Andrzej Lewiński
prof. dr hab. inż.
Uniwersytet Technologiczno-Humanistyczny im. K. Pułaskiego w Radomiu
a.lewinski@uthrad.pl

DOI: 10.35117/A_ENG_17_06_02

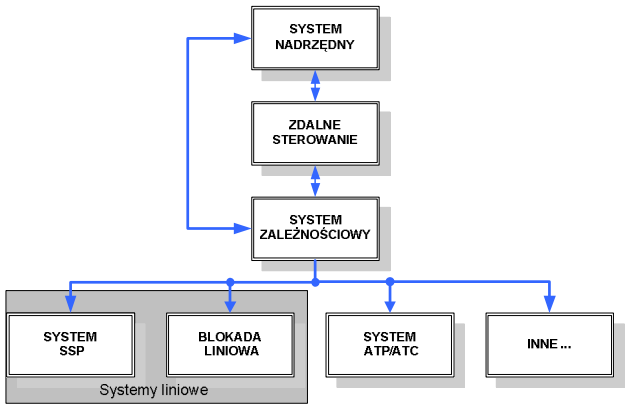
The threats of wire and wireless data transmission systems in rail traffic and management systems including cyber and terroristic attacs

Abstract: The paper deals with presentation of up to date state of protection in dissipated, computer railway control and management systems, including the future systems implemented in Polish State Railways based on wireless standards with regard the ETMS/ETCS solutions.

Keywords: Wired and wireless data transmission

Introduction

Control systems are mainly redundant (2 out of 2, 2 out of 3) computer controllers with very low intensity of damage with a fast, in the order of 0.001 - 0.1 sec, reaction to a detected single fault in the system, which ensures compliance with EU regulations, also in Polish railways, called Safety Integrity Level. A typical, currently operated railway traffic management and control system is a distributed computer system with the structure shown in Figure 1.

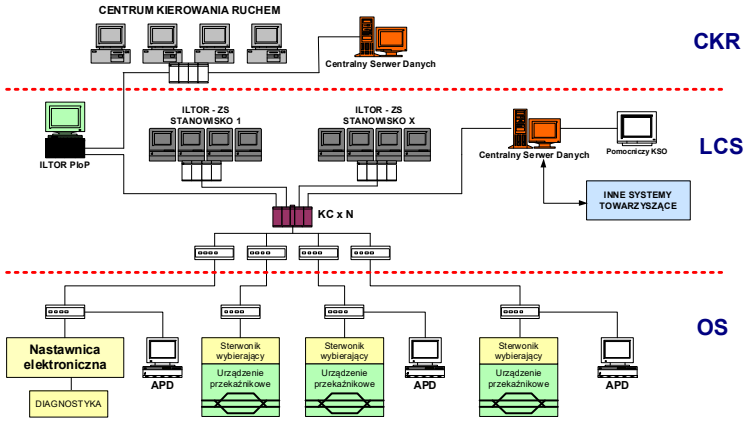


1. Typical structure of the railway traffic management and control system [6]

Between the subsystems, there is a transmission network exposed to interference but also to attacks of hackers and terrorists, which may interfere in the control process threatening security. A typical example of a traffic management and control system can be the ILTOR 2 [6]. The system [22] is widely used in the EU including Poland, where many terminals are installed, as well as servers and routers operating in the local network (ETHERNET). The structure of the system being a distributed computer control system whose subsystems and devices communicate through network standards is presented in Figure 2. The NSRK system includes

- superior systems,
- dependency systems,
- remote control systems,
- linear systems (ssp, line interlocks),
- ATP / ATC.

The computerized railway traffic management and control systems (ZSRK) have operated in the EU for over 40 years. These are distributed computer systems with hierarchical structure, i.e. dispatcher's superior system, dependency systems including stations and line interlocks, as well as local systems and object controllers assigned to switches and signalling devices as well as automatic crossing signalling systems, track vacancy control, etc. The basis of correct functioning is the effective transmitting the status of controlled objects and control commands.



