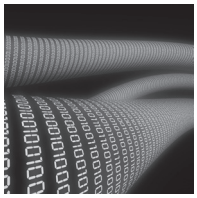


Archives of
Transport System
Telematics

Volume 4

Issue 4

November 2011

The safety analysis in the open transmission standards in railway applications

A. LEWIŃSKI[a], A. TORUŃ[b], L. BESTER[a]

[a] Kazimierz Pułaski Technical University of Radom, Faculty of Transport and Electrical Engineering, 29 Malczewskiego Street, 26-600 Radom Poland,

[b] Railway Institute; Signalling and Telecommunication Laboratory; 50, J. Chłopicki Street 04-275 Warsaw Poland,

EMAIL: a.lewinski@pr.radom.pl

ABSTRACT

The paper deals with functional and safety analysis of transmission in railway control systems, especially fail-safe applications (Line Block System, Dispatcher/Interlocking, Cross Level Protection and monitoring remote control). An analysis of the data structure is presented with recommended protection mechanisms to determine the indexes of time used for safety proof. 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). These methods correspond to the existing standards (EN-PN 50159-2, EN PN 50 129, EN PN 50126) and are recommended for safety transmission analysis in new railway control systems with public wireless transmission.

KEYWORDS: open transmission, wireless standards, BS EN PN 50159-2010

1. Conditions of safe data transmission

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

- Intentional or unintentional masquerade of another system in the railway control system (RCS),
- Attacks in order to access the transmitted information or send processed packets to the system,
- Removing, modifying or redirecting the data telegrams,
- Changing the order or repeating telegrams,
- Delay of telegrams.

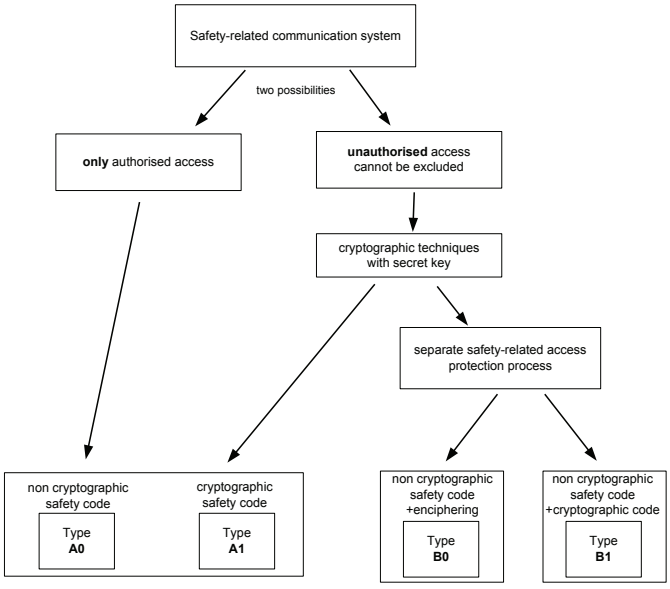


Fig.1. Classification of types of telegrams to the open transmission systems OTS according to EN 50159:2010 standard.

Therefore, the protection of transmitted data against such risks is the condition to access an OTS based system.

1.1. 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 cryptographic methods. Meeting these requirements is necessary in order to achieve the assumed level by an RCS system, the safety inviolabilities SIL.

- A0 – authorized access only, the integrity code of data is required, the cryptographic safety code is not required.
- A1 – unauthorized access is not excluded, the use of cryptographic safety code is required.
- B0 – unauthorized access is not excluded, encryption is required, the use of cryptographic safety code is not required
- B1 – unauthorized access is not excluded, the cryptographic code is required, the cryptographic safety code is not required [5].

1.2. Methods of protecting the telegrams

The detailed structure of telegrams for the safe transmission with recommended safe protection mechanisms of data is shown in Figure 2. In the paper it was confined to two telegram types – A0/A1 and B0.

