Braband Jens

Griebel Stephan
Siemens AG, Braunschweig, Germany

Advances in risk analysis in railway signalling

Keywords

risk analysis, level crossing, semi-quantitative method, safety, EN50126, EN50129

Abstract

The paper is concerned with the developments of risk analysis during the last decade, starting from full range quantitative risk analysis of e.g. a level crossing based on the CENELEC standards EN50126 and EN50129 up to semi-quantitative methods for risk analysis. To expedite this shift from pure quantitative approaches to a more categorized approach were the perennial challenges of insufficient availability of accurate data and the sheer complexity of the reality to be model quantitatively. The article contains both a presentation of a complete quantitative risk analysis for a level crossing as well as a discussion of the crucial points that will need improvement on the basis of a new semi-quantitative standard for risk analysis that has been issued as a national pre-standard in Germany. The relation to the current regulations stipulated by the European Railway Agency and recent publications on this issue are presented as well.

1. Introduction

The publication of the CENELEC standards for railway and in particular railway signalling in the late nineties and early "zeries" paved the way for an optimization of the allocation of the limited resources available to operators for measures minimizing the risk of harm to passenger. This is achieved by means of a risk analysis that – after having established a tolerable risk for the system under consideration with both operational and technical parts – derives the tolerable values characterizing the upper limit for the frequency of failures of the technical system. During the last decade these risk analyses started from full range quantitative risk analysis of e.g. a level crossing up to semi-quantitative methods for risk analysis. To expedite this shift from pure quantitative approaches to a more categorized, yet nevertheless based on a rigorous mathematical model, approach were the perennial challenges of insufficient availability of accurate data and the sheer complexity of the reality to be model quantitatively. Chapter 2 contains a complete quantitative risk analysis for a level crossing. Chapter 3 will highlight the current publications relating to semi-quantitative risk analysis methods and chapter 4 will outline future developments in the light of a new semi-quantitative standard for risk analysis that has been issued as a national pre-standard in Germany and the current regulations stipulated by the European Railway Agency

2. A quantitative risk analysis for a level crossing

2.1. Introduction

Though having been analyzed, modeled and scrutinized almost ad infinitum, the level crossing still serves as an excellent example to highlight the crucial issues at stake when performing a risk analysis in railway signaling.
The key ingredients are the existence of an tolerable risk, e.g. established via historic data, analysis of the operational environment so as to evaluate the barriers that prevent the technical failure of the system into an actual accident and thus to establish an unambiguously defined tolerable rate with which the so called hazard, caused by the failure of the technical system, is allowed to manifest itself.
A key characteristic of this approach is the all-embracing quantitative approach, that is one is

obliged to provided detailed numerical data as input into the formulas.

2.2. Objective

This chapter provides an example of a risk-orientated apportionment of safety requirements for a system from the railway signalling sector, a level crossing.
The objective of the analysis is to derive safety targets for a defined initiating event taking into account all operational, environmental and architectural conditions. This objective is attained by means of a "reversed" Event Tree Analysis. "Reversed" event tree in this context means to derive the tolerable frequency for the initiating event by inverting the way of calculation starting from the outcomes.
Neither the functionality nor the analysis bears any direct resemblance to the features of a particular type of level crossing. The major aim is to present an example of the methodology, rather than provide a detailed realistic analysis. In particular, the values used in the calculations are examples and should not to be regarded as factual.

2.3. System definition

The following example from the railway signalling sector, the automatic level crossing, has been the subject of many analyses for illustration purposes.
In this example, the automatic level crossing has been in operation for a period of 25 years and uses light signals to warn the road user and a distant (monitoring) signal to tell the train driver whether the level crossing is closed or not.
A diagram of the level crossing (LX) is given in the following figure:

