Andrzej Lewiński
Prof. dr hab. inż.
Wydział Transportu i Elektrotechniki
Uniwersytetu Technologiczno- Humanistycznego w Radomiu
a.lewinski@uthrad.pl

DOI: 10.35117/A_ENG_18_06_06

Security of Railway Control Systems and new information technologies

Abstract: The new information technologies, such computer techniques, wireless (open) transmission standards and satellite systems applied for positioning have a important influence for different approach to safety criteria of railway control systems. The “fail-safe” rule assumed for relay control systems is based on high reliability of applied relays (guaranteed number of switches) and rigorous maintenance (homologation) procedure. The implementation of redundant, parallel computer systems has modified the concept of safety towards Tolerable Hazard Rate, where safety of computer systems is defined as an intensity of critical (dangerous, catastrophic) failures including self-testing. The wireless technologies respect the threats and their influence for functionality, availability and reliability of railway control systems (defined as probability).

Keywords: Railway Control Systems; Fail-Safe; Tolerable hazard rate; Probability of critical failure

Introduction

From the beginning of the railway, there was a problem of ensuring the safety of train traffic. The security was dependent on the man - the traffic controller and his services related to ensuring the proper passage of the train on the route and within the railway stations [27]. These activities were performed by responsible, trained disciplined employees for whom the work was a "service". The first dependence devices (key) and the introduction of telephone communication depended on the safety of trains' movement: the traffic, the signalman and the people responsible for infrastructure maintenance. In spite of rigorously followed procedures, serious accidents occurred, mostly due to human error, less often due to the reliability of security devices motion.

Introduction of electrical devices: firstly relay, then a computer, and then forward-looking with open radio transmission, introduced a gradual elimination of human impact on the safety of railway traffic management and control systems. The control process first covered the on-duty traffic eliminating the possibility of erroneous setting of the course, but in the next step also took into account the correctness of the driver's behavior - his reaction to track-side signaling. In modern systems of management and control of railway traffic, connected with High-Speed Railways such as the ERTMS/ETCS system, train parameters are also controlled in the context of safe displacement to the so-called "electric visibility", where distances between trains and safe braking distance are ensured.

The article presents the evolution of security criteria over many years, corresponding to both EU standards and scientific methods resulting directly from these recommendations. The author would like to thank Ph.D. Eng. Andrzej Toruń from the Railway Institute in Warsaw and Ph.D. "with habilitation" Eng. Tomasz Perzyński, associate professor at the Faculty of Transport and Electrical Engineering, University of Technology and Humanities in Radom for sharing the results of many scientific and research works jointly carried out in this area

Safety of relay systems

A significant step in the development of train protection devices was the use of electrical (relay) devices in the 1940s. This section refers to the study [12], but the principles of designing, operating and maintaining relay systems can be found [2, 7].

Relay srk systems were designed as safe systems based on the fail-safe rule - no single damage can lead to incorrect control of external devices (siren, crossover). This means that in the case of relay srk devices, a single fault must force a change of the system state to one that is defined as a safe state (e.g. preventing the display of the enabling signal, exclusion of the possibility of setting the course, switching the crossover, ...). Achieving the safe state causes certain limitations in the availability of the system to control, but does not cause a railway hazard situation. The basic safety of electric circuits were achieved by:

a) application of appropriate structural elements of circuits, i.e. protection relays of a given class, transformers, current transformers, reactors, fuses,
b) appropriate shaping of the electric circuit, in accordance with the albums of typical systems developed by authorized railway units for individual railway traffic protection systems.

Due to the way of designing and assembly of devices, relay traffic control devices have been classified into two basic groups:

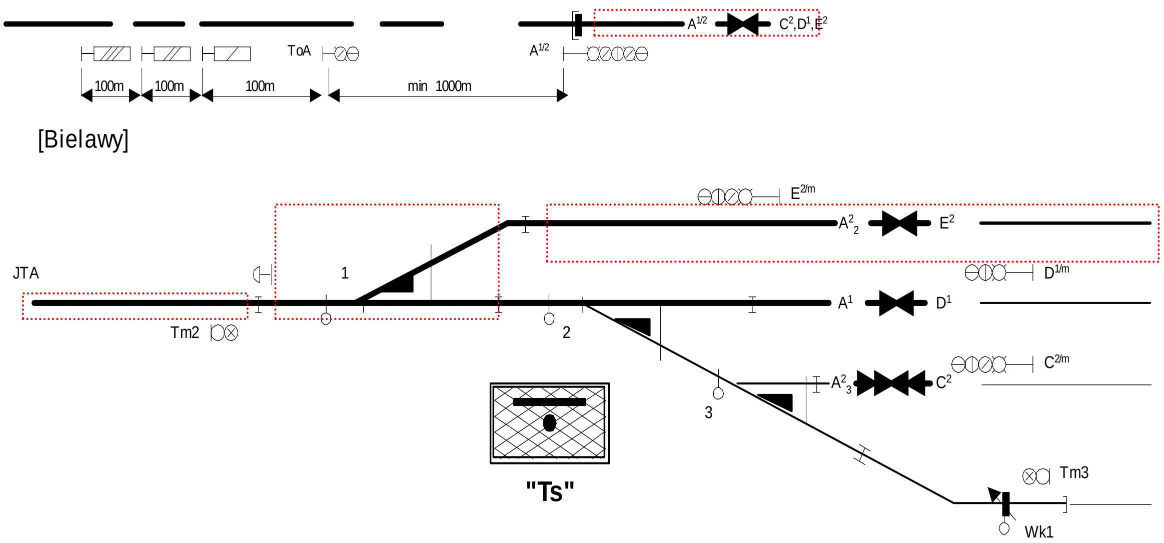
a) devices designed individually (e.g. station type E), for which design principles based on typical schematic albums were used and the principles of safe driving were defined depending on the track layout and movement characteristics of the object (station) in the form of a dependency table or waveforms .
b) geographical devices - interlocked (built in a modular structure i.e. IZH 111, CBP83, SUP-3, SUP-3M) defined as an association graph of typical functional modules.

