Evaluating Key Factors Influencing ERTMS Risk Assessment: a Reference Model

Katja Schuitemaker
Design, Production and Management Department,
University of Twente
Enschede, the Netherlands
e-mail: k.schuitemaker@utwente.nl

Heidi van Spaandonk
Safety Department,
ProRail
Utrecht, the Netherlands
e-mail: heidi.vanspaandonk@prorail.nl

Marco Kuijsten
Safety Department,
NS,
Utrecht, the Netherlands
e-mail: marco.kuijsten@ns.nl

Mohammad Rajabalinejad
Design, Production and Management Department,
University of Twente
Enschede, the Netherlands
e-mail: m.rajabalinejad@utwente.nl

***Abstract*— The European Railway Traffic Management system (ERTMS) aims to replace the various national train command and control systems in Europe, and will serve to improve cross-border interoperability, with the final aim of improving the competitiveness of the rail sector. As an additional effect, it is argued that implementation of ERTMS will improve safety. To provide insight into safety developments within the European railway system, this study evaluates ERTMS at both the national and international levels. For this purpose, international data from European ERTMS implementations is combined using data obtained from interviews with ERTMS stakeholders and safety experts from the Netherlands. Effects of the safety case regime, interoperability, deregulation and dynamic specifications on the European railway system have been researched. We present our findings into a reference model that describes the existing situation and shows what key factors are most suitable to improve the situation. The challenges are to improve resilience, to generate more awareness of interrelationships between hazards and risks, but even more: comprehending the safety architecture and creating cross-discipline understanding.**

Keywords - ERTMS; railway safety; interoperability; risk management.

I. INTRODUCTION

This paper is an extension to the work presented at the Seventh International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO) 2017 conference [1]. Safety has always been one of the key priorities in the railway industry. There have been many initiatives to improve railway safety in the Netherlands, some of them which are listed below:

- Reducing the number of train-on-train collisions by, among other actions:
  - Implementation of the Routelint system: providing train drivers with real-time information about nearby trains.
  - Implementation of the improved version of the Dutch Automatic Train Control System (ATB Vv).
- It has been argued that the implementation of the European Railway Traffic Management System (ERTMS) has beneficial effects on the overall safety level of the railway system [2]. As ERTMS seems to hold great promise at both the Dutch national and international levels, we will discuss this system in more detail.

The European Union (EU) has adopted Directives concerning the interoperability of the European railway system and railway safety. The implementation of these Directives is aided by committees such as the European Committee for Electrotechnical Standardization (CENELEC). The CENELEC European Norm (EN) 5012x is a family of standards that contain requirements and recommendations concerning processes to be followed for the development and assurance of safety-critical systems. As part of CENELEC, the EN50126 (The Specification and Demonstration of Reliability, Availability, Maintainability and Safety) describes a performance-based approach that includes proactive argumentation on why a system is acceptably safe. The railway industry in the Netherlands tends to follow the safety case regime recommended in EN50126. As early as the 1990s, the European Commission (EC) decided that passenger trains should be able to travel seamlessly across international borders in Europe. In 1998, the EC requested the foundation of the Union Industry of Signalling (UNISIG) and assigned this with the task of drafting the technical specifications for ERTMS. The International Union of Railways states that the goal of ERTMS is "to enhance cross-border interoperability and signalling procurement by creating a single Europe-wide standard for railways with the final aim of improving competitiveness of the rail sector" [3]. ERTMS is a command, control, signalling, and communication system for railway management and safe regulation. It is composed of two technical layers:

- European Train Control System (ETCS): the Automatic Train Protection (ATP) system that makes sure trains do not exceed safe speeds or run too close together.
- Global System for Mobile Communications – Railways (GSM-R): helps provide communication for voice and data services.

Beyond these two technical layers are the European Operating Rules (EOR) and European Traffic Management Layer (ETML).

ERTMS implementation can vary in:

- Level: basic concepts of the ERTMS.
- Baseline: corresponds to the version of the technical specifications.
- Version: modification of properties.
- Operation mode: various conditions required for managing various situations.

ERTMS has become the European standard for the Automatic Train Control (ATC) that facilitates an interoperable railway system in Europe. This means that ERTMS allows trains to run across borders without changing their control systems. Recently, the ERTMS European Deployment Plan (EDP) has set targets that by 2023 50% of the core network corridors will be equipped with ERTMS. The aim is to implement ERTMS Level 2 on key routes in the Netherlands by 2028. With these aims in mind, there is the promise of an increase of railway safety by implementation of ERTMS, which self-evidently would be very beneficial for railway industry and the general public. Some reasons why ERTMS is considered to increase railway safety include:

- ETCS supervises both the position and speed of trains to make sure they continuously remain within the allowed speed and distance limits, and, if necessary, it will command the intervention of the braking system to avoid any collision [2]. The train can continually receive authorisation to continue running at maximum allowed speeds through the GSM-R system (only available at ERTMS level 2 and when driving in the correct operation mode).
- Reduce the risk of human error [4]; for example, work-related errors caused by stress, tiredness, fatigue, and sleep disturbance.
- Decreasing the number of Signals Passed At Danger (SPADs) [5][6]. This can be explained by the fact that ETCS is able to intervene in the braking curve for a train driving at any speed.

However, there is evidence that implementation of ERTMS does not automatically mean a safer railway system. For example, in practice, in the Netherlands, SPADs still occur when driving with ERTMS [7], see Table I.

TABLE I. SPADs UNDER ERTMS

	2013	2014	2015	2016
SPADs under ERTMS Level 1	1	0	1	4
SPADs under ERTMS Level 2	9	10	16	15

However, these numbers are low, so they can only be considered as an indication, and not necessarily representatives of a trend. More studies, both scientific and industrial, question the safety benefits arising from the implementation of ERTMS.

At the international level:

- Smith et al. addresses issues relevant to the safe introduction of ERTMS into European railway systems [8]. These issues include technical system integration, technical system failures and human factor considerations.
- Laroche and Guihéry study the European Transport Policy, the role played by the EC, and the ERTMS innovation process in relation to innovation processes in surface transport, and the difficulties inherent in the implementation of an intelligent transportation system innovation [9].
- Ghazel addresses the regular evolving documents that give rise to successive ERTMS versions [10].
- The EC itself has studied past and current problems resulting from ERTMS implementation [11].

At the Dutch national level:

- The Ministry of Infrastructure and the Environment, ProRail and NS have collected information on ERTMS standard usage for safety systems, and the effects on various goals of the Railmap 1.0 [12].
- ProRail and NS executed a pilot to gain experience with driving under ERTMS [13].
- A specialised team investigated the sequence of events and decision-making processes in the Netherlands that have led to delays in deployment of the ERTMS train signalling systems in the High Speed Line (HSL) railway project [14].

This study evaluates the effects of the safety case regime, the inclusion of various ERTMS specifications, the exclusion of a responsible integrator, deregulation, and the final effects for risk assessment and safety. The focus is on risk management and safety of ERTMS as a System of Systems (SoS). We bring all our findings together and represent them into a reference model that illustrates the main line of argumentation. This reference model points out the key factors that are most suitable to address in order to improve the situation.

Section II provides an overview of the background of railway deregulation, ERTMS specifications, European interoperability, and cost reduction that are the results of changes in organisational behaviour. The methodology is discussed in Section III. Section IV explains findings with regard to the number of stakeholders and accompanying views, interests and interactions, possible local goal trade-offs, various interpretations, the decision-making processes, borders between disciplines leading to unique design realisations, and the relationship between overview and safety architecture understanding. Findings are discussed in Section V. Section VI summarises the findings, draws conclusions and highlights challenges.

II. BACKGROUND

Every railway system faces technical, managerial, organisational, and regulatory challenges. The subsystems can work perfectly individually, but together they can create a hazardous state. Many factors, both technical and socio-institutional, need to be combined to turn the challenge of one European train system into a great success, satisfying social needs for lower costs, better utilisation of infrastructure, and less complex logistics [15]. During this study, several developments in the rail industry appeared to have a great effect on the safety level of a railway system including ERTMS.

A. Deregulation

Regulation is required to prevent monopoly exploitation, to reduce asymmetry of information, to guarantee non-discriminatory access to any essential facilities and to monitor the performance of a service provider [16].