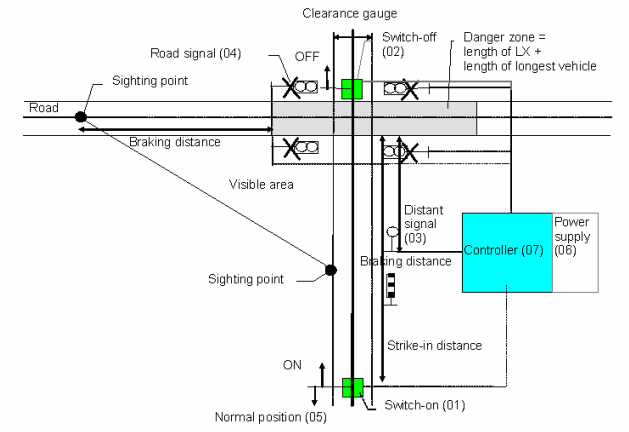

Figure 1. Level-crossing system (LX)

As a full system definition is beyond the scope of this example, only an informal functional description is given here. The following table provides an overview of the principal functional units involved.

Table 1. System overview

No.	Functional unit	Remarks
01	*LX* switch-on	Triggers activation of the *LX* when a train approaches (implemented by means of wheel detection equipment, e.g. an axle counter).
02	*LX* switch-off	Triggers deactivation of the *LX* once a train has left the crossing (implemented by means of wheel detection equipment, e.g., an axle counter).
03	*LX* monitoring	Displays the state of the *LX* to the train driver or interlocking (implemented e.g. by means of a distant signal) to allow monitoring of *LX* operation.
04	Road signalling	Displays the state of the *LX* to road users.
05	Normal position	Returns the *LX* to the normal position (no protection) if it is switched on and then not switched off within a certain time (due, e.g. to a detector failure when it invariably signalizes a train although it yet has left off the *LX* or the train stopping before the *LX*, etc.).
06	Power supply	Consists of the normal power supply system or, as a fall-back level, a battery capable of operating the *LX* for a limited period, e.g., 2 h. The battery voltage is monitored by the interlocking.
07	Control	Operates and controls the *LX*. A programmable electronic device which contains application software, site-specific data, etc.

A brief description of fault-free operation of the level crossing is given in the following enumeration.

a) An approaching train is detected by the switch-on element (01) and indicated to the controller (07). The distance of the switch-on element (01) from the level-crossing is denoted as the "strike-in distance".
b) The controller issues the command to activate the road signals (04) and waits until an indication of successful switch-on has been received. The distance between the sighting point and the level crossing is denoted as the "braking distance".
c) The controller issues the command to activate the distant signal (03), depicted by a small circle on a small vertical line perpendicular on a small horizontal line. The default position is off (danger). When the distant signal is off, an approaching train must stop at the level crossing and the driver may then switch on the level crossing manually using a key as the fall-back mode.

d) Traversal of the level crossing by the train is detected by a switch-off element (02) and indicated to the controller.
e) The controller issues the command to switch off the distant signal. After a delay, the road signals are switched off.

2.4. Hazard identification

In the railway sector, the initiating events at the system level are labelled as hazards according to the relevant CENELEC standards.
A complete analysis of the possible hazards is not performed; instead only the Hazard H as stated below is considered.

H = "Failure of level crossing to protect public from train"

It is interpreted as covering all situations in which the level crossing should warn the public (of approaching trains), but fails to do so.
The objective is now to determine the hazard rate HR (1/time) for H which is acceptable according to certain risk acceptance criteria. "Rate" is used in the sense of "instantaneous failure rate".

2.5. Event Tree Analysis

In order to determine the possible outcomes of the hazard H, one has to look at a scenario in which an individual encounters H. Hence as an example, one particular case of a motorist approaching an unprotected level crossing is considered, with P_{TR} denoting the probability of no train approaching, P_N the probability of timely notice of the train by the driver, P_{EA} the probability of an evasive action, and P_C the probability of an actual collision with the train.