Principle: fail-safe as the overriding safety requirement boiled down to the detection of a critical fault and a safe system response to the detected defect. In practice, both the principles of safe design and faults have been defined depending on their impact on the safety of the systems:

a) non-critical (safe) defects that limit the functionality of the system, causing disturbances in train traffic but without the possibility of causing train collisions,
b) critical defects - (dangerous), which introduce an immediate threat to safety and can lead to a dangerous situation - collision.

In practice, the implementation of the "fail-safe" principle is based on the use of appropriate elements - Class I (N) relays, where their damage asymmetry is used, assuming that a non-wake-up event (when the excitation circuit is closed) is more probable effect of, for example, interruptions in the relay coil circuit, and as unlikely due to constructional reasons the occurrence of the relay in the excited state after the power failure of the coil winding of the relay. And in the case of class II relays (C), the occurrence of both phenomena described above is assumed to be probable (damages eg remain in the excited state due to contact gluing).

Fig. **1** shows a fragment of an exemplary track system of a station with exemplary dependency records in the Table of Dependencies. This system (E} [21], is characterized by a fairly limited, but sufficient to conduct traffic on the station, a set of functions performed and basically provides the possibility of individual control of individual objects, ie switch, diversion, signaling device. This means in practice individual selection and adjustment of roads along with the control of the elements of these routes (unoccupied sections of insulated tracks and switches, the location of points and derailers, signaling states, ...) To ensure the safety of traffic at the station, in addition to checking the condition of route path elements, the system based on individually designed for each post of the dependence board excludes conflicting runs and controls the conditions for safe setting and releasing of route paths.



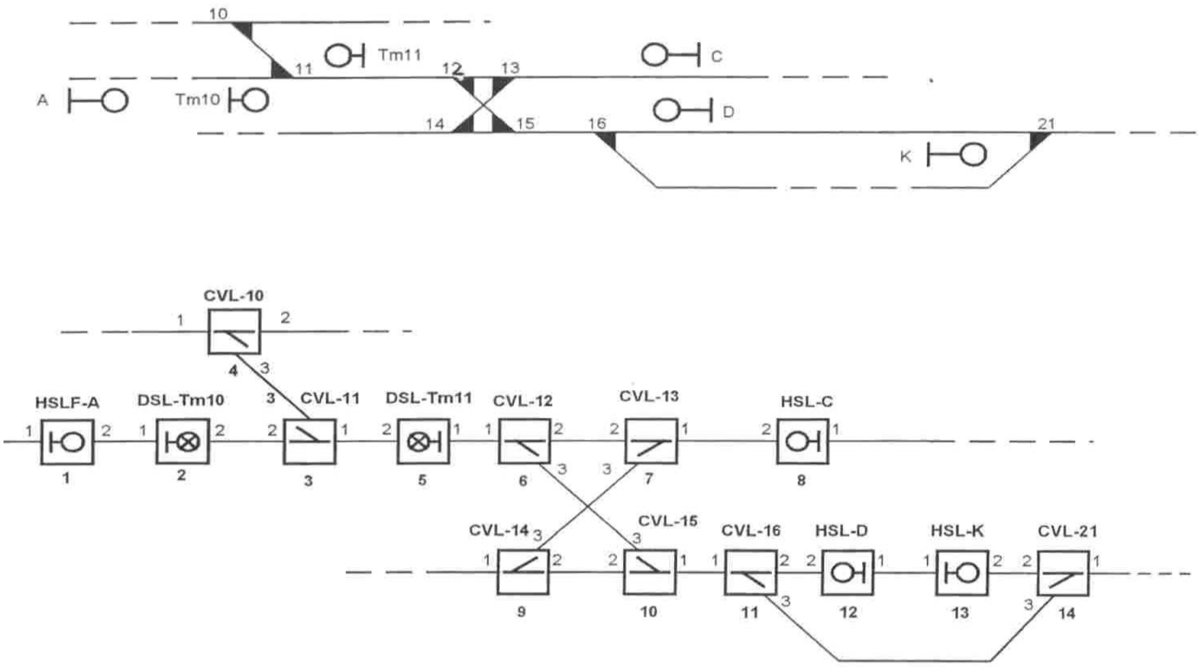
Lp	Przebieg	Opis przebiegu	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	1	2	3	4	5	6	7	8	9	Odcinki izolowane	
			Przebiegi pociągowe															Przebiegi manewrowe																			Zwrotnice i wykolejnice										
			A^2_3	A^1_1	A^2_2		C	D	E		S^2_3	S^2_1	S^1_2		M^2_1	L^1_1	K^2_1		Tm 3	C^m	D^m	E^m		Tm2					Tm 11	M^m	L^m	K^m	Tm13					1	2	3/Wk1	10/Wk6	11	12/13	14/15			
																								5	3	1	2						5	3	1	2										Torowe	Zwrotnicowe
1	A^2_3	Ze st. Bielawy na tor 3	−	+	+		+	+	+		+								+	+	+	+		+	+	+	+			+				+				+	−	+						A,3	1,2,$^3/_{Wk1}$
2	A^1_1	Ze st. Bielawy na tor 1	+	−	+		+	+	+			+							+	+	+	+		+	+	+	+				+				+			+	+	+o	+o					A,1	1,2
3	A^2_2	Ze st. Bielawy na tor 2	+	+	−		+	+	+				+						+	+	+	+		+	+	+	+					+				+		−								A,2	1

