Railway Safety and Security Versus Growing Cybercrime Challenges

Marek Pawlik(✉)

Warsaw Railway Research Institute, Chlopickiego 50, Warsaw, Poland
mpawlik@ikolej.pl

Abstract. Paper presents how safety and security of the railway system have changed over the years taking into account both internal and external factors. It takes into account internal changes in railway technology itself including more and more shifting to electronic, programmable and database systems and shifting from closed to open data communication systems. It also takes into account external changes pointing environmental circumstances, vandalism and terrorism challenges as well as cybercrime changes. Paper is focusing on cybercrime and cybersecurity. It identifies functions of the railway systems which are supported by IT based solutions. Paper subdivides identified IT based solutions by their influence on the safety and security as well as by their susceptibility to external influences including unauthorised attempts to influence the way they work. It shows how much susceptibility depends on internal and external data communication. Paper analyses different types of hazardous events influencing communication starting from relationships between possible undesirable events and threats, which are defined by RAMS railway standards. Conclusions are pointing sensitive IT solutions areas together with descriptions of the related challenges.

Keywords: Railway · Cybersecurity · Communication · Control command · Signalling

1 Introduction

Railways' safety was treated as doubtless requirement from the very beginning. It was obvious, that moving hundreds and thousands of tons would not be acceptable if safety would not be proven. At the same time it was obvious, that technical solutions may eventually malfunction especially as they were foreseen for long time operation in difficult circumstances (high stress, fatigue loading, dust, etc.) and also that the railway staff is not infallible. As a result from the very beginning it was necessary to define safety rules for technical constructions as well as safety related rules for operational purpose and verification of staff competences.

The key safety rule which was used from the beginning was a fail-safe concept. All technical solutions, which are safety critical, are constructed in a way, that ensures safe operation in case of degraded situations, disregarding technical part which is malfunctioning and the way it is damaged. The fail-safe concept was defined for mechanical solutions. This is why horizontal position of the arm of a mechanical

J. Mikulski (Ed.): TST 2019, CCIS 1049, pp. 57–68, 2019.
https://doi.org/10.1007/978-3-030-27547-1_5

semaphore had to mean STOP, while vertical position was not acceptable as reflecting permissible signal. It was so, as broken semaphore wire could result with dangerous situation – showing permissible signal, when route is not set or occupied by rolling stock. Accepting half-up semaphore position as proceed ensures STOP meaning for broken wire thanks to gravity (horizontal position – STOP, 45° angle – proceed).

Fail-safe principle was adopted for mechanical solutions, but it was working perfectly also for electromechanical and electrical solutions. For instance it was, and still is, checked whether short-circuits or lack of electrical connection do not cause dangerous situation. However for electronic solutions fail-safe concept had to be supplemented with additional rules, as it was reasonable to apply it only to general failures like lack of power supply for individual modules. It became not reasonable to apply fail-safe principle for wide range of errors which may occur within individual modules. That's why new safety concept was defined in early 1990s, and is known as Safety Integrity Level SIL-4.

Presently, after nearly thirty years railways are facing new challenge – ensuring cybersecurity. The question is whether SIL-4 is good enough for today risks associated with utilisation of off-shelf electronic components and using publicly known transmission technics, open transmission systems and considering cloud data storage together with cloud computing. Cybersecurity is a question for today.

2 Cybersecurity – How Far It Is a New Challenge

Railway traffic safety was important from the very beginning. The present cyber-crime risks could be compared to risks already present in old technical solutions. For instance the single-line token principle, which was frequently used in the past, which was based on singularity of the device assigned to specific section, could be encroached by preparation of the fake-token. However preparation of such token was really difficult. It was much easier to impose driver to pass signal at danger by forcing then by misleading the driver.

Presently, passing signal at danger (passing STOP without authorisation) is more and more difficult. Many lines are equipped with protection functionalities e.g. by applying automatic train control (ATC) systems like ETCS (European Train Control System imposed by EU law for all railway lines when signalling is upgraded especially when it takes place with use of EU funds). Such ATC systems including ETCS are using electronic, programmable elements and technologies which are considerably known to non-railway experts. That creates risk which is not comparable to fake-token. Railways have to be prepared for different kinds of cyber-crime including attempts to generate fake electronic signals allowing trains to run in dangerous situations.

