THE APPLICATION OF PUBLIC RADIO TRANSMISSION STANDARDS IN INNOVATIVE RAILWAY AUTOMATION SYSTEMS

WYKORZYSTANIE PUBLICZNYCH STANDARDÓW TRANSMISJI RADIOWEJ W INNOWACYJNYCH SYSTEMACH AUTOMATYKI KOLEJOWEJ

Andrzej Lewiński¹, Zbigniew Łukasik², Andrzej Toruń³

^{1,2} Faculty of Transport and Electrical Engineering

Kazimierz Pułaski University of Technology and Humanities in Radom

³ Railway Institute in Warsaw

e-mail: a.lewinski@uthrad.pl, z.lukasik@uthrad.pl, atorun@ikolej.pl

Abstract: *The work deals with the rules of safety communication applied in public, open data transmission systems according to obligatory standard PN-EN 50159-2011. The innovative systems manufactured by chosen manufactures applying such solutions and elaborated concepts of future systems giving new functional possibilities with regard to existing safety standards assigned to railway control and management.*

Keywords: *Railway automation, Open Transmission Systems, Standard PN-EN 50159:2011*

Streszczenie: *W pracy przedstawione zostały zasady bezpiecznego stosowania rozwiązań przesyłania danych w publicznych, otwartych systemach transmisji stosowanych w systemach zarządzania i sterowania ruchem kolejowych zgodnie z obowiązującą normą. PN-EN 50159-2011. Przedstawiono innowacyjne systemy wybranych polskich producentów stosujących takie rozwiązania oraz koncepcje systemów przyszłościowych, w których rozwiązania na otwartej transmisji radiowej dają nowe możliwości funkcjonalne w zarządzaniu i sterowaniu ruchem kolejowym przy zachowaniu obowiązujących standardów bezpieczeństwa.*

Słowa kluczowe: *Automatyka kolejowa, Systemy Transmisji Otwartej, PN-EN 50159:2011*

1. Introduction

The paper deals with application of public wireless computer networks in railway control applications. The obligatory UE standard for such transmission standards requires special protection procedures but the result solutions of such systems must guarantee the same level of safety (corresponding to SIL classification [12]) such typical cable connections, wire of fiber optics, now used in railway computer controllers. In the paper the examples of replacement the cable connections by radio transmission channels in typical SIL4 systems, and the future system such Changeable Block Distance is presented. The typical standards used in safety transmission systems are A0-A1 (with additional data – e.g. time stamps and safety code-CRC), B0 (enciphered message containing user data, non-cryptographic safety code and additional data) and B1 (with additional data, non-cryptographic safety code, and cryptographic code).

Using in Railway Control Systems (RCS) the open transmission systems can not reduce the assumed level of SIL and defined for this system (e.g., linear blockade, railway signaling system) safety requirement. In this analysis assumed that the time of executed procedures (i.e. the determination of code integrity, encryption) is the sum for those individual devices of the system. Method that can effectively improve the efficiency of information exchange is pre-grouping of telegrams (with limited size) for more devices before executing procedures related to coding, determination of integrity code and encryption. This analysis allowed for the evaluation of various methods of increasing the safety of data transmission in used the OTS in railway control systems, including in particular methods of ensuring the integrity and confidentiality of information. From received results the least time needed to execute the integrity code and in the case of CRC codes these times are comparable. However, for the hash function the best algorithm was SHA-1. The fastest method of encryption is AES and the most efficient is DES cipher. Currently, the railway control systems are computer systems with dispersed structure, in this case should be take into consideration reaction times of individual devices.

The implementation of the open transmission standards to railway control systems require the estimation of Tolerable Hazard Rate corresponding to EU standards. The transmission channel must satisfy the obligatory measures related to assigned SIL level. Both cable and wireless transmission standards must be analysed corresponding to hardware failure rates in railway control devices. The paper deals with failure analysis in some railway control systems including open transmission solutions. The result based on FTA methods is a good criterion for the introduction of new transmission technologies. The transmission subsystem is a part of safety computer system in railway control application, defined in EU standards EN 50129 [12] assumes the significantly low level of failures and redundant channel architecture (“2 from 2” or “2 from 3”). Such assumptions lead to very small value of probability of critical (catastrophic) fault related to multiple failures in independent processing channels.