1. An exemplary track layout of the station together with a table of dependencies

This system is best suited for small and medium-sized stations because for large stations it is difficult to properly design the circuits so that optimal operating and operating indices for the station can be achieved (mainly when defining conflicting events).

The JZH 111 interlocking relay system is shown in Fig. **2** [1, 3, 21], distinguished in its structure by the use of specific, repetitive relay blocks responsible for the operation and control of one specific type of device at the station (crossover, signaling device, ...) made in the form of a closed universal, repeatable, multi-relay assembled module.

The individual modules are connected to each other by appropriate logical paths, below are exemplary logical paths: selecting path of the route path, module access control, side protection search, setting the path elements, confirming modules, speed control (signal image), signal relays, automatic releasing the course, immediate release of the course. An example of how to connect the JZH 111 system modules is shown in Figure **2**.



2. An example of how to connect the JZH 11 system modules1

In practice, at stations operated by PKP PLK S.A. You can meet many srk relay systems both made in the process technology (devices type E, PB) and interlocked (IZH 111, SUP-3, OSA-H, ...), which are increasingly adapted to cooperate with computer control panels and are subject to centralization control as part of the construction of a local control center. This proves that these devices meet the assumed traffic functions, moreover, as demonstrated by the experience of over 50 years of operation of relay devices on the PKP network, they are characterized by high durability and reliability and guarantee the required level of technical safety (provided that the principles of their maintenance and operation are maintained, what becomes more and more difficult due to the passage of time to provide the right elements necessary for their safe operation (ie relays whose production is expensive due to the need to maintain expensive technology and falling demand on the market).

Computer systems safety

The philosophy of computer systems safety introduced in the 1970s assumed the same probability of distortions 1 → 0 and 0 → 1. This resulted in a different approach to the concept of security - **a critical defect was the result of more than one failure, there should be at least two independent defects in isolation from independent processing channels, In addition, any single, non-critical fault should be detected in a specified (by the standard) time.**

Tab. 1. Safety of rail traffic control systems in the EU

Assumptions	**Intensity of faults (per hour) [h^{-1}]**
Permissible accidents caused by a dangerous technical defect = 1 accident per year in the EU	**10^{-4}** For the entire rail system in the EU (all system installations)
1 dangerous defect on 10 leads to an accident	**10^{-3}** For the entire rail system in the EU (all system installations)
1 fault in 10 is a malfunction of the railway traffic control system	**10^{-4}** For the entire rail traffic control system in the EU (all srk installations)
A safety margin of 10: 1 ensuring an appropriate level of tolerance	**10^{-5}** For the entire rail signaling system in the EU (all signaling installations)
1000 complete signaling systems in the EU	**10^{-8}** For a complete signaling system (e.g. control in area or on a line)
10 subsystems that are part of one complete signaling system	**10^{-9}** For a signaling subsystem (e.g. a large centralized dependency system)
100 system components in one subsystem	**10^{-11}** For one system element (crossover controller, signaling device)
Factor 100: 1 between neighboring Safety Levels	**10^{-11}** (for the Security Level 4) **10^{-9}** (for the Security Level 3) **10^{-7}** (for the Security Level 2) **10^{-5}** (for the Security Level 1)

Table 1 presents the philosophy of security, as from the basic assumption (one critical event, catastrophic event, an i.e. accident with victims in people, translates into the reliability of systems, subsystems, devices and components used.) Interpreting Table 1 can state that the initial assumption - one critical event annually in the EU is the minimum of the acceptable level of THR risk, this translates into a reduced intensity of damage to components of the srk subsystems. Adoption of such intensities leads to an average failure intensity of a centralized control system of 10-5 / h, which gives an average damage intensity of 10- 3 / h in the entire railways in the EU (on average, one dangerous damage during the year).

The basis of the designed systems were redundant systems - multi-channel computer systems with independent power supply, multiple and independent and transmission channels as well as rigorously adhered to software standards and hardware configuration. This was determined by the EN 5012x group standards, in force in Poland after 2005. The basis for the new safety criteria introduced was the Tolerable Hazard Risk (THR) [14, 15] whose principles will be presented below.

The implementation of the security of computer systems used in the railways is based on the fail-safe principle [11]. There are many systems in the railway system which, due to potential threats resulting from their damage, have been properly classified [14]. Table 1 presents a new safety concept based on the reliability theory [6].

The concept of safe computer systems used in the railway industry assumes a very low intensity of faults, which with a total independence of processing channels (2 or 3) guarantees a negligible probability of a double or multiple failures - decisive for a catastrophic (critical) failure. The basis of the analysis is the acceptable, acceptable level of risk.

