Comprehensive approach to risk assessment and evaluation regarding constructioning of the first 25 kV 50 Hz AC traction power supply sections in Poland

Marek Pawlik[1,*]

[1]Railway Research Institute, ul. Chłopickiego 50, 04-275, Warsaw, Poland

Abstract. Railway lines in Poland are either equipped with 3 kV DC traction system or not electrified for traction purpose. Presently maximum line speed is 200 km/h while maximum train speed is 250 km/h. Speeding up limit for 3 kV DC traction is estimated to be around 220-230 km/h. Already present in Poland trains for 250 km/h are equipped with three electric power supply systems: 3 kV DC used in Poland, 15 kV 16,7 Hz AC used in Germany, and 25 kV 50 Hz AC foreseen to be used in Poland on high speed lines. Introducing 25 kV 50 Hz AC traction power supply will be associated with safety challenges, which have to be taken into account already during constructioning, starting even at the predesigned phase. Two key questions arise. First of all question regarding methodology, which should be used for safety level acceptance and secondly how to ensure that all safety aspects will be taken into account. Answering first question for railway safety experts seems to be easy – let's apply risk assessment and evaluation methodology described by EU regulation under Railway Safety Directive. The challenge is however to define risk acceptance criteria which will be required, and that is analysed in the paper. The second challenge is even more challenging. Author proposes using 10-by-10 safety matrix which was defined by the author in previous publications [9, 10]. Its concept as well as principles for its application for new type of power supply is also presented in the paper.

1 Introduction

Polish railway network is composed of 19.000 kilometres of railway lines mostly double track. Yearly reports being published by the PKP PLK S.A. (Polish Railway Lines) show, that with station tracks infrastructure is composed by 38.000 kilometres of tracks. Nearly 12.000 kilometres of railway lines (nearly 25.000 kilometres of tracks) are electrified. Electrified lines are double track and electrified together with station tracks. All presently electrified lines in Poland are using 3 kV DC traction system.

For many years the maximum line speed on the Polish railway lines as well as the maximum running speed of the Polish traction units which are running on those lines was 160 km/h. Presently maximum line speed is increased up to 200 km/h. At the same time maximum running speed of some new trains has reached 250 km/h. This shows, that from economical point of view line speeds at least on some lines should be increased minimum to 250 km/h to ensure sensible use of already existing trains and justifying purchase of such high speed trains.

In that respect the challenge is however the traction system [1]. Used 3 kV DC system is a bottleneck for speeding. Speeding up limit for 3 kV DC traction is estimated to be around 220-230 km/h. The trains for 250 km/h already purchased by PKP Intercity are therefore prepared to run under different traction supply systems. The vehicles for 250 km/h are already equipped with three above cited electric power supply systems.

2 Safety challenges associated with introduction of the 25 kV 50 Hz AC traction on railway lines

Introducing 25 kV 50 Hz AC traction power supply for the first time in Poland is a significant change possibly influencing safety of the railway system as a whole. This has to be analysed in details by the infrastructure manager, which will govern such infrastructure (not necessarily PKP Polish Railway Lines). The safety challenges should be taken into account already during construction, starting even at the predesign phase. Therefore identification of potential risks and defining safety requirements and necessary safety measures is a question to be discussed already now.

Defining safety requirements is directly associated with identification of risks. Defining risks requires defining 25 kV 50 Hz AC power supply system together with its borders and interfaces. It seems, that defining system is not a challenge itself. In that respect using definition of the subsystem "Energy" from the railway

* Corresponding author: mpawlik@ikolej.pl

interoperability directive [2] seems to be appropriate and quite enough. Subsystems are defined in annex II of the directive. The "Energy" subsystem is defined as "*The electrification system, including overhead lines and on-board parts of the electric consumptions measuring Equipment*". This shows on one side, that power supply to substations are outside railway system. Respective risks however should be taken into account, but it is proposed to take them into account as characteristics of the interface between national power system and subsystem "Energy". On the other side pantographs are not included in "Energy". They belong to the "Rolling stock" subsystem, which is defined as "*Structure, command and control system for all train equipment, current-collection devices, traction and energy conversion units, braking, coupling and running gear (bogies, axles, etc.) and suspension, doors, man/machine interfaces (driver, on-board staff and passengers, including the needs of persons with reduced mobility), passive or active safety devices and requisites for the health of passengers and on-board staff.*", and therefore includes not only current collection but also energy conversion systems and traction engines up to connection with insulated return to substation, which belongs to subsystem "Energy". Risks associated with that interface and with insulated return itself have to be taken into account.