Type A0/A1 has been used in closed transmission systems so far, implemented mostly in Profibus and Ethernet standards. Type B0 is basically proposed by most manufacturers of RCS systems with an open transmission channel, and it concerns both dedicated radio links and wireless Internet. In the case of a closed transmission with protocols of A0 and A1 type 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

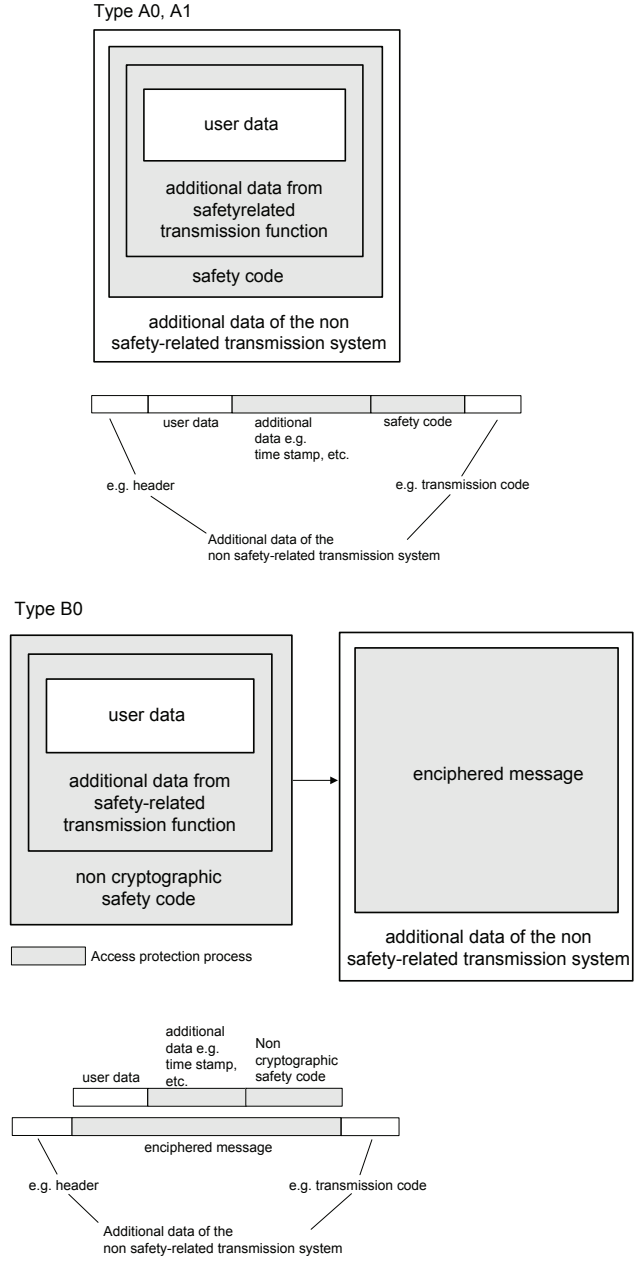
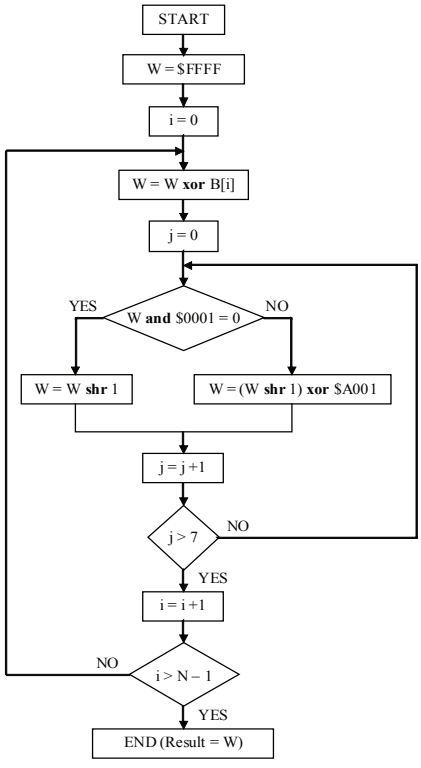


Fig.2. The structure of information in safe transmission systems according to EN 50159:2010 standard

has the character of physically closed, which excludes the threat of unauthorized access to the data, overhearing of transmission or inserting the extraneous telegrams.