2. Safety transmission related to open public standards in railway control applications

The rule of safe data transmission

Exchange of information in RCS using an open transmission must guarantee the safety of the transmission, in accordance with the recommendations for the required of safety level SIL, in this case it is necessary use the appropriate standards and mechanisms of cryptographic for transmission. Requirements and recommendations are defined in the current standard EN 50159:2010 [13] regulating such uses in the signaling systems. In an open transmission systems (OTS), data transmission between the systems participating in railway control process can be conducted using open transmission, both wired and wireless links, shared in network with public access. This is concern above all of specialized radio networks (GSM) and the Internet access (WiFi, WiMax). This means that information is transmitted by the broadcast system available to unauthorized users, thus transmitted data can be exposed to attacks such as:

- Intentionally or not intentional masquerade, of another system in the railway control system,
- Attacks in order to access to the transmitted information or send to the system processed packets
- Removing, modifying or redirecting of data telegrams,
- Changing the order or repeating telegrams
- Delay of telegrams.

Therefore, the system based on OTS must protect transmitted data against such risks.

Types of telegrams

Basic methods of protecting the transmitted information in open transmission systems (OTS) in RCS systems are shown in Figure 1. This Figure shows the classification of groups of transmission telegrams and assigned to them the cryptographic methods. Meeting these requirements is necessary in order to achieve the assumed level by RCS system, the safety inviolabilities SIL. We can distinguish following telegrams:

- A0 - authorized access only, required is integrity code of data, is not required the cryptographic safety code.
- A1 - it is not exclude the unauthorized access, required is use of cryptographic safety code.
- B0 - it is not exclude the unauthorized access, encryption is required, it is not required of cryptographic safety code.
- B1 - it is not exclude the unauthorized access, cryptographic code is required, is not required the cryptographic safety code [13].

Fig. 1 Classification of types of telegrams to the open transmission systems according to EN 50159:2010

Methods of protecting the telegrams

The detailed structure of telegrams for the safe transmission with recommended safe protection mechanisms of data is shown on Fig. 2. In the paper was confined to two types of telegram A0/A1 and B0. (The B1 type of telegram is not considered because is not applied yet in RCS).

The Type of A0/A1 it has been used in closed transmission systems so far, implemented mostly in Profibus and Ethernet standards. Basically type B0 is proposed by most manufacturers of RCS systems with open transmission channel, and it concerns both dedicated radio links and wireless Internet too. In the case of a closed transmission with protocols of type A0 and A1 the number of devices in the system is fixed and all participants in the transmission are known. Devices can be identified by the network addressing, so it has the character of physically closed, which excludes the threat of unauthorized access to data, overhearing of transmission or insert the extraneous telegrams. As the protecting codes of data on those systems is recommended to use cyclic redundancy code CRC used to detect random errors.

Open transmission systems insert an additional threat to the system such, for example, masquerade another system into a system of railway control or

intentionally modification of sending telegrams. To avoid this, it's necessary use the methods protecting against unauthorized access and which allows to verification of authenticity of data. In this range the standard recommends use of cryptographic techniques, encryption methods and authentication keys.

Fig. 2 The structure of information in safe transmission systems according to norm EN 50159:2010

The telegrams using these techniques are identified as type B0 in which are recommended procedures of authorization by using of a hash MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm). For verification the integrity of the data can be used the redundant coding technique CRC (Cyclic Redundancy Check), which protect against random errors and allows to detection of single or series of errors. However, encryption of data the block ciphers encryption with symmetric key such as DES, 3DES (Data Encryption Standard) or AES (Advanced Encryption Standard) with 128-bit keys that allow to reject erroneous telegrams and protect against the decoding.

In order to determine time and probabilistic indicators data transmission in OTS systems, the analysis of execution time for individual function to determine integrity code, encryption and decryption of data depending on the length of the telegram was conducted (assumed that the typical length of telegrams in the system have a 16 Bytes) and for two bandwidths 512 kb/s and 1Mbit /s. Most producers of

RCS system assume type B0 of telegram which uses cryptographic techniques with the secret key.

Data are encrypted in its entirety including integrity code such selection of protecting of telegrams is mainly ensue from use of wireless data transmission.

3. Closed and open transmission

The safety

Currently applied railway control and management systems belong to the group of modern devices based on new computer and microprocessor technique which ensure much more functionality and efficiency. According to railway standards [12], [13] it is possible to use both radio and cable transmission in railway control systems. Usually a system with radio transmission has one channel and the communication is realized by VPN gates (Virtual Private Network). The basic structure of open and closed transmission is presented on Fig 3. Such solution is now developed by [14].