Deregulation is the reduction or elimination of government power in an industry, usually promoted to encourage more competition within a specific market. Starting in the 1990s, in order to promote greater competition, the rail industry in Europe has been gradually restructured. On the one hand, vertical separation means that the management and ownership of infrastructure are totally separated from the operation of passenger and freight rail services. On the other hand, multiple operators are using the infrastructure. In some countries, infrastructure has been separated from train operations, whereas in others, this has not been the case. Privatisation and deregulation have led to an increased involvement of private actors, both nationally and internationally [17].

B. ERTMS specifications

The Union Industry of Signalling (UNISIG) was founded in 1998/99 at the specific instigation of the European Commission (EC) [18]. It was created to develop ERTMS specifications. The final version of ERTMS specifications was published by the EC following the approval of the Member States. In November 2012, the EC intentionally deleted ERTMS Functional Requirement Specifications, making these specifications no longer mandatory. The remaining System Requirements Specifications are written in a natural language. These specifications allow multiple interpretations [19].

C. Interoperability

The meaning of interoperability is two-fold. On the one hand, interoperability refers to a geographical interoperability among countries and among projects. On the other hand, it also refers to interoperability among suppliers. This opens the supply market and increases competition within the industry [20]. The result of this is the absence of a single entity that is responsible for the railway system as a whole.

D. Safety case regime

The safety case approach is goal-oriented, meaning that organisations should always seek for improvements in safety. It requires a detailed hazard analysis comprising causal analysis, a dedicated hazard identification focusing on the system under consideration, and a common cause analysis. A hazard is a potential source of harm in a system. Hazard identification is performed during risk assessment and within hazard control. The results of risk assessment are a set of safety requirements that define the required efficiency of safety functions. These can be assessed both quantitatively and qualitatively. Taken into consideration the identified hazards, risks should be reduced to an acceptable level. It has to be demonstrated that the risk is reduced to 'As Low As Reasonably Practicable' (ALARP). In the end, one is able to argue whether the system is acceptably safe.

E. Cutting cost and time

According to Rasmussen, systems and organisations continually experience change, as adaptions are made in response to local pressures and short-term productivity and cost goals. Several accidents such as Bhopal, Flixborough, Zeebrugge, and Chernobyl demonstrate that they have not been caused by a coincidence of independent failures and human errors, but by a systematic deterioration of organisational behaviour towards an accident under the influence of pressure towards cost-effectiveness in an aggressive, competitive environment [21].

In order to reduce the risk, Dutch national safety goals are approached through use of the ALARP-principle and standstill-principle. This means that all risks must be reduced such that they are below a threshold of practicability. For risks in the "ALARP area", all potential risk reducing measures must be evaluated in terms of cost efficiency, cost-benefit balance or some similar economic measure. Selected risk-reducing measures may be introduced based on experience or best practice in combination with cost-efficiency considerations [22].

III. METHOD

The objective of this empirical research is to identify key factors and interrelationships of the safety of ERTMS. Emphasis was placed on the ERTMS safety architecture, and the relationships between social and technical safety entities of ERTMS at both the Dutch national and international levels. The findings in this paper are based on international data from European ERTMS implementations, linked with national data obtained from semi-structured interviews based on questionnaires.

To investigate the nature of phenomena, we adopt qualitative and quantitative analysis methods in the form of standardised interviews. We used an interview guide with a list of questions generated in advance, allowing the same topics to be covered during interviews, and at the same time, if necessary, leaving room for more exploration of certain issues. This interview guide consisted of a brief description on one's background and relationship with ERTMS, open questions with regard to pros and cons of ERTMS, and more detailed question to cover specific topics. For this research, the data are transcribed and analysed using Grounded Theory data analysis [23]. By constant comparison, every new piece of data is compared with earlier data to find similarities and differences. The data was used for formulation of hypotheses, and hypotheses are verified logically on internal validity and external validity.

The topics discussed include the effects observed from inclusion of various ERTMS specifications, the exclusion of a responsible integrator, deregulation, and the final effects for risk assessment and safety. Systems under consideration are ERTMS Level 1 and ERTMS Level 2. Projects discussed during interviews are the five ERTMS-projects in the

Netherlands (Betuweroute, Port of Rotterdam, HSL South, Amsterdam-Utrecht and Lelystad-Zwolle).

Participants were Dutch ERTMS key stakeholders and safety experts from the Ministry of Infrastructure and the Environment, train operating companies, infrastructure managers, and independent consultants involved with the ERTMS national program, each representing their own viewpoint. For increasing validity and minimising subjectivity, we ensured each topic was discussed from various points of view (political, company, management, operations). The average number of years of experience of the participants varies from 2 to 14, with an average of 8. The educational background was mostly technical or safety related, with a few exceptions. Participants are informed about the aim of this study beforehand the interview. Also, it was explained that they should have in mind their own expertise when answering the questions, meaning, they should respond from their own viewpoint, not from someone else's viewpoint. Contact between researcher and participants has been direct.

Interviews lasted between 30 and 90 min. Data was collected between February 2016 and August 2016. In total, 15 semi-structured interviews were held, performed face to face. All interviews were audio recorded, transcribed verbatim, and summarised. Transcriptions were processed through qualitative inductive content analysis in order to develop a theory, and identify themes through repeated examination, comparison, abstraction, and data reduction. The material was abstracted and reduced to a set of themes. Resulting themes were quantified and integrated with the responses. The procedure was repeated to refine chosen themes. Two main categories were identified as a thread through transcriptions: (1) implications with regard to socio-technical safety; and (2) implications with regard to the safety architecture. Using the Design Research Methodology [24] as a supporting framework, key factors found were translated into a reference model, which graphically shows the current understanding of the safety challenges of ERTMS.

As for verification, summaries were send to the interviewee. Most interviewees made small corrections in the summaries. The reference model is logically verified by consistency, meaning there are no internal conflicts between interview answers, key factors and well-established literature. For this literature review, the high level goal is to identify supporting evidence and contradictions. For the search string:

Part 1

The first part captures keywords related to the system under consideration such as "*European Railway Traffic Management System*", "*ERTMS*" or "*ETCS*".

AND

Part 2

The second part captures keywords related to safety such as "railway safety", "safety case", "safety analysis", "*risk assessment*", "*risk analysis*" or "*risk evaluation*".

OR

Part 3

The third part captures keywords related to complexity and interdisciplinary such as "*architecture*", "*socio-technical safety*", "*decision-making process*", "*integral assessment*".

Next to this, we also verify logically on internal validity with the meaning of causes and effects of key factors that could be interchangeable, and external validity with the meaning of participant- and time dependency.

IV. FINDINGS

To obtain an understanding of the existing situation, we represent our findings by the creation of a reference model. This reference model consists of key factors and links among key factors that can come from resources, assumptions, or the experiences of stakeholders. In the end, many key factors influence safety of ERTMS, and result in a high complexity. A graphical representation is created to provide an overview. In order to limit the amount of information, this representation is divided into two parts: a lower part, and an upper part.

A. Reference model lower part

Next, we discuss the lower part of the reference model, representing implications with regard to socio-technical safety. Key factors identified include effects of the safety case regime and ERTMS specifications, and how the decision-making processes and missing integrator influence risk assessment.

1) Safety case regime

The safety case is the documented demonstration that the product, system or process complies with the relevant safety requirements. It can be seen as a risk- or hazard management framework, where the organisation identifies controls to deal with identified hazards and measures. Such controls must ensure the continued working of safety-related functions. The Netherlands evaluates risks using the ALARP-principle, described by EN50126, allowing cost-effectiveness of safety measures to be explicitly considered. In order to classify risks, hazards are categorised on frequency and severity, resulting in a risk matrix. High risks require mitigation or risk acceptation. The European Union Agency for Railways explains a shift from quantitative data to qualitative data [25]. As a result, organisations must come up with descriptions instead of numbers and observe data rather than just collecting data. This qualitative data is based on the logical reasoning of many experts. Stakeholders experience this regime as a challenge, as logical reasoning can cause multiple interpretations. Also, they experience the safety case approach as complex and time-consuming. For example, in practice, the safety case for the High Speed Line South resulted in only addressing major hazards due to time pressure [26].

