Archives of
Transport System
Telematics

Volume 6

Issue 3

September 2013

Safety transmission in railway application – cryptographic approach

A. LEWIŃSKI[a], **Z. ŁUKASIK**[a], **L. BESTER**[a]

[a] UNIVERSITY OF TECHNOLOGY AND HUMANITIES IN RADOM, Faculty of Transport and Electrical Engineering, Malczewskiego 29, 26-600 Radom, Poland

EMAIL: a.lewinski@uthrad.pl

ABSTRACT

The paper deals with assumptions for an open transmission in railway control applications ensuring the SIL4 safety integrity level. Using the public transmission standards, especially the wireless transmission (including radio access to Internet) requires the appropriate protection to ensure the data integrity (protection against fault and lost of transmission) and encoding (protection against unauthorized access). The estimated this way the THR values, even for single transmission channel does not differ for fault level of computer hardware in redundant structures. The theoretical results are compared with experimental tests of polish railway automation systems.

KEYWORDS: safety transmission, railway control computer systems, standard

1. Introduction

The transmission system of information used for control of rail automation devices must ensure a high level of data safety, this one safety level is detail defined in the rail standard PN-EN 50159-2011. The main criterion to admit of transmission standards for railway applications is to ensure an acceptable level of risk THR (*Tolerable Hazard Rate*) in accordance with the requirements of the standard PN- EN 50 126 and PN-EN 50 129. The THR ratio in railway signaling systems (RSS) should be occurring in accordance with the classification of SIL levels (*Safety Integrity Level*). Wireless communication between the individual components of the RSS systems must be prepared in such way, as to allow the fastest possible detection of false information while the break in the transmission link must cause transition of the system to "safe state", of course, in accordance with the procedure specified individually for corresponding of rail traffic control system. Safety transmission should ensure the protection of information against the corruption or loss, using appropriate protective techniques. In order to ensure the confidentiality, integrity and authentication mechanisms are used in cryptography algorithms such as 3DES (*Triple Data Encryption Standard*), AES (*Advanced Encryption Standard*) and the use of cyclic redundancy code CRC (*Cyclic Redundancy Check*). The paper presents requirements concerns the method of protect transmitted data, the criteria of ensure for an acceptable level of risk (THR) according to a given safety level of SIL and examples of implementation of wireless data transmission in selected rail traffic control systems [3].

2. Standards and protocols applied to safety transmission in railway systems

2.1 Conditions of safe data transmission

Exchange of information in railway signalling systems (RSS) 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 PN-EN

50159:2011 [13] regulating such uses in the signalling systems. In transmission systems, 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 signaling 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 transmission system based on the network with public access must protect transmitted data against such risks.

2.2 Types of telegrams

Basic methods of protecting the transmitted information in public transmission systems in RSS 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 safety inviolabilities SIL by appropriate RSS system. 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, and 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].

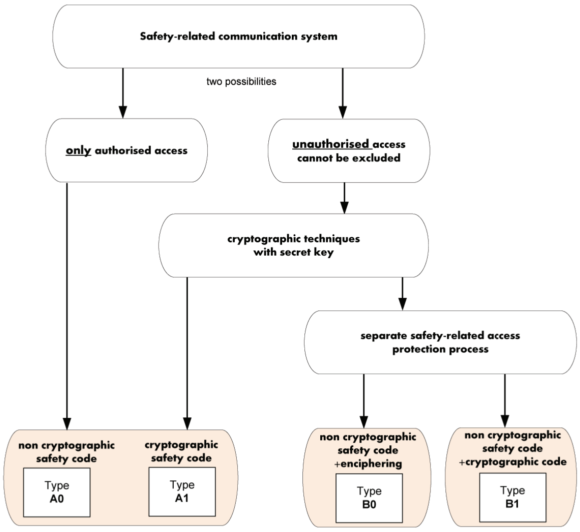
Safety-related communication system
two possibilities
only authorised access
unauthorised access cannot be excluded
cryptographic techniques with secret key
separate safety-related access protection process
non cryptographic safety code
Type A0
cryptographic safety code
Type A1
non cryptographic safety code +enciphering
Type B0
non cryptographic safety code +cryptographic code
Type B1

Fig. 1. Classification of types of telegrams to the open transmission systems according to PN-EN 50159:2011 standard [13]

2.3 Methods of protecting the telegrams

The detailed structure of telegrams for the safe transmission with recommended safe protection mechanisms of data is shown on Figure 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 RSS). The Type of A0/A1 it has been used in so-called closed transmission systems so far, implemented mostly in Profibus and Ethernet standards. Basically type B0 is proposed by most manufacturers of RSS systems with public 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.

