Concept of the railway safety, security and cybersecurity functional integrity levels

Marek Pawlik[*]

Railway Research Institute, 50 Chlopickiego str., 04-275 Warsaw, Poland

Abstract. Observed growing changes in the character and severity of the risks in rail traffic safety and rail transport security are associated with present development of utilized technical solutions. New hazards are coming out, besides known ones, including hazards associated with cyber-crime. As a result it is fully justified to undertake works dedicated to collect and settle all risks associated with technical solutions using modern technologies for acquisition, computing and transfer of the data, which are vital from the rail traffic safety and rail transport security point of view. Article defines rail transport systems safety, security and cybersecurity functional integrity levels thanks to knock-out and differentiating questions regarding identified key safety related functionalities. Proposed methodology was used for safety and security verification of a chosen homogenous rail transport system separated from the overall Polish railway system. Results have shown discrepancies in utilized protection measures. Proposed methodology can be used for assessment of existing systems as well as for specifying scopes of investments both for infrastructure and rolling stock modernizations. Applicability range covers railway transport, light rail services, metro, urban rail transport systems as well as rail based transport systems using autonomous vehicles.

1 Introduction

1.1 Technical safety and personal security

It is unambiguous, that all technical solutions, which are utilized by railway transport, are being defined, constructed and maintained having safety in mind. It is not so easy to declare, that railway system with all its solutions is safe, as incidents and accidents happen since time to time even if the amount of them is relatively low. Severity of the railway accidents is frequently high and therefore it is a real challenge to define how safe the railway system has to be to be declared as a safe one.

From the very beginning of the railway history safety was based on technical solu-tions and procedures. Technical solutions were, and still are, constructed in a way ensuring safe operation in case of errors, faults, failures, which may cause system malfunctioning. As degraded operational circumstances do appear during long lifecy-cles of the railway solutions it was, and still is, required to apply fail-safe principle. It means, that neither faults or failures nor errors or extreme external conditions, e.g. temperatures or loads, can lead to dangerous situations understood mainly as giving the train permission to run too far or too quick. As a result faults, failures, errors and extreme external conditions thanks to own inherent characteristics of the solutions lead to shifting responsibility from technical systems to staff and procedures in de-graded operational circumstances.

Applying fail-safe principle was, and still is, not appropriate for some technical so-lutions – for ensuring appropriate endurance of the tracks, embankments, bridges, as well as vehicles' bodies, running gears and auxiliary systems. In that respect safety since the beginning was, and still is, based on widely accepted codes of practice e.g. UIC leaflets, EN standards, OTIF specifications.

Moreover applying fail-safe principle is not appropriate for technical solutions which are utilizing electronic, programmable systems and modules for which huge catalogue of possible faults, failures and errors forefend verifications of the appropri-ateness and completeness of the fail-safe principle. That mainly applies to railway control command and signalling equipment.

It was obvious from the beginning, that technical safety is a must, but insufficient requirement. Railways had, and still have, to ensure personal safety on stations and in trains. They had, and sill have, to ensure safety of the cargo as well as minimized undesirable influence on environment. Up to the beginning of the twenty first century that was ensured by procedures and dedicated staff – by railway police. Presently they are more and more supported by electronic equipment, and therefore relationships between technical safety and personal & goods security starts to be blotted.

* Corresponding author: mpawlik@ikolej.pl

1.2 Railway traffic safety and rail transport security

Presently technical experts responsible for railway infrastructure – for tracks, switches and crossings as well as underlying embankments, bridges and viaducts as well as accompanying platforms, pathways and station buildings and their accoutrements apply nearly only technical solutions, which are fully in accordance with abovemen-tioned codes of practice e.g. Vignole railway rails fully compliant with EN 13674 standard series. To large extend approach based on codes of practice apply also for traction power supply and rolling stock as adequate technical documents directly define requirements for materials and constructions as well as for verifications of the final solutions.