On the basis of the experience gained by the railway companies all over Europe "Energy" subsystem is defined more precisely by a dedicated Technical Specification for Interoperability - TSI known as TSI ENE [3]. The 25 kV 50 Hz AC system's associated risks are minimised in the European countries using such power supply system by applying European technical standards dedicated to traction stationary equipment [4] and traction mobile equipment [5] as well as by applying dedicated European technical standard dedicated for coordination of electrical protection of stationary and mobile traction equipment [6].

As trains are passing state borders since a long time safety related challenges were also discussed by dedicated groups working within International Union of Railways (UIC). As a result UIC has published some leaflets dedicated to traction power supply [7].

Moreover railway tunnels' specific safety aspects are covered by another dedicated Technical Specification for Interoperability - TSI known as TSI SRT [8]. This TSI includes many different requirements e.g. for escape routes in railway tunnels, for ensuring places for rescue services in emergency, for communication, lighting, operational rules, as well as traction power supply both in relation to stationary traction equipment especially regarding reliability of traction system and its power supply in emergency situations and in relation to mobile traction equipment put in rolling stock especially regarding ability to run with fire on board of the train. All those detailed requirements [3-8] minimize risks by imposing defined solutions, however they are not linked with identification of risks.

2.1 Identification of the 25 kV 50 Hz AC power supply risks

For the 25 kV 50 Hz AC power supply system defined together with its borders and interfaces detailed list of risks have to be elaborated. This creates two detailed challenges. First it has to be pointed, that risk is associated with probability of a hazard and with foreseeable hazard consequences. This shows, that on one side some hazards can be assumed as not important as their probabilities are negligible and on the other side some hazards can be assumed as not important as their foreseeable consequences are negligible. However such decisions can only be taken after identification of hazards.

2.2 Identification of the 25 kV 50 Hz AC power supply hazards

The key challenge is to ensure taking into account all hazards associated with 25 kV 50 Hz AC system and its interfaces.

For this purpose it is proposed to use 10-by-10 safety matrix which was defined by author in previous publications [9-10]. Alternative overall safety models which exist are focusing on risk approach to safety un-appreciating technical approach to safety covering railway specific technical challenges. The most important railway specific safety model based on risk approach is a Safety Management System "SMS Wheel" tool prepared and disclosed by the Railway Agency of the European Union [11]. Unlike such models the 10-by-10 matrix is based on two directives. The Railway Interoperability Directive [2], which defines essential requirement "safety" for railway system as a whole and for separate subsystems including "Energy" subsystem defined as above, and the Railway Safety Directive [12], which defines "safety management" scope for railway undertakings and infrastructure managers. Matrix takes into account also security aspects and safety aspects associated with security supporting systems like access monitoring, LPR (Licence Plate Recognition) systems, fire detection, video screening, etc. as well as cybersecurity dimension of all systems, which are using electronic and programmable technical solutions. Security and cybersecurity aspects were defined on the basis of author experience and already discussed with experts dealing with safety in nuclear power plants and air transport which are keen in system approach to hazard identification and risk acceptance. The safety 10-by-10 matrix with security dimension is shown on Fig. 1.