Barua explains that one disadvantage of the safety case approach is that the explanation and interpretation of the desired performance levels expressed in the regulation can be both complex and challenging [27]. Nair identifies 25 studies citing ambiguities in the application of standards, such as the existence of multiple interpretations of the evidence requirements in the standards [28].

According to the ERTMS strategy group in Great Britain, initially the principal motivation for ERTMS was to further improve safety. "Over approximately the last ten years, capacity became a more significant influence and then, more recently, cost reduction [29]." Demonstration of compliance by reference to safety standards is usually costly and time-consuming [30]. Pressure towards cost-effectiveness can inadvertently lead to generating adaptive responses. According to Leveson [31], pressure towards cost-effectiveness and increased productivity is the dominant element in decision making.

2) ERTMS specifications

ERTMS is not fully specified. Rather it is a system architecture, which describes how a range of elements should function. Earlier studies explained that ERTMS specifications are unstable [9][32], written in informal language [10], non-consolidated [8] and incomplete [15][33]. To be more specific, missing parts concern management, integral system integration, and physical design. Therefore, stakeholders still claim that the specifications are not sufficient. These specification deficiencies have effects on system safety in the three ways described below.

- The management of railway signalling in ERTMS is not based on global rules, meaning they are customised to each country. Every country uses its own interpretation of the European Norm (EN) 50126. It is therefore difficult to compare the systems in terms of safety.
- As for system integration, the lack of harmonised specifications requires the development of various solutions for each project. As for safety, this implies a need for additional safety analyses.
- Open specifications that exclude physical design, result in unique ERTMS design realisations, and the occurrence of not fully compatible solutions for each system to be developed. Again, this implies a need for additional safety analyses.

In practice, updates to new systems are postponed in anticipation of new specifications, covering multiple requirements through one update. Experts explain that unstable specifications make it difficult to adopt innovations and that problems occur with adapting the new system to the old one. There is consensus among experts about the effects of the inclusion of various ERTMS specifications on the safety of the System of Systems (SoS). 93% of the participants explained the relationships between a high variety of ERTMS specifications and the decision-making process.

3) Decision-making

Today's ERTMS requires strategic safety decisions concerning functionality and policies. This process is based on criteria resulting from risk analyses, and organised through a specified organisation. Experts explain the open specifications complicate the architecture, but also safety decision-making processes. As a consequence of incompleteness, it could be possible to make a decision based on implicit factors. For example, as safety is sometimes seen as hindrance to effective marketing solutions, the focus can be on finishing on time and approving a design. In the case of a complex architecture, it can be difficult to identify hazards and what control measures must be taken by whom. Care should be taken that risk is evaluated using complete information.

According to the parliamentary commission that looked at the failed Fyra project, it seemed that safety had become a subject for negotiation [34]. As also described by Nusser [35], "Black box" approaches are regarded with suspicion – even if they show a very high accuracy of available data – because it is not feasible to prove that they will show a good performance under all possible input combinations.

Late safety inclusion is also questioned by Enserink in the context of major projects in the Netherlands: "It is strange to see how in many large projects, such as the Westerschelde tunnel, the Betuwelijn, and the 'Groene Hart' bored tunnel for the High Speed Line South, the discussions of safety issues and safety management took place at a very late stage in the project cycle" [36]. He also explains: "In all the examples in the planning phase, the analysts neglected the safety issues or these issues were temporarily stalled because of their complexity." According to Høj et al.: "Biased results may result from excluding certain events, different analytical methods and data, different modelling assumptions, different methods for including uncertainties, best estimates vs. estimates "on the safe side", etc." [37].

4) Integrator

EN50126 describes a simplified approach that helps organisations to conduct risk assessment and hazard control. This approach, the so-called hourglass model, provides an overview of the major safety-related activities that are required to reach an acceptable safety level for a technical system, including defining the corresponding responsibility areas. This hourglass model is shown in Fig. 1. This model provides an overview of major safety-related activities that are needed to ensure an acceptable safety level for a technical system, including the corresponding responsibility areas. As shown, responsibilities overlap. According to EN50126, risk assessment should be done at the railway system level, where it relies on system definition, and includes risk analysis and risk evaluation. This risk analysis includes hazard identification, consequence analysis, and the selection of risk acceptance criteria. Hazard analysis at the level of the system under consideration includes a causal analysis, hazard identification focusing on the system under consideration, and a common cause analysis. CENELEC requires that, during each project, responsibilities have to be clarified unambiguously in order to avoid gaps or overlaps.

The Dutch ERTMS program is a collaboration of stakeholders, not as if it were a single person that acts for certain purposes. Experts explain that without the ERTMS program being a legal entity, it is difficult to allocate hazards and risks, especially the ones on interfaces, to a responsible stakeholder. As for the Netherlands, what makes this even more difficult is a missing central designer, or indeed any party, that knows the entire complex system. Although the Common Safety Method (CSM) aims at an integral safety approach, the final report on the ERTMS pilot between Amsterdam and Utrecht explains that "overarching processes

between railway and train transportation are missing and that these are necessary for optimum implementation of ERTMS" [13]. One of the safety case principles is that those who create risks are responsible for controlling those risks. Experts explain that as a result, organisations feel responsible for their own processes, not for the integral railway system.

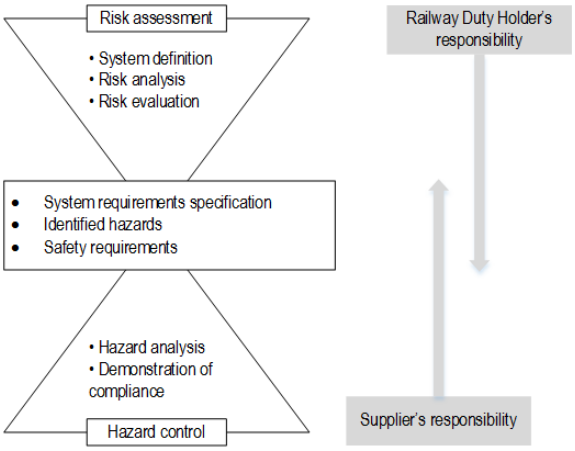

Figure 1. Hourglass model described by EN50126.

Lack of responsibility is also recognised by the Dutch Ministry of Infrastructure and the Environment [13]. This is a known challenge explained by Harvey: "Complexities at the organisational level can breed a culture in which no-one is willing to accept responsibility for risk and blame is always shifted to a higher level in the network [38]."

Next to the hourglass model, safety activities tend to be performed in parallel with systems engineering activities [39] [40]; see Fig. 2. Shown is the left side of the V-model [41]. Squares on the right represent well-known stages in system development. Squares on the left represent safety activities executed during each of the system development stages. For example, safety engineers analyse requirements for hazards and communicate these to system designers. According to Mauborgne et al., who defined a missing link between safety and systems engineering, the two activities are not always well integrated [42]. Experts explain communication of safety integration in the development phase as a challenge, especially with regard to defining interfaces.

Communication both within development teams and between individual developers is considered to be a source of safety-related faults in critical systems [43] [44]. According to Leveson, the defence community tried using the standard safety engineering techniques on their complex new systems, but the limitations became clear when interface and component interaction problems went unnoticed until it was too late, resulting in many losses and near misses [31].

5) Risk assessment

The generation of adaptive responses, complexity in decision-making processes and a missing overarching view affect risk assessment in the three ways discussed below:

- First, adaptive responses can depend on a number of assumptions. Such assumptions can be explicitly formulated, but the danger is in including these without being subject to uncertainty. Describing and making judgements about risks in advance can misguide risk assessment.
- Second, the decision-making process and risks assessment process are not always interrelated, resulting in a missing integral assessment in the Netherlands.
- Third, risk assessment must be performed at the railway system level. Experts indicate the challenge lies in the incorporation at the System of Systems (SoS) level, which requires an overview of all safety entities to be considered.

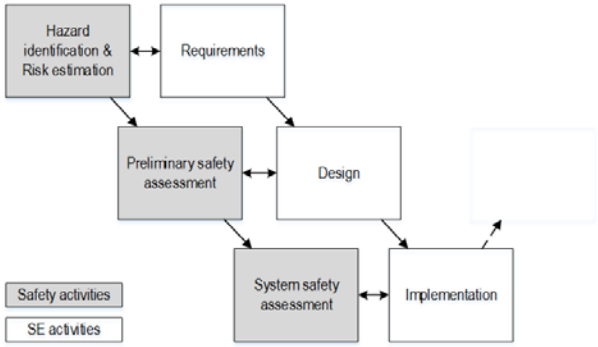

Figure 2. Relationships between safety and SE activities [38][39].

