Rapid Risk Assessment of Technical Systems in Railway Automation

Jens Braband
Siemens AG
Ackerstr. 22, 38126 Braunschweig, Germany
jens.braband@siemens.com

Abstract

The European Railway Agency (ERA) has the challenging task of establishing Common Safety Targets and Common Safety Methods throughout Europe. In this context, the harmonization of risk assessment methods is also discussed. The purpose of this paper is to present a new approach to risk assessment of technical systems in railway automation, which allows a rapid risk assessment while at the same time also allowing a rigorous check that the method is well constructed and robust. As a particular reference, a new German pre-standard, which lays out requirements for such semi-quantitative approaches, is taken into account. A particular method is constructed in this paper and the means by which compliance with legal and regulatory requirements can be demonstrated, is discussed. Although the paper deals with the European legal framework in railway automation, the approach can easily be generalized to other legal frameworks and other application domains.

1 Introduction

The European Railway Agency (http://www.era.europa.eu), established by European Regulation 881/2004, has the mission of reinforcing railway safety and interoperability throughout Europe despite continuing privatization. Central to its work on railway safety is the development of measures based on common safety targets (CST) and common safety methods (CSM), common safety indicators (CSI) and harmonized safety certification documents. For some work and problems related to the assessment of CST see Braband and Schaebe (2012).

The CSM describe how safety levels, the achievement of safety targets and compliance with other safety requirements are assessed in the various member states. As a first step, EC Regulation 352/2009 will finally come into force for the complete European railway sector by July 2012. In this regulation, a semi-quantitative risk acceptance criterion for technical systems (RAC-TS) similar to civil aviation has been introduced: *For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour*.

This criterion is limited to those technical systems where failure can lead to catastrophic effects, e.g. train accidents involving many fatalities, and for which there are no credible barriers or substantial mitigating factors that will prevent this consequence from materializing. The criterion can be used for the utmost critical functions performed by technical systems on railways such as speed supervision, control of the switch position, complete and permanent loss of the brake system, or loss of the traction cut-off function. This means that formally RAC-TS is related only to potentially catastrophic accidents, similar to the criterion related to hull loss accidents in civil aviation. In order to apply it also to other severity categories, RAC-TS must be embedded in a risk analysis method.

In this paper we focus on semi-quantitative risk analysis methods, which are very similar to the rapid risk assessment method approach advocated by Johnson (2011). In fact one purpose of the paper is to motivate and demonstrate that semi-quantitative methods are in fact rapid risk assessment methods, but satisfy additional requirements.

The paper is organized as follows: after a discussion of problems related to risk analyses, an applicable standard is reviewed, from which the requirements are taken. These requirements are compared to the requirements for rapid risk assessment methods. Then a new risk analysis method is constructed and some arguments and examples concerning the validation of the method are presented.

2 Problems with risk analyses in railway applications

Risk is a combination of accident severity and accident frequency. Accident frequency may be calculated by hazard frequency and the probability of a hazard developing into an accident. This probability is derived by taking into account the effectiveness of barriers. Barriers are understood as any means to prevent, control, or mitigate undesired events or accidents. Barriers must be under the control of the organization operating the system as they have to be enforced during operation. They can be of different origin, e.g. human actions, operational barriers, technical barriers.

It is well known that risk acceptance is an intricate topic and that risk analyses in railways may be quite time-consuming and tedious, in particular when they are performed quantitatively, see e. g. Braband (2005) for an overview. There exist simpler semi-quantitative methods, e.g. risk matrix, risk graph or risk priority numbers;

however, they often lack justification and it is not clear whether the derived results are trustworthy. So, a major research challenge is to construct dependable semi-quantitative methods.

In particular, schemes based on risk priority numbers (RPN) are widely used in Failure Modes, Effects and Criticality Analyses (FMECA) although it is known that they have not been well constructed and that their use may lead to incorrect decisions, for the following reasons:

- The risk of different scenarios that lead to the same RPN may differ by orders of magnitude.
- Scenarios with similar risks lead to different RPN.

This has already been observed by Bowles (2003) and has now also lead to cautionary advice in the standards.