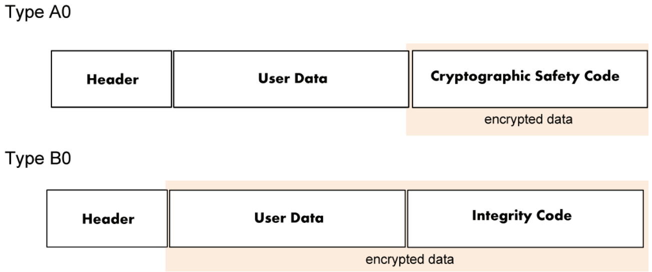

Fig. 2. The structure of information in safe transmission systems according to norm PN-EN 50159:2011 [13]

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 railway control systems is recommended to use cyclic redundancy code CRC used to detect random errors. In open (public) transmission systems we have to deal with 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. 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 (A*dvanced Encryption Standard*) with 128-bit keys that allow to reject erroneous telegrams and protect against the decoding. Data are encrypted in its entirety, including integrity code, such selection of protecting of telegrams is mainly ensue from use of wireless data transmission [1, 4, 5, 7].

3. Safety transmission in railway signaling systems

The transmission is a part of safety railway systems and must satisfy the obligatory recommendations of EU standards, especially the PN-EN 50159:2011 [13].

3.1 Closed safety transmission in existing railway signaling systems

The transmission system with fixed number of participants linked by a transmission system with well-known and fixed properties is so-called a closed transmission. This kind of realization of transmission is ensure the fail-safe and high reliable of railway control processes. This transmission is the safety transmission and allows to safe flow of information between all sub-systems in railway traffic control and management systems. The safety transmission in this case is based on transfer of status telegrams, commands (and related acknowledgements). The closed transmission system assumes:

- Only authorized access is accessed.
- Known maximal number of data connection.
- The transmission medium (coaxial or coupled pair of copper cables, fiber optic) is known and fixed connected to data transmitting/receiving devices.

In such situation the probability of unauthorized access is significantly small, but in closed transmission network may operate both protected and unprotected transmission devices.

The very good example of safety and closed transmission application is interlocking system MOR-3 (KOMBUD S.A.) from Fig.3. This system may cooperate with master/dispatcher system MOR-1, or another system such EbiScreen (Bombardier Transportation ZWUS S.A. or ILTOR (Siemens)).

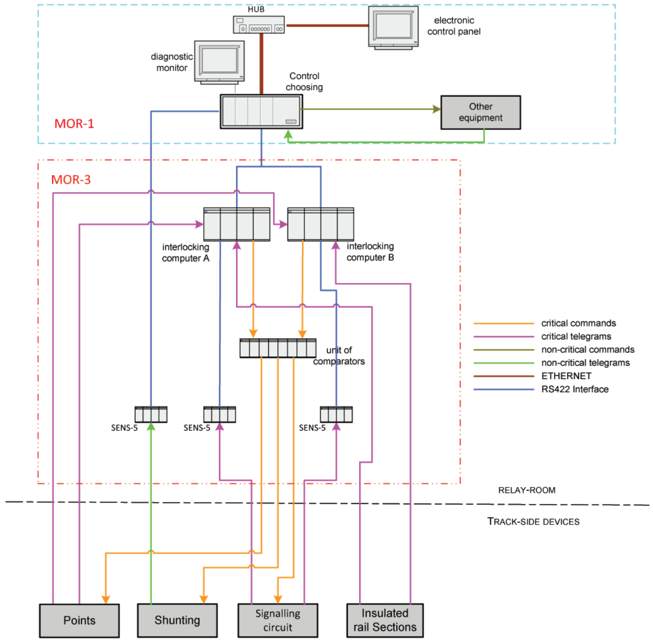

Fig. 3. The safety transmission in the interlocking system MOR-3 [6]

In the system the three following layers are distinguished:

- User Interface – electronic (computer desk) – devices of service and visualization layer designed towards better monitoring of railway control devices and traffic situation in the dispatcher area
- Interlocking System – system responsible for safety setting and releasing of routes together with monitoring of all controlled devices (communication of dispatcher desk with rail equipment via input/output devices from User Interface
- Rail devices and systems – point drives, rail circuits, signaling equipment, etc.

In typical railway practice of control systems, the MOR-3 system may be treated as system of station devices composed from control computers (in duplicated "2 from 2" structure) and safe output circuits – fail-safe comparators. All messages are transmitted using RS-422 serial connections or industrial Ethernet standards. The command telegrams transmitted from interlocking control computer (duplicated microcontroller channels). In the system the following types of telegrams may be assumed, such commands to point, semaphore (including maneuver signaling), insulated rail section, universal object controller and control area controller.

3.2 Example of wireless data transmission in railway control applications

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 signalling systems.

