XVIII SCIENTIFIC-EXPERT CONFERENCE ON RAILWAYS RAILCON '18

REDUNDANCY OF THE NEW GENERATION OF RAILWAY SIGNALLING SAFETY DEVICES AS BASIS FOR ACHIEVING THE NECESSARY SAFETY

Dejan TOŠIĆ [1]
Vladimir HABUŠ [2]
Milan POPOVIĆ [3]
Mirjana DŽUDOVIĆ[4]

Abstract *– Design, manufacture, installation and exploitation of signalling safety devices shall comply with the required level of safety which must be fulfilled throughout the whole period of their use. The developments in the field of electronics and its application in design and manufacture of safety devices has led to gradual replacement of relay signalling safety devices used in railways by the new generation devices (electronic devices). This technology change required finding of new technical solutions and improvement of the existing ones in order to maintain and improve the level of the required safety of railway traffic. The existing application of redundancy in realization of signalling safety devices has been raised to a higher level with a tendency of further development.*

Keywords – redundancy, safety, SIL, CENELEC

1. INTRODUCTION

According to a general definition used in railway terminology, redundancy represents the existence of a number of items (signals, elements, assemblies of different parts of devices) which exceeds the smallest number necessary for execution or transmission of the required information. Redundancy, understood in such a manner, has been rarely applied at the beginning, but has been used more and more with the development of the first relay signalling safety devices and has achieved its full expansion, that is, mandatory application, with the development of technology and appearance of electronic signalling safety devices.

Important terms necessary for good understanding of the lecture:

1. According to the definition from EN 50129:2003 [1], a fault represents an irregular condition which can cause a defect of device (for example resistor) which then leads to failure of that element and after that to the fault of the device itself.

2. Failure is irregular operation due to a fault, that is, impossibility to perform a proposed function because of the appearance of a fault.

3. According to the [1], reliability of a device is defined as capability to perform a function under the stated condition and stated time period.

4. According to the [1], safety represents protection from unacceptable levels of risk.

The main objective of use of redundancy during design, that is, manufacture of signalling safety devices is to improve safety of their operation (prevent that fault of an element inside the device affects the safety of the device).

There are several different ways to achieve redundancy within safety devices but the most common one with signalling safety devices in railway traffic is hardware redundancy (redundancy including repetition of function). It represents the existence of multi-item configuration “m-out-of-n“ where “m“ represents the minimum necessary number of items for the execution of a function, while “n“ represents the total number of items ($m \leq n$).

2. HISTORICAL OVERVIEW

At the beginning of development of relay signalling safety devices and in order to achieve the required safety of their operation, first or second class

[1] Directorate for Railways, Nemanjina 6, 11000 Belgrade, Serbia, dejan.tosic@raildir.gov.rs
[2] Hinka Wuertha 6, 10000 Zagreb, Croatia, vladimir.habus@xnet.hr
[3] Directorate for Railways, Nemanjina 6, 11000 Belgrade, Serbia, milan.popovic@raildir.gov.rs
[4] Serbian Railways Infrastructure, Nemanjina 6, 11000 Belgrade, Serbia, mirjana.dzudovic@srbrail.rs

relays were used as executive and control elements of the device. First class relays, due to their design solutions (maximum safety but also reliability in operation) are used as executive elements in the configuration "1-out-of-1". In order to fulfil the safety requirements the manufacturers, when using the second class relays as executive elements, if necessary, use hardware redundancy (repetition of function) in the configuration "1-out-of- 2" in fail stop manner of operation (if one relay fails, the function is not performed).

In order to check the fulfilment of requirements related to safety and security of operation, relay signalling and safety devices underwent a check known as "safety analysis". Only after the reception of positive results upon a safety analysis of a signalling safety device, this device was allowed to be used in practice.

An important disadvantage of relay signalling safety devices produced as presented above is the cost of their manufacture.

Rapid development of electronics, semiconductor elements and their assemblies as well as their price which has rapidly decreased following the degree of their development, led to the appearance of signalling safety devices mostly made by combining different electronic components. Signalling safety devices designed and manufactured in such a manner include a much larger number of elements which importantly increases the possibility of fault and they are generally less reliable than the mechanic ones, which requires application of additional measures in order to increase their safety. In order to improve the safety of electronic devices in the above mentioned fail stop manner of operation we use the redundancy in the configuration "2-out-of-2" (if one item fails the device stops working since the processing of both items is compared and they need to provide the same output). It is important to mention that aeronautics always use fail operate principle (if one element or item fails, the aircraft must still be certain to fly!). A similar fail operate principle exists in railways but only with the devices used to secure level crossings because the driver on the road must not be put in danger.

Hardware redundancy of relay signalling safety devices is realized, as already mentioned above, by doubling the elements while with electronic signalling safety devices this is achieved by doubling of functionally identical items. In both cases the following principle should be achieved – safety in the first place.

It should be noticed that, despite the impossibility to use the method of safety analysis with electronic signalling safety devices, as well as the higher possibility of fault in one of the items, redundancy in the configuration "2-out-of-2" can nevertheless fulfil the safety requirements defined by the existing European norms in order to achieve the higher level of safety (SIL 4).

3. MANNERS OF SOLVING PROBLEMS DUE TO THE OCCURRENCE OF A FAULT

There are three basic techniques used to improve or maintain the basic characteristics of safety systems in cases of possible faults: avoiding of faults, camouflage of faults and tolerance of faults.

Avoiding of faults is a technique on which we will not spend much time since it concerns strong processes of control regarding design, testing, quality control and similar procedures which include a much higher level of engagement of human factor.