3 What for Railways Are Using IT Technologies

In order to discuss railway cybersecurity it is important to identify what for railways are using IT technologies. Of course they are presently used for different purposes.

Looking on the railway lines and stations:

- IT support is utilized for design e.g. for planning tracks geometry, calculations of amounts of materials e.g. amount of ballast, verification of appropriateness of place for storage of the materials, technology planning e.g. design of technological roads, design of power stations, subdivision of tracks into sections appropriate for foreseen speed, etc.
- IT support is utilized for construction both for new railway lines and for upgrading existing lines and stations, e.g. for measurements of the tracks, structure gauges, overhead lines, for semi-automatic and automatic construction equipment e.g. for levelling, lifting, lining and tamping machines, for after construction verifications, etc.
- IT support is utilized for operation e.g. for setting proceed signals at the trackside signals, for preparation and transmission of the electronic movement authorities, for authentication of the received authorities, for checking train runs against envelopes, for displaying passenger information, for voice announcements, for emergency braking systems, for continuous collecting of the data reflecting the state of equipment, for diagnostic, etc.
- IT support is utilized for supporting degraded operation e.g. for supporting decision processes, for collecting data about incidents, accidents and near misses for identification of reasons and for elimination of such reasons in the future, for supporting accident commissions by credible data showing all information relevant for accident analyses.

Looking on the railway rolling stock:

- IT support is utilized for design e.g. for individual components and for overall vehicle design, e.g. for calculations and verifications of power equipment, engines, braking systems, doors control, movable steps, ticketing, passenger information systems, passenger emergency calls for establishing communication with driver, passenger emergency brakes, air conditioning and heating, lights, etc.
- IT support is utilized for construction both for new railway vehicles and for renewal of existing ones, e.g. for verification of cabling and wiring, for checking functionalities and their interconnections, etc.
- IT support is utilized for operation e.g. for traction steering, running, braking, and on-board equipment continuous verification for diagnostic purpose and on-board equipment steering e.g. air conditioning, voice announcements, doors opening and closing, etc.
- IT support is utilized for supporting degraded operation e.g. for emergency stop and communication with line-side staff, as well as for collecting credible data showing all information relevant for accident analyses.

Out of that wide range article focuses only on cybersecurity of the solutions supporting operation. However it is more and more reasonable and required to take cybersecurity into account for all different types of systems utilizing IT based and electronic, programmable components.

3.1 Operating Railway Lines with IT Supported Functionalities

Operation starts with timetabling and have to be supported by diagnostic functionalities. However it seems reasonable to focus on three key groups of functions which are supported nowadays by electronic programmable components and IT based algorithms – on signalling, communication and emergency systems and devices. They are marked in a symbolic way on Fig. 1, which is showing urban rail in one of the Italian cities.

Signalling is composed by interlocking, co-working track occupancy checking system, point machines, trackside signals, block centre preparing electronic movement authorities and trackside equipment sending authorities.

Communication ensures operational voice connections between trackside staff and drivers as well as voice announcements. It is composed by many devices interconnected by fibre optic and copper cables as well as by radio.

Additional devices dedicated for emergency are influencing signalling and communication ones as well as braking, lighting, emergency announcements, etc.

Fig. 1. Signalling, communication and emergency components funicolare between Petraio and Fuga [own elaboration]

A set of devices for signalling, communication and emergency support together with their purposes and interconnections which are defined in design phase, constructed during building or re-building and verified during commissioning have to be checked

regularly to ensure appropriate functioning which could be corrupted by different kinds of failures, misuses as well as by inappropriate maintenance or unauthorised interventions e.g. cyber-crime.

3.2 Operating Railway Rolling Stock with IT Supported Functionalities

Operation starts with timetabling and have to be supported by diagnostic functionalities. However it seems reasonable to focus on three key groups of functions which are supported nowadays by electronic programmable components and IT based algorithms – on steering, driving & braking and passengers' support components. They are marked in a symbolic way on Fig. 2, which is showing Koleje Mazowieckie train at the Siedlce station in Poland.