The technical safety aspects are following:

- T1 - malfunctioning safety – what can happen when systems and/or devices are not working properly;
- T2 - construction safety – what can happen when systems and/or devices are affected by exceptional stress, fire, or construction or natural disaster;
- T3 - electrical safety – what can happen in case of overvoltage, short-circuits, presence of electric arch between pantograph and overhead line, lightning, etc;

- T4 - preventing unauthorized access and fire – how to ensure appropriate protection against unauthorised access and fire and how to ensure that cases when such protection is broken are notified immediately to respective operational, security and emergency staff;
- T5 - wheel/rail interaction safety – how to ensure protection against derailment in different circumstances and how to ensure appropriate relationships between lengths of the braking distances and spacing of trains imposed by localisations of signals and signs along the tracks;
- T6 - control command and signalling – active safety systems ensuring operational safety and their inherent safety based on fail-safe principle and safety integrity level SIL4 ensuring route setting on stations, train spacing on sections and protection against switching points under running trains;
- T7 - power supply/signalling interaction safety – the ways which are used to ensure minimisation of risk of negative influence from power supply on signalling and control command especially via insulated return and conversions of the energy;
- T8 - safety of the operational rules and staff competences – covering all operational circumstances especially present in degraded modes of operation over lifecycle of technical systems as well as building, verifying and keeping staff competences and health;
- T9 - preventing panic – staff communication in emergency and public address systems, evacuation ways and doors, emergency lighting, etc.;
- T10 - IT support for safety – ensuring collection of relevant data acquisition, storage, transmission and processing for improving safety on the basis of accidents and incidents analyses and reporting.

Two of them are marked with grey background as they are associated with safety aspects not taken into account in the Railway Interoperability Directive [2].

The operational safety management is composed of aspects pointed and described in the Railway Safety Directive [12] and are following:

- O1 - safety Policy;
- O2 - maintenance safety;
- O3 - operational safety;
- O4 - risk assessment;
- O5 - risk assessment monitoring;
- O6 - exchange of safety relevant information;
- O7 - activities in emergency situations;
- O8 - analysing accidents & incidents;
- O9 - internal monitoring of the safety system;
- O10 - safety improvement plans.

Moreover it is important to take into account cyber security aspects. Presently in Poland they are taken into account only for some kinds of technical solutions. Present situation on the Polish railway network is shown on Fig. 2 on the basis of the 10-by-10 matrix. Here there are two different intensities of grey. For some types of solutions cybersecurity is legally required, namely for signalling and control command systems and devices e.g. for electronic interlockings and block systems. This is marked with dark grey not only in relations to control command and signalling safety but also in relations to safety aspects which apply to such systems and devices like: malfunctioning safety, safety of the control command systems inherent operational rules, and IT support for control command and signalling. Infrastructure managers and railway undertakings are already requesting safety proves for other types of systems especially those supporting security although it is legally not required. It is marked grey on the 10-by-10 matrix. Base on that it can be assumed, that generally cybersecurity of electronic and programmable safety technical means (marked dark grey) is and should be required, while cybersecurity of security technical means (marked grey) is requested by users but not required legally as shown on Fig. 2. below.

Operational safety management aspects

Technical safety aspects

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
T1	x	x	x	x	x	X	x	x	x	
T2	x	x	x	x	x	X	x	x	x	
T3	x	x	x	x	x	X	x	x	x	
T4	x	x	x	x	x	X	x	x	x	
T5	x	x	x	x	x	X	x	x	x	
T6	x	x	x	x	x	X	x	x	x	
T7	x	x	x	x	x	X	x	x	x	
T8	x	x	x	x	x	X	x	x	x	
T9	x	x	x	x	x	X	x	x	x	
T10	x	x	x	x	x	X	x	x	x	

Fig. 1. Safety matrix 10-by-10 with security dimension marked in grey. (own elaboration).

Operational safety management aspects

Technical safety aspects

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
T1	x	x	x	x	x	x	x	x	x	x
T2	x	x	x	x	x	x	x	x	x	x
T3	x	x	x	x	x	x	x	x	x	x
T4	x	x	x	x	x	x	x	x	x	x
T5	x	x	x	x	x	x	x	x	x	x
T6	x	x	x	x	x	x	x	x	x	x
T7	x	x	x	x	x	x	x	x	x	x
T8	x	x	x	x	x	x	x	x	x	x
T9	x	x	x	x	x	x	x	x	x	x
T10	x	x	x	x	x	x	x	x	x	x

Fig. 2. Safety matrix 10-by-10 with cybersecurity dimension marked in grey. (own elaboration).