Camouflage of faults is any technique preventing the fault of an element or assembly to produce an error which could endanger the safety of operation. An example of camouflage that will be presented in this paper and which is the most frequently used in design and manufacture of electronic signalling safety devices is majority deciding system.

Tolerance of faults relies on camouflage of faults but including detection and localization of a fault and then reconfiguration of the system (process of elimination of the faulty element and returning of the system in operational state) in order to eliminate the influence of a faulty component or module.

As it can be noticed, the process of majority deciding which basically represents the redundancy of the system is present in the techniques of camouflage and tolerance of faults.

4. HARDWARE REDUNDANCY

In order to achieve resistance to failures of a safety system today we most usually use, hardware redundancy (physical multiplication of hardware). There are three basic types of application of hardware redundancy, passive, active and hybrid, and this paper will mostly concern passive hardware redundancy which is the most frequently used with electronic signalling safety devices.

Passive hardware redundancy is based on the principle of majority voting and its main task is to tolerate the occurrence of a fault on an item. Generally speaking, the attention will be directed toward "n" modular redundancy (NMR) but through its most used subset of triple modular redundancy (TMR).

NMR, that is TMR, has the task to reconcile safety and reliability, that is, to improve as much as possible the reliability of the system without reducing its safety.

As it can be seen on the figure 1, the basis of TMR is the existence of three items on which the method of majority voting is applied and which defines the result at the output of the system. If output signals on "2-out-of-3" modules are identical, that signal will occur

at the outlet of the system, while the signal of the faulty module (output signal on that module is different from the signal at the outlet of the other two modules) will be hidden and it will not affect the final result but it will be indicated as a disorder which does not affect safety.

In order to improve the safety of operation with the systems using TMR and with the occurrence of design errors during manufacture of modules, today some manufacturers of signalling safety devices chose the heterogeneity of the modules themselves (for example the use of different microprocessors in each of the modules and different software in items). This certainly provides better quality products, but does not eliminate the main disadvantage of TMR which is the occurrence of comparator failure which represents a "unique point of failure".

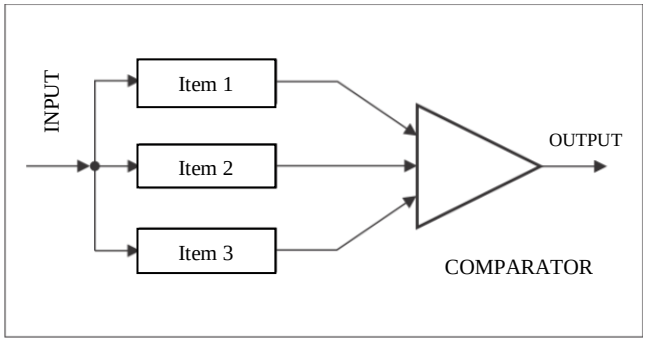

Fig. 1. Example of redundancy

Certainly, there are some techniques which can moderate or completely overcome this deficiency, which will not be treated by this paper since their application by all means leads to more complex devices and therefore increases their cost.

5. SAFETY INTEGRITY LEVELS (SIL) AND THEIR APPLICATION

Impossibility to apply safety analysis while testing electronic signalling safety devices required a new approach to the problem of control of their safety and reliability before placing them on the market. The solution has been found with the adoption of European norms (CENELEC) and recommendations defining safety integrity levels (SIL) that must be fulfilled by signalling safety devices before placing them in service (EN 50128 and [1]), determining who can do the testing and issue certificates to confirm that a certain signalling safety device has a certain level of safety, as well as methods by which every railway administration defines admissibility of a risk as prerequisite for the choice of a SIL (EN 50126).

It is here also very important to mention that in all the EU member states electronic signalling safety devices used on corridors must possess a certificate confirming the highest safety level (SIL 4), issued by an independent certified body (body of type A according to ISO/IEC 17020:2012).

6. CONCLUSION

The aim of this paper was to provide a short overview concerning the application of redundancy in design and manufacture of signalling safety devices. The subject is certainly much wider and new solutions are still being developed in order to (reconcile contradictory requirements) maintain and improve the safety of the existing systems, but also to improve reliability and availability of those systems. Since [1] has not yet defined the levels of reliability of signalling safety devices, although its meaning and manner of calculation has already been determined, on the market of the Republic of Serbia can be found electronic signalling safety devices with SIL4 realized by configuration "2 of 2","2 of 3" or double "2 of 2". The end user, that is the infrastructure manager, shall decide which of those solutions is appropriate but with a mandatory requirement according to which the device should possess a certificate of the highest safety SIL4, as prescribed by the "Rule on Technical Requirements for Signalling Safety Installations" ("Official Gazette of the RS", No 18/16).

As another warning to the infrastructure managers, it is important to mention that when deciding on the purchase and installation of electronic signalling safety devices which obtained a licence for installation before the adoption of the Railway Safety and Interoperability Law („Official Gazette of the RS", No 104/13, 66/15, 92/15 and 113/17) they should check with the manufacturer or provider whether they possess a SIL4 certificate issued by a certified body (before the adoption of the above mentioned law and rule, electronic signalling safety devices did not have to possess the SIL4 certificate) in order not to breach the applicable rules.

REFERENCES

[1] CENELEC standard EN 50129:2003 Railway aplications – Communications, signaling and procesing systems – Safety related electronic systems for signalling;

[2] Vladimir Habuš, Fault, error, failure–some of the basic railway signal–security devices, Traffic Automation, Zagreb/Copenhagen, 2005