For example, misjudgements happened in relationship to the Piper Alpha accident in 1988: a series of events considered of low risk prior to the accident. Adaptive responses lead ultimately to related problems, having unforeseen ramifications in addition to system complexity, and therefore, to further unexpected behaviour, which reduces system safety [45]. At the technical level, much attention is given to safety issues, but hardly any attention is paid to safety at the level of decision-making [36]. According to Aven, the benefits related to the activity studied, as well as strategic and political aspects could be decisive for the decision making but may not be captured by risk assessment [46]. According to Harvey, the many and varied interactions among the individual components of a SoS produce emergent behaviour, which cannot be predicted on the basis of the performance of the individual subsystems in isolation [38].

The described relationships are shown in the lower part of the reference model of ERTMS in Fig. 3. This reference model represents the existing situation on implications with regard to the socio-technical safety of ERTMS. All ellipses represent key factors meaning those influencing factors that are considered as the core factors or root causes. The links describe the existing relationships. Not all relationships come from direct experiences. Therefore, these relationships are indicated as an assumption. The existing qualitative value of a key factor is represented by means of a '+' or '-'. For example, the '+' next to 'number of different ERTMS inclusions' indicates a high degree. Quantitative classification of whether or not participants experience a challenge in one of the key factors is shown in Fig. 4.

B. Reference model upper part

Next, we discuss the upper part of the reference model including implications with regard to the safety architecture.

Key factors identified include the effects of the deregulation and the increased number of stakeholders with their own specific languages and cultures. Also, how dynamic specifications have resulted in unique design realisations. We argue how the quality of overview influences risk assessment, and therefore, the overall safety level of ERTMS. Some key factors are safety related items that fundamentally contribute to a successful system operation [47].

1) Deregulation

Available historical data on fatal railway accidents has shown a solid gradual improvement in railway safety over the past three decades. However, this trend has slowed down since the late 1990s [48]. Increasing regulation, standardisation and systematisation have paid safety dividends, although an adverse effect is the increase in regulation. Safety regulation has increased a hundred-fold between 1947 and 2008 [49]. Experts indicate the deregulated organisation results in many stakeholders. As is also concluded by Iglesias [50], incomplete/unstable specifications of ERTMS are further hampered by company specific requirements.

2) Number of stakeholders

At the national level, the change from one national actor to multiple commercial actors shows an increase in operators (CFL, NS, SNCB, etc.) using ERTMS tracks. Also, with previous Dutch automatic train protection (ATB) tracks, only one manufacturer (Alstom) was involved. With ERTMS and the tendering of subsystems, various manufacturers (Alstom, Ansaldo, Bombardier, etc.) are involved. Stakeholders within the ERTMS program include train operating companies, infrastructure provider and independent consultants. At the international level, infrastructure managers (Deutsche Bahn, INFRABEL, ProRail, etc.) from various countries must collaborate in order to provide a seamless transition.

In the first place, the rising number of parties involved entails a considerable diversity of points of view, skills, responsibilities, and interests. Experts explain the challenge lies with the many interests, creating the risk of compromising too much on safety. For example, the train derailment in Hilversum shows that the commercial character of maintenance, specifically the introduction of market forces, has led to an unavoidable interplay of forces. According to the Dutch safety board: “In this context, the train derailment in Hilversum teaches us that the related interests can gradually and unnoticed apply pressure on the management of safety risks [51]”.

3) Language and culture

Laurino explains that the historical world-wide railway framework is modified to country specific approaches to public policy, geographical context, transport system, economic situation, business and regulatory environment [52]. On top of this, countries use their own language, making intersectional challenges even more complex. Somerville describes that much of the work of professionals is knowledge-based and reflects their professional discipline, training and culture [53]. As an example, experts explain differences in both language and culture can lead to different people doing the same job, but working in different ways, leading to differences in understanding the overall risk assessment and evaluation. For this reason, risk perception can be different per organisation, even different per stakeholder.

For these reasons, at both the international level and national levels, stakeholders experience difficulties with understanding their respective systems. This is also described by Forsberg [4], who states that the new societal organisation, where rail transport is controlled by an increasing number of mainly private actors, intersectional issues and decisions have increased among the various actors. This happens particularly since mishaps or accidents are often caused by circumstances or weak links between them.

4) Boundaries

Experts explain the increased number of stakeholder viewpoints in ERTMS result in a complex architecture. They explain a system becomes complex when it is composed of many components that interact with each other. Complex intersections affect clarity of boundaries among subsystems within the system and between the system and its interaction with the environment.

Dekker explains that with increasing complexity, boundaries of what constitutes the system become fuzzy; interdependencies and interactions multiply and mushroom [54]. According to Rasmussen [21], people under pressure tend to explore and sometimes cross boundaries of safe operations.

5) ERTMS specifications

With the gradual implementation of a single signalling system through the EU, the EC has opted for radical innovation for all Member States. In the same vein, the Netherlands has opted for innovation in the form of a systems leap from traditional ATB to ERTMS. This can be contrasted with, for example, Belgium, which has opted for a more incremental development. Preferences vary at both the international and national levels. The signalling system for the Netherlands – Germany trajectories (remote monitoring) differs significantly from the signalling system for the Netherlands – Belgium – France trajectories (more autonomy for the train driver), which is more in line with ERTMS Level 2. Therefore, to migrate to ERTMS Level 2, France does not have to change much. To migrate to ERTMS Level 2, Germany and the Netherlands face a break with the past. Both the signalling systems and the automatic train protection systems are still markedly different from one EU country to another [55]. In addition, the various ERTMS levels include varying technical requirements and applications.

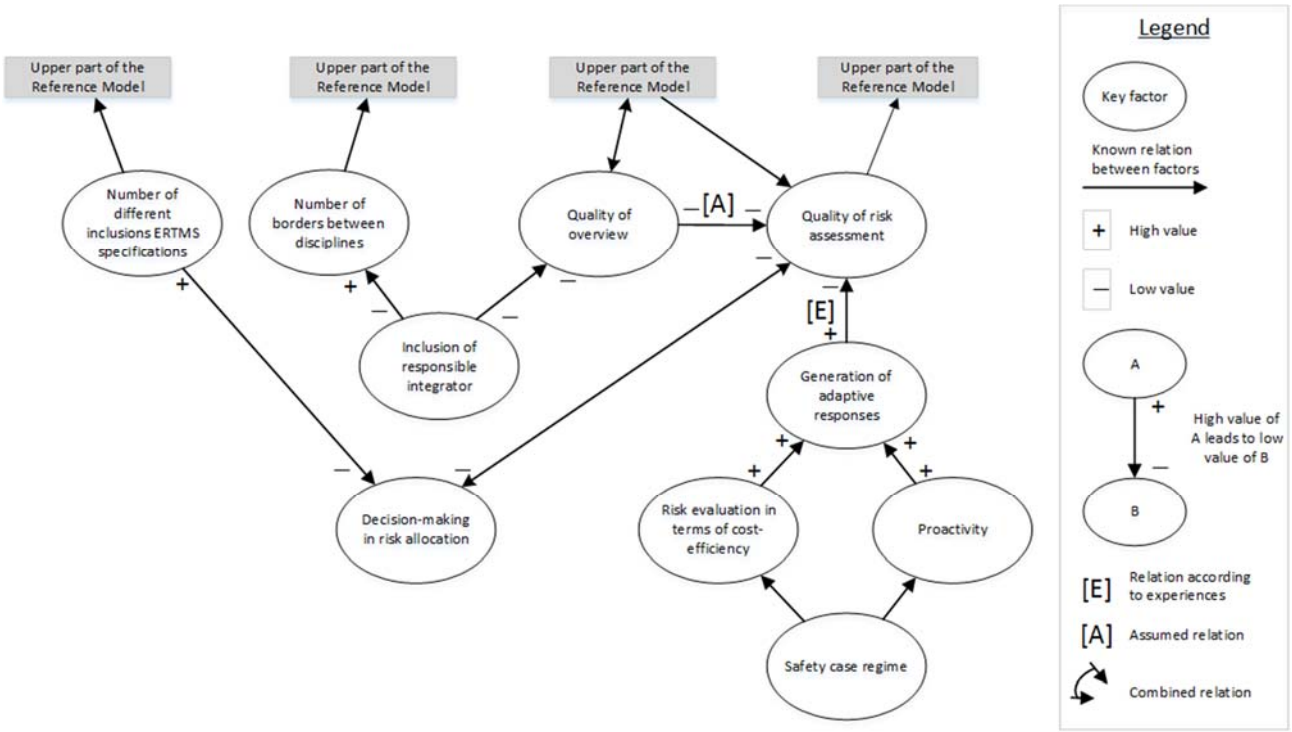

Figure 3. Lower part of the reference model on implications with regard to socio-technical safety of ERTMS.

