ISSN: 1231-4005
e-ISSN: 23540133
DOI: 10.5604/01.3001.0010.3088

SECURITY OF TELECOMMUNICATIONS SYSTEMS IN TRANSPORT

Mirosław Siergiejczyk

Warsaw University of Technology
Faculty of Transport
Koszykowa Street 75, 00-662 Warsaw, Poland
tel.: +48 22 2347040,
e-mail: msi@wt.pw.edu.pl

Stanislaw Gago

Railway Institute
Railway Traffic Control and Telecom Division
Chłopickiego Street 50, 04-275 Warsaw, Poland
e-mail: sgago@ikolej.pl

Abstract

The article presents the selected elements affecting reliability and security of the telecommunications networks, which support transport services. In terms of telecommunications security, the selected methods and mechanisms, which allow providing the required level of reliability and availability of the telecommunications networks, in the fault-free operation and emergency modes, were discussed. In the article, attention was paid to the impact of a way of operation and maintenance on security of the telecommunications networks, and also on a correlation between the telecommunications system security and the security culture within the administrative and decision-making bodies.

The telecommunications networks used in transport ensure the broadly understood safe provision of data transmission services. Telecommunications networks consist of hardware and software systems, and the data transmission security depends both on hardware and software. It is a set of methods and mechanisms, which provides a high level of the system's reliability and availability by selecting the appropriate system structure.

Keywords: *security, transport, telecommunications, reliability, availability*

1. Introduction

The telecommunications networks designed for the needs of transport differ from the public telecommunications networks. In transport, the telecommunications networks constitute a tool of operation that supports transport services; however, the public networks constitute commercial networks providing telecommunications services for citizens. Both types of these networks use the same technical solutions but they very often differ in architecture, and provided services, e.g. GSM public system and GSM-R railway system. Such a situation has lasted for years and there is no indication that it will change.

On the European Commission forum, the conceptual work on the possibility of using broadband integrated radio networks in "critical missions", i.e. in the crisis situations including civil protection and help in the event of disasters and accidents *(PPDR- Public Protection and Disaster Relief)*, i.e. police, fire department, and ambulance *(the so-called "Blue light" services)* and in the industries, which modern societies cannot live without, i.e. providing the availability of electricity, fuel, gas, water, and basic transport services – with particular emphasis on road transport (ITS) and rail transport, is already in progress. UIC also established cooperation with CCBG Group *(Critical Communication Broadband Group)*, formed in 2012, the task of which is to develop the next generation network standards for private networks of special purpose,

such as railway, power engineering, public transport, military communications, emergency communications, etc. [4, 8, 9].

The above-mentioned applications and other similar ones will become even more important as we are currently entering the era of maintenance-free trains and autonomous road vehicles.

The telecommunications networks, designed to handle the above tasks, must be solid, reliable, safe, constantly available and offer small delays. In many research centres, the research work on using new technologies and ICT techniques, which support the land transport sector management, is carried out [2, 11].

In terms of rail transport, three options are basically analysed:

1. The rail transport uses independent ICT networks because in Europe, the passive parts of telecommunications networks (rights of way, telecommunications cables, cable ducting) often constitute the railway property. For the railway radio communication, the radio bands were separated, however, the active parts, i.e. telephone exchanges, radiotelephones, were adopted for the railway purposes, e.g. GSM-R system.
2. The rail transport uses public ITC networks because the progress in coding, compression and security of data sent in the public networks lead to the use of these networks for the purposes of the rail transport. The drawback of this solution is the fact that the data security would be dependent on the network owner and not on the data owner, and moreover, there would be surely the difficulties in obtaining decades-old guarantees of quality and service prices.
3. In some cases, the rail transport uses SOTM systems (*SatCom On The Move*), e.g. for modernisation and construction of railway lines, in commercial applications and travel information systems, as well as in supporting the security systems and more rational use of the rolling stock, etc.