Codes of practice also exist for control command and signalling equipment installed both trackside and onboard. However in that respect technical documents define functionalities and safety verification rules generally omitting materials and the way how to construct technical solutions. This is largely linked to relatively quick development of technical solutions utilized for control command and signalling. As a result fail-safe principle and codes of practice are not sufficient for ensuring technical safety. Since twenty years in that respect railway signalling solutions respect so called Safety Integrity Levels defined by EN standards dedicated to reliability, availability, maintainability and safety – RAMS standards [3÷7]. Control command and signalling systems and devices inherent safety is assessed in case of electronic, digital and programmable solutions against Safety Integrity Level SIL-4 defined by tolerable hazard rates

10-8÷10-9 for hazardous events per hour, which may be caused by random failures and external factors and recommended technics for minimization of hazards associated with human mistakes. The SIL based approach is required for control command under interoperability directive [2], which is applicable to new technical solutions. At the same time risk based approach is required under railway safety directive [1]. Both however omit security challenges, which the railways are facing all the time.

Railways are using presently technical solutions based on electronic, digital, pro-grammable components not only for control command and signalling but also for supporting security staff – for generating emergency alerts, video monitoring, communication, supporting rescue and evacuation. In that respect SIL-4 based approach is not required. As a result it is reasonable to ask whether safety and security are fully ensured and whether they are ensured similarly well in relation to different risks which are presently common. Safety and security impact reference model was defined to answer those questions.

2 Safety and security impact reference model SSIRM

Safety and security impact reference model SSIRM is based on identification of functions which are supported by electronic, digital and programmable solutions. Safety is treated not only as an overall requirement which has to be ensured in normal operation but also as inherent characteristics of the technical solutions which ensure safety in degraded modes of operation. Key functionalities, understood as groups of individual functions, which influence railway traffic safety are shown at figure 1.

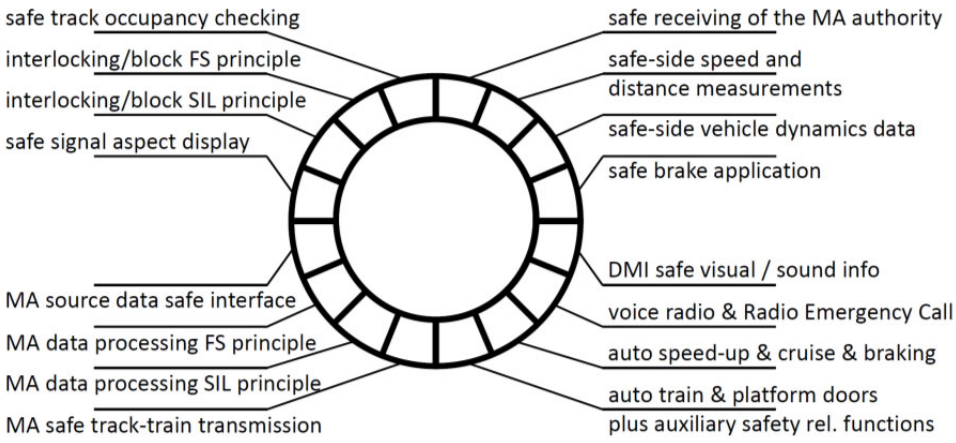

Fig. 1. Safety and Security Impact Reference Model SSIRM, safety related functionalities
FS – fail-safe principle, SIL – safety integrity level SIL-4 principle, MA – digital movement authority, DMI – driver machine interface /own elaboration/

Safety domain.

Sixteen functionalities can be subdivided into five groups. The first group (upper left) represents classic signalling equipment installed trackside. The interlocking and block systems are due to respect fail-safe principle and ensure Safety Integrity Level SIL-4. This would however not ensure safety if track occupancy checking or displaying signal aspects do not respect safety rules. Applying fail-safe and SIL-4 principles are required for individual solutions, however overall

verification has to be performed taking into account dependences between elements working together.

The second group (lower left) represent control command equipment installed trackside. Its role is to prepare an electronic movement authority for the train on the basis of data taken from signalling equipment. The way how the data is taken cannot change the data in the wrong side neither on signalling nor on control command side. Data processing has to respect both fail-safe and SIL-4 principles. Prepared move-ment authority has to be sent in a safe way. Data acquisition, data processing and data transmission have to technically safe in all operational circumstances.

The third group (upper right) represents control command equipment installed onboard of the traction vehicles. Movement authorities have to be received, verified and respected. Obtaining digital movement authority is worth only if onboard equip-ment ensures reliable and safe information about relationship between location and speed of the train in relation to the braking curves imposed by authorities taking into account distance and speed measurements as well as considering vehicle dynamics. From safety point of view it is necessary to ensure also safe application of the brakes taking into account both full service brake and emergency brake.

