocessor system of automatic of the level crossing of the SPA-4 type is a benchmark in the paper manufactured through Bombardier Transportation Katowice (Poland).

1. INTRODUCTION

Systems of the control of the traffic because of the character bound to transport of people and commodities and the possibility of the possible collision, of tasks which they are realizing, they have to meet special requirements concerning to safe operating. Safe setups have to react to every interference with the signal or damage to the element in the safe way what means in case of entering devices to the composition of the railway crossing e.g. stopping of the traffic of cars.
A principle is a essential feature of safe realizations of computer systems of the control of the rail traffic "fail-safe", speaking, that single damage (of equipment, software) or the interference isn't able to cause the dangerous situation, at assuming, that probability of the occurrence of double damage (multiple) is small negligibly. Detection of single errors is assumed additionally in the relatively short time and detecting damage by the suitable reaction to the fact of the system. The criterion is an important other person exert 4 (Safety Integrity Levels) who is included in norms of the European Committee of Normalization in CENELEC Electrotechnics. Level of safety 4 he is highest and he is determining, that intensity of damage (the probability of the occurrence of damage in the unit of the time) is taking away for the single system element 10E-11.
A computer system of automatic of the level crossing of SPA-4 type was accepted as the source of reflections in the paper produced through Bombardier Transportation in Katowice.

2. MAIN TRENDS PERMITTING RELIABILITY TO REACH THE HIGH LEVEL AND OF SAFETY IN COMPUTER SYSTEMS OF THE CONTROL OF THE RAIL TRAFFIC

It is necessary in the range of computer systems of the control of the rail traffic to consider issues of safety and reliability in two levels:

- of technical devices, creating the infrastructure of the system of the control of the rail move,
- of software of the system.

In order to be up to requirements of safety the system has to consist of two computers bound to oneself in the suitable structure, which is making the suitable processing of data and the mutual check-up possible etc. at least. Other systems which are based on one unit are also existing. The utilized computer is other for obtaining required conditions of safety as the hot reserve.
Suitable software operations are being executed for safety of single-channel systems. They are relying on encoding data and the converting of two programs on one unit who are testing themselves one another. He is best when applications are written by programmers' different groups.
Multichannel systems most often two-channel or three-channel they are being named suitably "2 from 2" and "2 from 3", whom safety is ensured by redundancy of equipment and software in. Results are being compared in these solutions from two computers, and with condition of safe work systems "2 from 2" full compatibility of all effects obtained on outputs of active channels is and the occurrence of some error is making the safe reaction of the system. In the system "2 from 3" the negative effect makes joining in action 3 of computer, and an effect is being taken under the remark to the processing identical on two computers. [1],[4]

2.1 STEERING SETUPS

System of automatic of the level crossing of SPA-4 type was designed on the basis for Programmable Logic Controllers of the MINICONTROL type of the Austrian manufacturer Bernecker & Rainer. The setup of the control contains two PLC drivers, which everyone is realizing the program steering irrespective from. Drivers are merged by means of the TTY interface, behind the matter of whom synchronization of action is being realized both of channels and detection treated as one of errors in signalling of possible lack of parallelism of their action.

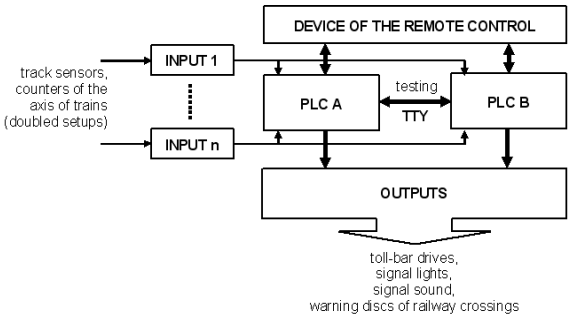

Fig. 1: Example of the configuration of PLC drivers in the system of automatic of the level crossing of SPA-4 type

He is a task of PLC drivers generating of signals of output logical actuating signals steering signalling and executive devices on the basis of current values. Information about occurring of errors or failure-free work of signalling and information about the state of signalling (turn on by the state or stand-by) is being sent for devices the remote control of ERP-6 type by means of the transmission network. This information is being generated independent in every of two drivers of signalling. [5],[7].