The telecommunications networks used in transport should primarily ensure the broadly understood safe provision of data transmission services. The currently used telecommunications networks consist of hardware and software systems (hardware/software), and therefore, the data transmission security depends both on hardware and software [3, 10].

According to one of definitions, the telecommunications security is understood as a set of methods and mechanisms, the use of which provides a high level of the system's reliability and availability by selecting the appropriate system structure, among others, redundancy of individual elements.

The security of telecommunications networks can be divided into:

- IT security, i.e. protection against: hackers, crackers, viruses, trojan horses, worms, etc.,
- telecommunications security, i.e. self-repairing networks, firewalls, access passwords, biometrics, tunnelling, encryption, dedicated protocols, etc.

The telecommunications security is also understood as a set of methods and mechanisms, the use of which provides the required level of availability and service continuity by selecting the appropriate system structure and network topology or the appropriate level of radio coverage. However, the communications security constitutes security measures that prevent unauthorised persons from obtaining useful information by acquiring and familiarising with the transmitted messages.

Within the telecommunications system, the quality of provided services *(Quality of Service – QoS)*, which includes a certain probability of a false call, data transmission (transfer) delay, limited jitter (delay change within the assumed limits), and the assumed bit error rate, is an important parameter that demonstrates the system proper operation.

2. Telecommunications network reliability

The task of any telecommunications network is to transfer information within the specified time and with a specific bit error rate. The telecommunications network is a system, which must be characterised by high reliability and provide a high security level of transferred data. The reliable

access to the telecommunications services is a very important issue for the Manager of transport infrastructure because it can directly affect the safety of travelling people and transported goods and traffic flow.

The telecommunications network reliability may be interrupted by [1, 12]:

1. Physical disruption of the connection, e.g. cable break, teletransmission system malfunction, or the loss of a digital channel.
2. Damage or overload of the network equipment.
3. Malfunction of the legal or illegal operator.
4. Intentional network operation disruption.

Re. 1. Damage to telecommunications lines

In order to reduce the effects of damage to teletransmission lines, it is important to earlier predict (design) the alternate routes of information transmission, as well as to develop the procedures providing the correct response time, procedures and modes for reporting failures, and to have alternative temporary solutions.

Re. 2. Damage or overload of the network equipment

In order to reduce the risk of damage to the network equipment, at the network designing and implementation, it is important to adopt the renowned suppliers' solutions, and to use the proven network power supply and air conditioning systems, the appropriate class and redundancy of transmission devices, remote control and monitoring of interference, and also to have long-term guarantees for the installed system [5]. For exceptional situations, it is crucial to develop scenarios of the system restart and data recovery or automatic restarts of the system's parts (in case of the inability to restart the entire system).

In case of the possibility of the network overload, it is crucial to create priority channels or to introduce a guaranteed transmission band for particularly important calls, and to predict the possibility of disconnecting the network from other ones by a protective node.

Re. 3. Malfunction of the legal or illegal operator

The minimisation of risks due to malfunction of the legal or illegal operator should involve:

- selection of solutions minimising the necessity of the operators' intervention,
- clear division of powers,
- training and verification of the operators' qualifications,
- documentation of the conducted interventions,
- masking the network operation elements against the operator, within the range of which it does not have permission,
- introduction of self-learning and warning systems, and those impeding the erroneous operations.

Re. 4. Intentional network operation disruption

In order to prevent the intentional network operation disruption, first of all, it is important to provide the infrastructure security, e.g. by the protected access to telecommunications rooms using code locks, and keeping a register of entering and leaving people, and to install the monitoring systems of entering the premises, and to introduce:

- systems recording the attempts of interference,
- central monitoring and management of the network,
- division into zones and areas of access for operators,
- hierarchical access authorisation system.

It is also important to take care of the emission security by:

– using the devices with reduced emissions of electromagnetic radiation,
– screening of peripheral devices,
– masking the process of classified information processing,
– carrying out the processing of implicit information in shielded rooms,
– galvanic separation of power supply devices from the public power grid.