The cyclic redundancy code CRC used to detect random errors is recommended to use as the data protecting code in those systems. Open transmission systems insert an additional threat to the system such as, for example, masquerade another system into a system of railway control or intentional modification of sending telegrams. To avoid this, it is necessary to use methods protecting against unauthorized access and which allow verification of data authenticity. In this field the standard recommends the use of cryptographic techniques, encryption methods and authentication keys. Telegrams using these techniques are identified as type B0, in which procedures of authorization using hash MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm) are recommended. For verification of the data integrity, the redundant coding technique CRC (Cyclic Redundancy Check) can be used, which protects against random errors and allows detecting single or series of errors. However, the encryption of data using the block ciphers encryption with 128-bit symmetric key such as DES, 3DES (Data Encryption Standard) or AES (Advanced Encryption Standard) that allow to reject erroneous telegrams and protect against the decoding.



B[i] – the next byte of data fields in the amount of N

Fig.3. Example of CRC32 encoding algorithm.

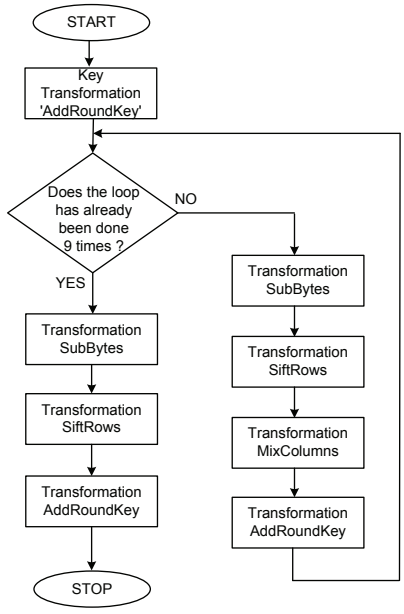


Fig.4. Encryption algorithm AES-128.

2. Time analysis of information flow

In order to determine the time and probabilistic indicators of data transmission in OTS systems, the analysis of execution time for individual functions to determine the integrity code, the encryption and decryption of data depending on the length of the telegram was conducted (assuming that a typical length of telegrams in the system is 16 Bytes) and for two bandwidths of 512 kb/s and 1Mbit /s. Most producers of RCS system assume type B0 of telegram, which uses cryptographic techniques with the secret key. The data is encrypted in its entirety including the integrity code. Such selection of telegrams protection results mainly from the use of wireless data transmission. During the encryption, the ensured confidentiality and integrity of the data affect the number of operations executed by individual algorithms (Fig. 3 and 4). In the AES encryption with a 128-bit key, the algorithm executes 10 rounds in order to transform each byte. This algorithm operates on blocks of data, which are 128 bits (16 bytes) long; therefore there is no need to collect more data, because each such block can be processed independently. However, for code CRC-32 the algorithm executes eight operations and protective properties of the CRC code depend on the size of the protected data block and the degree and form of the polynomial.

Figure 5 shows a comparison of two basic algorithms used in standard B0: CRC-32 and AES algorithms.

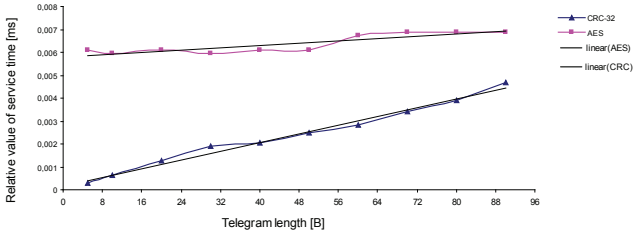


Fig.5. The value of the procedure relative time as a function of the length of telegrams

For selected models of telegrams A0/A1 and B0, the time of information protection has been analytically defined (see Table 1) for the typical lengths of telegrams in the railway control systems.