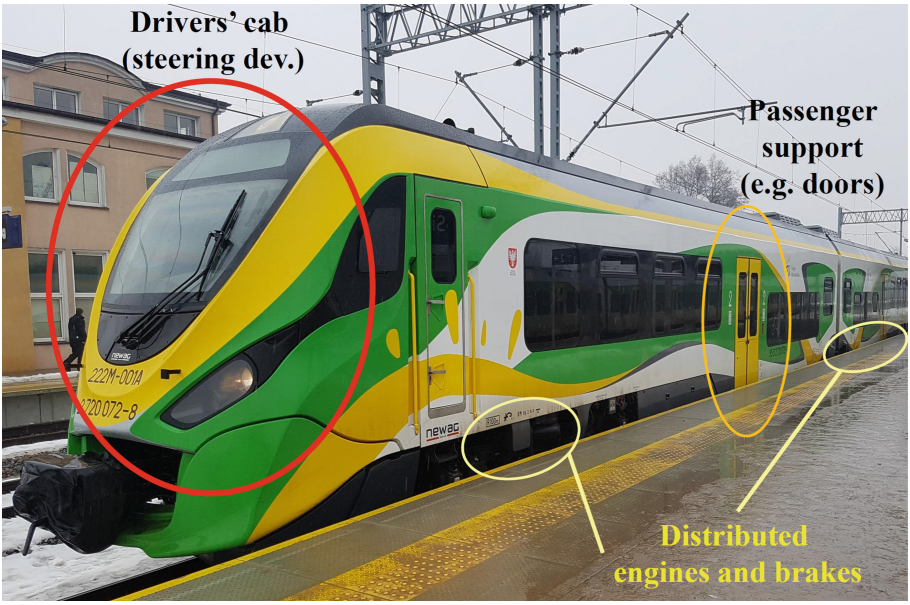

Fig. 2. Steering, driving & braking and passengers' support components Koleje Mazowieckie train at Siedlce station [own elaboration]

Steering devices are operated by driver from driving cab. It covers pantographs, engines, brakes, horn, vigilance as well as signalling, communication and emergency, namely voice and data communication, emergency stop by radio, receiving and using movement authorisations, verification of running parameters, etc.

Key role is played by engines and braking systems, which are also not free from electronic, programmable and IT based solutions. In case of diesel and electrical multiple units both engines and brakes are distributed. In case of classic train composed by locomotives and wagons or coaches engines are located in locomotives, but brakes are distributed.

Passenger trains are also equipped with passengers' support devices like on-board broadcasting and passenger information systems, ticketing, air-conditioning and heating, lights, passenger emergency brakes, etc.

All devices and their interconnections are precisely defined for each type of vehicle, and verified during commissioning for each individual vehicle. Design, construction as well as commissioning are supported by IT based systems. However they have to be checked regularly to ensure appropriate functioning which could be corrupted by different kinds of failures, misuses as well as by inappropriate maintenance or unauthorised interventions e.g. cyber-crime.

3.3 IT Support for Transport Security

Ensuring traffic safety is not enough. Railways have to ensure also transport security. That is based on dedicated staff and procedures, which are also supported by electronic, programmable and IT supported components e.g. video-monitoring, emergency communication, automatic info about opening of cabinets, etc.

Also such technical means have to be protected against unauthorised interventions.

4 How Railways Are Specifying Requirements for Electronic, Programmable and IT Based Components

4.1 Requirements for IT Based Technical Systems Supporting Traffic Safety

Traffic management, namely signalling and control command components are covered by one of the RAMS standard - EN 50129 [8] dedicated for railway signalling reliability, availability, maintainability and safety. Works on software components are required to respect dedicated requirements described in another RAMS standard – EN 50128 [7]. All utilized communication means have to follow requirements applicable to communication systems for rail transport signalling described in another RAMS standard – EN 50159 [9]. Overall signalling and control command have to be covered by safety proving document, called safety case, which is proving safety integrity level SIL-4. Proving takes into account the way how software has been prepared, the way how communication has been established and all components together with their relationships taking into account operation, maintenance and overall system conditions. The overall dependencies are shown at Fig. 3 and is described in the main railway RAMS standard – EN 50126 [5, 6].