In the ITC networks, the protection of the users' information should be carried out with the use of security measures, which prevent unauthorised people from obtaining useful information by acquiring and familiarising with the transmitted messages, and also the measures of protecting information from loss [3, 9]. The information protection measures may include, among others, the following methods:

– information transmission only between the ports specified by the user,
– messaging systems separated from subscriber systems,
– very high probability of information transfer,
– information cannot be collected in a non-volatile manner within the network.

It is extremely important to develop a strategy ensuring the maintenance of the necessary level of security as well as the preparation of plans for the system operation in the situations of extreme danger. These scenarios are referred to as Disaster Recovery (infrastructure recovery after failure), and they constitute processes and procedures related to recovery and maintenance of technical and critical infrastructure for a given organisation after natural or man-made disasters [7], [12].

The operators of the ITC networks providing services for transport should specify the Disaster Recovery strategy for their network, which will be a basis for this functionality implementation. Firstly, it is crucial strictly to specify the following issues and requirements:

– definition of failure,
– ultimate recovery time,
– level of services, which are priority after recovery (connection types, value added services),
– recovery method (manual intervention, remote reprogramming, locating the personnel).

The Disaster Recovery planning is basically part of a larger process of the operation continuity planning and it should include a definition of the procedures for recovery of applications, data, hardware and communications [6]. There are three basic phases included in the measures related to disasters:

– preparation phase (phase carried out prior to the occurrence of failure or disaster),
– phase of starting the repair (phase starting at the time of diagnosing the failure or disaster and taking early action to restore the system efficiency),
– repair phase (phase beginning a few days or a week after the occurrence of failure or disaster).

During the network design process, some scenarios, in which the system's individual elements are subject to failure or damage, e.g. due to fire or disaster, should be developed. The scenarios of these types of events will make it possible to specify critical elements for the entire system functioning, and to select the appropriate method of their protection. Redundancy is a common method that allows increasing the network reliability, security and availability, and it means redundancy of devices or the use of additional elements. It refers both to information stored in the registers and to the hardware elements, which can be duplicated in different ways, inter alia, n+1, 1+1, 1:n. Redundancy may refer to making copies of all data or only data, the value of which is particularly important. Redundancy may be subject to:

– the entire system,
– individual subsystems (e.g. teletransmission system, switching system, on-board network system),
– individual elements that comprise the system (e.g. management system, switching node, etc.),
– individual components included in the system's elements (e.g. processor cards of switching nodes, interfaces).

It is obvious that the greater redundancy is, the more reliable the system is, which means shorter time of the system unavailability during the year. However, along with an increase in hardware redundancy, the system maintenance costs also increase and the delay effects resulting from switching between redundant subsystems and even elements must be also taken into account.

While creating a plan for the Disaster Recovery application, several options should be considered:

- duplication of all the network backbone systems and placing them in another remote location. The restoration of the network functionality is the fastest in this option, although the cost is the highest. It will be also necessary to use additional telecommunications links;
- Disaster Recovery application is provided by the third party (e.g. operator of another network);
- distribution of all the key devices in different locations, which will limit the impact of damage to individual elements.

3. Telecommunications security in the "Transport institution"

The telecommunications network operation in the transport organisation is operation within the boundary between the personnel involved in the telecommunications technique and the personnel dealing with the provision of transport services.

The activities related to the management of operation and maintenance of telecommunications networks should last 24 hours a day and seven days a week. The telecommunications networks security also depends on the performed activities.

While constructing the telecommunications network, it should be taken for granted that each network, even the best designed and implemented one will be subject to failure and damage. Depending on the quality of performance, used materials and devices, the damage may occur at different frequencies. Therefore, the organization of the network service and maintenance is necessary regardless of the network size. However, the network size and the number of users depend on the structure of operational services [7, 8, 10].