According to the standard [13], the system's safety depends not only on the intensity of damage but on the detection of single and double (multiple) damages. For this purpose, the Tolerable Hazard Rate (THR) has been introduced. This coefficient can be calculated from dependencies:

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \tag{1}$$

where: λ_i – the intensity of damage for the channel i, $t_{d_i}^{-1}$ – system response time to error since the creation of the channel i.

According to UIC and CENELEC recommendations for safety systems, a factor of 100: 1 is assumed between the intensity of faults for neighboring safety levels. The concept of safe computer systems used in the railway industry assumes a very low intensity of faults, which is the total independence of processing channels (2 or 3). With the safety of srk systems classified to SIL-4, there is also a time to diagnose single faults:

$$T_{sf} = \frac{k}{1000 \cdot \lambda} \tag{2}$$

and double faults:

$$T_{2sf} = \frac{2}{\lambda} \tag{3}$$

where: k - a redundancy factor of 1 for "2z2" and 0.5 for systems ‘2z3”, λ - sum of medium intensity of damage to elements, which simultaneous damage may lead to hazard.

The formula (1) shows that for systems with one processing channel, the THR value corresponds to the intensity of damage λ . In turn, for a system consisting of two processing channels, the pattern takes the form $\lambda \frac{2t_d}{t_{FT}}$, which means that the intensity of critical damage has been reduced to a degree 2td/tTF, where td is the reaction time to damage, and tTF is the average time until damage occurs in the channel.

Safety levels mentioned in the table refer to railway traffic management and control systems, srk systems are classified as the highest, fourth level of safety (SIL4).

Tab. 2. Safety classification in traffic management and control systems in the EU

LEVEL	**Required security status**	**Consequences of error**	**Characteristics of the railway system**	**The name of the system used in railways**
4	**Very high**	Loss of human life	Protection against derailment and collision of trains	Safety system Fail-safe system
3	**High**	Damage and loss of health	Ensure proper train driving	High level safety system
2	**Average**	Environmental pollution	Ensuring the control of train movement	A system with a significant level of security
1	**Low**	Loss of property	Ensuring passenger service	Low safety system
0	**Not applicable**	Loss of information that does not affect safety	Ensuring proper maintenance of the railway	Not connected with safety

In connection with Poland's entry into the EU structures, the following standards have become applicable: PN-EN 50126 [24], PN-EN 50128 [25] and PN-EN 50129 [26].

The PN-EN 50126 standard specifies reliability, readiness, availability, and security (RAMS - Reliability, Availability, Maintainability, and Safety), as a process based on the system life cycle (system life cycle). In this process, the individual steps of the system and procedures related to the approval were defined before moving on to the next stage. (specification of requirements, design, implementation, etc.).The PN-EN 50128 standard specifies the procedures and technical requirements for the design of the secure electronic system software for control and protection on the railway, [10]. It should be noted that this standard is not fully obligatory.

The PN-EN 50129 standard defines the requirements for the design, testing, acceptance, and approval of electronic systems, subsystems and signaling devices related to safety in railway applications].

Taking into account such parameters as system response time to error since detection, system response time to error since creation, time of system component testing, average TMBF times of system components, THR can be determined. Permissible values of the THR coefficient for SIL safety levels are presented in tables 3 [13].

Tab. 3. Permissible THR values compliant with binding standards

THR (per hour per function)	**SIL** (Safety Integrity Level)
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

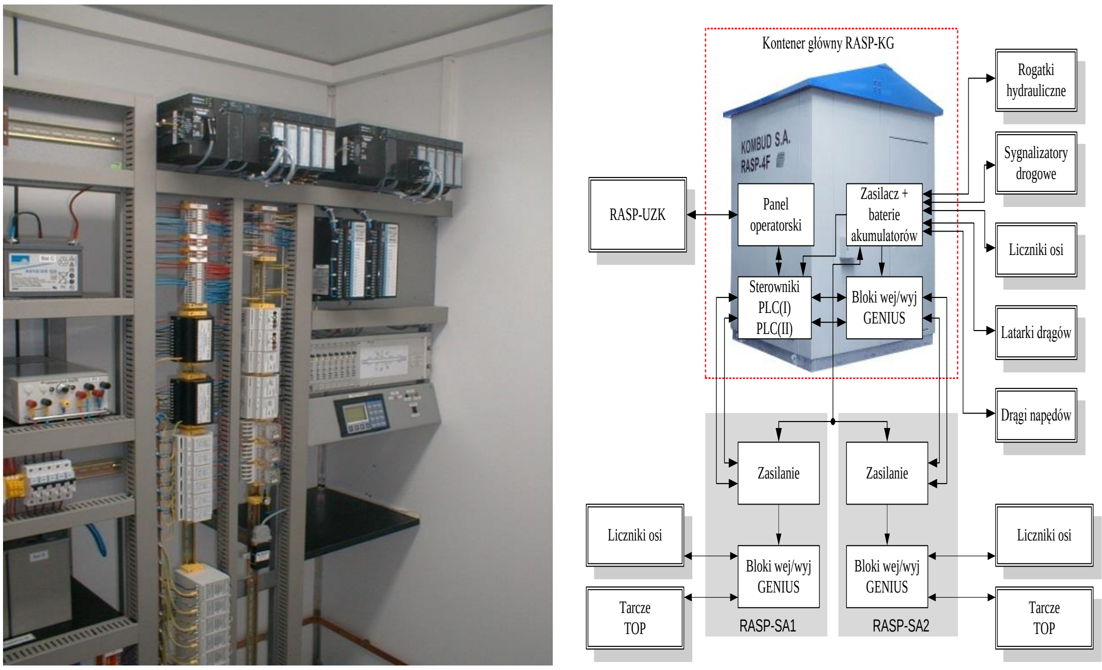
which means that the intensity of critical damage has been reduced to a degree 2td/tTF, where td it is the reaction time to damage, and tTF is the average time until the damage occurs in the channel.