Digital movement authority available onboard can be utilized by manually operated trains and by automatically operated vehicles. Therefore the four remaining functionalities are subdivided into two groups (lower right). Group fourth representing cab signalling by visual and audible information as well as radio communication between train driver and trackside staff together with emergency calls. The fifth group representing automatic driving – automatic speed-up, cruise and braking as well as functions which are necessary for safe access and egress including platform doors control and auxiliary auto train functionalities. The sixteen fields on the ring can be used to represent safety aspects by colors.

Security domain.

Control command and signalling functionalities have to be complemented by security related ones. Security domain is shown at figure 2. It is also composed by five groups of functionalities. The first group (upper left) represents solutions which are due to ensure basic passenger safety. Passenger information systems are very important both trackside and onboard in case of emergency, to prevent panic, to support evacuation etc. Railways are also due to ensure fire safety and electrical safety. More and more that is also supported digitally and therefore has to be considered.

The following groups (lower left) represent systems ensuring protection against crime and vandalism as well as enhanced protection for passenger health. The second group covers solutions enabling passing alarms to dedicated staff and video monitoring systems. The third group covers emergency call installations as well as medical equipment like e.g. automatic external defibrillators AED.

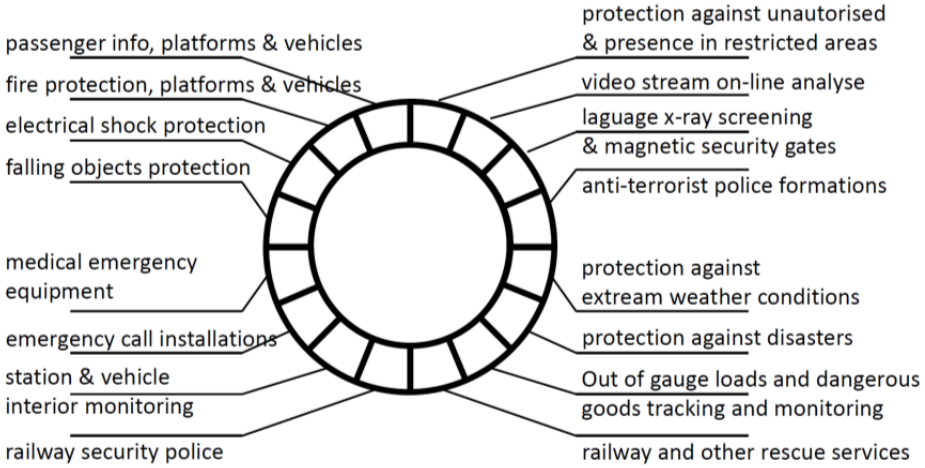

Fig. 2. Safety and Security Impact Reference Model e-SSIRM, security related functionalities /own elaboration/

The fourth group (upper right) is representing enhanced technical means against crime, vandalism and terrorism. It covers protection against unauthorized access and presence based on simple solutions as well as video stream analyzers, which are able to detect persons entering restricted areas e.g. passing from one platform to another over tracks, unattended luggage, fake crowd, running persons, etc. As a result appro-priate information is automatically identified and communicated to security staff immediately providing chance to react in due time and not only to document hazardous events for further investigations. Additionally stations and platforms can be protected by language screening and magnetic gates. That is already in use in some cases, however it is questionable especially in case of traffic in agglomerations.

The fifth group (lower right) represents technical protection means against natural and construction disasters. Also such technical solutions are already in use in some places e.g. in case of high speed lines going through seismic areas, in case of long railway tunnels and so on.

3 Enhanced impact reference model e-SSIRM and safety, security and cyber-security Functional Integrity Levels FIL

Safety of the data transmission.

It is visible for experts, that risk associated with data transmission systems has to be treated very seriously, especially as wireless communication technics are more and more used for train control [9, 10]. However simple SSIRM model does not fully take into account data transmissions. As a result of considerations regarding cybersecurity it was therefore enhanced by adding data transmissions in a form of connections between different fields on the safety ring and between different fields on the security ring. Adding connections representing data transmission systems on one side enables showing safety by colors similarly to the fields. On the other side adding connections provides flexibility which ensures easy way for showing different transmission media arrangements covering individual transmission systems and complex transmission systems serving different functionalities as well as wired and wireless transmission systems and their relationships with safety and security functionalities.