It can be determined that:

- maintenance of the telecommunications network's elements in the technical efficiency requires systematic preventive work (inspection, measurements) and well-organised activities, constituting a reaction to events within the network,
- network maintenance is a set of all the technical and organisational activities aimed at maintenance of the structure of telecommunications devices in the state making it possible to meet the required functions of these devices,
- maintenance includes technical and diagnostic operation, periodic inspection and repairs of telecommunications equipment,
- information about events within the network basically comes from two sources: from the network monitoring system and from the network users reporting technical problems,
- properly organized network service manages – network, failure and the network users. The service personnel should be subject to appropriate trainings, as well as carry out the analysis of interference and malfunction, and be aware of the importance of individual malfunction for operators, users and administration.

The telecommunications network maintenance is an activity within the boundary between a technique and users, and it should allow for:

- unification and centralisation of a way of storing information about clients (subscribers), as well as quick and easy access to the information by authorised organisational units,
- mutual use of stored information by proper organisational units and services,
- monitoring of the technical condition of GSM-R network resources,
- determination of the operation efficiency of the maintenance units,
- planning of GSM-R network expansion for the customers' needs,

and provide:
- a full set of data on subscribers, as well as the network structure and its efficiency,
- precise and fast testing of links,
- definition and generation of reports,

and ensure the security and confidentiality of stored information.

The activities related to the management of operation and maintenance of GSM-R network should last 24 hours a day and seven days a week.

The telecommunications networks' security also depends on the performed activities, which may include:
- network administration,
- monitoring of operation of the network's elements, automatic detection of threats and overloads in the network,
- teletransmission traffic management,
- management of resources,
- management of services,
- archiving the states of devices and reports,
- localisation and removal of damage and failure to the network's elements (optical fibre cables, active devices of networks, radio equipment),
- network passporting (records of the network resources, maintenance of the network's technical and operational documentation),
- systematic inspection and preventive maintenance work,
- activation and deactivation of the network termination (connection and disconnection of the network users),
- preparation of reports on the state of networks and services,
- network reconfiguration, including changes in network structure configuration, elimination of the network's elements, network expansion with new elements.

The entities that have an impact on the telecommunications system security also include its users (stakeholders), i.e. administration, carriers, infrastructure operators. These are the entities that comprise "*organisational and decisive being*" related to transport security. The security culture of this Organisation is a product of individual and group values, attitudes, perceptions, competence and models of behaviour, which determine the commitment, style and knowledge of "*healthy organization*" conditions and security management.

The security culture is used as a framework programme for discussing risks and activities that mitigate the adverse effects of these risks from the perspective of a man, technology and organisation (interested institutions). The security culture indicates two key factors that affect the transport security, i.e. motivation and morale. These factors are associated with other basic ones: training, appropriate procedures, instructions, operation schedules, management style and organisational principles.

The first challenge for Organisation should include determination of "*Resilience*" of the system, i.e. "*the system's natural capability to control its operation (before or after interference) so that it can maintain operability after the occurrence of interference or operate properly during the interference*". In the initial phase of the Organisation action, there is little knowledge on unexpected incidents, and therefore, the risk assessment process, in which the following elements should be defined, should be carried out:
- main threats – technical, organisational or human factors,
- activities reducing the risk and improvement of resistance to a risk of failure or damage,
- conditions of improving the capabilities of learning in an active way by interested "beings".

The security improvement of the Organisation should be achieved with the use of research activities and joint action (meetings/conferences) of the Organisation users in terms of:
- diagnosing (risk identification),

- planning of activities (risk assessment and mitigating activities),
- taking measures (performance),
- assessment (evaluation of implementation and knowledge / awareness),
- acquisition of knowledge.

The main task of the Organisation should be the development of "System resilience" strategy in terms of security improvement. In complex systems, such as the telecommunications network, this strategy is described by flexible rules, the keywords of which include:

- redundancy, in order to carry out controlled degradation of the system and make it possible to "reflect" or recover the operational capability (system flexibility),
- capability of redundancy management,
- capability of maintaining common security concepts in the Organisation.

The security principles presented in the strategy should be implemented in the technology, organisation and within the personnel.