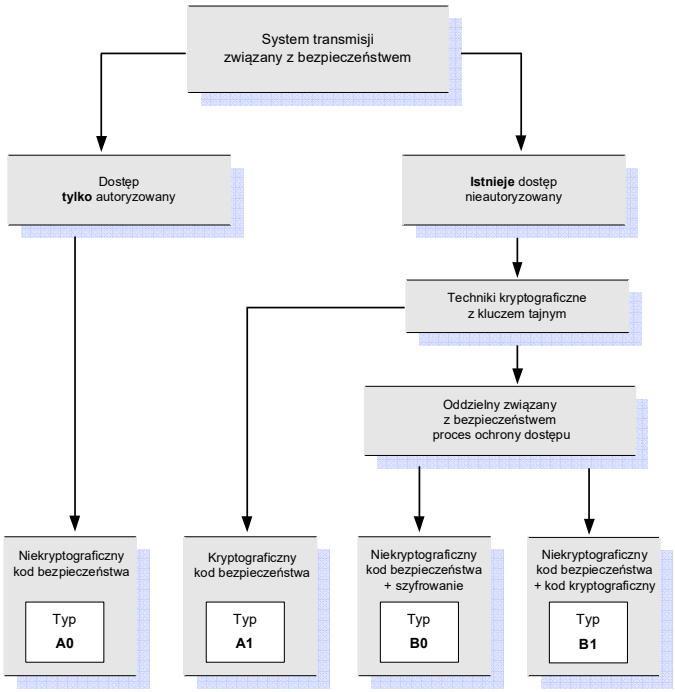
2. Contemporary traffic control centre - ILTOR-2 [22]

However, the problem of the robustness of data transmission systems between subsystems and elements on threats caused by attempts to take over and change the information sent has not been addressed so far. Railway traffic management and control systems must meet stringent standards regarding the organization of the system (EN-PN 50 126) [15], equipment configuration (EN-PN 50 129) [16], software (EN-PN 50 128) [14] and transmission (EN-PN 50 159) [17], but so far there is no research to assess the resistance of these systems to threats caused by attacks.

Security of transmission in supervision and control systems of railway traffic

Since 2005, when Poland accessed the EU structures, the transmission rules are regulated by the applicable standards (CENELEC). The basis was the EN 50159.1 standard, which regulated wired transmission in NSRK systems, but its application did not apply to systems already in operation where manufacturers could use their own solutions, not necessarily compliant with the requirements of the standard.

The standard PN-EN 50 159-2011 allows the use of wireless transmission standards provided that the same level of functionality and security is ensured as in existing implementations using cable transmission. This applies to both wired and wireless transmission standards. The basic criterion is to ensure an acceptable level of risk (THR) in accordance with the applicable standards PN-EN 50 126 and PN-EN 50 129 [8, 9, 10, 13]. This means that the THR [12] indicator for srk systems classified to a given SIL safety level should not exceed the maximum value provided for this level.



3. Classification of transmission protections for open transmission systems [17]

The transmission of information must be carried out in such a way that the detection of erroneous information is possible as soon as possible, and the interruption in the transmission link must cause the system to transition to a "safe state" in accordance with the procedure specified for the srk system in question. This state is defined for individual types of systems individually and, for example, "safe condition" in axle counting systems, means "busy section" status signalling, "safe state" signalling for traffic signals can mean switching on the train approach warning, and in signalling systems forcing the display on the semaphore of "signal prohibiting S1". Therefore, in order to ensure correct operation of the SRK system, appropriate measures should be taken to prevent distortion or loss of information resulting from disruptions or unconscious or intentional (unauthorized) service activities. In the case of secure transmission systems, the information must be secured by additional bits or encrypted. Other safeguards may be used as long as they provide the required level of security.

In open transmission systems, the transmission is carried out using a radio network, the Internet network or through shared connections with public access. This means that information is sent via a transmission system available to unauthorized users, so that the data sent may be vulnerable to attacks, such as removal or impersonation of senders for srk devices operating on the network.

An open but also closed transmission system is exposed to the following types of threats:

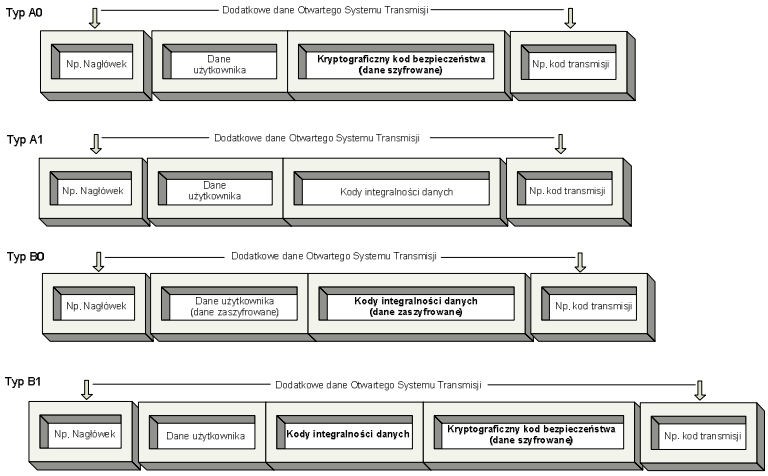
1. Masquerade
2. Insert,
3. Repetition
4. Removal,
5. Change of order,
6. Delay.

NSRK systems have also been used to secure the transmission of information against the following threats:

1. Masquerade, meaning intentional or unintentional "impersonation" of another system for the srk system. According to the standard, it is recommended to use cryptographic techniques through the use of encryption algorithms and authentication keys. In the

proposed concept, to preserve the required level of security, encrypted VPN tunnels with IPsec protocols, DES encryption algorithms (3D Encryption Standard), 3DES and AES (Advanced Encryption Standard) were used. However, the use of the Diffie-Hellman key agreement algorithm eliminates the possibility of intercepting packets through eavesdropping on the communication channel.

2. Insertion, i.e. attacks related to obtaining access to transmitted information or sending processed packages. The proposed solution uses tunnelling mode, using the IPsec protocol (Internet Protocol Security), which protects all packets sent between hosts. IPSec prevents any modification of packages, offers secure, strong cryptography and IP level authentication. The use of the Diffie-Hellman key agreement algorithm eliminates the possibility of intercepting packets through eavesdropping on the communication channel.
3. Repeat. To avoid the repetition of packets, the IPsec - ESP header in Encapsulating Security Payload, which provides authentication, originality and data integrity, was used. Additional protection against repetition of packets is ensured by attaching another number to each packet.
4. Removal. Protection against attacks of removal, modification, repetition or redirection of telegrams to other recipients is carried out by ISAKMP (Internet Security Association and Key Management Protocol) crypto mechanisms, min 3DES, SHA-1 or MD5, DH2 in accordance with the recommendations of the standards.
5. (and 6.) Change of order, delay. Changing the order and delay of telegrams has been solved by using IPsec (IPsec tunnel and ISAKMP packet format) as well as time control.



4. Information structure in secure transmission systems in accordance with with the PN-EN 50159-2 standard [17]

The solutions proposed in the concept also allow to eliminate other threats, such as: the phenomenon of a hidden or discovered station, the effect of interception, distortion of packet data, distortion of the CRC checksum of the telegram.

Taking the recommendations of the standards, the structure of the open transmission telegram was adopted in the concept of using an open network, model B0 (Figures 3 and 4). Thus, the required form of information and the appropriate process of its processing were ensured by applying methods of protection against the abovementioned transmission threats in the STO network.

According to the adopted classification of systems associated with secure transmission, a specific classification of transmission groups has been adopted below:

• A0 - only authorized access, no cryptographic security code is used,

• A1 - without excluding unauthorized access, it is recommended to use a cryptographic security code,

• B0 - without excluding unauthorized access, no cryptographic security code is used, encryption is required,

• B1 - without excluding unauthorized access, no cryptographic security code is used, cryptographic code is required.

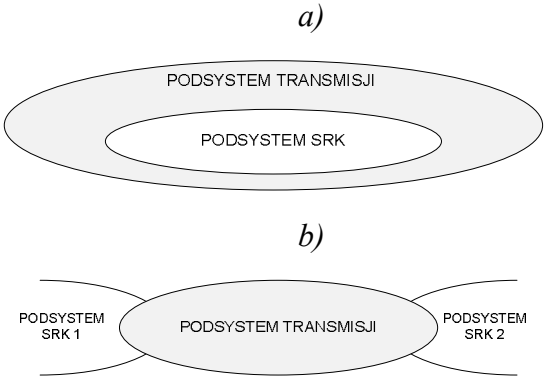
The form of information for each type of safe transmission is shown in the diagrams shown in Figure 4.

Currently, solutions are being developed by various companies producing SRK devices using open transmission, mainly based on wireless radio standards.

A properly conducted analysis regarding the assessment of the impact of the transmission system used on the parameters of reliability and safety of the SRK system requires an individual analysis related to a specific type of application. This means that every time the transmission system is used in srk devices, in accordance with the applicable standards, requirements and recommendations [2, 3, 14, 15, 16, 17, 18, 19, 20, 21, 23], the appropriate procedure must be followed, the stages of which are defined as follows:

1) application,
2) threat analysis,
3) risk reduction,
4) assigning the system to SIL security levels,
5) specification of safety requirements.

Each of the above-mentioned points requires separate justification and appropriate documentation. With regard to srk systems, particular attention should be paid to the risk level estimation (PN-EN 50126). The intensity of damages for the set SIL level is determined by the following standards: PN-EN 50126, PN-EN 50128, PN-EN 50129. For example, for traffic control systems responsible for safety, the value from the range $10^{-9} \leq THR < 10^{-8}$ for the level SIL 4.



5. a.) System structure with open transmission inscribed in a redundant system
b.) Serial structure of the single-channel open transmission system

Usually, the proposed transmission systems are single-channel systems, therefore, the tolerable THR level (Tolerable Hazard Rate) [12], is equal to the intensity of damage. For SIL4, it should be included within limits $10^{-9} \div 10^{-8}$ [h^{-1}]. In the case when it concerns two- or three-channel systems, the time of detecting the fault becomes significant, which allows for

higher intensity of faults in the transmission channels. Schematic dependence of the transmission subsystem and srk in the system with open transmission is shown in Figure 5.

In the case of using as a medium of wireless transmission, one should additionally take into account characteristic indicators concerning transmission, protection or coding. The length of the CRC security code (Cyclic Redundancy Code) becomes important in this case.

A typical security of data integrity is the cyclical redundancy code CRC-32 (Cyclic Redundancy Code) with the assumed Hamming distance. The probability of incorrect PF transmission is then [6], [7],

$$P_F = \sum_{i=D}^{N} \frac{N!}{i!*(N-i)!} * p^i * (1-p)^{N-i} \quad (1)$$

where :

D –Hamming distance,

N – the length of the codeword,

p – bit probability of error, the typical value is assumed 10^{-4} for radio transmissions [107]).

Tab.1. Probability of correct transmission in the bit error rate function BER [12]

Probability correct telegram transmission P_S	**BER - bit error rate (telegram 500B)**	**BER - bit error rate (telegram 1000B)**
1	0	0
0.9	0.00021	0.000105
0.8	0.00044	0.000221
0.7	0.00071	0.000356
0.6	0.00102	0.000510
0.5	0.00138	0.000692
0.4	0.00183	0.000915
0.3	0.00240	0.001203
0.2	0.00321	0.001608
0.1	0.00459	0.002299

For telegrams with the length of 500B and 1000B, the probability of incorrect transmission is respectively:

$$P_{F500} = 6.98x10^{-11}, P_{F1000} = 1.74x10^{-8} \quad (2)$$

and the probability of a correctly transmitted telegram:

$$P_S = (1 - BER)^N \quad (3)$$

where : N – the length of telegram,
BER - bit error rate (calculated from the formula),
The probability of correct transmission of telegrams 500 and 1000B is shown in Table I.

Examples of safe transmission in NSRK systems and resistance to threats

In the Polish railway system, distributed traffic control and control systems have been in use for many years, in which data transmission is an integral part. Security devices compliant with CENELEC standards requirements are the basis for the admission of these systems to operational use, for operational tests in the case of systems using wireless standards.

Distributed computer system with wired transmission

The basis for safe and reliable implementation of railway traffic control processes is to ensure a safe and correct flow of information between the systems involved in this process. In srk systems, transmission is associated with the transfer of control commands between devices, e.g. commands, driving permits, etc. and confirmations of their implementation, e.g. reports, location reports, etc.

Secure data transmission in both closed and open srk systems must meet the requirements and recommendations set out in the previously mentioned applicable standards. A system in which [6] is considered to be a closed system is:
- only authorized access is allowed,
- the maximum number of connection participants is known,
- the transmission medium, usually copper wire or optical fibre, is known and permanently connected to communicating devices.

In this case, the probability of unauthorized access can be considered as negligible, although both secured and unsecured equipment can work in the network.

A good example of a secure transmission system is the connection of elements of a centralized MOR-3 system (produced by KOMBUD SA [4], [5]) shown in Figure 6. This system can work with the MOR-1 master system or other such system, e.g. EBISCREEN produced by BOMBARDIER TRANSPORTATION ZWUA SA. The basic functional layers: user interface level (MOR-1), computer station equipment and performance circuits (MOR-3) were distinguished in the presented diagram.

The system includes the following functional layers:
- User interface, i.e. the electronic control panel. The operating and visualization layer devices are used to visualize the status of srk devices and the traffic situation in the supervised circle.
- Dependency system, i.e. a system responsible for the safety of setting and releasing waveforms, and control of the state of controlled devices. It communicates with track-side devices via the input and output unit and with the user interface layer (control panel).
- Track-side equipment and systems, i.e. switch drives, track circuits, signalling devices, etc.

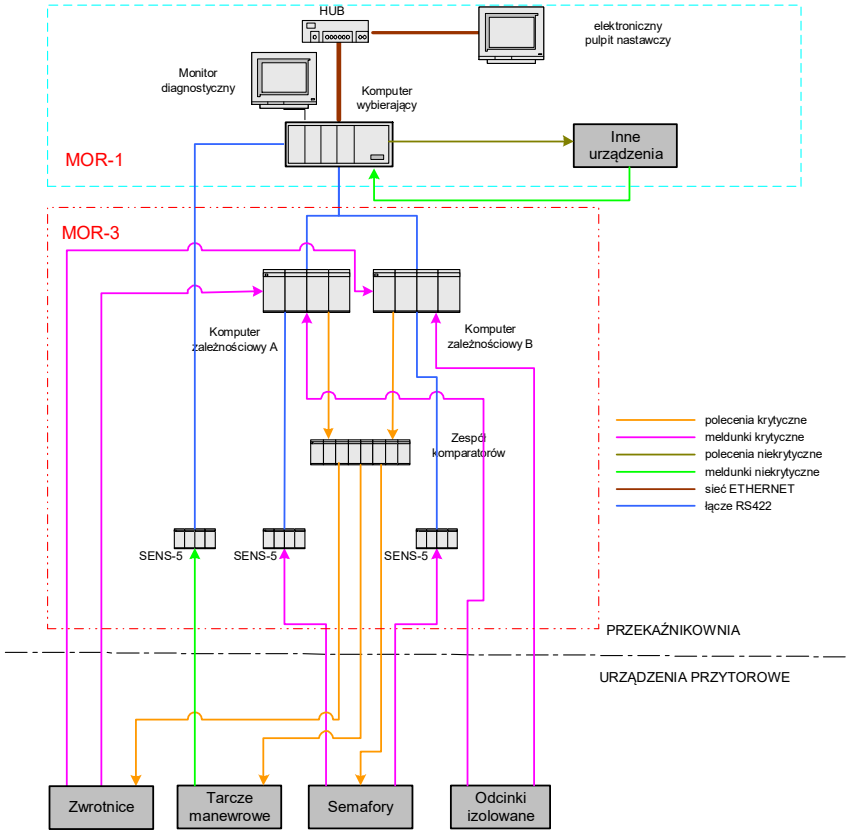
The basic functional layers have been distinguished on the presented diagram: user interface level (MOR-1), computer station equipment and executive circuits (MOR-3).

In practice, the MOR-3 system is understood as a station equipment system consisting of dependency computers and executive components with the use of safe comparators.

Information from the SENS measurement system is transferred to computers via RS422 serial links, and individual computers are connected via Ethernet. The Ethernet network is also used to connect computer station equipment with an electronic control panel.

The command telegram to the dependency controller is sent by the selection controller constituting the user interface element. The following groups of orders were distinguished:

- instructions to the crossover,
- semaphore orders,
- orders to the manoeuvring disc,
- orders to the insulated section,
- orders to the universal element,
- instructions to the element related to the control of the area.



6. Transmission system in the MOR-3 dependence system [4], [5]

The transmission system has a significant impact on the safe operation of the MOR-3 system. Disruptions in transmission, treated as defects at the hardware level (PN-EN 50120-1 standard), can potentially lead to system malfunctions or even to dangerous states. That is why in the MOR-3 transmission software a lot of procedures have been applied to prevent the emergence of a dangerous situation.

The basic security of transmission is the CRC data integrity code (Cyclic Redundancy Code). It is assumed that an additional excess of length of n bits causes a significant reduction in the intensity of damage λ_N to the level λ_{NT} in the way:

$$\lambda_{NT} = \lambda_N 2^n \qquad (4)$$

It means that for n=32 the intensity of dangerous distortions decreases 4 10^9 times.

The MOR -3 system uses:

- Cyclic CRC Redundant Code 32 bit, providing Hamming distance D = 4 for the coded area up to 4000 bytes in length, used to secure the entire telegram.
- Cyclic 8-bit redundant CRC code with polynomial generating Hamming distance D = 4, for coded area of several bytes. Used for additional coding of the telegram header.

Other safeguards include methods such as coding important and sensitive information in the body of the telegram, i.e. telegram type tag, command type flag; special sets of codes have been chosen so that the Hamming distance for a given set of codes is maximum.

In addition to coding, security measures have also been introduced to increase the level of transmission security:

- differentiation of the telegram headers for channels A and B and the different location of the telegram,
- diversity of the length and content of individual telegrams together with information overload,
- time criterion causing that the lack of a correct telegram in about 1 s is interpreted as a pause in transmission and causes the system to transition to a safe state,
- damage to transmission cables, transmission and power cards, causing a break in transmission and a safe system reaction.

An important safeguard is the so-called "Telegram of life". The selection controller should send a life telegram to the dependency controller every 5 seconds. The lack of a telegram of life for more than 10 seconds causes the system to go into emergency mode, and after another 10 seconds, all semaphores and manoeuvring discs are set to stand.

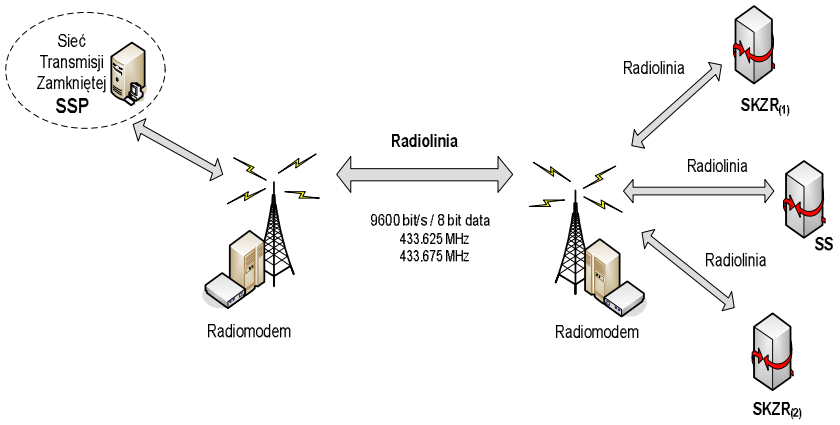
The system's authors estimated that the applied protections ensure that the probability of not detecting telegram distortion is less than $2.39 * 10^{-14}$, which is a much better indicator than the probability of damage to the computer in a single channel calculated for the entire system operation time.

Future system with open wireless transmission

In the concept of a safe transmission system proposed by the KOMBUD S.A. Radom [4] (Figure 7) uses a radio channel, i.e. open transmission system, to transmit information in the subsystem of impact devices occurring in the B and C category crossings with EST_KRG radio transmission controllers, being information from heads and commands for the Top, and the corresponding ones in the container with the EST_KR controller, being information sent in the local container network.

The subsystems marked on the drawing are: SKZR (occupancy control system), control system at the station (SS) and transitory signalling system (SSP). In this concept of a secure transmission system, an open radio channel was used to transmit information in the subsystem of interaction devices. The radio channel is used to transmit information between controllers cooperating with wheel sensors and ssp system controllers. Such configuration allows to eliminate the need to make cable connections from the impact points, i.e. sensors remote from the passage. In the current phase of experimental research, the radio connections are treated as backup channels, basic transmission uses existing cable, fibre optic and copper strands.

The open transmission system is based on a radio link providing access authorization control. Satellar Satellar radio mods from Satel were selected for communication purposes. The transmission takes place in the channel 433.725 MHz with the interval of neighbouring channel 25 kHz, with the speed in the radio channel up to 19200 bit/s. The transmission equipment used is characterized by high reliability MTBF about 522,500 h, which was confirmed by an appropriate certificate.



7. Structure of the rail traffic control system with radio transmission [4]

Assuming that the level of reliability for both closed and open transmission is characterized by the intensity of failures λ_N is the order of 10^{-4}, allows to estimate the intensity of dangerous failures assuming no detection of distortion in the CRC32 integrity code used at the same level as in closed systems with cable transmission (4), i.e. $10^{-4}*2^{-32} = 4*10^{-13}$, which gives the basis for passing the transmission subsystem to the SIL 4 level. However, it should be assumed that this is the minimum intensity of failures, and taking into account the disturbances, breaks and faults of the equipment and programmed protocols in practice can significantly increase this value.

In the ESTER system concept (ESTER-economical system for remote control and control of railway traffic), telegrams conforming to the B0 transmission type were adopted, using cryptographic techniques with a secret key and data encryption in full including the data integrity code. As the encryption algorithm, the AES standard with 128-bit key was adopted, to such encrypted data an additional data integrity code is attached, which allows to reject rejected telegrams and protects them from being decrypted. In contrast, to control the integrity of data, the CRC redundant coding technique was used to prevent accidental errors, allowing detection of single or serial errors.

Resilience of NSRK systems to hacker and terrorist threats

The mentioned PN-EN 50 159 standard took into account failures, damages and errors of transmissions caused by improper operation of systems and devices, but did not assume destructive human action. In recent times, there have been situations when intentional interference with the system involving the takeover of control on the railway line, or associated damage to the execution equipment can clearly lead to critical situations, a large disaster. Such situations were not anticipated 20 - 30 years ago, when the first computer systems with a distributed structure with cable transmission were implemented. On the other hand, open wireless transmission systems admitted to use, while focusing on controlled access authorization and integrity control of transmitted telegrams, do not take into account the possibility of specialized hacking attacks typical of the advanced Internet, e.g. massive attack of a huge number of server blocking telegrams.

In the case of currently operated systems with cable transmission, the following threats resulting from a terrorist act can be listed:

- Intentional damage to transmission cables with the possibility of interference in the control.

• Interference with controllers and other circuits, e.g. transmission and power cards that change the control program. This applies to unauthorized access to control cabinets and other external devices of the system.

• Unattended access to the dispatch centre, e.g. master system, local control centre, duty station. There is then both an attempt to change the software and related deliberate and catastrophic commands not controlled by the approved and currently used software controlling the correct work of dispatchers.

To effectively prevent the above threats, we should effectively control the integrity of transmission cables. In addition to the "telegrams of life", the state of sections, signalling devices and switchgears should be dynamically controlled in accordance with the control commanded by the dispatcher. It seems intentional to shorten the time of the "telegram of life" below 0.5 sec. Which will practically exclude mechanical interference. Breaks in transmission, e.g. less than 0.5 s, should initiate emergency procedures related to full system state control.

Other encoding of life telegrams is recommended, e.g. by providing cryptographic security, e.g. standard B0 mentioned in the standard.

All control cabinets and casings of external devices should have an alarm system informing the security services about an attempt to interfere. This is connected with the service authorization and appropriate control procedures along with the registration of access to such facilities in the dispatch centre. You can implement the mobile service authorization currently used in other similar secure systems only when servicing.

Proper security policy in dispatch centres, local control centres, traffic control stations and control rooms should be introduced. The A/V monitoring and full authorization of employees and their activities ought to be also work.

All IT services related to the service of computer controllers in all facilities should include appropriate security procedures only trusted and reliable companies, certified IT specialists, monitoring and registration of all activities, especially those related to the software.

Most of the threats listed and methods to counter them include future-oriented systems, wireless open standards. Any break in wireless transmission should generate the same procedures as cable break. The admission of a system with wireless transmission requires reference and counteracting all threats listed in Chapter 2.

Conclusions

In order to confirm safe wireless transmission, also open, in a similar way, it is necessary to analyse other systems currently and in the future used in Polish railway system, especially closed systems with full authorization of access:

-Existing "track - vehicle" communication systems (SHP, KHP, SOP)

-Future systems related to the ETRMS / ETCS standard using wireless transmission to/from the vehicle.

The work shows that proper protection against terrorist and hacker threats can be ensured by the appropriate security policy introduced, both in systems with cable installations as those with wireless systems also with open standards, where such interference is more likely.

In addition, a theoretical analysis can be carried out to assess the impact of threats on transmission security, taking into account the analytical models recommended for this purpose by the mentioned CENELEC and UIC standards such as Markov processes, verified by simulation methods (MATLAB / SIMULINK).

However, it seems necessary to conduct experimental tests with attempts to break into control computers and subject system statistical analysis of obtained experimental,

laboratory and exploitation results carried out on facilities made available by the Railway Institute in Warsaw and interested railway automation companies.

This type of research work will show quantitative and qualitative indicators of the resistance of traffic management and control systems in rail transport to loss of communication, distortion and the possibility of incorrect control. These indicators will be developed both by analytical methods, models of systems and their verification, as well as based on the results of laboratory and operational tests.

References

[1] Grant MNiSW pt:„Wpływ nowych technologii informacyjnych na poprawę funkcjonalności i bezpieczeństwa ruchu pociągów" nr 4T12C00529. Politechnika Radomska 2006.
[2] Instrukcja WTB-E10 – Wytyczne techniczne budowy urządzeń sterowania ruchem kolejowym w przedsiębiorstwie PKP stanowiące załącznik do zarządzenia nr 43 Zarządu PKP z dnia 09.09.1996r z późniejszymi zmianami.
[3] Instrukcja, konserwacji, przeglądów oraz napraw bieżących urządzeń sterowania ruchem kolejowym Ie-12 (E-24) PKP PLK S.A. Warszawa, 2005r.
[4] KOMBUD S.A. – materiały Zakładu Automatyki KOMBUD S.A. w Radomiu.
[5] KONTRON S.A. – materiały Kontron East Europe sp. z o.o.
[6] Lewiński A., „Nowoczesne systemy telematyki kolejowej", Wydawnictwo Politechniki Radomskiej, Radom, 2012, ISBN 978- 83- 7351-506-2.
[7] Lewiński A., Bester L.: „The Analysis of Transmission Parameters in Railway Cross Level Protection Systems with Additional Warning of Car Drivers", materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST 2012, 10-13.10.2012, Communications in Computer and Information Science 329), Springer-Verlag Berlin Heidelberg 2012.
[8] Lewiński A., Łukasik Z., Perzyński T., Ukleja P.: „The Future Generation of Railway Control Systems For Regional Lines Including New Telematic Solutions". Archives of Transport Systems Telematics, volume 7, issue 3, 2014. (s. 13-17). ISSN 1899-8208.
[9] Lewiński A., Łukasik Z., Toruń A.: „The application of public radio transmission standards in innovative railway automation systems". Journal of KONBiN 2(26) 2013, s. 123-136, ISSN 1895-8281.
[10] Lewiński A., Perzyński T., Toruń A.: "Risk Analysis as a Basic Method of Safety Transmission System Certification". Communications In Computer and Information Science no. 239. Springer 2011.
[11] Lewiński A., Perzyński T., Toruń A.: „The Analysis of Open Transmission Standards in Railway Control and Management", materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST 2012, 10-13.10.2012, Communications in Computer and Information Science 329), Springer-Verlag Berlin Heidelberg 2012.
[12] Lewiński A., Perzyński T.: „Akceptowalny poziom ryzyka jako kryterium bezpieczeństwa w transporcie kolejowym", prace konferencji Wydziału Transportu Politechniki Radomskiej Logi-Trans 2007.
[13] Lewiński A., Toruń A.: „The efficiency analysis of train monitoring system applying the Changeable Block Distance method", 23-26.10.2013, materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST2013, monografia,

COMMUNICATIONS IN COMPUTER AND INFORMATION SIENCE (395), Springer-Verlag Berlin Heidelberg 2013.
[14] Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.
[15] PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikowanie i wykazywanie Nieuszkadzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS). Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia.
[16] PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.
[17] PN-EN 50159: 2010. Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania.
[18] PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Porcedura analizy rodzajów i skutków uszkodzeń (FMEA).
[19] PN-EN 61025:2007 Analiza drzewa niezdatności (FTA).
[20] PN-EN 61078:2006 Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie.
[21] PN-IEC 60300-3-9:1999 Analiza ryzyka w systemach technicznych.
[22] SIMIS-W. Sterowanie Ruchem Kolejowym, materiały seminaryjne firmy Siemens Technika Transportowa, Zakopane 2000.
[23] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998r.