Such representation enables easy way to visualize systems which have to respect safety related requirements for transmission systems [7] together with their relationships with equipment components which have to respect safety related requirements for hardware modules [6] and for software modules [5]. The overall assessments are however supported only visually while it would be helpful to create an add on to Safety Integrity Levels SIL-4 requirements which are mandatory for individual technical systems supporting safety.

Functional integrity levels for safety, security and cybersecurity.

Ten groups of functionalities, five dedicated to data transmission based technical means supporting railway traffic safety and five dedicated to data transmission based technical means supporting railway transport security, were used to prepare sets of questions containing two types of questions – knock-out questions and differentiating questions. The knock-out question can receive value “0” and value “1”. The differentiating question can receive values “1” and value “2”. Additional set of questions was prepared for transmission systems to reflect resistance against internal malfunctioning, extreme external conditions and cyber-crime. Also in that respect knock-out and differentiating questions were defined.

Examples of the safety related knock-out questions.

1 Whether all tracks with their full length are covered by track occupancy systems?
2 Whether all track occupancy systems fully apply fail-safe rules?
3 Whether all track occupancy systems utilizing electronic, programmable or simply digital solutions have safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
4 Whether all station interlockings, line block systems and level crossing protection systems fully apply fail-safe rules?
5 Whether all station interlockings, line block systems and level crossing protection systems have safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
6 Whether all track sections are protected by visible track-side signals or visualised in the cabs on-board in all trains permitted to run?
7 Whether all signal types are included in safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
8 Whether all technical solutions for data acquisition from interlockings, line block systems and level crossing protection systems (used for digital movement authorities) do not influence, under any foreseeable circumstances, safety of the interlockings, block systems and level crossing protection?
9 Whether all technical solutions used for data acquisition from interlockings, line block systems and level crossing protection systems fully apply fail-safe rules?
10 Whether all technical solutions for data acquisition from interlockings, line block systems and level crossing protection systems have safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
11 Whether all technical solutions for data processing for electronic movement authorities have safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
12 Whether all messages, especially those containing movement authorities, contain data enabling sender authentication?
13 Whether all messages, especially those containing movement authorities, contain data enabling verification of validity?
14 Whether on-board control command equipment verifies sender authentications and message validities of all received messages, especially those containing movement authorities?
15 Whether on-board control command equipment properly estimates and takes into account errors of the distance and speed measurements?
16 Whether on-board control command equipment properly estimates and takes into account train braking dynamics?
17 Whether all on-board control command elements are fully taken into account in safety cases elaborated by producers and verified by independent safety assessors proving SIL-4?
18 Whether on-board control command equipment provides drivers with visualisation of the electronic movement authorities? or Whether on-board equipment automatically changes speed using on-board control command elements?

19 Whether voice radio communication is provided for drivers and signalmen ? or Whether on-board equipment automatically controls and commands on-board and trackside equipment (e.g. pantograph, main circuit-breaker, train doors and platform doors)?
20 Each knock-out question may have positive answer (YES = 1) or negative answer (NO = 0). The overall value is a product of all of them. Even a single negative answer is a knock-out for safety of a whole solution.

Differentiating questions for safety.

1 Whether control command messages contain data which are used by on-board control command equipment for verification of completeness and coherency of all received messages?
2 Whether on-board control command equipment verifies cryptographic protection of all received messages?
3 Whether drivers are informed by control command about latest places for starting braking and warned before equipment interventions?
4 Whether automatic braking interventions are using more than one braking mode (full service braking and emergencbraking)?
5 Whether receiving emergency signal automatically initiates braking which ensures stopping in a place appropriate for evacuation and for security and rescue staff interventions?

Differentiating questions for Security.

1 Whether emergency medical equipment, especially automated external defibrillators, are available in all stations in areas accessible for passengers and provides with appropriate signs and instructions?
2 Whether video-monitoring system used for providing security is equipped with video-stream analyser ensuring immediate generation of security warnings?
3 Whether luggage scanning is provided?
4 Whether protection against possible natural disasters is provided?
5 Whether tracking of dangerous goods is provided?

Differentiating questions for Cybersecurity.