During operation of the telecommunications networks, a number of undesirable situations may occur. The key undesirable situations may include:

- technical error, e.g. network connection loss (poor resilience of technical infrastructure),
- unforeseen human errors due to poor training and insufficient knowledge – too few well-trained employees (poor resistance to risk in the organisation),
- the lack of good communication between individual beings in the organisation – mentally different risk assessment,
- poor ability to handle crisis situations (poor resistance) due to bad crisis training.

Therefore, it is important to include the mitigation activities, which should contribute to reduction of the effects of undesirable situations. The key mitigation activities include:

- redundancy in the telecommunications networks in order to improve the technical resistance,
- the improved organisational resilience in the event of a failure to the telecommunications network by creation of better procedures in the entire Organisation (administration, carriers, infrastructure operators),
- the increase in the number of appropriately trained employees responsible for security in order to improve the resilience within the Organisation,
- the organisation of "meetings" between the most important entities (administration, carriers, infrastructure operators) in order to improve predictability of defects,
- the modernisation of training scenarios for anticipated crisis situations, the objective of which will include the improvement of resilience.

4. Conclusion

The security of telecommunications networks supporting the transport service implementation is very important because it involves or contributes to the safety of travelling people and transported goods, and also supports the effective management of transport companies. It can be found that the telecommunications networks are a tool for creating better and more efficient transport services, and therefore, they have to be optimised for individual modes and types of transport. The common feature of these networks is that they consist of wired and wireless parts, which results in the fact that the security of transmitted information is more complex than in the specialised public networks, and moreover, the effects of incorrectly transmitted information may be even tragic.

The information security in the telecommunications networks constitutes a multithreaded problem, and it is impossible to describe all the issues related to security problems in one article, especially that these networks are used for transport control, direction and management.

A separate issue, which was not referred to in this article, is the security of the telecommunications networks' software that should be included in the essential elements determining the security of these networks.

References

[1] Anderson, D. J,. Brown, T. J, Carter, C. M., *System of Systems Operational Availability Modeling*, Sandia National Laboratories, October, 2013.

[2] Cheng, S. Y., Seah, Y. H. L., *Optimising complex networked systems availability*, DSTA HORIZONS, 2013.

[3] Fry, Ch., Nystrom, M., *Monitoring and network security,* Wyd. Helion, Gliwice 2010.

[4] Gago, S., *Some practical problems occurring in control and telecommunications system of High Speed Railways*, Scientific Conference on High Speed Railways, Warsaw 2011.

[5] Kuhn, D. R., Kacker, R. N., Lei, Y., *Advanced Combinatorial Test Methods for System Reliability*, Annual Technical Report, Reliability Society, 2010.

[6] Malkawi, M. I., *The art of software systems development: Reliability, Availability, Maintainability, Performance (RAMP)*, Human-Centric Computing and Information Science, Springer Link, ISSN: 2192-1962 (Online), 2013.

[7] Qiu, S., Sallak, M., Schön, W., Cherfi-Boulanger, Z., *Epistemic parametric uncertainties in availability assessment of a Railway Signalling System using Monte Carlo simulation*, Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds), Taylor & Francis Group, ISBN 978-1-138-00123-7, London 2014.

[8] Siergiejczyk, M., Gago, S., Pawlik, M., *Safety of the new control command European System*, ESREL, Wrocław 2014.

[9] Siergiejczyk, M., Gago, S., *Issues of the GSMR system security in terms of the rail transport,* Logistics, No. 6/2012, Eds. ILiM, Poznań 2012.

[10] Siergiejczyk, M., Gago, S., *Selected problems of reliability and security of information transmission in the GSM-R system,* Railway Problems – Journal 162, Warsaw 2014.

[11] Siergiejczyk, M., Krzykowska, K., Rosiński, A., *Reliability-exploitation analysis of the alarm columns of highway emergency communication system*, Journal of KONBiN, No. 2 (38), 2016.

[12] www.dtic.mil/ndia/2012/TEST/13836_Hartzell.pdf *Interpreting Reliability and Availability Requirements for Network-Centric Systems.*