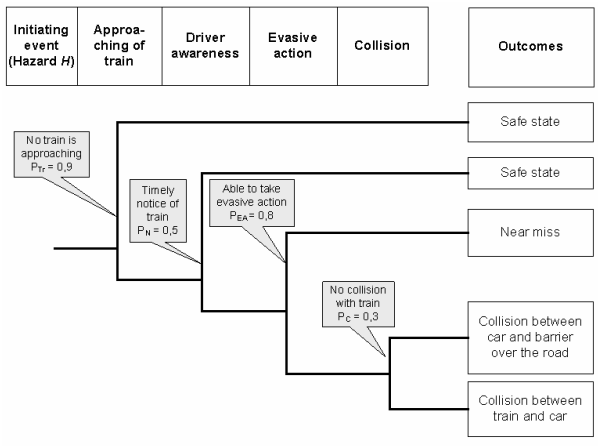

Figure 2. ETA for the level-crossing system

Thus two types of accidents ("Collision between train and car" and "Collision between car and level crossing") are identified. The figure above shows the external risk reduction factors between the initiating event, i.e. the hazard, and the outcomes, i.e. the accidents.

2.6. Quantitative analysis

The benchmark figures of an existing Railtrack's Railway Group Safety Plan (1997/98) are taken as the targets for the individual acceptable level of the risk (TIR) for an individual motorist: "Reasonably practicable schemes will continue to be implemented with the aim of ensuring that automated level crossings expose the individual occupants of road vehicles to a risk of fatality no greater than one in 100,000 regular users per annum by the year 2000".
In order to define a broadly acceptable limit, an additional safety factor of 10 is added. This means that the individual risk derived from $R_i < 10^{-5}$ fatalities/(person×year) for a regular user should be less than 10^{-6} per year. Thus the TIR value is established at less than 10^{-6} per year.
In order to obtain the approval from the authorities, the railway undertaking has to prove, that the actual individual risk of fatality (*IRF*) is less or equal to *TIR*. The following derivation of the acceptable rate for the hazard is based on the equation for *IRF* from [6]. This mathematical model for the determination of individual risk takes account of the causality leading from the initiating event, i.e. the hazards, to the outcomes, or accident sequences.

a) It is assumed that an individual uses the level crossing with a usage profile, which is described by the number of times it is used N (per year). For reference, a total exposure per usage E may be defined (i.e. E is the time needed to traverse a LX).
b) In this example, the individual is exposed to the hazard H. The probability that the individual will be exposed to the hazard depends additionally on the hazard duration D and the exposure time E of the individual to the hazards. This probability consists of the sum of the probabilities that the hazard already exists when the individual enters the system (approximately HRxD) and the probability that the hazard will occur while the individual is exposed (approximately HRxE).
c) From each hazard, one or more types of accident sequences may result. This is described for each hazard by the outcome probability Ck that an accident Ak will occur. This probability stands for the external risk reduction factors obtained by ETA. For each associated type of accident Ak

there is a corresponding severity. At the individual level, this is related to the probability of a fatal accident, Fk, for a single individual (see table below). For the sake of the example, the accident severity was estimated and compared with the railtrack data.

Table 2. Risk reduction parameters for accidents

No. k	Accident A_k	Risk reduction factor C_k	Probability of fatality F_k
1	Collision between train and car	0,1×0,5×0,2×0,7 = 0,007	0,2
2	Collision between car and *LX*	0,1×0,5×0,2×0,3 = 0,003	0,05

This gives rise to an individual risk of a fatality defined by

$$IRF = N \times HR \times (D + E) \times \sum_{\text{accidents } A_k} (C_k \times F_k) \quad (1)$$

This equation can be evaluated either by using mean values or by inserting appropriate parameters (e.g. percentiles) of statistical distributions for the input parameters.
If the individual risk turns out to be less than the target individual risk, the calculated or estimated hazard rate (HR) is called tolerable hazard rate (THR).
For the purpose of this example, a motorist is considered to cross a railway line repeatedly, say N = 1 000 times a year. Other users such as pedestrians or cyclists are not taken into account.
Based on operational experience it is assumed that the hazard H, if it occurs, lasts much longer than the individual exposure time, which would be the time to cross the LX. This means we can ignore the individual exposure time E. As a pessimistic value, a hazard duration time of D = 10 h is assumed, which is the time a failure of the LX, which results in a dangerous state of the system, lasts (until negated or repaired).
The tolerable hazard rate (THR) for H can be calculated by inserting the parameters as follows:

$$\begin{aligned} \text{IRF} &= \text{N} \times \text{HR} \times (D + E) \\ &\times \sum_{\text{accidents } A_k} (C_k \times F_k) \\ &= 1000 \times \text{HR} \times 10 \\ &\times (0{,}007 \times 0{,}2 + 0{,}003 \times 0{,}05) \\ &\le \text{TIR} = 10^{-6} \ \textit{per year} \end{aligned} \quad (2)$$

This yields a tolerable rate for the occurrence of the initiating event, i.e. the hazard, of approximately 7x10-8 h-1, corresponding approximately to one tolerable failure of the level crossing to protect public from train per 1 600 years.