One such example of the implementation of wireless transmission in railway applications is system of railway management and area control ESTER [4], which can be distinguished on the following subsystems:

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

The basic structure of this system is presented on Fig.4.

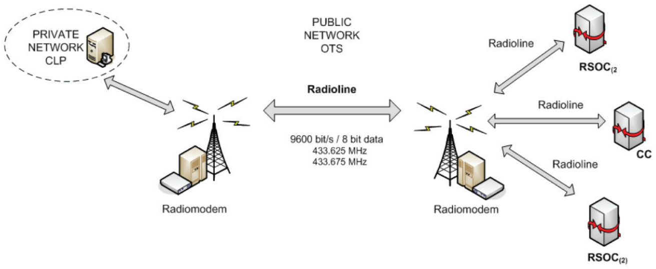

Fig. 4. The experimental structure o Railway Signalling System with OTS (*Open Transmission Standard*) [7]

4. Measures and safety criteria

4.1 Measure of the error probability and THR coefficient

The base of safety systems analysis in railway control applications is Tolerable Hazard Rate (THR) - measure defined with respect to failure rate *(λi)* in channel *"i"* and connected time of system reaction (t_d) after failure in this channel [3, 9 - 11].The idea of safety computer systems 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.

For system assigned to SIL4 level, the THR *(failure intensity per hour)* is defined as follows: $10^{-9} \le \mathrm{THR} < 10^{-8}$**.** The transmission critical failure together with hardware modules must satisfy the above condition. Assuming that the level of reliability for both of transmission closed and open characterized by intensity of failure λ_N is on level of 10^{-4}, it is possible to estimate the intensity of the dangerous failure λ_{NT} [13]:

$$\lambda_{NT} = \lambda_N \cdot 2^{-c} \tag{1}$$

where: c – number of redundancy bits in integrity protection CRC code

For basic protection of transmission a CRC 32 applied in presented MOR systems, the failure rate $\lambda_N = 10^{-4}$ gives the critical failure rate $\lambda_{NT} = 2{,}39 \cdot 10^{-14}$.

For open transmission system the 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 (*Mean Time Between Failures*) 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.

In order to estimate the probability of undetected bit error in the telegram P_F, this probability is given by [1 - 2]:

$$P_F = \sum_{i=D}^{N} \frac{N!}{i! \cdot (N-i)!} \cdot p^i \cdot (1-p)^{N-i} \tag{2}$$

where: P- probability of undetected i- number of errors, N- codeword length, p-bit error probability (for radio transmissions the accepted value is 10-4), i- number of errors in n codeword length

The probability of undetected telegrams corresponding to parameters *N, p* and *i*, for presented ESTER system are shown in Table 1.

Table 1. **Probability of undetected P_F, *i*- number of errors in n codeword length**

telegram length *N*=160 bit			
BER	***i*=1**	***i*=2**	***i*=3**
10^{-3}	$1.3 \cdot 10^{-1}$	$1.1 \cdot 10^{-2}$	$5.7 \cdot 10^{-4}$
10^{-4}	$1.5 \cdot 10^{-2}$	$1.2 \cdot 10^{-4}$	$6.5 \cdot 10^{-7}$
10^{-5}	$1.5 \cdot 10^{-3}$	$1.2 \cdot 10^{-6}$	$6.6 \cdot 10^{-10}$
10^{-6}	$1.5 \cdot 10^{-4}$	$1.2 \cdot 10^{-8}$	$6.6 \cdot 10^{-13}$

For estimation the probability of error in telegram regarding to the Hamming distance P_H, the following values were estimated [1 - 2]:

$$P_H = p^d \cdot (1-p)^{N-d} \tag{3}$$

where: d - Hamming distance, N - codeword length, p - bit error probability (for radio transmissions the accepted value is 10-4),

In this case obtained results are shown in Table 2.

Table 2. **Probability of undetected P_H, *i*- number of errors in n codeword length and *d*-Hamming distance**

telegram length N=160 bit							
BER	**d=1**	**d=2**	**d=3**	**d=4**	**d=5**	**d=6**	**d=7**
10^{-3}	$8.5 \cdot 10^{-4}$	$8.5 \cdot 10^{-7}$	$8.5 \cdot 10^{-8}$	$8.5 \cdot 10^{-13}$	$8.5 \cdot 10^{-16}$	$8.5 \cdot 10^{-19}$	$8.5 \cdot 10^{-22}$
10^{-4}	$9.8 \cdot 10^{-5}$	$9.8 \cdot 10^{-9}$	$9.8 \cdot 10^{-13}$	$9.8 \cdot 10^{-17}$	$9.8 \cdot 10^{-21}$	$9.8 \cdot 10^{-25}$	$9.8 \cdot 10^{-29}$
10^{-5}	$9.9 \cdot 10^{-6}$	$9.9 \cdot 10^{-11}$	$9.9 \cdot 10^{-16}$	$9.9 \cdot 10^{-21}$	$9.9 \cdot 10^{-26}$	$9.9 \cdot 10^{-31}$	$9.9 \cdot 10^{-36}$
10^{-6}	$9.9 \cdot 10^{-7}$	$9.9 \cdot 10^{-13}$	$9.9 \cdot 10^{-19}$	$9.9 \cdot 10^{-25}$	$9.9 \cdot 10^{-31}$	$9.9 \cdot 10^{-37}$	$9.9 \cdot 10^{-43}$