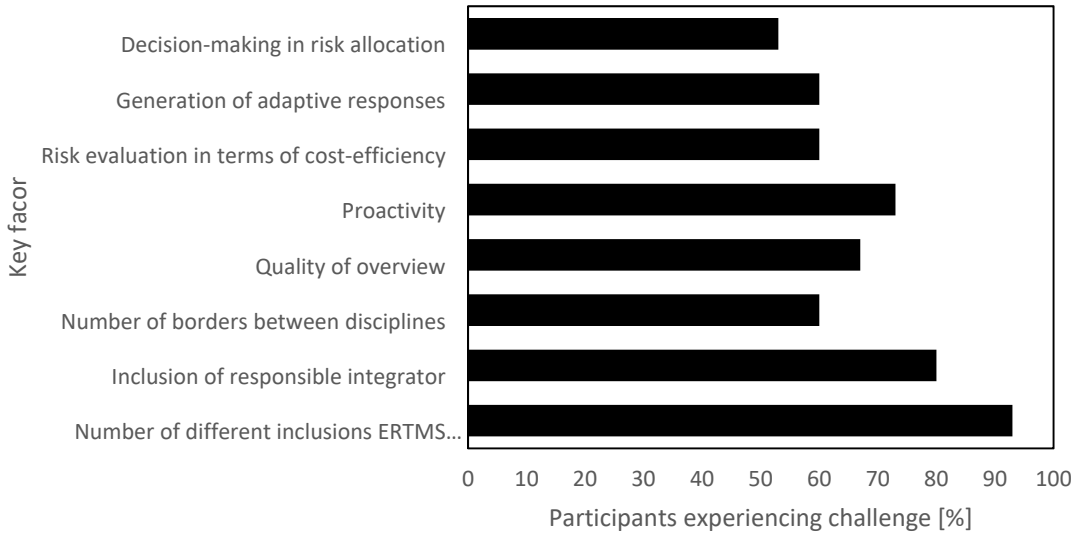

Figure 4. Participants experiencing challenges in key factors.

Various ERTMS subsystems have been tendered. In practice, the various stakeholders, even at the Netherlands national level where there have been 5 ERTMS-projects so far (see Table II), every subsystem is considered unique, and requires customised procedures and processes. Next to the 5 ERTMS-projects, Table II also shows which manufacturer was contracted, what ERTMS level was implemented, and when the track became operable.

TABLE II. ERTMS-PROJECTS IN THE NETHERLANDS

Project	Supplier	ERTMS level	In service date
Betuweroute	Alstom	2	2007
Port Rotterdam	Alstom	1	2009
High-Speed Line South	Thales/ Siemens	1 and 2	2009
Lelystad-Zwolle railway	Alstom	2	2012
Amsterdam-Utrecht railway	Bombardier	1 and 2	2013

The various levels have been defined to allow each individual railway administration to select the appropriate ERTMS/ETCS application trackside, according to their strategies, to complement their trackside infrastructure and to achieve the required performance [57]. Considering only permitted disparities, such as varying ERTMS levels (0, STM, 1, 1 infill, 2, 3), already result in 31 possible transitions; see Table III.

TABLE III. ERTMS POSSIBLE TRANSITIONS

To / From	0	STM	1	1 infill	2	3
0						
STM						
1						
1 infill						
2						
3						

Once a hazard scenario is identified, it is not trivial to identify all the possible causes in the system [33]. In other words, a system that is new, or particularly complex, can generate scenarios that are not generated during hazard analysis of previous comparable systems. Stoop also comments on the underestimation of ERTMS development: "There has been tension between incremental progress on the one hand and implementation in an existing railway network on the other hand with the ambitions on innovative ERTMS and public-private partnership" [14].

A higher level involves less side track equipment, but more on-board equipment. This change also implies that many of the costs of the signalling system will migrate from infrastructure managers to train operators. Infrastructure managers anticipating developments, whereas operators are reluctant to upgrade existing rolling stock [56], could be an explanation for the varying preferences.

6) Borders between disciplines

Experts explain employees are often focused on their own job. Ascribing meaning to data, so that it could be more readily used by others, is of less importance. Experts know a lot about their own subject, though knowledge of each component is limited. As a result, data is set and send to the next disciplines.

This is also explained by literature. As described by Baxter [58], borders between disciplines have been largely maintained despite efforts at creating interdisciplinary teams by involving domain specialists in the design process. The success of system implementation is dependent on effective cross-discipline communication. The borders between disciplines are a known challenge for the safety of Systems of Systems [41].

7) Comprehending the architecture

Problems often arise at these borders due to a lack of shared understanding among the developers of subsystems. Gaps in assumed knowledge can influence both understanding and integration. The majority of the experts (87%) indicated difficulties with comprehending the architecture, and how this low comprehension affected the accomplishment of their tasks. One of the safety architects tried to obtain insight, by creating physical overviews of the SoS.

Leveson [59] states that lack of shared understanding among the developers of subsystems create coordination problems, ambiguity, and conflicts among independent decisions.

8) Number of unique design realisations

In practice, various preferences and implementations of ERTMS subsystems result in many transitions among various subsystems. In other words, implementation is unique for every project, and dependent on stakeholders, the environment, and activities. Table III shows just a fraction of the number of possible transitions. As a result, systems can be incompatible. For example, the two implementations made by Alcatel (Dutch part of the railway) and Alstom (Belgium part of the railway) that differed too much, so that a so-called gateway (network node) was necessary to transition from one system to another.

As is also explained by Leveson [57], the interconnectivity and interactivity among system components implies that greater complexity leads to vastly more possible interactions than could be planned, understood, anticipated or guarded against. As also concluded by Smith [8], the existence of many versions of ETCS with technical problems require a backup system.

9) Number of procedures and processes

In the end, when using ERTMS, the complexity of technology, use, and processes of the railway system increases. Experts indicated that the technological developments in ERTMS are underestimated. A failure when using ETCS can have up to 100 causes. Train drivers and signallers must find a solution through applying difficult procedures and processes, while using limited technical system knowledge. A large number of human resources

executing unique safety-critical procedures, increase the risk for human errors and therefore, influence the overall safety level of the system.

10) Local goal trade-offs

Stakeholders that are involved in multiple projects can have, depending on the meeting, various goals. Experts explain the creation of fuzzy boundaries and the lack of understanding of the safety architecture, allow local actors to change their conditions in one of its corners for good reasons, and without apparent consequences. This can bring immediate gains on some local goal trade-off. In other words, the decision-making process can be person-focussed, instead of organisation-focussed.

Both Leveson [59] and Dekker [54] explain that with a high number of widely distributed interacting components in an organisation, small 'drifts' in procedure or policy will not necessarily be identified as risks to the safety of the SoS.

11) Overview

As stated before, according to EN50126, risk assessment should be done at the railway system level. Taking into account that any party that knows the entire complex system is missing, experts explain a challenge when considering the integrated system. For the creation of the total safety architecture, an integrator should create an integral coherence of the safety architecture and the define interdependencies between elements. An overview is necessary to define a complete, comprehensive, and defensible argument

Earlier research explained the need for a comprehensive approach to obtain better understanding of the complex nature of hazards, and understand interrelatedness of all factors that play a role in risk assessment [60]. The complexities of an entire SoS may be more obvious when analysing the overall system architecture and therefore managed more effectively [39]. However, a lack of a system overview can be a major barrier to evolve systems.