Risk matrices are a well-known tool in risk assessment and risk classification, and are also used in the railway domain (see for example EN 50126 (1999) or Braband (2005)). Some major problem of such risk matrices are:

- Risk matrices must be calibrated to their particular application.
- The results depend on the system level to which they are applied.
- The parameter classes must be concisely defined in order to avoid ambiguity and misjudgments.
- It must be defined which frequency is meant, e.g. accident or hazard frequency.
- It is not directly possible to take barriers or risk reduction factors into account in the risk matrix.

However, if these problems can be overcome, risk matrices are a well-accepted and easy-to-use tool, and can be useful for risk prioritization. When risk matrices are to be applied in the railway domain, they need to be applied in combination with a method which can additionally take into account the effect of barriers and their related risk reduction. Typical candidates for additional methods would be the fault tree analysis (FTA) in a quantitative analysis or semi-quantitative tables as used by risk priority numbers.

In conclusion for the railway domain rapid - in particular semi-quantitative - methods are very attractive and already widely used, but their justification is often questionable. Only a few approaches (see Bepperling (2008) and Milius (2010)) have been presented so far where semi-quantitative methods have formally been validated. A standard for the use of such methods, or against which methods can be validated, has been missing so far.

3 Construction of a semi-quantitative risk analysis method

3.1 DIN V VDE V 0831-101

Recently this German pre-standard DIN (2011)has clearly set out requirements for semi-quantitative risk analysis methods. It is now possible to construct a method and validate it with respect to these requirements. There are in total 28 requirements. Not all of these relate to construction of the method - some concern its application. Table 1 gives an informative overview of the requirements; the mandatory requirements appear in bold. For more details we have to refer to DIN (2011).

Construction	**A1**	**State reference units and application scope.**
	A2	**Be conservative in your assessment.**
	A3	Make sure parameter granularity is sufficient.
	A4	**Work out a user guide.**
	A6	**State clearly the applicable system level**
	A8	Allow for hazard classification.
	A12	**Assessment of accident severity**
	A13	**Assessment of accident frequency**
	A14	Description of all barriers
	A15	**The tables should be compatible.**
	A17	**Assessment of human reliability**
	A18	**Assessment of operational barriers**
	A19	**Assessment of exposition**
	A20	**Assessment of external barriers**
	A21	Assessment of technical barriers
	A22	**Take into account dependencies of barriers.**
	A23	**Calibrate the method (against a RAC).**
	A24/ A25	**Assure proportionality between risk and criticality.**
	A26	**Small changes lead to small changes.**
	A27	**A safety requirement has to be derived.**
	A28	**Give rules on how to derive the Safety Integrity Level**
Application	**A5**	**Justification of parameter choice**
	A7	**Identify hazards systematically.**
	A9	**Work out hazard scenarios.**
	A10	**Justify the choice of the relevant scenario.**
	A11	**Document results in a hazard log.**
	A16	**Identify safety-critical application conditions.**

Table 1: Summary of requirements

3.2 Requirements for rapid risk assessment methods

Johnson (2011) has gathered principles from leading application examples to define basic principles for rapid risk assessment methods:

1. Consistency between different ‘analysts’ looking at similar incidents;
2. Repeatability: the same ‘analyst’ should derive similar findings for similar incidents looked at over a period of time;
3. Economy: not more than one day’s training in safety management or hazard analysis should be necessary;
4. Validity: Rapid risk assessment techniques should be confirmed and refined using all available information about previous accidents and incidents;
5. Applicability: should be applicable to operational tasks and must support everyday decision making.

3.3 Risk Score Matrix approach

In this paper, a semi-quantitative approach is proposed that fulfils all requirements of the German pre-standard DIN V VDE V 0831-101 and also Johnson’s criteria. It is called the Risk Score Matrix (RSM) and consists of the application of a risk matrix and score tables for

assessment of the barriers, similar to RPN schemes. The complete approach is shown in Figure 1, including additional and alternative steps. The final result consists of hazard rates (HR) related to the functional failures of the technical system and the assumptions on which the analysis rests, which may turn into safety-related application rules (SAR). This process is explained in detail in the following chapters.

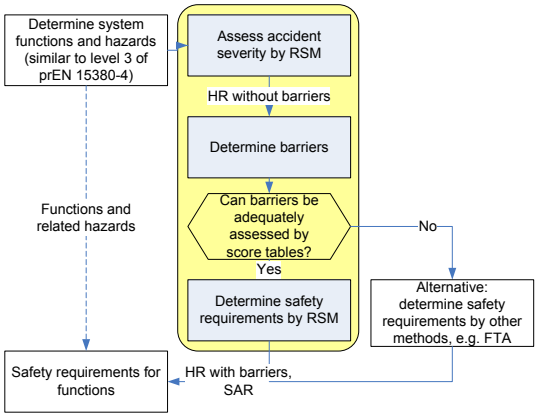

Figure 1: Overview of the Risk Score Matrix model

4 Description of the approach

4.1 System definition

The discussion in this paper focuses on technical systems only. According to EU Regulation 352/2009, a technical system is a product developed by a supplier including its design, implementation, and support documentation. It should be noted that:

- The development of a technical system starts with its system requirements specification and ends with its safety approval.
- Human operators and their actions are not included in a technical system. However, their actions may be taken into account as barriers mitigating the risk.
- Maintenance is not included in the definition, but maintenance manuals are part of the product.
- Technical systems can be subject to a generic type approval, for which a stand-alone risk acceptance criterion is useful.

A function is defined in prEN 15380-4 (2010) as a "specific purpose or objective to be accomplished that can be specified or described without reference to the physical means of achieving it." A function level is a "level, to group functions of equal purpose". The distinction between levels is described informally as follows:

- First-level function: functional domain that encompasses a set of functions related to the same general focus or service for the considered (rolling stock) system.
- Second-level function: related to a specific set of activities that contribute to completion of the functional domain defined at the first level (at this level, it is not said how a second-level function is to be implemented).
- Third-level function: related to a specific activity out of the related set of activities, it encompasses a set of tasks (a function at least at level 3 should be supported as much as possible by one single subsystem).

It is proposed to use prEN 15380-4 (2010) which contains up to five hierarchical levels. Taking into account the definition of function level, level 3 seems to be the most appropriate for the application of RAC-TS. At least it does not seem reasonable to go into more detailed levels such as level 4 or 5. Table 2 gives a non exhaustive list of functions to which RAC-TS may be applied. Although prEN 15380-4 (2010) relates to rolling stock only, it can be extended to infrastructure functions quite easily, e.g. by identification of all interfaces of other functions to rolling stock. Some functions (or at least interfaces) are already defined. In Table 2, some examples of level 3 functions related to signalling are proposed.

Code	Function description
=LBB	Detect track vacancy
=LBC	Detect train at a particular spot
=LBD	Locate train
=LCB	Determine train description
=LDB	Provide diagnostics
=LEB	Supervise driver vigilance
=LEC	Automatic train stop
=LED	Supervise braking curve
=LEE	Supervise maximum train speed
=LFB	Optimize train running
=LGB	Monitor switch
=LGC	Lock switch
=LGD	Monitor derailer
=LGE	Lock derailer
=LGF	Monitor level crossing
=LHB	Provide signal information
=LJB	Provide cab radio
=LKB	Display state to driver
=LKC	Display state to dispatcher
=LKD	Transmit commands

Table 2: Examples of signaling functions

4.2 Risk matrix

A suitable risk matrix has already been proposed and justified in Braband (2011), see Table 3. The table shows intolerable and tolerable combinations in a frequency scaling of √10 and has been calibrated to match RAC-TS. Safety targets would be chosen at the boundary between these two regions (medium gray shading). This scaling is compatible with the common scaling for Safety Integrity Levels (SIL), as two classes form one SIL. Note that for higher severity levels a slight risk aversion has been taken into account and that there are no particular safety requirements for category A.

HR	B	C	D	E
n. a.				
10^{-5}/h			Intolerable	
$3x10^{-6}$/h				
10^{-6}/h				
$3x10^{-7}$/h				
10^{-7}/h				
$3x10^{-8}$/h				
10^{-8}/h	Tolerable			
$3x10^{-9}$/h				
10^{-9}/h				RAC-TS

Table 3: Proposed risk matrix

The corresponding accident severities are defined in Table 4. Classification can be performed based on a qualitative estimate of the typical accident severity or based on statistical data (fatalities and weighted injury score (FWI)). Note that "typical" does not mean worst case; in a safety sense, it should be interpreted as a typical bad outcome, i.e. worse than average. When considering statistical data, it should be noted that railway accident severity statistics are often highly asymmetric and skewed, so that particular care has to be taken when evaluating such statistics.

ID	Combinations	FWI range	Typical FWI
E	Multiple fatalities	2≤FWI	5
D	Single fatality or multiple serious injuries	0.2≤FWI<2	1
C	Single serious injury or multiple light injuries	0.02≤FWI<0.2	0.1
B	Single light injury	0.01≤FWI<0.02	0.01
A	-	FWI<0.01	n. a.

Table 4: Consolidated severity categories

4.3 Assessment of barriers

The model generally takes into account the following types of barriers:

- possibility to avoid accident by human interaction (H)
- possibility to mitigate the hazard by an independent technical system (T)
- operational barriers (B)
- low demand frequency (D)

The presence and efficiency of these barriers together with the severity category determines the outcome of the assessment and thus the appropriate safety requirements that will have to be achieved for the technical system under evaluation. The assessment is carried out via a score scheme where scores are allocated to the barriers and then these scores are added to calculate the total risk reduction, starting from the risk matrix in Table 3. Since the scores for the barriers are added instead of multiplied, this means that the scores allocated are given in a logarithmic scale where each score represents a "risk reduction" with a factor of $\sqrt{10}$ and two scores represent a reduction of one order of magnitude (i.e. one SIL). It should be noted that the effectiveness of the barriers must be monitored in operation, typically as a part of the operator's safety management system.

The total risk reduction is then calculated as the sum of scores, possibly reduced by a score accounting for the level of independence of the different barriers present. This is to avoid adding several barriers that are functionally dependent on each other and that are likely to fail simultaneously.

It should be noted that such a semi-quantitative assessment method may not fit all particular problems; e.g. there may be rare cases when other barriers occur and need to be taken into account. Also, some of the tables may be overly conservative, e.g. the assessment of human reliability by parameter H. In such cases, it is advised to apply first the risk matrix (Table 3) without any barriers and evaluate the barriers by an alternative method, e.g. Fault Tree Analysis, Event Tree Analysis or Markov models, as appropriate for the particular problem.

For the sake of brevity, it is not possible to present and discuss all score tables. Instead, the focus will be on the assessment of human reliability to demonstrate the principle.

4.4 Assessment of human reliability

In some situations, it can be foreseen that there are still barriers present after the failure of a technical system due, for example, to the driver or staff observing the problem and acting correctly. Human interaction can also, in some cases, be carried out by passengers or third persons. Examples could be staff or passengers correctly using on-board fire extinguishers in case of fire or similar situations. Evaluation is based on three tables (5a, 5b and 5c) and calculates a combined score as the sum of the following sub-scores:

- type of task
- stress level at which the task is performed
- environmental conditions under which the task is performed

The approach is similar to simple screening techniques in human reliability assessment, e.g. Accident Sequence Evaluation Program (ASEP), e.g. Sträter (1997), or the approach validated by Hinzen (1993). Such approaches are known to be pragmatic and generally conservative. Note that also alternative assessment schemes could be transformed into similar tables. This assessment of human barriers does not pretend to give a deep and exact description of the human actions to be carried out and their reliabilities. It merely intends to give a conservative order estimate and does not replace further ergonomic studies, e.g. on the design of human-machine interfaces.

Pre-conditions for the application of this assessment are:

- Operators must be properly trained and have sufficient experience.
- There must not be any goal conflicts in performing the task, e.g. safety vs. performance.

A – score	Action type	Comment
4	Skill-based	Well-known and trained skill-based action
2	Rule-based	Rule-based action that has been appropriately trained and managed
0	Knowledge-based	But no routines or rules are defined.

Table 5a: Action type assessment

W – score	Work environment	Comment
1	Good conditions	The work is performed under normal conditions with regard to sight, noise, physical forces and weather.
0	Adverse conditions	The working conditions are adverse with regard to at least one factor: lighting, noise, physical forces (e.g. excessive vibrations) or adverse weather conditions (too cold, too hot, etc.).

Table 5b: Work environment assessment

ST – score	Stress level	Comment
1	Optimal	
0	Excessive demands	The work load is very demanding. The stress level is high, e.g. work under time pressure.
	Insufficient demands	The work performed is not very demanding and mostly routine.

Table 5c: Stress level assessment

The combined score is then calculated from Tables 5a, 5b and 5c as H= A + W + ST.

4.5 Assessment of barrier dependence

For every barrier that is taken into account, it must be analyzed whether its risk reduction is independent of the other barriers. If it is not, some scores will be subtracted from the score of the barrier, in accordance with Table 6b below. If the correlation is strong, the new barrier may reduce the risk only marginally.

Tables 6a and 6b can be justified on the basis of experience with conditional failure probabilities in human task analysis, e.g. Sträter (1997) and common cause analysis of technical systems.

The reduction of the barrier score is calculated by Table 6b, which gives the reduction of the barrier score Φ as a function of the original barrier score (top row) against the dependence of the new barrier with respect to all previous barriers.

Dependence class	Comment
Independence (I)	There is no functional dependence between the factors; no common causes for failures exist.
Low dependence (LD)	The barriers are statistically independent; no significant physical influence. Related to human tasks, the task is performed by a different person at a different location and in a different operational situation.
Medium dependence (MD)	The mitigating factors have a single common cause failure – if one barrier fails, there is a slightly increased chance that the other also fails. Related to human tasks, e.g. two of the following characteristics are the same: same person, same location or same operational situation.
High dependence (HD)	The barriers have more than one common cause. If one barrier fails, there is a significantly increased chance that the other also fails.
Complete dependence (CD)	Several common causes. The new barrier will not be taken into account.

Table 6a: Dependence classes

Φ	1	2	3	4	4+i
I	0	0	0	0	0
LD	0	0	-1	-1	-(i+1)
MD	0	-1	-1	-2	-(i+2)
HD	0	-1	-2	-3	-(i+3)
CD	-1	-2	-3	-4	-(i+4)

Table 6b: Dependence assessment

4.6 Validation of the Risk Score Matrix method

It is not possible to give all arguments concerning the requirements from Table 1 here, but it is possible to outline a few of the key arguments, whose fulfillment is quite obvious by the construction of the tables. For examples of the complete validation of semi-quantitative approaches, see Bepperling (2008) and Milius (2010).

The scope as well as the units of measurement are well defined by Table 2 and RAC-TS, so A1 and A6 can be fulfilled. As all tables are constructed conservatively, A2 is met. The granularity of the method is set to $\sqrt{10}$, which fits well to the SIL scale and is reasonable, so A3 can be fulfilled. As this scaling is used consistently throughout all tables, A15 is complied with. The tables shown in this section also meet the respective requirements A12, A13, A17, A18 and A22. The method is also calibrated appropriately against RAC-TS, so A23 follows. The method is monotone with respect to risk (A24), i.e. a higher risk gains a more demanding safety requirement. Also, small changes in the parameters lead only to small changes in the safety requirements (A26).

4.7 Is Risk Score Matrix a Rapid Risk Assessment Method?

We justify the construction of the Risk Score Matrix against the criteria defined by Johnson (2011)

1. Consistency: in particular requirements A1 and A4 would support this jointly with the requirements for justification A5 and A10.

2. Repeatability: this is supported by the harmonized function list from table 2 as well as the requirements for the construction of the tables and also A4 and A5
3. Economy: if the analyst is experienced with respect to the system and the application conditions then one day's training in the Risk Score Matrix method would be sufficient
4. Validity: the tables are based on experience and the method has been validated against all requirements of the standard DIN (2011)
5. Applicability: the method is applicable also to operational tasks, if they include use of technical systems, but they are not intended to be used in daily operations or missions. This is due to the different scope of risk assessment of technical systems in railways and military missions

Finally we conclude that RSM is indeed a rapid risk assessment method, although dedicated to a very particular purpose. It can also be observed that the standard DIN (2011) defines more particular and detailed requirements for semi-quantitative methods than Johnson (2011) does for rapid risk assessment methods. The major difference is that DIN (2011) has more detailed requirements on the construction of the method.

4.8 Examples

In some cases, like =LGB from Table 2, RAC-TS is directly applicable. The main hazard would be that the status of a switch would be determined wrongly so that a train may run over a switch which is set in an incorrect direction. If passenger trains at high speed ran over this switch, then ID E would be determined from Table 4 leading to a THR of 10^{-9} per operating hour per switch. Some human mitigation may be possible (e.g. at low speed) and there is also the possibility that the switch is not set in the branching direction (50% chance), so that the overall score (due to Tables 5a to 5c) may be assessed as 1, leading to a THR of $3x10^{-9}$ per operating hour per switch.

In another example, =LGF from Table 2, the main hazard would be that road traffic would not be protected by the level crossing and the consequence might be a collision at the level crossing, from which ID D as the typical accident severity would be derived from Table 4 leading to a THR of 10^{-8} per operating hour per level crossing. Additionally, human mitigation may be possible (e.g. at low speed or with good sight) by the road users, so that the score (due to Tables 5a to 5c) may be assessed as 1. However, this mitigation is not independent from the severity estimate. Additionally, it can be taken into account that level crossings are not allowed on high-speed lines and often avoided on lines with high traffic density. Thus, finally a score of 1 may be assessed, leading ultimately to a THR of $3x10^{-8}$ per operating hour per level crossing.

5 Conclusion

The risk acceptance and setting of THRs for technical systems can be based on a risk score matrix as explained in this document taking into account a set of typical barriers. This approach is compliant with EC regulations as well as with requirements of the relevant standards.

When using the new Risk Score Matrix approach, mutual recognition will also depend on the list of functions to which the risk matrix is applied. So, the use of a common risk score matrix will facilitate the mutual recognition process, but not lead to an automatic approval.

It has been demonstrated that the Risk Score Matrix is truly a rapid risk assessment method.

6 References

Bepperling, S. (2008). Validation of a semi-quantitative approach for risk assessement on railways (in German), PhD thesis, Technical University of Brunswick

Bowles, J (2003) An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis, Proc. RAMS2003, Tampa

Braband, J. (2005). Risk analyses in railway automation (in German). Hamburg, Eurailpress

Braband, J. (2010). On the Justification of a Risk Matrix for Technical Systems in European Railways. In E. Schnieder (Ed.), FORMS/FORMAT 2010 (pp. 237-288). Springer

Braband, J. and Schaebe, H. (2012): Assessment of National Reference Values for Railway Safety - A Statistical Treatment, Proc. ESREL2012, Helsinki

CENELEC (1997) EN 50126 Railway applications –The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

CENELEC (2010) prEN 15380 Part 4: Railway applications – Classification system for rail vehicles – Function groups

DIN (2011) Semi-quantitative processes for risk analysis of technical functions in railway signalling (in German), DIN V VDE V 0831-101

EC (2009) Regulation No. 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council

Hinzen, A.(1993): The influence of human factors on railway safety (in German), PhD thesis, RWTH Aachen, 1993

ISO (2010) DIS 26262: Road vehicles – Functional safety

Johnson, C.: Using Rapid Risk Assessment Techniques to Combat Degraded Modes of Operation, Proc. ISSC2011, Las Vegas, 2011

Milius, B. (2010). Construction of a semi-quantitative risk graph (in German), PhD thesis, Technical University of Brunswick

Sträter, O. (1997) Evaluation of Human Reliability on the Basis of Operational Experience, PhD thesis, Technical University of Munich