This shows, that for safety aspects of the technical means influencing safety, and not only security, cybersecurity have to be seen as a must although it is not clearly stated in binding acts and regulations e.g. for traction control.

As a result following technical safety aspects can be shown as the ones to be analysed in details when introducing 25 kV 50 Hz AC power supply:

- T1 - malfunctioning safety;
- T2 - construction safety;
- T3 - electrical safety;
- T4 - preventing unauthorized access and fire;
- T7 - power supply/signalling interaction safety;
- T10 - IT support for safety;

with focus on following safety management aspects:

- O2 - maintenance safety;
- O3 - operational safety;
- O7 - activities in emergency situations;

as shown on Fig. 3 below.

The first four technical aspects are rather obvious. There is no doubt, that in case of malfunctioning or exceptional stress safety has to be ensured. The electrical safety aspects are also obvious when analysing power supply system as well as prevention against unauthorized access and fire.

Two technical safety aspects are not obvious – power supply/signalling interaction safety and IT support for safety.

The interaction with signalling starts with influence on track occupancy systems disregarding whether track circuits or axle counters are used on stations and along the railway sections between stations.

The IT support for safety starts with remote control and remote monitoring of devices in power supply substations and sectioning points and of different kinds of electrical switches used for maintenance and for protection e.g. against overvoltage due to lightning.

Operational safety management aspects

Technical safety aspects	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
T1	x	x	x	x	x	x	x	x	x	x
T2	x	x	x	x	x	x	x	x	x	x
T3	x	x	x	x	x	x	x	x	x	x
T4	x	x	x	x	x	x	x	x	x	x
T5	x	x	x	x	x	x	x	x	x	x
T6	x	x	x	x	x	x	x	x	x	x
T7	x	x	x	x	x	x	x	x	x	x
T8	x	x	x	x	x	x	x	x	x	x
T9	x	x	x	x	x	x	x	x	x	x
T10	x	x	x	x	x	x	x	x	x	x

Fig. 3. Safety matrix 10-by-10 safety aspects marked grey are to be taken into account before introduction of the 25 kV 50 Hz AC power systems. (own elaboration).

For all marked areas both safety and security needs to be analysed as well as cybersecurity in case of technical solutions, which are using electronic and/or programmable technical means.

On the basis of those areas and different kinds of incorrect technical states of systems and devices constituting "Energy" subsystem as well as malfunctioning of interfaced systems and wrong functioning of interfaces as well as on the basis of possible external circumstances detail list of hazards have to be prepared for the defined technical solution before it is installed. Preferably before it is designed as already at design phase additional technical safety requirements and/or safety means probably need to be taken into account.

2.3 The 25 kV 50 Hz AC power supply hazard log

Identification of hazards is a first step in system approach to safety. Usually all identified hazards are grouped and put into big tables reflecting their step by step analyse up to the statements, which are influencing everyday operation as well as ever and again maintenance and repair. Proposed step by step approach is shown as a table on Fig. 4.

	T1/O3				T1/O2					T1/O7			T2/O3
Identified hazards													
Associated functions													
Associated device													
Hazard description													
Hazard reasons													
Remarks													
Potential consequences													
Existing safety means													
Frequency level *)													
Severity category *)													
Risk acceptance *)													
Additional safety means													
Responsibility split **)													
Frequency level *)													
Severity category *)													
Risk acceptance *)													

Fig. 4. Step by step approach to hazards(own elaboration):
*) as defined in EN 50126 [13]
**) as defined in regulation 2013/402 [14]
and where T1/O3 means hazards which can occur due to malfunctioning of systems and/or devices and influence ensuring safety during operation; T1/O2 means hazards which can occur due to malfunctioning of systems and/or devices and influence safety during maintenance and operation after maintenance; T1/O7 means - hazards which can occur due to malfunctioning of systems and/or devices and influence activities in case of emergency. And T2/O3 and following areas have to be understood in a similar way.