2.2 STEERING PROGRAM

His redundancy is most often a met method of the assurance of safety in computer systems from the point of the view of software. A change for the program of the emergency control of the steering application is a method with the other person in case of detecting of damage (both methods are operating on the level of the system, they are reacting to errors of hardware by itself this way, how and software). It is possible in standard realizations to meet two basic structures possessing the capacity of detection of redundant software or of tolerating errors:

- n Version Programming (nVP) assumes n execution of similar programs and selecting of the effect by the special comparing application,
- n Recovery Block (nRB) assumes replacing of the damaged program through the next equivalent program (from the sequence) executed in the application at present after the assertion of the error. [2],[8]

The steering program is rising in the activating PROSYS system delivered by the manufacturer of drivers. Program is being executed in the sequential mode. The length of the cycle is 15÷25ms of the quantity of warning devices, the quantity given to the application of sensing devices and extra elements. Programs were written on the level of assembler of the processor 6303. A possibility of the automatic conversion from the level of the internal language to the level of logical schemata is existing in PLC drivers. [3]

The modification of programs consists for the concrete application on adding or removing software blocks realizing working of each devices out without infringing the structure of the program. This essential meaning has preservation of relevance containing all elements of the system to the standard configuration of tests of correctness of software which are carried out from the point of view in nominal quantities.

It is necessary because of reliability of software to notice not detected errors of the project, casual errors of using and defect of resistance to interferences also during operating. Indeed software should for safe systems of the control of the rail move be free from errors from the assumption (semantic, syntactic, of side effects of compilers, operating systems and tool applications), still the practice of using steering computers and programmed drivers is showing that states following e.g. of the incapacity are existing from hanging up of the application or 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

They are existing in the setup of the control of the SPA-4 system two irrespective operating channels A and B: beginning from power supply, the battery of batteries, drivers, sensing devices, and having ended in warning devices. An independent elaborating of output signals steering each warning devices is following on the basis of current values of actuating signals in every of channels. Every of channels possesses one's independent sources of actuating signals.

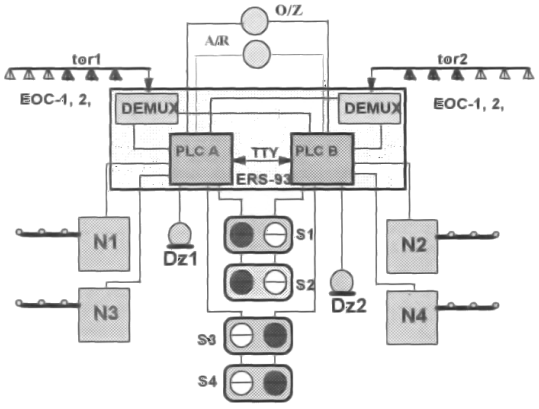

Fig. 2: Redundant structure of the system of automatic of the level crossing of SPA-4

Warning devices installed on the railway crossing, they are assigned to channels independent of their quantity and the kind this way A and B, in order to in case of malfunction of one of channels of the control, the other channel was ensuring protection being enough of the railway crossing when a train is being brought closer to him. [7]

3.2 DIVERSIFYING OF PROGRAMS STEERING IN THE CHANNEL A AND B

Programs for PLC drivers in the channel A and B they were work out by through programmers' independent units.. Diversity of programming languages and tools was also taken into consideration (of compilers).
Diversity of programs is taking into consideration among other things:

- two independent source programs,
- using various areas for two separate drivers by memories of RAM resulting about the application,
- diversifying of the structure,
- various methods of the realization of the same functions.