12) Risk assessment

Experts indicate knowledge and understanding of the total safety architecture are of primary importance to foresee hazards and risks. The creation of the overall safety architecture requires full knowledge of the risks involved. Organisations manage risk by identification, analysis, and evaluation. Safe operations are achieved by setting and achieving relevant goals.

Without understanding the purpose, goals and decision criteria used to construct and operate systems, it is not possible to completely understand and most effectively prevent accidents [31]. Strong knowledge implies a low degree of uncertainty, and poor knowledge implies a high level of uncertainty [46].

13) Safety

Experts acknowledge complexity in safety. It is assumed that richer understanding of risk assessment improves safety.

Effective management of risk allow an organisation to improve its safety performance. "Practical safety is risk management" and once that link has been clearly established, the role of safety becomes significant and its value-add more measurable [61].

These described relationships are shown in the upper part of the reference model in Fig. 5. This reference model represents the existing situation on implications with regard to the safety architecture of ERTMS. All ellipses represent key factors, meaning those influencing factors that are considered as the core factors or root causes. The links describe the existing relationships. Not all relationships come from direct experiences. Therefore, these relationships are indicated as an assumption. The existing value of a key factor is represented by means of a '+' or '-'. For example, the '+' next to 'number of different ERTMS inclusions' indicates a high degree. Quantitative classification of whether or not participants experience a challenge in one of the key factors is shown in Fig. 6.

V. DISCUSSION

As for the interviews, we assure the basic quality of the data by forwarding the summary of the interview to each participant, asking for their feedback, and made corrections if there were any misinterpretations.

The reference model is logically verified by consistency, meaning there are no internal conflicts between the key factors, and well-established literature to identify supporting evidence and contradictions. Relationships between safety overview and risk assessment, comprehension of the safety architecture and safety overview, and comprehension and risk assessment, are labelled as assumptions, because they are not described from direct experiences. We verify logically on internal validity and external validity.

As for internal validity of the reference model, causes and effects of a key factor could have been interchanged. For example, a low degree of comprehension of the architecture that leads to a low degree of quality of overview. On the other hand, a low degree of quality of overview that leads to a low degree of comprehension of the architecture. Also, we experienced two causal relationships between fuzzy boundaries and comprehending the architecture, and between various languages and cultures and variety in inclusion ERTMS specs. In the reference model, this is shown through a combined relationship.

As for external validity, findings are person and time-related. Various participants have various experiences. They can interpret a key factor in a different way. Participants with experience between 10 and 20 years will allow fewer generalisation then participants with 5 years of experience and varying backgrounds. Also, statements of participants about topics that fall outside of their expertise are less reliable than the statements of participants that have direct experience with the topic. For these reasons, care is taken that collected data is relevant. Data obtained within the participant's expertise, based on direct experience, is valued higher than the data from an unexperienced participant. We prevent asking leading questions or emphasising a specific detail of the topic. Challenges of key factors and their interrelationships must be suggested by the expert. An

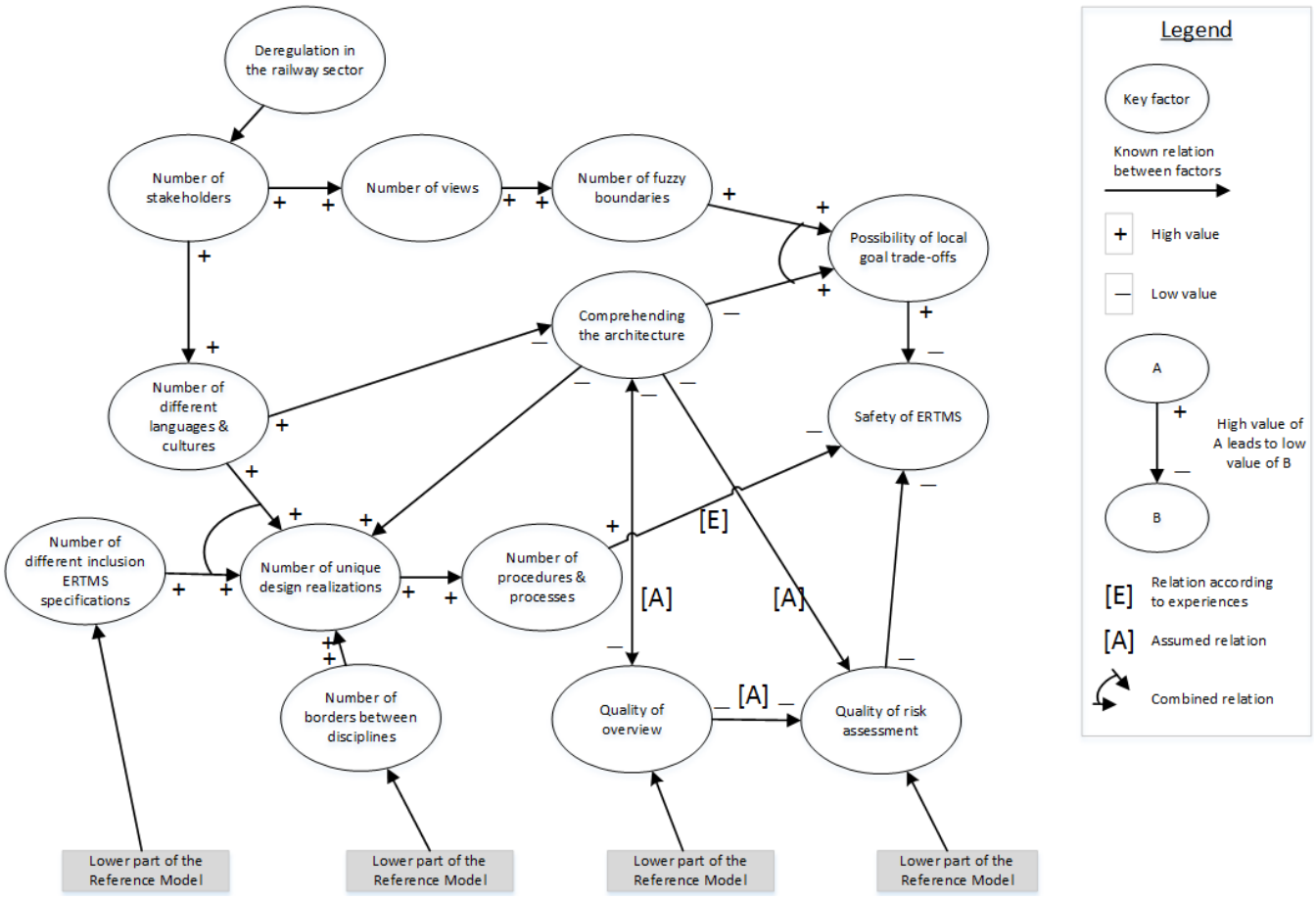

Figure 5. Upper part of the reference model on implications with regard to the safety architecture of ERTMS

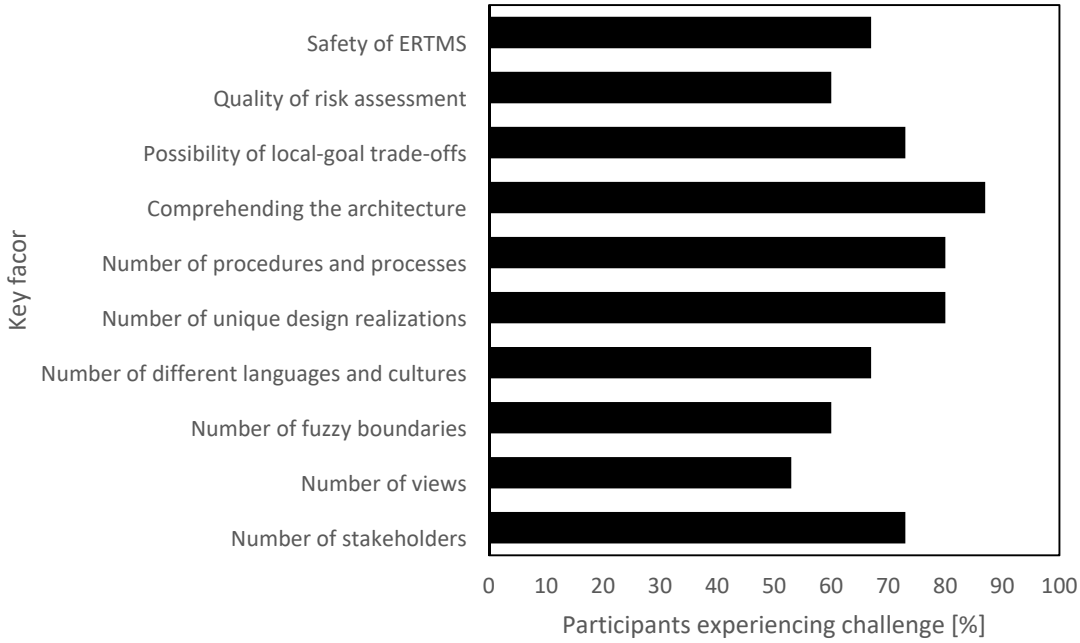

Figure 6. Participants experiencing challenges in key factors

explanation of a real-life example or experience suggested by the participant was valued higher.