In this way, it was possible to assess the safety of a typical level crossing signal system (RASP4 produced by KOMBUD S.A [29], [30].) Classified to the highest level of SIL4 security. It is a typical two-channel system (Fig. **3**), two independent PLC controllers perform all the functions specified in the standards and ordinances. PLC controllers are built on the basis of two identical sets built on cassettes, creating two independently operating controllers with mutual data exchange and synchronization of work over the Ethernet bus. The single driver is included:

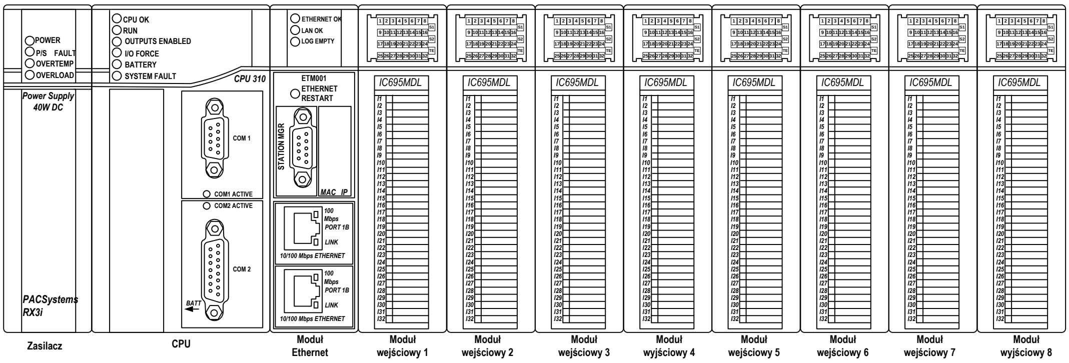
- baseplate IC695CHS012,
- IC695PSD140 DC power supply,
- central unit type IC695CPU310,
- IC695ETM001 communication interface,
- discrete input module IC694MDL660,
- discrete output module IC694MDL754

For the equipment used, the authors provided the following MTBF values (average time between occurrence of damages) based on data of the manufacturer / distributor of equipment (Astor Kraków company):

a) baseplate IC695CHS012 - 761 000 [h]
b) DC power supply IC695PSD140 - 1,092,000 [h]
c) Central Unit IC695CPU310 - 638,000 [h]
d) communication interface IC695ETM001 - 992,000 [h]
e) discrete input module IC694MDL660 - 6,393,000 [h]
f) discrete output module IC694MDL754 – 553 000 [h].



3. Dual channel implementation of the RASP-4F automatic crossing signaling



4. Automatic RASP-4F drive signaling cassette

Controller configuration contains the different number of modules, which assuming the worst case (serial reliability structure) leads to resultant MTBF value for individual sets:

1 set with 2 modules e) and 1 module f) - 144 374.4267 [h]
2 set with 3 modules e) and 1 module f) - 141 185.9945 [h]
3 set with 4 modules e) and 1 module f) - 138 135.3490 [h]
4 set with 6 modules e) and 2 module f) – 106 832.6186 [h].

The authors ensured a sufficiently short time to detect a single failure and transition to a safe state. (This time, tsf, is much shorter than the expected average time between failures of both computers.) According to the PN-EN 50129 standard, the detection time of a single fault meeting the condition ,tsf <= k/(1000 * a), where □k = 1.0 for systems „2 z 2", a – 1/MTBF.

The authors adopted the following values for the THR calculation:
- time of cyclical testing of inputs / outputs (T) 250 ms
- error response time (NT) 1s,
which gives the value of error response time (SDT) equal to 0.0003125 [h] and as a result gives the THR value below every 10e-1, in accordance with the PN-EN 50129 standard for SIL4. The calculated time of detecting individual errors (TSF) meets the criterion resulting

from the limit value referenced to the estimated MTBF value for the "2 out of 2" system given in the PN-EN 50129 standard.

The THR can also be determined on the basis:

- operational data (i.e. systems currently in operation) based on the data from operation (the time required for verification is over 10 years [x]),

- forecasting data calculated based on the principles of reliability estimation of electronic devices based on the MIL [xx} standard.

Both methods supplement the safety assessment in accordance with the mentioned national standards and regulations.

Systems security with new information technologies

A very good example of the impact of new information technologies on the security of traffic management and control systems in transport is the European Rail Traffic Management System ERTMS (obligatory implementation in the EU Member States). The subsystem directly responsible for the ETCS train safety (European Train Control System) has been defined for three levels of control, the Polish railway system has been implemented on selected sections of the level 1 line, work is underway on the implementation of level 2 which is directly related to the safety of trains with increased speed (CMK line) [5], [14]. The introduction, as a mandatory ERTMS / ETCS system using radio transmission, should ensure that the high level of functionality and interoperability in servicing passenger trains, including control and monitoring of the high-speed rail network (KDP) as the main objective, is achieved).