3.3 SYNCHRONOUS EXECUTING OF PROGRAMS BY PLC DRIVERS IN BOTH CHANNELS

Programmable Logic Controllers in channels A and B working merged with the serial TTY interface, which an information exchange is occurring between them in order determining compatibility through of the decision layer of the system about switching on or switch off signalling in both channels.

3.4 TESTING CORRECTNESS OF WORKING OF MODULES AND DEVICES OF THE SYSTEM UP-TO-DATE

Steering programs contain procedures testing correctness of working of feeding setups moreover apart from procedures realizing each functions of system of automatic of the level crossing devices, of devices of warning and selected modules as well as the procedure and mechanisms of self-testing of steering setups. Testing by the result he is visible behind the case of devices of monitoring and he is undergoing registration and he is able to underlie diagnostics of devices of the system.
It is being taken by intermittent or continuous testing system of automatic of the level crossing SPA-4 devices from working of the program in the time, particularly:

- of continuity of the thread of bulbs of traffic signalling lights,
- regularities of the state of bulbs of warning discs on railway crossings,
- of continuity poles of toll-bar drives,
- of attendance of signals from track sensors on particular modules for input drivers,
- of communication of every PLC driver with organizing the remote ERP-6 check-up,
- of efficiency leading the signal from sensing devices of opt isolators mediating in track sensors to drivers A and B,
- of attendance of the network voltage,
- values of the voltage of accumulators,
- of communication between channels A and B,
- of position of poles of toll-bar drives (whether they are located in the proper position).

Communication between drivers in the channel A and B is permitting signalling comparing the value of the signal switch on signalling in both channels, synchronization of the control of lamps of signal lights and the information exchange in order switch on the simultaneous assurance in both channels. If values of signals switching on in the channel A and B they are differing from through the time exceeding 5s, is following detecting of the error of lack of synchronization. In order to include signalling, a condition has to in one channel at least apply of switching on (principle “1 from 2”) so that signalling is accepted to the wait state, a condition has to in both channels at the same time apply of switching off (principle “2 from 2”).

3.5 TESTING THE STEERING PROGRAM UP-TO-DATE

The steering program, the beyond with procedures realizing each functions of the system, contains also verifying procedures correct executing oneself verifying every software cycle and the procedure correctness of current values of system of automatic of the level crossing parameters (e.g. of counters of trains).
Integrity of the algorithm of the steering program is being tested in every cycle of the program. This working is enabling with damage to areas driving to the fragments sure of the non-performance of the cycle of the application, of the RAM to detect bound errors.
The type applied to the SPA-4 system of the driver possesses mechanisms of self-testing, so how:

- the operating system is verifying whether executing of the cycle of the program isn't exceeding the time limit (150 ms),
- a control amount of contents of the memory of the program is being verifying after the stopping of every cycle,
- codes of all instructions of the program are being tested,
- a level of the voltage of the battery is being tested of maintaining of the memory of RAM. [3]

4. CONCLUSIONS

In practical solutions to computer systems of the control of the rail move upsizing of safety is reached

through redundancy most often (excess). She is being realized in the most simple solution through the two-channel construction of setups, relying on the application two in parallel of working functional channels and for comparing of their work and two independent programs written by programmers' various units.
The setup is safe all the more, both channels are functional for them more diversified. It is being linked to the bigger complexity, and the same with smaller reliability of the setup and with heavy expenses.
Computer systems of the control of the rail move should be realized and configured requirements specific from fulfilling equipment:

- high level of reliability,
- susceptible for entering conditions of safety (the analysis and detecting errors 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 how many devices of using and how many external devices,
- possibility of work in specific, tough conditions (the temperature, dampness, vibrating)

Safety of the system of automatic of the level crossing of the SPA-4 type is resulting from the type about applications of modern technologies (of programmable drivers), is based on two channels of the control, diversity of applications in the channel A and B, chances of immediate detecting of faults in devices and applications (self-testing), like also on the chance to drive monitoring of work of the system of both registration of all events and the breakdown.

5. REFERENCES

[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.