1 Whether in case of detecting loss of communication for signalling automatic reconfiguration of communication system takes place or automatic switch on of the backup communication system takes place to ensure traffic control by technical means (and not only procedures)?
2 Whether safety related personnel is equipped with backup communication means?
3 Whether in case of detecting loss of communication for control command automatic reconfiguration of communication system takes place or automatic switch on of the backup communication system takes place to ensure train running supervision?
4 Whether in case when control command system is out of order trains can be driven on the basis of the signal aspects displayed on the track-side signals?
5 Whether technical systems and devices supporting security, especially video-monitoring systems are provided with backup power supply?

All questions are defined and described in a dedicated monograph [8].

Knock-out questions for safety are shown in table 1. as an example. Differentiating questions for safety, security and cybersecurity are shown in table 2. Each knock-out question may have positive answer (YES = 1) or negative answer (NO = 0). The overall value is a product of all of them. Even a single negative answer is a knock-out for safety of a whole solution. Each differentiating question also may have positive or negative answer, however in this case YES = 2 while NO = 1. Safety, security and cybersecurity are therefore represented by a vector.

$$[\,safety\,, security\,, cybersecurity\,] \tag{1}$$

in other notation

$$[\ \mathrm{SF},\ \mathrm{SC},\ \mathrm{CS}\ ] \tag{2}$$

where:
SF – product of all answers regarding safety,
SC – product of all answers regarding security,
CS – product of all answers regarding cybersecurity.
The Functional Integrity Level for safety, security and cybersecurity, FIL level, is defined as a sinus of an angle between vector and reference geometrical plane, for which maximum vector is perpendicular.

$$FIL_{SF,\,SC,\,CS} = sin\left(\begin{matrix}32 & 0 & 0\\ 0 & 32 & 0\\ 0 & 0 & 32\end{matrix}\ ,[SF, SC, CS]\right) \tag{3}$$

For $SF \neq 0$ and $SC \neq 0$. and $CS \neq 0$.
If $SF \neq 0$ or $SC \neq 0$ or $CS \neq 0$
then $FIL_{SF,\,SC,\,CS} = 0$.

where:
$FIL_{SF,\,SC,\,CS}$ is a safety, security and cybersecurity functional integrity level

An angle between vector and geometrical plane (represented by matrix) may only be right (=90°) or acute (<90°). Maximum FIL value equals “1” (as a sinus of 90°) when products of the answers regarding safety, security and cybersecurity are equal to each other. Growing discrepancies between products of the answers causes dropping of the FIL keeping it > zero for non-zero values of the SF, SC and CS.

4 Conclusion

Presently technical means based on data acquisition, processing, transmission and storage are widely used for supporting railway traffic safety as well as rail transport security. Therefore safety, security and cybersecurity

should be seen as complementary topics, which have to be provided on similarly high level. It is not reasonable to provide high safety for some functionalities and no safety for the others. The cyber-attacks which have already happened did not affected control command or signalling equipment but passenger information systems and timetabling.

References

1. Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (EU OJ L 138/102).
2. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (EU OJ L 138/44).
3. European Standard EN 50126-1:2017, Railway applications —The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Ge-neric RAMS Process.
4. European Standard EN 50126-2:2017, Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Sys-tems Approach to Safety.
5. European Standard EN 50128:2011, Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems.
6. European Standard EN 50129:2003/AC:2010, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
7. European Standard EN 50159:2010, Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems.
8. Pawlik M.: Railway safety and security functional reference model built on data transmission based systems (Referencyjny model funkcjonalny wspierania bezpieczeństwa i ochrony transportu kolejowego przez systemy z transmisją danych). ISBN 978-83-7814-908-8, Warsaw University of Technology Publishing House (Oficyna Wydawnicza Politechniki Warszawskiej), Warsaw 2019.
9. Lewiński A., Perzyński T., Ukleja P.: *Possibility of Use the Wireless Communication in Protection of Rail Traffic on the Regional Line*, Railway Reports, issue **175** (June 2017), ISSN 0552-2145, Railway Research Institute, Warsaw 2017, pp. 53-58
10. Gradowski P.: *Upgrading the railway infrastructure technical parameters using the example of the Control-Command and Signalling subsystem with the EC verification certificate*, Railway Reports, issue **182** (March 2019), ISSN 0552-2145, Railway Research Institute, Warsaw 2019, pp. 131-146