The time of information exchange can be represented as the sums of the delays, which are mainly based on partial encryption / decryption and encryption and decryption of transmitted data:

$$T_C = T_K + T_T + T_D \quad (1)$$

where:
T_C – the time of a single cycle of information exchange
T_K – the time of data encryption
T_T – the time of data packet transmission
T_D – the time of data decryption

Examples of results of the time of a single cycle of information exchange Tc (telegram length 6 [B]) and the rate of transmission 512kb/s and 1Mb/s for each telegrams protecting feature are as follows:

Table 1. Average time of telegram protection

Type of telegram / Length of telegram	A0, A1 CRC-32	B0, CRC-32(DANE)+AES
10 [B]	0.0812 [ms]	0.146 [ms]
20 [B]	0.305 [ms]	0.166[ms]

Table 2. The time of a single cycle of information exchange Tc

Capacity of link	512kb/s	1Mb/s
Functions protecting the telegrams	The time of a single cycle of information exchange Tc	
AES	0.103 [ms]	0.059 [ms]
CRC-32	0.092 [ms]	0.048 [ms]

In the analyzed model of B0 telegram, the generating of data integrity code does not make long delays; the biggest delays originate from the data encryption procedures. However, the best method of encryption is the AES with 128-bit key encryption, which guarantees a high protection. Systems working in an open transmission system significantly limit the number of supported devices; the delays result from data encryption procedures and from 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 the equation of time of a single cycle of information exchange Tc. A method for shortening the information exchange time in the system can be the pre-grouping of data for a large number of working devices, before coding process, integrity codes and encryption. For the analyzed variant of the OTS transmission system, the number of devices supported by the system allows to save determination of time in the exchange of information. Errors of the data telegram in the case of open transmission it rejection causes of telegram in its entirety and a temporary loss of transmission. The data is sent cyclically and the single error does not affect the system work. Assuming the probability of bit error for OTS transmission at the level of $p = 10^{-4}$ (for the radio network), the probability of undetected error, e.g. for CRC-32 code, can be estimated based on equation (2), which for the telegram length of 4 and 20 bytes is: $P(4)=9{,}6^{-34}$, $P(20)=3{,}2^{-33}$, respectively.

$$P_{np} = N_b * p * 2^{-32} \quad (2)$$

where:
P_{np} – the probability of undetected error
N_b – the number of bits of information
p – the probability of bit error for radio network

3. Conclusion

Using the open transmission systems in RCS systems cannot reduce the assumed level of SIL and the safety requirements defined for this system (e.g., section block, railway signalling system). In this analysis it has been assumed that the time of executed procedures (i.e. the determination of code integrity, encryption) is the sum for those of individual devices of the system. The pre-grouping of telegrams (with limited size) for more devices before executing procedures related to coding, determination of integrity code and encryption is the method that can effectively improve the efficiency of information exchange. This analysis allowed for the evaluation of various methods of increasing the safety of data transmission in the used OTS railway control systems, including in particular

methods of ensuring the integrity and confidentiality of information. Based on the received results, the least time needed to execute the integrity code and CRC codes, these times are comparable. However, for the hash function the best algorithm was SHA-1. The fastest method of encryption is the AES and the most efficient is the DES cipher. The railway control systems are now computer systems with dispersed structure; in this case the reaction times of individual devices should be taken into consideration.

Bibliography

[1] Standard BS EN 50159:2010 "Railway applications – Communication, signalling and processing systems. Safety-related communication in transmission systems".
[2] JAŹWIŃSKI J., WAŻYŃSKA – FIOK K.: „Safety and reliability of railway control system" (Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym), WKiŁ Warsaw 1982
[3] SZOPA T.: „Reliability and safety" (Niezawodność i bezpieczeństwo). Publishing House Warsaw University of Technology. Warszawa 2009
[4] NOWAKOWSKI W. „The use of ASN.1 notation to the specification of information exchange protocols in the signaling systems" (Zastosowanie notacji ASN.1 do specyfikacji protokołów wymiany informacji w systemach sterowania ruchem kolejowym). Dissertation, Radom University of Technology 2009
[5] 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