https://doi.org/10.26552/com.C.2008.3.57-60

Radomir Brkic – Zivoslav Adamovic *

THE IMPLEMENTATION OF SAFETY AND RELIABILITY OF DATA TRANSMISSION IN RAILWAY SIGNALLIZATION SYSTEMS

The focus of this paper is the safety and reliability of data transmission in railway systems at increased and high train speeds by means of technological devices of new generation. Routes in railway traffic are protected with new microprocessing signalling devices, the reliability and availability of which, thanks to new techology, may be projected to a necessary, i. e. desired value.

Key words: ETCS, automatic control, automatic guidance, safety, reliability, availability.

1. Introduction

So far, the conventional signalling system that involves fixed distances between the main signals and pre-signals makes the given task harder and limits the existing riding power of the rail. Contrary to this, the ETCS (European Train Control System) – supported line train leading – is independent of dividing the railroad into track sections and it provides the possibility of viewing the actual condition of the railroad ahead and with no limits.

Although mixed traffic railroads would require keeping of the conventional signals in the initial period – because of the lower speed freight trains – as emergency and lower hierarchy level in case of a main system failure, the main automatic leading system works as an 'overlay-system' representing the first safety system controlled by software.

2. Concept of an electronic signal box

Very important advantages of electronic signal boxes lie in the possibilities offered by a system-specific application of modern processing technology. Other than this, these advantages include:

1. Lower purchasing value of the device;
2. Considerably reduced construction requirements and fixed equipment;
3. Minimized scope of maintenance;
4. Ensured unification of work places for the train dispatchers – independent of the equipment supplier – and high level ergonometric equipment in the work places of dispatchers and the operative center dispatchers;
5. Simple integration of additional automatization and disponing functions; standardization of the interface for computer systems higher up in the hierarchy;
6. Creating conditions necessary for an integrated system of automatic leading.

1.1. Starting points for the safety microcomputer module

Possible places of application for the safety microprocessor module – safety microcomputer – are:

- the electronic signal box, the vital ETCS computer
- the terminal computer for handling signals and branches
- the vital element of every module and the main element in the safe signal transmission and crypto communication.

All these places in the signal structure differ very much in the quantity of the hardware necessary for the main module, software necessary in relation to the function it performs, factors of the environment, necessary reliability, etc.

Therefore, a global developing aim can be defined as follows:

- To develop a microprocessor module for those application places in the field of rail signallization where the systems i.e. subsystems must be fail-safe;
- To construct a 'hard core' that can be programmed by the 'main program' to work fail-safe invariably, regardless of the location of the application places;
- To compose the module from reliable components of the leading world producers;
- To achieve an MTBF 'reasonably' longer than 1 year, that is between 10,000–15,000 hours.

Unlike the so far safety signalling systems based on relays, there are neither electronic components, nor systems that can be found on the market which show the necessary 'fail-safe' behavior. Since the processor itself has no inherent safety, an adequate concept must be found to guarantee fail-safe behavior using 'redundancy' – which in fact means the management and control of the managing hardware with one special unit capable of detecting all functional mistakes that may cause danger to the process.

* **Radomir Brkic[1], Zivoslav Adamovic[2]**
[1]Railway College Belgrade,E-mail: rbrkic@drenik.net
[2]Technical Faculty, Zrenjanin, Serbia

The processing results from the two systems are compared and in case they are not identical, the comparing function itself and the next safety action must redirect the system into a safe-side position. This concept is possible with the configurations '2 out of 2' and '2 out of 3'.

These are the main problems that every system must solve and the 'internal mechanisms' that must achieve the above fail-safe behavior:

- Every single failure must be identified and must result in a safety reaction of the system;
- Double or multiple failures cannot happen if the safety concept of the system enables full comparison of results (during the entire course of the processing, and not only at its end) and condition of both channels, including memories;
- Not a single failure in one channel can have a similar effect on the other channel. The channels must be independent from each other;
- Both channels and the whole module must be completely tested and with no mistakes in either hardware or software before releasing the system into work. In other words, the system must be guaranteed as mistake-free before starting up the system.

Fig. 1 shows an illustrative example of a basic two-channel configuration of the safety microcomputer by Siemens Company. This configuration is safe-designed so that the two identical microcomputers work in synchrony with their:

- Central processing units CPU 1 and CPU 2;
- Belonging memories for entering and reading of the RAM 1 and RAM 2 data;
- Memories which are programmed for fixed values that can be reprogrammed as needed, EPROM 1 and EPROM 2;
- The configuration contains common ingoing and outgoing modules;
- Reception (1) and Release (2) which establish connection with the exterior elements; the system has one common tact-giver to synchronize the work of the two identical channels.