Identification of hazards have to take into account safety related hazards, security related hazards and cybersecurity hazards for systems and devices within "Energy" subsystem and its interfaces. Each hazard has to be named and put into a table which will form a hazard log. Each identified hazard has to be well understood and therefore it is necessary to point all functions and all systems and devices which are

associated with individual hazards. It is important to see not only main functions and devices but also other ones which are affected because risk analyses on the basis of the RAMS standard [13] cannot be applied independently of hazards which are dependent from each other.

Each hazard has to be described. As a result tables describing hazard logs are usually big and difficult to be printed. For instance for constructioning of the four track coverage between Gdańsk Główny and Gdańsk Śródmieście the hazard log can be printed on A0 format paper with font 10 on 12 pages. This makes such analyses quite complex, but as a result of such analyses a number of design and technical changes are being introduced e.g. for quoted coverage as a result of risk analyse even concrete has been changed.

For each hazard primary and secondary reasons have to be pointed. The reasons are important for the identification of the hazards with common reasons. Hazards which occur due to the same reasons have to be analysed together especially from the point of view of safety measures and risk level acceptance. Appropriate remarks have to be put in hazard log.

Identification of each hazard has to be concluded by pointing and describing potential hazard consequences as well as existing safety means which protect against those consequences. This closes identification of hazards and forms a basis for risk analyse.

As risk is associated with frequency and severity of occurrence of a hazard respective analyses have to be done for each hazard and reflected in hazard log.

Frequency levels defined in RAMS Standard [13] are following: *frequent (likely to occur frequently), probable (will occur several times), occasional (likely to occur several times), rare (likely to occur sometime in the system life-cycle), improbable (unlikely to occur but possible) and highly improbable (extremely unlikely to occur)*. Pointing frequency level has to be based on expert judgement. As such judgement is important for risk acceptance choosing experts for risk analyses is a tricky decision which has to be based on judgement of experts' experiences. Therefore it is usually treated as setting "council of elders".

As risk is based on frequency and severity the next step is to define severity category for each hazard. Severity categories defined in RAMS Standard [13] are following: *catastrophic (affecting a large number of people and resulting in multiple fatalities, and/or extreme damage to the environment), critical (affecting a very small number of people and resulting in at least one fatality, and/or large damage to the environment), marginal (no possibility of fatality, severe or minor injuries only, and/or minor damage to the environment) and insignificant (possible minor injury)*.

The frequency levels and severity categories form a basis for risk acceptance, which is on this basis defined as intolerable, undesirable, tolerable or negligible and associated respectively with following activities: *intolerable - risk shall be eliminated; undesirable - risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority; tolerable - risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders; negligible - risk is acceptable without the agreement of the railway duty holders*.

Risk acceptance judgement is usually marked by making respective cell red for intolerable risk, yellow for undesirable and tolerable risk and green for negligible risk. Colours allow quick understanding where additional analyses are necessary. For all hazards for which risks is red additional safety measures have to be defined. Such measures may be used to lower probability of hazard occurrence and/or hazard potential consequences. After adding such measures, e.g. after re-design or adding extra filters or redundancies, frequency levels and severity categories have to be defined for such hazard once more. As re-design may change frequency and consequences for other hazards such second step is due to cover not only hazards with red risk but all of them.

Moreover second step is used also to verify the yellow risks. They are acceptable under certain circumstances which are associated mainly with split of responsibility. Usually they are based of shifting responsibility from constructioning entity to user. A good example is to point firefighting equipment and backup power supply e.g. for control equipment. Of course they have to be provided during construction, but during years of operation they have to be checked and maintained in appropriate way and in appropriate moments. Shifting responsibility is very important as such information in hazard log gives certainty, that further user includes such activities in his internal regulations, which have to be supervised by infrastructure manager safety management system required as a basis of the safety authorisation without which offering railway infrastructure for railway transport is legally forbidden.

3 Conclusions

Introduction of the 25 kV 50 Hz AC power supply have to be carefully prepared and cannot be based on foreign technical regulations only as it has to work in a different environment e.g. different signalling equipment which work cannot be affected by power supply insulated returns. As a result detail analyses should be undertaken already now. It is proposed to start from an overall safety picture defined by 10-by-10 matrix defined by author in previous publications. Based on that it has been shown that: malfunctioning, construction, and electrical safety as well as preventing unauthorized access and fire, ensuring power supply/signalling interaction safety and ensuring IT support for safety have to be taken into account and analysed in relation to all possible hazards which may occur during 25 kV 50 Hz AC power supply operation and maintenance as well as during activities in emergency situations. It is proposed to create a hazard log and use the frequency and severity concept for accepting individual hazards on the basis of risk acceptance and shifting some well-defined

responsibilities to the future user of the new type of power supply based on 25 kV 50 Hz AC traction solutions. As a result effectively paper proposes use of a scientific comprehensive approach to risk assessment and evaluation for the 25 kV 50 Hz traction system introduction.

References

1. M. Lewandowski, *Traction solutions for high speed railways [Trakcje w kolejach dużych prędkości]*, Logistyka, **3**, 1301-1305 (2012) [in Polish]
2. Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (EU OJ L 191/1 of 18 July 2008) with further changes (which is to be superseded by Directive (EU) 797/2016)
3. COMMISSION REGULATION (EU) No 1301/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'energy' subsystem of the rail system in the Union
4. European Standards dedicated to traction stationary equipment: PN-EN 50119:2009/A1:2014-01 (overhead contact line); PN-EN 50122-1:2011/A1:2011 (electrical safety); PN-EN 50149:2012 (contact lines); PN-EN 50163:2006 (traction power supply voltages)
5. European Standards dedicated to traction mobile equipment: PN-EN 50317:2012 (dynamics between pantographs and contact lines); PN-EN 50318:2003 (validation of simulations); PN-EN 50367:2012 (pantograph and contact line interoperability)
6. European Standard PN-EN 50388:2012 dedicated for coordination of electrical protection of stationary and mobile traction equipment
7. Leaflets of the International Union of Railways (UIC) dedicated to traction power supply: UIC 600 - Electric traction with aerial contact line; UIC 606-2 - Installation of 25 kV and 50 or 60 Hz overhead contact lines; UIC 616 - Rules for electric traction equipment; UIC 618 - Rules for traction transformers and reactors; UIC 642 - Special provisions concerning fire precautions and fire-fighting measures on motive power units and driving trailers in international traffic
8. COMMISSION REGULATION (EU) No 1303/2014 of 18 November 2014 concerning the technical specification for interoperability relating to 'safety in railway tunnels' of the rail system of the European Union
9. M. Pawlik, *Bezpieczeństwo kolei w kontekście powiązań pomiędzy dyrektywami o bezpieczeństwie kolei i o interoperacyjności kolei, analiza z punktu widzenia zarządzania bezpieczeństwem [Railway safety in the context of relationships between railway interoperability directive and railway safety directive, analyse from the point of view of safety management]*, Przegląd Komunikacyjny [Transport Review], **9**, 11-20 (2016) [in Polish] ISSN 0033-22-32
10. M. Pawlik, *Safety, security and cybersecurity in railway operation*, Safety and Reliability – Theory and Applications (Taylor & Francis Group, London, 2017) ISBN 978-1-138-62937-0
11. Wheel – description of the "SMS Wheel" tool prepared for verification of the Safety Management Systems of the railway companies, and disclosed by the Railway Agency of the European Union http://www.era.europa.eu/tools/sms/Pages/SMS.aspx#SMS
12. 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) (EU OJ L 164/44 of 30 April 2004) with further changes (which is to be superseded by Directive (EU) 798/2016)
13. EN 50126-1:1999 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (which is to be superseded by FpprEN 50126-1:2017)
14. Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 (EU OJ L 121/8 of 3 May 2013) with further changes 3.5.2013