Table 1 shows the trend of changes with respect to error probability at 1, 2 or 3 bits in the telegram (code word). While Table 2 shows the changes in the probability of error in the telegram, depending on the Hamming distance d. From presented results it obvious that requirements recommended for SIL4 corresponding to standard [13] must assure the minimum Hamming distance d = 4.

For other protections should be included methods such as coding of important (sensitive) information's in the area of the telegram, i.e.: the marker type of telegram, the marker type of command (order) were selected special collections of code so that the Hamming distance for a given set of codes was maximal.

In addition to coding also introduced the security, to increase the level of transmission safety:

- diversity of headers of telegrams for channels A and B and the different locations of the telegram
- diversity in length and content of the particular telegrams with excess information,
- the time criterion, causing the lack of a important telegram within about 1 s is interpreted as a interruption in transmission what causes transition of the system to a safe state,
- damage to the transmission cables, transmissions card and power card, causing an interruption in the transmission and safe system response.

An important protection is the so-called "Telegram life". The choosing controller should at every about 10 s to the dependency controller a telegram life. No "telegram life" for more than 10 seconds makes practical the system is transition in a standby, and after another 10 seconds will set the all of semaphores and shunting plates to signal stop [4, 6 - 9].

The dual transmission channels in closed transmission system satisfy the THR requirements (including repetitions of telegrams). But the single transmission channel in B0 with appropriate encryption may be also applied to SIL4 THR requirements.

5. Conclusion

In the railway signaling systems the transmission is treated as an important part of safety system according to PN-EN 50159:2011 standard, especially THR value assigned to SIL4. In the systems with closed transmission, the transmission channels are redundant (duplicated) and applied CRC integrity code for data protection give the critical failure λ_N rather small, significant less than recommended THR value. In the systems with open transmission standard only single transmission is applied, but the result λ_N value satisfies the SIL4 requirements according to additional cryptographic protection. (Another problem may be connected with availability, because only authorized access may guarantee the transmission without delays.)

The future research works are connected with Internet access to data transmission in railway control applications, but for safety radio transmission the important problem with fast access, small delays and authorization corresponding to PN-EN 50159:2011 standard must be successfully explained.

Bibliography

[1] BESTER. L.: „The Analysis of Integrated Safety System in Land Transport According to Unguarded Cross Level Systems", Ph.D dissertation Technical University of Radom, October 2012

[2] GOLDSMITH A.: "Wireless Communications", Cambridge University Press, New York, USA 2005

[3] JAŹWIŃSKI J., WAŻYŃSKA−FIOK K.: „Safety and Reliability of Railway Control System" (Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym), WKiŁ Warsaw 1982

[4] KOMBUD S.A. Technical Documentation

[5] LEWIŃSKI A, BESTER L.: „Additional Warning System for Cross Level". In J. Mikulski (Ed.): TST 2010, CCIS vol. 104, pp. 226–231, Springer, Heidelberg (2010)

[6] LEWIŃSKI A., PERZYŃSKI T.: The Reliability and Safety of Railway Control Systems Based on new Information Technologies. In J. Mikulski (Ed.): TST 2010, CCIS vol. 104, pp. 427–433, Springer, Heidelberg (2010)

[7] LEWIŃSKI A., TORUŃ A., BESTER L.: „Methods of Implementation of the Open Transmission in Railway Control Systems" (Sposoby realizacji transmisji otwartej w systemach sterowania ruchem kolejowym). Logistyka 3/2011

[8] LEWIŃSKI A., TORUŃ A.: „The Changeable Block Distance System Analysis". In J. Mikulski (Ed.): TST 2010, CCIS vol. 104, pp. 67–74, Springer, Heidelberg (2010)

[9] 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*)

[10] Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defense (1991)

[11] PERZYŃSKI, T.: The Problems of Safety of Computer Nets Applied in the Railway Control. PhD dissertation – Technical University of Radom, Faculty of Electric Engineering and Transport, Radom (2009), (*in Polish*)

[12] Standard PN-EN 50129:2003 Railway applications – Communication, signalling and procecssig systems – Safety-related electronic systems for signalling

[13] Standard PN-EN 50159:2011. Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems