ISSUES REGARDING INFORMATION SAFETY IN DIGITAL NETWORK OF RAILWAY RADIO COMMUNICATIONS

ZAGADNIENIA BEZPIECZEŃSTWA INFORMACYJNEGO W SIECI CYFROWEJ RADIOŁĄCZNOŚCI KOLEJOWEJ

Mirosław Siergiejczyk

Warsaw University of Technology

e-mail: msi@wt.pw.edu.pl

***Abstract:** In this paper there are presented both architecture and more important functions and range of services of GSM-R (Global System for Mobile Communication – Rail). GSM-R is used for management and signaling support in railway transport. Particular attention was drawn to selected issues of IT and mobile security of services provided by GSM-R.*

***Keywords:** radio-communication systems, GSM-R, railway transport, safety*

***Streszczenie:** W referacie przedstawiono architekturę oraz ważniejsze funkcje i usługi systemu cyfrowej telefonii komórkowej GSM-R. System GSM-R jest to system wykorzystywany dla potrzeb wspomagania zarządzania i sterowania w transporcie kolejowym. Szczególną uwagę zwrócono na wybrane problemy związane z bezpieczeństwem teleinformatycznym usług realizowanych z wykorzystaniem systemu GSM-R.*

***Słowa kluczowe:** radiolączność, GSM-R, transport kolejowy, bezpieczeństwo*

1. Introduction

GSM-R networks are used worldwide, also in European countries. In the nearest future GSM-R is going to be built also in Poland. Communication system currently used by Polish railways, occupying 150 MHz has already been exploited, and therefore does not meet current technical requirements, norms and standards and does not obtain required functionality. Assumptions of International Union of Railways (UIC - French: Union Internationale des Chemins de fer) took into account mainly unification of European railway communication systems by implementing EIRENE (European Integrated Railway radio Enhanced Network) project [3]. Implementation of GSM-R has measurable financial benefits for railway sector. The capacity of railway lines highly improves and state border crossing time is reduced to minimum. Thereby the provided services level increases (e.g. by implementing parcels monitoring). GSM-R is a digital mobile network used for needs of railway transport. It provides digital voice communication and digital data transfer. GSM-R offers developed functionality of GSM. Its infrastructure is located nearby railway line. GSM-R is designed to support systems implemented in Europe: ERMTS (European Rail Traffic Management System) and ETCS (European Train Control System), which task is to collect and transfer continuously rail vehicle data, such as speed or geographical location. GSM-R is a transmission medium for ETCS, it mediates information transfer to a driver and other rail services. Implementation of mentioned above systems indeed improves railway traffic safety, allows to diagnose railway vehicle in real time and to introduce parcels and cars monitoring. Moreover, due to precise distance definition between two trains the capacity of individual railway lines can be highly increased.

2. Information safety in digital railway radio-communication systems

A function of every telecommunication network is to transmit data in defined time and with defined error rate. GSM-R network is a telecommunication system, which must be characterized by high reliability and ensure high security level of transmitted data in railway environment. Reliable access to telecommunication services is very important issue for Railway Infrastructure Manager as it has direct effect on railway traffic safety and flow.

Cooperation of GSM-R with ETCS (*European Train Control System*) level 2 within ERTMS (*European Railway Traffic Management System*) imposes on GSM-R a requirement expressed by maximum possible unavailability period which

for ETCS level 2 and 3 equals 4 hrs per 10 years (accessibility of 99,995%) and for other voice and data transmission services – 8 hrs per year (accessibility of 99.91%).

Key issues that influence the system safety is security of radio interface and elements connected with it directly (e.g. transceiver). Each information transmitted by radio waves is exposed to possibility of wiretapping and interception. Therefore connections should be encrypted in the way that its content would not be opened and possible to be read by accidental user.

Encrypting does not apply only to Railway Emergency Call (REC) due to required short time of its setup. Encrypting demands application of corresponding digital algorithm for cryptography both on network and mobile station side. However, before the information is encrypted, the network must identify the user by performing the authorization procedure, known also as authentication. This procedure is based on electronic signature idea. Authorization is performed by using AuC (Authentication Centre) register and SIM (Subscriber Identity Module) card, in which Ki authorization key is stored. This is GSM-R most cryptic parameter, hence it is not transmitted in any network interface, and its reading from SIM card is properly protected. Authorization procedure starts at network side with calculation from Ki authorization key and randomly generated RAND number (RANDOM number) so called SRES number (Signed RESponse). RAND parameter is transmitted to mobile station (MS) at the moment of connection setup.

The terminal performs similar procedure to AuC register by calculating SREMS number basing on encryption key saved on SIM card and RAND parameter. This value is transmitted to mobile switching centre (MSC) where it is compared with earlier appointed SRES parameter. If the numbers equal each other then the connection setup procedure is continued. The next stage is message encrypting, which demands calculating both in AuC register and on Kc encryption key terminal side. Value of calculated values must be consistent, otherwise the encrypting procedure will not be continued. Encrypted are voice signal, data and signaling and this operation is proceeded both on circuits from base transceiver station (BTS) to terminal and backwards.

Transmitted data reading requires decrypting, performed each time by the algorithm used also in encrypting process.

3. Subscriber identification module safety

Each SIM card is connected with International Mobile Subscriber Identity (IMSI) which is used by the network in many procedures, i.e. connection setup and

actualization of localization. IMSI number transmission in radio interface without protection may lead to fixing subscriber's position by undesirable person. To avoid this kind of dangerous situations, Temporary Mobile Subscriber Identity number (TMSI) is introduced. Its length is half shorter than IMSI number.

Due to the fact that TMSI is randomly generated in VLR (Visitor Location Register) it is not possible to predict its value. TMSI is valid only in individual connection area of mobile station.

Apart from IMSI to each SIM card is assigned PIN code (Personal Identification Key) and eight-digit unblocking PUK code (Personal Unblocking Key).

An important element influencing safety is terminal verification. All radio terminals working in network should be monitored for legal use and their IMEI(*International Mobile Equipment Identity*) numbers should be placed on one of the following lists: white, grey or black. All mentioned above processes - authorization, encrypting, protection from unauthorized terminal usage and access to SIM module content affect the safety and are standard mechanisms functioning in every GSM-R network.

4. Telecommunication safety

Telecommunication safety is understood as an ensemble of methods and mechanisms, using of which ensures high level of accessibility and system reliability by choosing proper system structure, i.e. definition of e.g. separate elements redundancy. GSM-R destination and its influence on rail traffic safety puts on designers an obligation to provide the system with interferences and failures resistance.

It is extraordinarily important to develop a strategy providing maintenance of necessary safety level and to prepare plans of system functioning in situations of particular risk. These scenarios are called Disaster Recovery and contain processes and procedures related to recovery or maintenance of technical infrastructure critical for particular organization after natural or man-made disasters.

According to priority level of services which must be maintained after recovery, one can identify GSM-R critical devices and secure their redundancy.

Among them are individual cards and telecommunication lines. Practically, it is recommended that all stationary communication connections, TRX transceivers in BTS base stations, Base Station Controller (BSC) cards and Transcoder and rate Adaptation Unit (TRAU) cards were redundant.

A natural method allowing to increase network reliability, safety and accessibility is redundancy. It applies both to register - stored data and device elements that

could be doubled in many ways, e.g. $n+1$, $1+1$, $1:n$. To redundancy are subordinated:

- system – as a whole;
- individual subsystems, e.g. BSS, Network Switching Subsystem (NSS), Operation and Maintenance Center (OMC)
- individual system elements, e.g. MSC, Home Location Register (HLR);
- individual elements of system elements, e.g. MSC chip cards, interfaces.

Apart from doubling individual system elements, redundancy is applied also to such elements as MSC chip cards or interfaces. This type of redundancy is called ‘internal redundancy’ and is currently used by all GSM-R devices producers. MSC and HLR are NSS basic units and it is recommended that they all were dimensioned during implementation as $n+1$. Providing MSC redundancy is particularly important due to two functions: Voice Group Call Service with particular regard to Railway Emergency Call (REC) and point-to-point calls necessary for functioning of ETCS.

Usage of two MSCs with one BSC should not be a recommended solution for railway communication system because of the following:

- in case of MSC failure, restoring network functionality requires manual switching a controller to reserve centre,
- in case of BSC failure the entire GSMR failure occurs.

Redundancy of BSS in case of GSM-R should be performed with double coverage performed by BTS (co-located or alternate) on railway lines with ETCS and many BSC connected with the first or the second MSC. Quantity of BSC should be planned in such way, that every railway line with ETCS was connected with at least two BSCs connected with two different MSCs. On railway lines without ETCS coverage may be single as it is shown in fig. 2a or 2b and BTS connected alternately with two different BSCs connected with two different MSCs if possible.

Redundancy is also important in teletransmission systems. Usage of self-healing SDH structures, providing two optical paths as reserve transmission system are examples of telecommunication network redundancy that increase reliability and work safety. Self-healing SDH structures demand optical-fibre rings. The owner of railway infrastructure in Poland - PKP PLK S.A. within railway lines modernization lays optical-fibre traces on both sides of modernized railway tracks. Optical-fibre cables, i.e. basic cable and closing cable are laid in separate pipes of cable ducts on both sides of railway track. It gives opportunity of realization of

optical-fibre rings and thereby self-healing teletransmission SDH rings. So, for railway line E65 Warsaw – Gdynia is designed optical-fibre ring, i.e. there was designed connection of two adequate optical fibres in cables on both sides of railway track. Optical fibres will be connected in Warsaw and Gdynia. In order to increase reliability of optical-fibre rings one should predict possibility of switching (crossing) optical fibres of the first cable with spare fibres of the second cable in consolidation point, e.g. in Local Control Centre, which would indeed increase reliability (accessibility) of optical-fibre ring, and thereby reliability of teletransmission systems (system would be resistant not only for one failure in optical-fibre cables ring). Railway Infrastructure Manager, having certain sum of money at their disposal must specify, which system structure is the most profitable, not only from financial point of view, but also considering future system operation. It is recommended that on railway lines, on which GSM-R should cooperate with ETCS level 2 or 3, reliability mechanisms were used. Architecture of GSM-R as well as SDH allow designers to adapt already existing solutions to ETCS requirements.

5. Conclusions

By analyzing possible options of radio-communication railway line infrastructure and on-board radio-communication devices together with possible alarm messages initiated by drivers, traffic controllers and line inspection staff one can state, that current and target states have precisely described procedures of safe railway traffic (RADIOSTOP and REC functions).

Migration period will require development of new procedures for the system of safe control of railway traffic. For transitional stage there should be developed and produce dual-system transceivers (GSM-R/VHF 150 MHz) both for drivers (driver's cab radio set) and for controllers. Moreover, for transitional stage there is also needed development of STM module allowing traction units with installed ETCS running on railway lines with only analog communication VHF 150 MHz.

Infrastructure maintenance employees working on railway lines with installed GSM-R should be absolutely equipped with mobile GSM-R devices with REC function. On producing mentioned above devices as well as on developing proper procedures railway traffic safety will depend. Particular role in this process, apart from executors, play certification units authorized to evaluate railway traffic devices.

6. References

- [1] Białoń A. Masterplan wdrażania ERTMS w perspektywie krajowej i wspólnotowej. *Transport i Komunikacja* 2010, nr 2 [Białoń A.: ERTMS Implementation Masterplan in Domestic and EU Perspectives. *Transport i Komunikacja* 2010, No.2].
- [2] Gago S.: Niektóre problemy praktyczne występujące w układach sterowania i telekomunikacji KDP. Konferencja Naukowa Koleje dużych prędkości. 15 listopada Warszawa 2011 [Gago S.: Selected Practical Issues of High-Speed Rail Signaling and Telecommunications Systems. Scientific Conference on High-Speed Rail. Warsaw, 15th November 2011].
- [3] International Union of Railways, Project EIRENE – Functional Requirements Specification, 2006.
- [4] International Union of Railways, Project EIRENE – System Requirements Specification, 2006.
- [5] Markowski R. Założenia i ogólny opis systemu GSM-R. Konferencja naukowo-techniczna „Europejski System Sterowania Pociągami (ETCS/ERTMS)”, Poznań, 28-29 października 1999. [Markowski R.: Assumptions and General Description of GSM-R. Scientific and Technical Conference ‘European Rail Traffic Management System (ETCS/ERMTS), Poznań, 28th-29th October 1999.]
- [6] Pawlik M. Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS. *Technika Transportu Szynowego* 2007, nr 1 [Pawlik M.: Polish National Plan of Implementation of European Rail Traffic Management System. *Technika Transportu Szynowego* 2007, No. 1]
- [7] Pawlik M., Żurkowski A.: Ruch i przewozy kolejowe. Sterowanie ruchem; KOW, Warszawa 2010 [Pawlik M., Żurkowski A.: Railway traffic. Signaling. KOW, Warszawa 2010]
- [8] : Siergiejczyk M., Pawlik M., Gago S.,; Safety of the new control command European System. „CRC Press/Balkema, 2015. Przelaskowski K.: Eksploatacja systemu GSM-R w kolejnictwie europejskim. Przegląd Telekomunikacyjny Nr 2-3, 2003 [Przelaskowski K.: GSMR Exploitation in European Railways. *Przegląd Telekomunikacyjny* No. 2-3, 2003]
- [9] Sauthier E., Poutas L., Radio bearer capacity and planning for ETCS Solutions for BSS redundancy, 10th December 2003

- [10] Seminarium: Radiolączność w kolejnictwie wczoraj – dziś – jutro, SITK RP, Radom 2003 [Seminar: Railway Radio-Communication Yesterday – Today – Tomorrow, SITK RP, Radom 2003]
- [11] Siergiejczyk M.: Wybrane zagadnienia systemów sterowania ruchem i łączności dla kolei dużych prędkości w Polsce. Konferencja Naukowa Koleje dużych prędkości. 15 listopada Warszawa 2011 [Siergiejczyk M.: Selected Signalling and Communication Issues of High-Speed Rail in Poland. Scientific Conference on High-Speed Rail. Warsaw, 15th November 2011]
- [12] Siemens: Bezprzewodowa łączność GSM-R. Nowe Sygnały nr 29, KOW, Warszawa 2001 [Siemens: Wireless Communication GSM-R. Nowe Sygnały No. 29, KOW, Warszawa 2001].
- [13] Simon A., Walczyk M. Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo. Wydawnictwo: Xylab, Kraków 2002 [Simon A., Walczyk M.: Mobile Networks GSM/GPRS. Services and Safety. Xylab, Kraków 2002]
- [14] UIC ERTMS Users Group, 30/09/98 „ERTMS/ETCS RAMS Requirements Specification”.

Prof. Mirosław Siergiejczyk, PhD. Eng. - scientific fields of interest of the paper co-author concern among other issues of architecture and services provided by telecommunications networks and systems, especially from perspective of their applications in transport, reliability and operation of telecommunications networks and systems, modelling, designing and organizing telecommunications systems for transport.