In the case of the implementation of the ETCS system, the following security criterion has been adopted: new technological solutions cannot reduce the existing level of security. The case of the ETCS system could be used to refer to traditional systems (current systems with constant block spacing based on insulated sections and a line block) and show how new technologies radically reduce the probability of a critical error

The basic issues related to the ERTMS / ETCS system relate to:

- improving safety (driver monitoring),
- increasing the capacity of railway lines, especially KDP lines,
- implementation of a new communication standard using the ERTMS / GSM-R system, and in the future more effective radio transmission standards, including LTE or WiFi [9].

Trains equipped with onboard ERTMS / ETCS system devices will be informed about which ERTMS levels are served in a given area when the balis group passes that informs about approaching a given ERTMS / ETCS area. Onboard equipment (in accordance with the on-board track-side compatibility) upon receiving entry information into the area will switch to the ERTMS/ETCS system level, which is defined as part of the system development project.

The first level is an overlay for station and line devices that preserve the dispersed nature of railway traffic control. The ERTMS / ETCS level 1 device ensure that the train will not travel beyond the boundary of the set and established a route, and that it will not exceed the speed allowed on any route section. The track equipped with the first level devices uses switchable and non-switchable eurobalises. In addition, it can be equipped with an Euroloop or radio used to update information transmitted via eurobalise or to two-way tor-vehicle communication for the pre-processing of information by track-side equipment.

The second level ERTMS / ETCS is a traffic control based on continuous, digital, bi-directional radio transmission. The track is equipped with additional Eurobalises in addition to radio control centers (RBC). At the same time, semaphores can be removed from the track, as their functions are taken over by continuous digital transmission. Variable information can easily be transmitted over a radio channel so that eurobalises no longer have to be switchable. Level three is the development of level two by transferring track occupation control from track-side equipment to vehicle equipment. This allows for controlling the succession of trains according to the principle of a movable block spacing and enables the abandonment of track circuits and axle counters.

Train travel from the point of view of rail traffic control devices can be presented by the approach presented by the stochastic process. In many works [10, 15, 16] to describe the transitions between the states responsible for typical train behavior, homogeneous, stationary and ergodic Markov process is indicated.

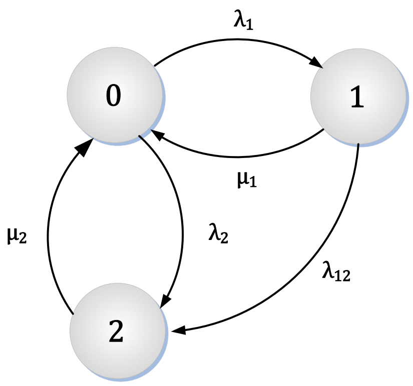
This train protection process is presented in the figure **5** [18].The states presented correspond to the following situations:

0 – the state of correct driving according to the last information received, the driver driving the traction vehicle according to the last-received driving license until the next information about the new driving license is received,

1 - the state of correct implementation of the control procedure (in accordance with the signal display presented on the signaling device or according to the on-board computer),

2 - emergency stop or speed decrease resulting from the situation where the control has been lost (emergency braking forced by the ATP system - in the conditions of the Republic of Poland - AWS system AWS).

Transitions between states are related to the occurrence of basic parameters in the performed procedures implemented in railway traffic control devices. In further considerations, we assume the adoption of a maximum block spacing length of 1500 m (a minimum distance of 1300 m is not mandatory in these analyzes) for a maximum speed of 160 km / h, and parameters λ and μ specifying:



5. Universal control and train control model

- λ_1 – the intensity of the required rides for correctly received driving permits 106,67h^{-1} (corresponding to the time of preparation for displaying the enable signal to the traction vehicle 33,75s),
- μ_1 – intensity of typical service amounting to 300 h^{-1} (Inverse service time 12s),
- λ_2 – intensity for incorrect interpretations regarding the requirements (failure rate) of 0,000227687 h^{-1} (associated with the occurrence of 2 rides ended by an emergency stop in a year),
- λ_{12} – intensity of erroneous interpretations in relation to requirements (failure rate) 0,005952381 h^{-1} (associated with the time occurring during emergency trips, 1 per week)

- μ_2 – intensity of emergency service amounting to 72 h^{-1} (the inverse of the emergency response time of 50 s).

The differential equations used to describe transitions between states are based on:

- the distance and speed parameters presented above and λ_1 – the intensity of events related to the departure of the train on the permission signal or the received driving license (MA) and the information received about the next driving procedure,
- λ_{12} – the intensity of an event related to the wrong train driver reaction or the incorrect operation of the ATP system,
- λ_2 – the intensity of the incident related to the implementation by the braking signal (without the participation of the driver) until the train is completely stopped,
- μ_1^{-1} – the time necessary to display to the driver information about the next operation - train driving procedure taking into account safety conditions,
- μ_2^{-1} – the time necessary for the driver to start driving after the train is automatically stopped.

In existing srk devices, which are used to drive a train based on a fixed block distance (occupancy of subsequent sections), it is based on the display of the signal allowing driving, while obtaining information about the occupancy of the traction vehicle traveling along the railway line.

The sense of the above sequence of events is obvious. Therefore, the state P2 can be treated as the operational (functional) coefficient, which is responsible for the effectiveness of the control. This means that the train control method is related to the capacity of the railway line resulting from the possibility of occupying subsequent track sections.