As for the relationships that are labelled as assumption, we plan to verify them in a real ERTMS case that, at this moment, is setting up their risk analyses and evaluations.

VI. CONCLUSION

Evaluating risks using the ALARP-principle involves complex and challenging explanations and interpretations of the desired performance levels. Time pressure and pressure towards cost-effectiveness can inadvertently lead to generating adaptive responses, wrong/missing identification of hazards and safety risks, and also to safety concessions. Addressing primarily potentially catastrophic risks automatically means accepting the remaining risk.

Both internationally and nationally, stakeholders have different preferences for ERTMS design. In addition, specification interpretations by train operators, infrastructure providers and manufacturers vary markedly.

A system integrator that knows the entire complex system, misses. A system model cannot be built by a bottom-up aggregation of models, derived from research in the individual disciplines, but by a top-down, system-oriented approach based on control theoretic concepts [21]. At the same time, a trade-off using bottom-up aggregation can provide information that helps to focus on more detailed problems of subsystems. Both implicit data-exchange and a missing integral view make it hard to perform a comprehensive safety assessment.

Both international and national preferences, changing specifications, varying stakeholders and various manufacturers led to a unique realisation for every subsystem. Similarly, the occurrence of further transitions with accompanied complexity and procedures and processes that multiply and have wider ramifications. The checking of the critical specifications in natural language is a burdensome task.

Since there is no integral view, local actors can change their conditions without, what at first glance may seem, apparent implications. This in turn leads to a system of a wide variety of subsystems, and the associated increase of transitions that affect safety. In view of this, in order to develop a safe system, the key role is that of the safety architect to define an integral safety architecture, representing:

- Safety functions.
- A top-down risk assessment at the railway system level that relies on system definition, and includes risk analysis and risk evaluation.
- A bottom-up hazard analysis of the system under consideration.

Split-responsibility results in stakeholders that lack insight into cross-border information. Understanding relationships between risk and design can aid in communication between safety engineer and designer. Clear communication regarding safety, which supports critical system development, is essential.

In practice, the unstable specifications and various interpretations are a major problem when dealing with such systems. The consequences are significant: the five ERTMS-projects in the Netherlands (Betuweroute, Port of Rotterdam, HSL South, Amsterdam-Utrecht and Lelystad-Zwolle) are all different [12] in design and use, let alone the wider European variants.

The current integral architecture lacks integrated knowledge, traceability, and consistency. As for safety, this means that the lack of availability of information makes it difficult to find a root cause for each hazard.

Assuming that a safety assessment is conducted in a professional and scientific way, it will meet some standards on quality. For example, all the steps of the assessment are traceable, all assumptions are recorded, and all analysis principles and methods adopted are justified [46]. To meet unforeseen events and surprises, and to identify safety requirements at the system level, a systems engineering approach to safety must be treated adequately in the context of the social and technical system as a whole. As Kecklund [62] also explained: “It became clear that the work of several organisations and authorities at the societal level has implications for railway safety, and therefore, it is important that established channels for communication and co-operation among these parties exist, and that there is a level that affords an overall, holistic perspective.”

Current challenges concern an interdisciplinary approach on both the social and technical level, and how parts interact and fit together. Accompanying questions concern the acceptability of the level of incompleteness. ERTMS is a great example of a complex system, subject to an increasing number of stakeholders, various interpretations of requirements, where overall responsibility is split. As for safety, many and varied interactions among the individual components is to be approached proactively and qualitatively where time drain and pressure towards cost-effectiveness can inadvertently lead to generating adaptive responses.

These challenges require improvements in resilience, more awareness and sensitivity for interrelationships between hazards and risks, but even more: comprehending the safety architecture and creating cross-discipline understanding.

In this study, the effects of the safety case regime, interoperability, deregulation and dynamic specifications on the ERTMS have been researched at the Dutch national level.

Achieving an interoperable and safer railway system by implementing ERTMS appears not to be straightforward for three key reasons:

- The safety case argument involves descriptions and observations that require explanations and interpretations from various stakeholders having various points of view, skills, responsibilities and interests into the outcomes of the assessments.
- For the Dutch situation, the absence of central designer and overall processes lowers the degree to which the parties succeed in effectively harmonising various processes.
- An increased number of actors has caused a lack of insight into cross-border information.

Specifications allowing multiple interpretations result in a wide variety of design choices, disparities among systems, possible little recognition of hazards and risks, and needlessly cumbersome procedures.

REFERENCES

[1] K. Schuitemaker and M. Rajabalinejad, "ERTMS Challenges for a Safe and Interoperable European Railway System," Proceedings of the 7th International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO 2017), pp. 17-22, April 2017.

[2] European Commission, "ERTMS – European Rail Traffic Management System," Available from: http://www.ec.europea.eu [retrieved: March, 2017].

[3] International Union of Railways, "SafeCulture: A method for assessing organisational safety at interfaces," UIC, 2004.

[4] R. Forsberg, "Conditions affecting safety on the Swedish railway – Train drivers' experiences and perceptions," Safety Science, vol. 85, pp. 53-59, 2016.

[5] Ministry of Transport, Public Works and Water Management, "Cost benefit analysis of implementation strategies for ERTMS in the Netherlands," 2010.

[6] Ministry of Infrastructure and the Environment, "Beleidsimpuls Railveiligheid," 2016.

[7] Prorail, "Jaarrapport 2015. Analyse STS-passages" Unpublished.

[8] P. Smith, A. Majumdar, and W. Y. Ochieng, "An overview of lesson learnt from ERTMS implementation in European railways," Journal of Rail Transport Planning & Management, vol. 2, pp. 79-87, 2012.

[9] F. Laroche and L. Guihéry, "European Rail Traffic Management System (ERTMS): Supporting competition on the European rail network?" Research in Transportation Business & Management, vol. 6, pp. 81-87, 2013.

[10] M. Ghazel, "Formalizing a subset of ERTMS/ETCS specifications for verification purposes," Transportation Research Part C, vol. 42, pp. 60-75, 2014.

[11] European Commission, "ERTMS – FAQ on ERTMS," Available from: http://www.ec.europa.eu [retrieved: March, 2017].

[12] Ministry of Infrastructure and the Environment, "ERTMS kennisboek versie 2.0," 2014 Available from: http://www.rijksoverheid.nl [retrieved: March, 2017].

[13] Ministry of Infrastructure and the Environment, "Eindrapport Lessen uit het rijden onder ERTMS Level 2 in Dual Signalling omstandigheden," 2015 Available from: http://www.rijksoverheid.nl [retrieved: March, 2017].

[14] J. Stoop, J. Vleugel, and J. Baggen, "Testing the untestable: towards pro-active safety assessment," Proceedings of the 9th International probabilistic safety assessment and management conference (PSAM 9), May 2008, pp. 784-791, ISBN: 978-988-99791-5-7.

[15] L. de Haan, J.L.M. Vrancken, and Z. Lukszo, "Why is intelligent technology alone not an intelligent solution?" Futures, vol. 43, pp. 970-978, 2011.

[16] OECD. Structural reform in the rail industry. Policy roundtables. 2005.