Fig. 3 The basic structure of open and closed transmission

Special cryptographically methods, which defend before unauthorized access, are very essential from viewpoint of safety. On the basis of formula (1) it is possible to calculate dangerous failure rate λ_{NT} . For commonly CRC32 (Cyclic Redundancy Check) code, the value of failure rate λ_{NT} can be calculated [5], [7]:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \quad (1)$$

where λ_N is a failure rate of all faults in transmission channel, $p_{UE}=2^{-C}$ is a probability of undetected failure due to the performance of the transmission code (C – number of redundancy bits).

Assuming that failure of all devices is row 10^{-04} , failure rate of dangerous fault (for CRC32 code) amounts [2]:

$$\lambda_{NT} = \lambda_N \cdot 2^{-32} = 10^{-4} \cdot (4 \cdot 10^9)^{-1} = 2,5 \cdot 10^{-14} \quad (2)$$

In analyzed model of B0 telegram generating of data integrity code do not make long delays, the biggest delays are contribute the data encryption procedures.

However, the best method of encryption is AES with 128-bit key encryption, which guarantees high protect. In systems working in open transmission systems significantly affect on limiting the number of supported devices the delays are result from procedures to encryption of data and redundancy in the length of telegrams with encrypted data. The number of devices depends on the time cycle of a telegram and it can be defined from equation of time single cycle of information exchange T_c . A method for shortening of time information exchange in system can be pre-grouping of data for a large number of working devices, before coding process, integrity codes and encryption. For the analyzed variant of the transmission system OTS, the number of devices supported by the system allows to save determinism of time in the exchange of information.

The second application of OTS is experimental system of railway management and area control [13] with structure presented on Fig.4. the following subsystems may be distinguish:

- Cross Level Protection System (CLP),
- Station Control System (CC),
- Rail Section Occupancy Control System (RSOC).

The transmission uses 433.725 MHz channel (with 25 kHz separated distance) with 19200 bit/s transfer rate. The THR analysis assumes the serial reliability structure with single transmission channel with B0 type of telegrams, 128 bit key in AES coding algorithm and 32 bit CRC. The applied transmission equipment has certified MTBF about 525600 h ($\lambda_N = 0.18 \cdot 10^{-5}$). It is mean, that in worst case the THR depends on CRC32 protection corresponds to SIL4 requirements.

Fig. 4 The experimental structure of Railway Control System with OTS

The open transmission applications in railway control and management systems

The very good example of introduction of open transmission standard instead existing cable connection is innovative system of cross level protection (fig. 5) [15]. The applied B0 type transmission with duplex structure of radio-connection ("2 from 2") satisfies SIL4 requirements.

Assuming value of failure rate and time t_d [15] and open transmission characteristics the estimated THR value equals to $5.56 \cdot 10^{-12}$ (this THR value is similar to existing cable realization of cross level protection systems).

Fig. 5 Example structure of cross level protection system with OTS

4. The future of open transmission in railway control according to CBD

The changeable block distance system

The Absolute Changeable Block Distance System (CBD)_A conception assumes the time spacing control used dynamic block section between trains. The length of block section may change in time according to the current traffic situation in the controlled section of railway line. This means that the distance between trains is changeable and its actual length is the result of processing information about position and speed of all following supervised trains in the given railway line [7], [8]. The rule of the Absolute Changeable Block Distance (CBD)_A presented in the Fig. 6 and Fig. 7 bases on the virtual block section with not fixed reference

points (connected with distance between station) but flexible modified corresponding to given traffic situation. This method may be compared with “electronic visibility” when the actual speed depends on position and speed of a previous train.

It is the Absolute Changeable Block Distance $(CDB)_A$ when the second train receives the permission of drive (ZNJ) to the place nearer than calculated on last report about position (LR – location report) of a previous train. (It is connected with assumption about “zero distance” stop immediately after sending the location report (R_oP_1) and total breaking way with overlap of second train.)

The distance control process is shown at the Fig. 7. According to CBD_A rule the “train 2” receives movement authority (ZNJ_2) about precise position with respect to calculated localisation of “train 1”. If the case of calculated distance between train 2 and 1 is shorter “train 2” (KP_1) receives from Radio Block Centre new permission (ZNJ). ZNJ (movement authority) includes a collection of information on the validity of the permission, location of the end of movement authority, target speed at the end of authority, temporary speed restriction and static speed profiles. Finally when the driver outrun MA parameters train system automatically start – “service brake – emergency brake”.

Fig. 6 The open transmission application in Train Management and Control System including the (absolute) Changeable Block Distance Infrastructure

Fig. 7 The rule of Absolute Changeable Block Distance

Delay in open transmission systems in CBD railway application

The proper position of train depends on speed train, because the loss of GPS signal may be connected with distance. In the GPS space segment there are atom clocks. Depending on level of precision, in the PPS (Precise Positioning Service) time is assumed as $\sim 100\text{ns}$ but on SPS level (Standard Positioning Service) as $\sim 300\text{ns}$. Such high precision is necessary, because the slightest error can cause the measurement errors in the order 0,5 m.

When the system establishes connection again (finding satellites, synchronization, reading navigation dispatch), there appear considerable delays. In the situation of a lack of information essential to determine actual configuration of satellites, time of delay run into even a dozen or so minutes and is called Time to First Fix (TIFF). In GPS system the process of bit synchronization appears every 6s (sometimes there is a need to confirm and repeat it again). When the train drive in tunnel and communication interrupts, renewed connection can take 30s (it is time indispensable for finding a position and to correct time) [10]. For these reasons the delay in GPS system can be estimated:

$$T_{GPS} = T_s + \Delta T \quad (3)$$

where:

- TrS - time of synchronization / loss of transmission (6.0 – 30.0 s)
- ΔT - timemeasurement error (0.000001 – 0.000003 ms)

The GPS delay in train speed function is presented in Table 1.

Table 1. The train distance covered during a loss of transmission with the GPS system

Time	Speed of train			
	60km/h	100km/h	160km/h	250km/h
	16,66m/s	27,77m/s	44,44m/s	69,44m/s
6s	99,96 m	166,62 m	266,64 m	416,64 m
15s	249,9 m	416,55 m	666,6 m	1041,6 m
30s	499,8 m	833,1 m	1333,2 m	2083,2 m

Typical delay data telegram time ($T_{\text{DGSM-R}}$) in the GSM-R (GSM) standard is a sum of the individual partial times: [10], [11]

$$T_{\text{DGSM-R}} = T_S + T_R + T_{\text{FTY}} + T_{\text{DT}} + T_{\text{RC}} \quad (4)$$

where:

- TrS - conection establish time (2.0 - 10.0 s),
- TR - registration at network time delay (30-40s),
- TrFT - maximum time of wrong transmission (1 s),
- TDT - data transmission time delay (1s),
- TRC - recovery time - not interrupted (7s).

Delays in the CBD system

It is possible to estimate the queue length N and the average waiting time for service T_s [9]:

$$N = \frac{\lambda}{\mu - \lambda} = \frac{\frac{\lambda}{\mu}}{1 - \frac{\lambda}{\mu}}, T_s = N \frac{1}{\lambda} = \frac{1}{\mu - \lambda} = \frac{\frac{1}{\mu}}{1 - \frac{\lambda}{\mu}} \quad (5)$$

where:

- λ – intensity of packets sent per unit time ($1/\lambda$ – mean time between appearance of the packets),
- μ – the intensity of packet service ($1/\mu$ – average service time of packets).

Based on equation (4) the length of the queues and time of delay (waiting for/and service) may be estimated in Train Control System based on Changeable (absolute) Block Distance (CBD) [6].

According to the estimates in section 2, assumed that each train in a controlled area communicates with the center at least once per second, and the average service time of telegram (packet) is:

- 1s. (normal transmission –with t_{DT} of service),
- 15s (short loss of GPS signal, normal GSM-R transmission)
- 65s. (15s in GPS and 50 sec. in GSM-R as a worst case of transmission loss in both systems).

The values of important queues and delays are gathered in the Table 2.

Table 2. Values of N I T_s in CBD system

Number of trains per 100sec.		$\mu=1^{-1} \text{ s}^{-1}$		$\mu=15^{-1} \text{ s}^{-1}$		$\mu=65^{-1} \text{ s}^{-1}$	
	λ	N	Ts	N	Ts	N	Ts
2	0,02	0,02	1	0,42	0,21	Queue grows infinitely due to the inability of service ($\lambda > \mu$)	
5	0,05	0,052	1,05	3	60		
8	0,08	0,087	1,08				
12	0,12	0,13	1,13				
20	0,2	0,25	1,25				

5. Conclusions

The open transmission with public standards gives the new possibilities of optimal and functional railway control, protection and management with the same level of safety defined in EU standards (SIL). Such applications are ecological and low cost in the case of wide spread usage but require the special safety solutions on the transmission levels (protocols with cryptographic and integrity protection both in authorized access and data transfer).