Assuming a maximum block length of 1500 m and a maximum speed of 160 km / h and parameters for the Markov model shown in Figure 5:

- λ_1 – the intensity of the required rides for correctly received driving permits 106,67h^{-1} (corresponding to the time of preparation for displaying the enable signal to the traction vehicle 33,75s),
- μ_1 – intensity of typical service amounting to 300 h^{-1} (the inverse of the service time of 12s),
- λ_2 – intensity for incorrect interpretations regarding the requirements (failure rate) of 0,000227687 h^{-1} (associated with the occurrence of 2 rides ended by an emergency stop in a year),
- $\lambda 12$ – intensity of erroneous interpretations in relation to requirements (failure rate) 0,005952381 h^{-1} (associated with the time occurring during emergency trips, 1 per week)
- μ_2 – associated with the time occurring during emergency trips, 1 per week 72 h^{-1} (the inverse of the emergency response time of 50 s)

after substituting the above equations and calculations, we obtain a value for a fixed block interval of P_{2FBD} =2,401·10^{-5}.

The ERTMS / ETCS system is an intelligent overlay for existing rail traffic control and management systems that ensure a high level of safety. All trains not equipped with onboard devices of the ERTMS / ETCS system will receive the driving license (MA) by displaying a signal display on the siren. Traction vehicles equipped with onboard ERTMS / ETCS Level 1 system equipment shall be allowed to drive after crossing the balis group placed in front of the signaling device, while for level 2 the driving license will be picked up by the traction vehicle from the radio control center (RBC) via the secure rail network global mobile communication system ERTMS / GSM-R. Traction devices have the ability to work according to different plans (levels and modes), taking into account the conformity of onboard equipment with track-side devices. Existing rules of cooperation of onboard devices with appropriate track-side devices ensure cooperation in i.e. "down", i.e. a traction vehicle equipped with level 2 devices can drive on railway lines with level 2 and level 1 devices installed, while traction vehicles equipped with level 1 devices may operate move only on railway lines equipped with the same level.

Trains equipped with onboard devices of the ERTMS/ETCS system will be informed about their control in a specific railway area limited by balises defining also the appropriate system level.

Level 1 is an overlay for traffic control devices used at stations and on routes and is treated as a distributed control system. Level 1 devices of the ERTMS / ETCS system ensure that the supervised traction vehicle will not travel for the designated permit for driving on the route on which it moves and the traction vehicle is traveling with the supervision of not exceeding the permitted speed on the traversed railway. In the track, where level 1 is built-up, in the control areas, eurobalises are used, both in a switchable and non-transferable version. In addition, track railway infrastructure may be equipped with a euro pallet or a radio used to update information transmitted between the track and the traction vehicle or to two-way communication of the traction vehicle to update the vehicle information on the trackside equipment [18].

Assuming a maximum block spacing length of 1500 m and in this case for a maximum speed of 160 km/h and parameters for the Markov model shown in Figure **1**:

– λ'_1 – the intensity of the connection before the balis (semaphore) is λ_1=166,67h^{-1} (with reference to 21,6s),
– μ'_1 – estimated (intensity) services of 360000 h^{-1} (related to max 10 ms) it is connected with the assumption of synchronization time when driving 1 m,
– λ'_{12} – intensity of damaged telegrams from balis leading to train stop 0,33*10^{-9}/h ,
– λ'_2 – the intensity of onboard equipment failures in accordance with THR for onboard equipment 1x10^{-9},
– μ'_2 – the intensity of switching onboard devices to the dedicated mode for non-equipped trains amounting to 0.03333 h (associated with 120 s, the time of implementation of driving in the mode of a train not equipped)

after substituting the above equations and calculations, we get the value for the ERTMS / ETCS level 1 $P_{2ETCS\ L1}$ =3,003·10^{-8}.

The analytical calculations carried out show how the new system (ETCS) significantly minimizes the occurrence of a catastrophic event (P_2}.

Conclusions

The article presents the evolution of the concept of safety of railway management systems and control over recent years. The entry point was the adoption of the security level of relay srk systems. The presented solutions of JZH and E systems were based on the concept of a safe relay, whose most probable damage did not affect the safe control of external devices.

The commonly used computer systems discussed were based on redundancy and a relatively short fault detection time. The resulting parameter was THR (Tolerable Risk Level) whose values were defined in the applicable standards (PN EN 50 159).

The next step was the introduction of open transmission standards based on public networks, mainly wireless [9]. Research confirms that the use of typical communication standards based on wireless Internet access using appropriate procedures, especially cryptographic methods, allows to provide the same level of security as in the case of previously used cable transmissions in distributed computer systems. In general, starting from relay systems to future implementations based on open transmission, the same fail-safe principle applies: any single fault cannot lead to a dangerous situation. In computer systems, the detection time is additionally determined. In systems based on public networks, the minimization of the delay time is additionally analyzed (caused, for example, by the loss or distortion of the transmission and related repetition, etc.), which allowed providing the same level of functionality as in the systems implemented so far, both computer and relay.

In each model presented (constant block spacing, level 1), the probability of state 2 is significant from the point of view of unavailability of the system (state 2 corresponds to the uncontrolled emergency stopping of the traction vehicle caused by faulty operation of signaling devices or automatic traction vehicle control devices). We can see that each subsequent level of traction vehicle inspection reduces the probability of state 2, so the availability of the entire system is improved. This is related to the idea of the ERTMS / ETCS system: better bandwidth, availability and, as a consequence, better parameters of railway traffic, including high-speed railways [2, 6]. This work also contains a similar analysis for level 2 and 3 of the ETCS system, showing a significant reduction (by three orders of magnitude) of the probability of a catastrophic event occurring.