The system checks if the signals from both channels are identical in every tact step, in the following way: the tact-giver turns on both processors (TACT 1 and TACT 2) and a comparator ('C' signal – control in Fig. 1) The comparator checks the content of the collectors in both microcomputers (BUS 1 and BUS 2) and compares them. Only in case that the comparator (in every tact) establishes the identical status of both channels, it generates the signals "OK" (no mistake) on its exit, which triggers the next working cycle of the tact-giver.

Otherwise, in case there is any discrepancy in the signals coming from Channel 1 and Channel 2, which is transparently shown on BUS 1 and BUS 2, or in case of any mistake on the comparator, the comparator 'chokes' the 'OK' (no mistake) signal driving the tact-giver into rest, which ultimately means stopping the process: the whole configuration (module) stops its work directing the system to the 'safe side'.

So, this obviously shows that the work of both processors and all the activities that are related to further process operation are controlled in the earliest phase of every tact.

This early control, as an internal mechanism for identifying mistakes even in the earliest phase, is supported by a special additional checking program, which periodically checks the complete status of the system. Also, all the inside data, before their entry into the memory, are subject to automatic comparison and correction.

It is clear that this kind of safety concept assumes safety functions of the tact-giver and the comparator, implying that they must be 'fail-safe' designed, i.e. that every mistake on one of the elements of these modules must be reflected in the ultimate instance in the content of the BUS signal.

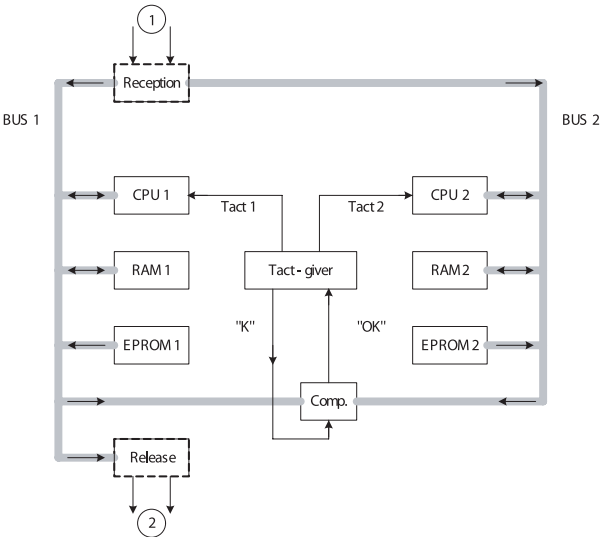

Fig. 1 Basic structure of the two-channel safety microcomputer

2. Principles of safety in the railway signalling systems

The signalling systems are not immune from failure and, therefore, due to their specific role, they must be designed and constructed so that even in case of disturbance and failure they do not endanger the safety of the traffic, which implies that they must be signal-safe and technically-safe.

This 'fail-safe' behavior is achieved by implementation of the signalling principles and safety criteria and using highly reliable devices regardless of the technology.

As a defined measure of safety, the international railway organization UIC, i.e. its committee ORE, has defined in its recommendations on the basis of so far experience and the achieved level of technical development 'the mean time between two dangerous failures' – 'MTBF', as a reliability measure in between two

failures. For example, for an electronic signal box this means, respectively:

- That the mean time between two dangerous failures (MTBF) must not be closer than 100 years;
- That the mean time between two failures (MTBF) must not be closer than 4 months (2880 hours).

2.1. The purpose and the functioning principle of the signalling/safety devices

Fig. 2 illustrates the role of the system of railway signallization with modalities of implementation of the safety principles.