The analysis of CBD system with open radio transition shows, that assuming typical delays related to transmission failures must be restricted with respect to number of transmitters and time of service in the dispatcher center. For CBD system the lost of transmission requires the switch to the classical fixed distance

control with insulated rail sections (for normal operation the number of train may be 20). Cause of delay in the GPS and GSM-R networks, the CBD system cannot be a main source of safety information of train localisation and must work together with existing speed and distance measurement train systems (odometer). The presented system may be treated as an additional radio transmission overlay into existing infrastructure (disability of it has no influence for fail safe operation of now exploited rail control systems).

6. References

- [1] Benoit Latre,P, De Mil, IngrMoerman,and others,: Maximum Throughput and Minimum Delay in IEEE 802.15.4. X. Jia, J. Wu, and Y. He (Eds.): MSN 2005, LNCS 3794, 2005.c_Springer-Verlag Berlin Heidelberg 2005
- [2] Lewiński A.: The open transmission public standards in railway control computer systems – state of art and future, The II East Europe Doctoral School, Krynica 2012
- [3] Lewiński, A., Perzyński, T., Toruń A.: The risk analysis as a basic designed methods of safety open network transmission applied in railway control systems. LogiTrans Conference, Szczyrk (2010), (in Polish)
- [4] Lewiński A., Perzyński T.: The reliability and safety of railway control systems based on new information technologies. Communications In Computer and Information Science 104. Springer 2010'. Transport Systems Telematics
- [5] Lewiński A., Toruń A., Bester L.: „Methods of implementation of the open transmission in railway control systems” (Sposobyrealizacjitransmisjiotwartej w systemachsterowaniaruchemkolejowym). Logistyka 3/2011
- [6] 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
- [7] A. Lewiński, T. Perzyński, A. Toruń: „The Analysis of Open Transmission Standards in Railway Control and Management”. Communications in Computer and Information Science 329), Springer-Verlag Berlin Heidelberg 2012),
- [8] Lewiński A., Toruń A.: „The Changeable Block Distance System Analysis”. Communications in Computer and Information Science (104), Springer-Verlag Berlin Heidelberg 2010
- [9] Tanenbaum A.S.: „Computer networks”, Prenice Hall PTR, New Jersey 1996.
- [10] Winter P. and other: Compendium on ERTMS. ISBN 978-3-7771-0396-9, UIC, (1st edition 2009)

- [11] Quality of Service Test Specification* form 11.09.2003 and parameters: GSM-R Interfaces Class 1 Requirements. SUBSET-093, 11.10.2005
- [12] Railway applications - Communication, signaling and processing systems. Safety-related electronic systems for signaling. International standard PN-EN 50129-2010
- [13] Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems. International standard PN-EN 50159 – 2010.
- [14] BOMBARDIER ZWUS Transportation S.A. Technical Documentation
- [15] KOMBUD S.A. Technical Documentation

Prof. PhD. Eng. Andrzej Lewiński. Graduate Warsaw University of Technology, Faculty of Electronics. Head of the Electronics & Diagnostics Department in Faculty of Transport and Electrical Engineering, Kazimierz Pulaski University of Technology and Humanities in Radom. Author's scientific interests are connected with designing and modeling of safety computer systems for railway applications, especially with reliability and correct software for such systems.

Prof. PhD. Eng. Zbigniew Łukasik. Graduate Saint Petersburg State Electrotechnical University. Rector of Kazimierz Pulaski University of Technology and Humanities in Radom. Head of the Process Automation Department (Institute of Automatics and Telematics, UTH Rad.) in Faculty of Transport and Electrical Engineering. Authors scientific interests are connected with: process automation, information technology, signal processing, industrial control systems, robotics, control and management systems in transport.

M.Sc. Eng. Andrzej Toruń. Graduate Warsaw University of Technology, Faculty of Transport. Manager of Railway Traffic Control and Telecom Division in Railway Institute in Warsaw. Authors scientific interests are connected with modeling of safety computer systems for railway applications.