Other methods [28, 29] can also be used for safety analysis, such as, for example, FTA tree analysis (Fault Tree Analysis) supplemented with time dependencies [20], it becomes a strong security tool.

In summary, new information technologies introduced over the last years provide a level of security, no worse than in relay systems traditionally recognized as safe. New information technologies control a man (driver, duty controller) minimizing the occurrence of a critical event determined by reduced intensity (THR) or the probability of such an event occurring

Source materials

[1] Album schematów – zbiór przykładowych rozwiązań – geograficzny system stacyjnych przekaźnikowych urządzeń srk typu CBP83, 1985r.

[2] Dąbrowa – Bajon M. „Podstawy sterowania ruchem kolejowym" – ISBN 83-7207-343-0 Oficyna Wydawnicza Politechniki Warszawskiej 2002,

[3] Geograficzny, zblokowany system urządzeń stacyjnych zrk typu JZH 111 – dokumentacja techniczna, Katowice 1977

[4] Grant MNiI pt:„Wpływ nowych technologii informacyjnych na poprawę funkcjonalności i bezpieczeństwa ruchu pociągów" nr 4T12C00529. Politechnika Radomska 2006.

[5] Jaźwiński J., Ważyńska - Fiok K.: „Bezpieczeństwo systemów", PWN Warszawa 1993

[6] Jaźwiński J., Ważyńska – Fiok K.: „Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym", Zeszyt 95, WKiŁ, Warszawa 1982

[7] Karaś S. „Urządzenia zabezpieczenia ruchu kolejowego" wyd. 3, WKiŁ W-wa 1986,

[8] Kombud – materiały Zakładu Automatyki KOMBUD S.A. w Radomiu

[9] Kontron – materiały Kontron East Europe sp. z o.o

[10] Lewiński A. „Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego" Politechnika Radomska Monografie nr 49/2001

[11] Lewiński A., Perzyński T., Toruń A, „ETCS jako metoda poprawy funkcjonalności i przepustowości na liniach kolejowych",materiały konferencji LOGITRANS2015

[12] Lewiński A., Perzyński T., Toruń A., „Tendencje rozwojowe systemów srk, na przestrzeni ostatnich lat", Problemy Kolejnictwa, Zeszyt 3, 2014,

[13] Lewiński A., Perzyński T., Toruń A.,: "Risk Analysis as a Basic Method of Safety Transmission System Certification". Communications in Computer and Information Scienc 239), Springer-Verlag Berlin Heidelberg 2011

[14] Lewiński A., Perzyński T.: „Akceptowalny poziom ryzyka jako kryterium bezpieczeństwa w transporcie kolejowym", prace konferencji Wydziału Transportu Politechniki Radomskiej Logi-Trans 2007

[15] Lewiński A., Perzyński T.: The reliability and safety of railway control systems based on new information technologies. Communications In Computer and Information Scienece 104. Springer 2010'. Transport Systems Telematics

[16] Lewiński A., Torun A., Perzyński T.: "The Analysis of Open Transmission Standards", materiały Międzynarodowej Konferencji Transport Systems Telematics Tst2014, Monografia, Communications In Computer And Information Sience, Telematics – Support Of Transport, Nr 329, Springer-Verlag Berlin Heidelberg 2012 in Railway Control and Management

[17] Lewiński A., Toruń A. The changeable block distance system analysis, Springer – Verlag Heilderberg 2010 – J. Mikulski (Ed.) TST 2010 CCIS 104, 2010

[18] Lewiński A., Toruń A., Gradowski P: "Modeling of ETCS with respect to functionality and safety including Polish Railways conditions", materiały Międzynarodowej Konferencji Transport Systems Telematics Tst2014, Monografia, Communications In Computer And Information Sience, Telematics – Support Of Transport, Nr471, Springer-Verlag Berlin Heidelberg 2014

[19] Lewiński A., Toruń A.,: " The Changeable Block Distance System Analysis", Communications in Computer and Information Science (104), Springer-Verlag Berlin Heidelberg 2010

[20] Magott J., Skrobanek P., Timing analysis of safety properties using fault trees with time dependencies and timed state-charts, Reliability Engineering & Systems Safety, 2012, vol. 97, Nr 1

[21] Mickiewicz T., Mikulski A., „Elektryczne urządzenia zabezpieczenia ruchu kolejowego – urządzenia stacyjne" WKiŁ Warszawa 1968,

[22] Miksza E., „Zblokowany system sterowania ruchem kolejowym na stacjach typu IZH 111" WKiŁ Warszawa 1979,

[23] Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defense

[24] Norma PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikowanie i wykazywanie Nieuszkadzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS). Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia.

[25] Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.

[26] Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.

[27] Norma PN-EN 50159: 2010. Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania.

[28] Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Procedura analizy rodzajów i skutków uszkodzeń (FMEA),

[29] Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA),

[30] Norma PN-EN 61078:2006 Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie,

[31] Norma PN-IEC 60300-3-9:1999 Analiza ryzyka w systemach technicznych,

[32] Quality of Service Test Specification" form 11.09.2003 and parameters: GSM-R Interfaces Class 1 Requirements. SUBSET-093 z 11.10.2005r.

[33] Winter P. and other: Compendium on ERTMS. ISBN 978-3-7771-0396-9, UIC, (1st edition 2009)

[34] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998r.,