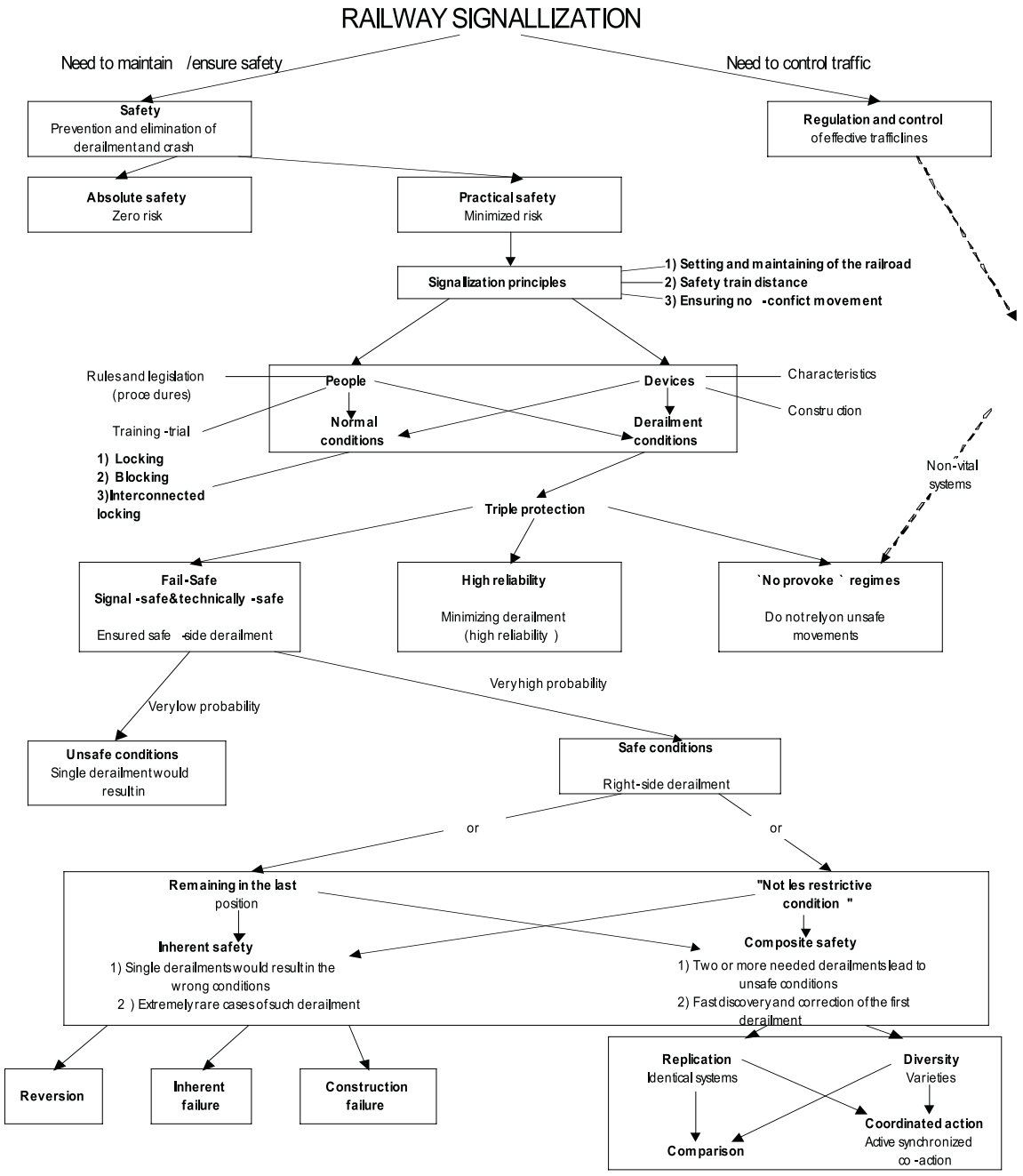

Fig. 2 The role of the railway signallization system with modalities of implementation of the safety principles

Fig. 2 clearly illustrates that the two basic purposes of the railway signallization are:
- control and management of the traffic;
- ensuring safety in railway traffic.

3. Conclusion

The issue of achieving complex safety with standardized module solutions has been laid down as a possible concept in this work. The possible applications are in: electronic signal boxes, vital ETCS computers, terminal computers for controlling signals and branches, and as basic elements in transmission of safety data and crypto communication.

In all these possible applications there are considerable differences in the scope of necessary hardware for the basic module, the necessary software in relation to the function, the factor of environment and also the necessary reliability in the safe data transmission.

The new technology implies a close connection between the hardware and the software, where the software controls the hardware safety. The procedures, steps and the sequences of operation are included in the software, more precisely in the program, which is especially important for the safe data transmission.

References:

[1] ADAMOVIC, Z. BRKIC, R.: *The Reliability Engineering,* The Association for Technical Diagnostics of Serbia – TEHDIS, Belgrade, 2004.
[2] BUSSE, K., FELTEN, F.: *Safe Data Transmission through Airwaves for the First Time in a CBI*, SIGNAL+DRAHT, 4/2005.
[3] BRKIC, R.: *Quality Analysis of Reliability and Safety of a Railway System*, The scientific-professional magazine Technical diagnostics - TEHDIS, Belgrade, 2006.
[4] BRKIC, R.: *Application of New Technology in the Integrated Railway System*, XXIX May Convention of Railway Maintainers of Serbia and Montenegro, Vrnjacka Banja, 2006.