2.7. Analysis of the outcomes and definition of necessary action

On completion of the analysis, it is the task of the designer or manufacturer of the level crossing to investigate whether the tolerable hazard rate can be achieved by his system or if architectural or design changes need to be made so as to meet the quantitative targets.

2.8. Conclusion

As the previous chapters have truly demonstrated, this quantitative approach renders seemingly highly accurate results. Yet one has to be aware of the fact that all this presumed accuracy hinges on the quality of the input data. Were these inaccurate or, sometimes better, not existent, one would be at quite a loss lacking an alternative and nonetheless trustworthy approach.
With the passing of the last decade, numerous experts have devoted themselves to this endeavour of building models that deliver trustworthy results on the basis of a rigorous yet flexible model.
The next chapter delineates the main features of this way forward.

3. Semi-quantitative methods for risk analysis

3.1. Problems with risk analyses in railway applications

It is well known that risk acceptance is an intricate topic and that risk analyses may be quite time-consuming and tedious [5], in particular if they are performed quantitatively. 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 consists in constructing 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:

- 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 [2] and has now also lead to cautionary advice in the standards.
Risk matrices are a well-known tool in risk assessment and risk classification, also in the railway domain (see for example [3]or [7]).An example and brief analysis of the advantages and drawbacks can be found in [5].
In conclusion for the railway domain semi-quantitative methods are very attractive and already widely used, but their dependability is questionable. Only a few approaches (see [1] and [11]) have been presented so far where semi-quantitative methods have formally been validate. But a standard for the use of such methods or against which methods can be checked has been missing so far.

3.2. Construction of a semi-quantitative risk analysis method

3.2.1. Requirements for semi-quantitative risk analysis methods

Although semi-quantitative risk analysis methods are very popular in many application areas, they have been justified only informally. Requirements for such methods were not clear in the past, but recently a German pre-standard DIN V VDE V 0831-101 has clearly set out the requirements. So, it is now possible to construct a method and validate it with respect to these requirements. There are in total 28 requirements, but not all relate to construction of the method. The following table gives an overview of the requirements; the mandatory requirements appear in bold. For more details we have to refer to [9].

3.2.2. Risk Score Matrix approach

A semi-quantitative approach is proposed which fulfils all requirements of the German pre-standard DIN V VDE V 0831-101. The model is called Risk Score Matrix (RSM) and consists of the application of a risk matrix and semi-quantitative score tables for assessment of the barriers. The complete approach is shown in *Figure 3*, jointly with additional and alternative steps. The final result consists of the hazard rates (HR) related to the functional failures (as hazards) of the technical system and the assumptions on which the analysis rests, which may turn into safety-related application rules (SAR).

Table 3. Summary of requirements

Construction	**A1**	**State clearly reference units and application scope.**
	A2	**Be conservative in your assessment.**
	A3	Make sure your parameter granularity is sufficient.
	A4	**Work out a user guide.**
	A6	**State clearly the system level to which the method applies.**
	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 risk acceptance criterion).**
	A24/ A25	**Assure proportionality between risk and criticality.**
	A26	**Small changes in the parameters lead to small changes in the result.**
	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.**