Proven SIL-4 is a must, however additionally railways are defining availability requirements. It is not enough that probability of a failure affecting safety is very low. It is also required, that in case of failure system can be put in operation after repair in adequately short time. Availability, which mainly depends on repair times in reality also depends on operating, maintenance and overall system conditions, which are not only related to systematic and random failures but also to human factors, operational and maintenance procedures and logistic circumstances, as well as to external disturbances, preventive and corrective maintenance.

Random failures affecting safety cannot occur more then 10^{-8} times per hour for SIL-4 systems. Proving is usually based on technical structure and mean times between failures MTBF.

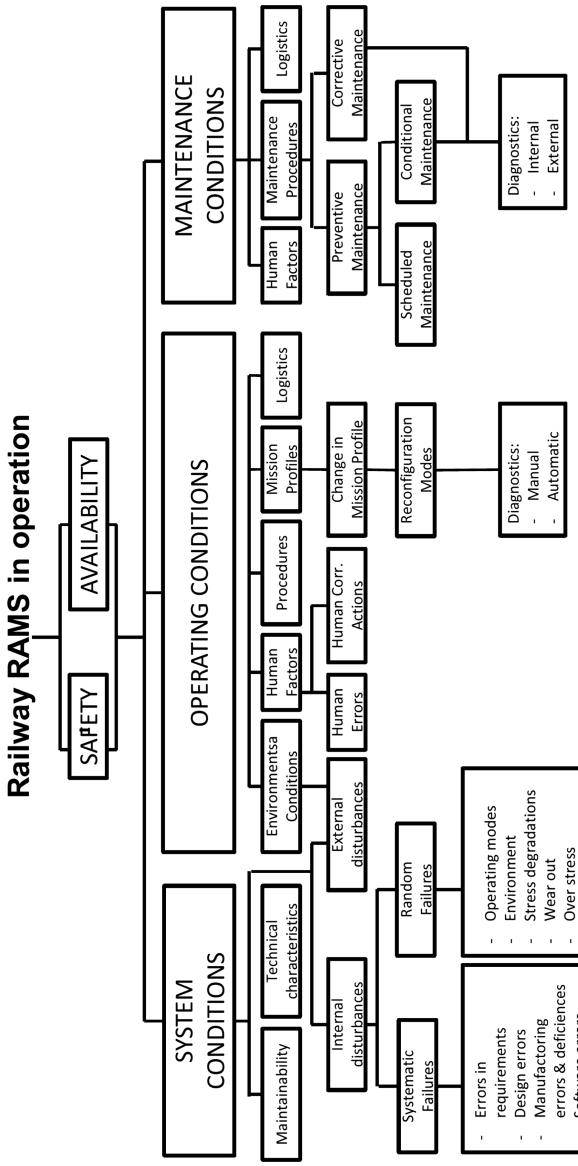

Fig. 3. Safety and availability relationship to operational, maintenance and overall system conditions as depictured in EN 50126 [5]

Systematic failures are more difficult to be taken into account. Verification in that respect is based on quality management and a set of technics which are subdivided into strongly recommended and recommended for different SIL levels. Railway traffic safety was important from the very beginning in nineteen century safe principle and the safety integrity levels.

4.2 Requirements for IT Based Technical Systems Supporting Transport Security

Methodology which is shortly described above in Sect. 4.1 up to now applies only to signalling and control command equipment. It is not legally required for all other types of technical solutions which are dedicated for supporting railway transport security. It is not applicable e.g. for passenger information systems, fire protection systems, electrical protection systems, etc.

All such systems are seen as potential source of troubles starting from traffic disturbances, but requirements are defined case by case, and there is no standard even in relation to the way how such requirements have to be defined and communicated.

4.3 Enlarging Applicability of RAMS Standards

RAMS standards [5÷9] are seen on the European level as a key for cross-acceptance of technical solutions for railways for all solutions which are utilizing electronic, programmable and IT based components. That's why their applicability is just being enlarged. Basic RAMS standard EN 50126, which is pointed by Polish legal documents as the one issued in 1999, has been recently replaced on a European level by a set of two standards EN 50126-1:2017 [5] and EN 50126-2:2017 [6]. It is already agreed, that their applicability will be enlarged. It was officially accepted in January 2019 by Member States, and will be in force since June this year.