[17] G. Alexandersson and S. Hultén, "The Swedish Deregulation Path,"Review of Network Economics, vol. 7, issue 1, pp. 1-19, March 2008.

[18] UNIFE, "UNISIG, An industrial consortium to develop ERTMS/ETCS technical specifications," Available from: http://www.ertms.net [retrieved: March, 2017].

[19] European Union, "Commission Decision of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system," Official Journal of the European Union, vol. 55, pp. 1-51, February 2012.

[20] UNIFE, "A Unique Signalling System For Europe. The long journey to an interoperable railway system," Availale from htttp://www.ertms.net [retrieved: March, 2017].

[21] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," Safety Science, vol. 27, pp. 183-213, 1997.

[22] N.P. Hoj and W. Kroger, "Risk analyses of transportation on road and railway from a European Perspective," Safety Science, vol. 40, pp. 337-357, 2002.

[23] B. G. Glaser and A. L. Strauss, "The Discovery of Grounded Theory: Strategies or Qualitative Research," Weidenfeld and Nicolson, London, 1967.

[24] L. Blessing and A. Chakrabarti, "DRM, a Design Research Methodology," Springer-Verlag London, 2009.

[25] European Railway Agency, "Intermediate report on the development of railway safety in the European Union," 2013 Available from: http://www.era.europa.eu [retrieved: March, 2017].

[26] K. Schuitemaker, J.G. Braakhuis, and M. Rajabalinejad, "A Model Based Safety Architecture Framework for Dutch High Speed Train Lines," Proceedings of the 10th International Conference on System of Systems Engineering (SoSE), May 2015, pp. 21-29, 2015.

[27] S. Barua, X. Gao, and M.S. Mannan, "Comparison of precriptive and performance-based regulatory regimes in the U.S.A and the U.K.," Journal of Loss Prevention in the Process Industries, vol. 44, pp. 764-769. 2016.

[28] S.Nair, J.L. de la Vara, M. Sabetzadeh, and D. Falessi, "Evidence management for compliance of critical systems with safety standards: a survey on the state of practice," Information and Software Technology, vol. 60, pp. 1-15, 2015.

[29] ERTMS Strategy Group, "National ERTMS Business Requirements," Available from: http://www.rssb.co.uk [retrieved: March, 2017].

[30] D. Falessi, M. Sabetzadeh, L. Briand, E. Turella, T. Coq, and R. K. Panesar-Walawege, "Planning for Safety Standards Compliance: A Model-Based Toolsupported Approach," IEEE Software, Vol. 29, pp. 54-70, 2011.

[31] N.G. Leveson, "Engineering a Safer world, Systems Thinking Applied to Safety," The MIT Press, 2011.

[32] H. Priemus, "Mega-projects: Dealing with Pitfalls," European Planning studies, vol. 18, pp. 1023-1039, 2010.

[33] T. Pasquale, E. Rasaria, M. Pietro, and O. Antonio, "Hazard Analysis of Complex Distributed Railway Systems," Proceedings of the 22nd International Symposium on Reliable Distributed Systems (SRDS'03), October 2003, pp. 283-292, ISSN: 1060-9857, ISBN: 0-7695-1955-5.

[34] Tweede Kamer Der Staten-Generaal, "Verslagen van de openbare verhoren," Available from: http://www.tweedekamer.nl [retrieved: March, 2017].

[35] S. Nusser, "Robust Learning in Safety-Related Domains. Machine Learning Methods for Solving Safety-Related Application Problems," Doctoral Thesis, Univ., Fak. Für Informatik, 2009.

[36] B. Enserink, "Integral assessment – putting safety on the agenda for mitigation and preparedness," Safety Science, vol. 39, pp. 93-105, 2001.

[37] N.P. Høj and W. Kröger, "Risk analyses of transportation on road and railway from a European Perspective," Safety Science, vol. 40, pp. 337-357, 2002.

[38] C. Harvey and N. A. Stanton, "Safety in System-of-Systems: Ten key challenges," Safety Science, vol. 70, pp. 358-366, 2014.

[39] T. Kelly, "A Systematic Approach to Safety Case Management," SAE Technical Paper, pp. 239-248, 2004.

[40] N. Yakimets, S. Dhouib, H. Jaber, and A. Lanusse, "Model-Driven Safety Assessment of Robotic Systems," IEEE Intelligent Robots and Systems (IROS), pp. 1137-1142, 2013.

[41] P. Rook, "Controlling Software Projects," Software Engineering Journal, vol. 1, pp. 7-16, 1986.

[42] P. Mauborgne, S. Deniaud, E. Levrat, E. Bonjour, J. Micaëlli, and D. Loise, "Operational and System Hazard Analysis in a Safe Systems Requirement Engineering Process – Application to automotive industry," Safety Science, vol. 87, pp. 256-268, 2016.

[43] K. J. Hayhurst and C. M. Holloway, "Challenges in software aspects of aerospace systems," Proceedings of the 26th Annual NASA Goddard, August 2002.

[44] Lutz, R, "Analyzing software requirements errors in safety-critical, embedded systems," Proceedings of IEEE International Symposium on Requirements Engineering, pp. 126-133, 1993.

[45] J. Bradley, M. Efatmaneshnik, and M. Rajabalinejad, "Toward a Theory of Complexity Escalation and Collapse for System of Systems," Proceedings of the 10th International Conference on System of Systems Engineering (SoSE), pp. 7-11, 2015.

[46] T. Aven, "Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management," Routledge, 2014.

[47] M. Rajabalinejad, A. Martinetti, and L. A. M. van Dongen, "Operation, safety and human: Critical factors for the succes of railway transportation," Proceedings of the 11th System of Systems Engineering Conference (SoSE), pp. 1-6, 2016.

[48] ERA, "Intermediate report on the development of railway safety in the European Union," 2013.

[49] A. S. Townsend, "Safety Can't Be Measured – An Evidence-based Approach To Improving Risk Reduction," Gower Publishing, 2013.

[50] J. Iglesias, A. Aranz, M. Cambronero, C. de la Roza, B. Domingo, J. Tamarit, J. Bueno, and C. Arias, "ERTMS deployment in Spain as a real demonstration of interoperability. Near future challenges," 9th World Conference on Railway Research, 2011.

[51] The Dutch Safety Board, "Train Derailment Hilversum," 2014. Available from: http://onderzoeksraad.nl/ [retrieved: March 2017].

[52] A. Laurino, F. Ramella, and P. Beria, "The economic regulation of railway networks: A worldwide survey," Transportation Research Part A, vol. 77, pp. 202-212, 2015.

[53] I. Sommervile, R. Lock, T. Storer, and J. Dobson, "Deriving Information Requirements from Responsibility Models," Proceedings of the 21st International Conference on Advanced Information Systems Engineering, pp. 515-529, 2009.

[54] S. Dekker, "Drift into failure: from hunting broken components to understanding complex systems," CRC Press, 2011.

[55] European Transport Safety Council (ETSC), "Transport accident and incident investigation in the European Union," Available from: http://www.etcs.eu [retrieved: March, 2017].

[56] European Railway Agency, "Analysis of Potential Interoperability Problems Final Report WP4," Available from: http://www.era.europea.eu [retrieved: March, 2017].

[57] European Railway Agency, "Subset-026—2 v300," Available from: http://www.era.europea.eu [retrieved: March, 2017].

[58] G. Baxter and I. Sommerville, "Socio-technical systems: From design methods to systems engineering," Interacting with Computers, vol. 23, pp. 4-17, January 2011.

[59] N. G. Leveson, "A new accident model for engineering safer systems," Safety Science, vol. 42, pp. 237-270, 2004.

[60] K. Schuitemaker, M. Rajabalinejad, and J.G. Braakhuis, "Model-based safety architecture framework for complex systems," Proceedings of the European Safety and Reliability Conference (ESREL), pp. 3611-3618, 2015.

[61] S. Merchant, "Role of Safety and Product Integrity," Procedia Computer Science, vol. 8, pp. 443-451, 2012.

[62] L. Kecklund, E. Olsson, A. Jansson, G. Kecklund, and M. Ingre, "The Train Project: Effects of organizational factors, automatic train control, work hours and environment: suggestions for safety enhancing measures," Proceedings of the Human Factors and Ergonomics Society 47th Meeting, pp. 1835-1839, 2003.