Enlargement of the applicability of the RAMS standards covers individual pointed solutions in design and construction of the infrastructure, power supply and rolling stock. Those solutions are pointed in an annex linking standards with Technical Specifications for Interoperability (TSI) issued as annexes to binding European Commission Regulations.

Moreover TSI specifications, due to rapid changes in electronic and programmable components technologies as well as IT technologies, are stating, that all changes in the RAMS standards will be binding without a need to reflect them in the TSI specifications.

As an addition TSI specifications are also changing requirements for the bodies, which are verifying safety cases. Since June such verifications can only be performed by entities which are accredited as Assessment Bodies for risk acceptance under railway safety directive [1]. That is reflected also in a change of the directive, which took place in 2016 within so called fourth railway package. A new directive regarding railway safety [2] will be introduced in Polish law in the mid of June 2020. This directive will heighten requirements for the risk acceptance and further enlarge RAMS standards applicability.

The question is whether it is good enough for ensuring cybersecurity for IT based solutions utilized by railways. It seems it is certainly not. It is enough to point some

examples. First, railway freight operators pay for infrastructure, which was requested, even if it was not used. That was necessary to end blocking infrastructure by some operators few years ago. Presently as a result freight operators request paths for trains only when they are sure, that the trains will be ready. As a result Polish Railway Lines are using internet based system for timetabling (SKRJ) offering freight operators an interface for ad-hoc setting of the paths. Presently about seventy operators are using that system, but legally speaking it has to be opened for all freight operators in the European Union latest in 2020 in the light of the fourth railway package.

Polish Railway Lines are using multilevel database containing all data necessary for asset management (SILK). System contains data necessary for dispatching, for maintenance and renewals: ortofotomaps, buildings, public roads and roads owned by railways, land attitude, tracks, switches, bridges, viaducts, signals, are put over maps, which were made available by the main country geodesist. All kinds of documents like feasibility studies, reports reflecting state of the constructions, maintenance recommendations, reasons for local speed restrictions, etc. are also put into SILK as a main database ensuring relations between documents and geographical coordinates of the infrastructure elements. This system is accessible only for infrastructure manager employees, but it is accessible over public network.

Such systems cannot be treated as cyber-crime resistant without appropriate prove.

5 Cybersecurity – What Is Being Done on the European Level

Complex IT based systems are supporting different sectors of national economy. Cybercrime challenge has already been seen many times, even in railway environment – e.g. German railway timetabling and passenger information systems were corrupted causing hundreds hours of delay. As a result dedicated directive concerning measures for a high common level of security of network and information systems has been accepted [3] as a measure supplementing directive dedicated for electronic communications networks and services [4]. Special safety measures are defined on one side for the companies producing and ensuring distribution of the electricity, oil production and managing oil transmission pipelines, and gas supply. On the other side similar requirements regarding cybersecurity are defined for banking and credit institutions, for entities ensuring financial market infrastructure, for health care sector including hospitals and clinics, as well as for drinking water supply and distribution and digital infrastructure together with authentication services raising cyber-crime immunity. The most common attracts are those ones which are blocking systems by rapidly growing amount of requests.

Directive [3] is covering also transport systems: air transport carriers, airport managing bodies and entities operating ancillary installations contained within airports and traffic management control operators providing air traffic control services, as well as inland, sea and coastal passenger and freight water transport companies, ports' managing bodies and entities operating works and equipment contained within ports, as well as road authorities responsible for traffic management control. It covers also railway transport. It that respect it is pointing at rail transport infrastructure managers and railway undertakings, as the ones which are due to introduce safety measures

against cyber-crime and which are due to be involved in national and European exchange of cybersecurity relevant alerts and best practices.

6 Cybersecurity – What Is Being Done by Individual Companies

All entities belonging to pointed types are obliged to undertake works ensuring better preparation for cybersecurity related risks. Polish Railway Lines as well as railway transport operators had to identify all IT based systems which could be affected (example are shown above in Subsect. 4.3), and analyse their immunity taking into account the way they were purchased.

There are two general ways to purchase software based systems – selection based purchasing and specification based purchasing. Many systems were bought by selection based processes in the past. Nowadays practically all such systems are purchased by specification based processes. The key questions regarding cyber-security are first – how to define required, necessary security?, second – how to check whether declared security is true?, third – how to ensure, that required security is useful and sufficient? This questions are common disregarding whether software based system is for oil company, air traffic or health care sector. Therefor railway companies have to learn the lesson already learnt by others. The overall process already established for specification based IT purchase processes is shown at Fig. 4.

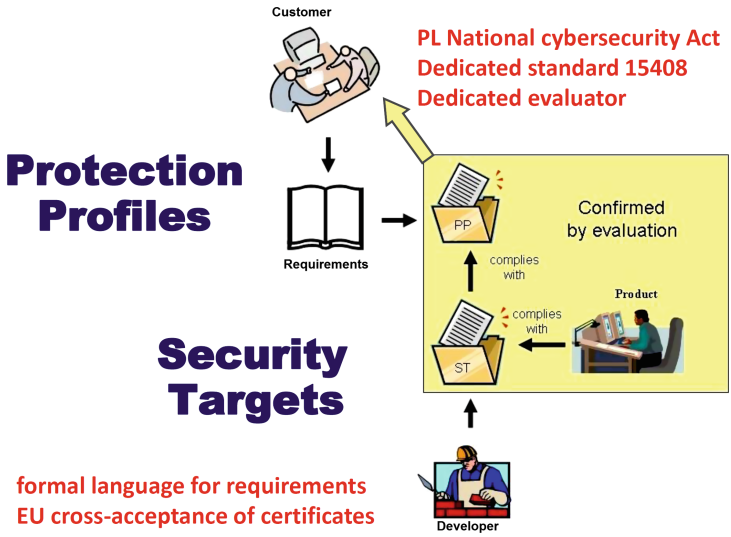

Fig. 4. Specification based IT purchase process utilizing verification of the security target by use of protection profile [10]

Customer is due to define in a formal language, described in a 15408 standard [10], cybersecurity related requirements in a form of protection profile. Such PP profile is given to developer, which is preparing a separate document describing in the same formal language achieved, ensured security targets. Verification of the software based systems is performed by authorised evaluating entities, which are cross-accepted under cybersecurity directive [3]. Such entity has already been established in Poland on a national level, but did not performed any work for railway sector up to now.

7 Conclusion

There is no doubt, that RAMS standards have to be applied not only for signalling and control command but also for wide range of technical electronic, programmable and IT based solutions utilized by railway companies. This is however not enough for ensuring cybersecurity. Additional measures have to be undertaken especially for IT based systems which were constructed without defining protection profiles and without verifications of the security targets against protection profiles. It is necessary to verify cybersecurity of systems in use, especially for SKRJ and SILK, but also for a number of others, and to change the way they are developed in the future.

The RAMS standards have to be learnt and adopted by companies undertaking construction works for railway lines and stations as well as by rolling stock producers. Probably Polish versions of the EN 50126-1 and EN 50126-2 [5, 6] will be available at the end of 2019. This however is waiting for confirmation from the Polish Committee for Standardization PKN.

Polish entity authorised for evaluation of the security targets against protection profiles has to be accredited and has to start cooperation with Polish Railway Lines as an infrastructure manager and with key railway operators like PKP Cargo, Intercity, Przewozy Regionalne as well as with key railway IT service providers, especially with Informatyka Kolejowa.

References

1. Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive) (Official Journal of the European Union, L 164/44, 30.4.2004)
2. Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (Official Journal of the European Union, L 138/102, 26.5.2016)
3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union, L 194/1, 19.7.2016)

4. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33), amended by: Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 (OJ L 171/32, 29.6.2007), Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 (OJ L 167/12, 29.6.2009) and Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 337/37, 18.12.2009)
5. European Standard EN 50126-1:2017, Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process
6. European Standard EN 50126-2:2017, Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety
7. European Standard EN 50128:2011, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems
8. European Standard EN 50129:2003/AC:2010, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
9. European Standard EN 50159:2010, Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
10. ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model