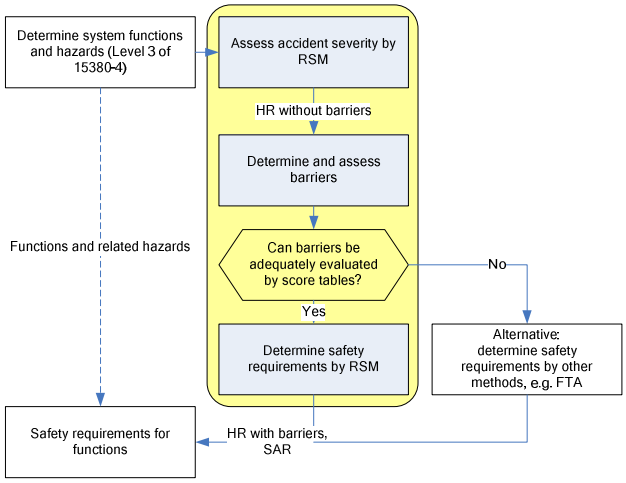

Figure 3: Overview of the Risk Score Matrix model

3.2.3. 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 (external) barriers mitigating the risk
- Maintenance is not included in the definition, but in maintenance manuals.
- Technical systems can be subject to a generic type approval, for which a stand-alone risk acceptance criterion is useful.

A function is 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 defined in prEN 15380-4 (2010) [8] as "level, to group functions of equal purpose". It is proposed to use [8] which contains up to five hierarchical levels. Taking into account the definition of function level, level 3 in [8] 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 4* gives some examples of functions to which RAC-TS may be applied. Although [8] 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 included in group K. In the following table, some examples of level 3 functions related to signaling are proposed.

Table 4: Examples of signalling functions

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 grade crossing
=LHB	Provide signal information
=LJB	Provide cab radio
=LKB	Display state to driver
=LKC	Display state to dispatcher
=LKD	Transmit commands

3.2.4. Risk matrix

A suitable risk matrix has already been proposed and justified in [5], see the following table. The table shows intolerable and tolerable combinations in a frequency scaling of √10. Safety targets would be chosen at the boundary between these two regions (medium gray shading).

Table 5: Proposed risk matrix

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

The corresponding accident severities are defined in *Table 6.* 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, e.g. 90% percentile.

Table 6: Consolidated severity categories

ID	Combinations	FWI range	Typi-cal 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.

3.2.5. Assessment of barriers

Serving as "obstacles" between the hazard and the actual accident, so called "barriers" have to be taken into account, differentiated according to the following types:

- possibility to avoid accident by human interaction (H)
- possibility to mitigate the hazard by an independent technical system (T)
- operational environment (B)

– demand frequency assessment (D)

The presence and efficiency of these barriers together with the severity assessment determine the outcome of the assessment and thus the appropriate safety requirements that will have to be achieved for the technical system under study. 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 5*. 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.

The complete 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.

3.2.9. Validation of the Risk Score Matrix method

It is not possible to give all arguments concerning the requirements from *Table 3* here, but it is possible to sketch 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 [1] and [11].

The scope as well as the units of measurement are well defined by Table 4 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 $\sqrt{10}$, 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 monotonous 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. Current developments and outlook

It rests to analyze in detail the pros and cons that an application of the method presented in chapter 3 to the example in chapter 2 were to bring about. Yet it can be stated right away that it would result in both a simplification and also in a more resilient analysis. This is due to the fact that the dependence on changing statistics and varying operation profiles were to diminish. Further analysis on this matter will be published.

Besides various other developments the following ones are to be counted among the most promising:

1. The European Railway Agency has set up special Task Forces dedicated to elaborating further the approach presented in chapter 3. Apart from the more general statements that will find their way into future European legislation, the accompanying documents with guidelines and examples provided by ERA will serve at least as the catalyst for models that will suit industries that do not necessarily dispose of the obliged accuracy of their data.
2. The German standardization committee for railway signaling is detailing the already published national pre-standard on risk analysis by working on the second part that will put it into practice, that is to say, that will provide concrete derivation of safety requirements for selected functionalities of the signaling system. This approach will be based on the principles outlined in chapter 3 of this article.

Though finding a model that is well equilibrated between the longing for accurate quantitative procedures and the reality determined by limited resources and scarcity of exact data seems to be an perennial task, the approach presented in chapter 3 of this article seems to come as close as reasonable possible to this state of equilibrium.

References

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

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

[3] Braband, J. (2005). *Risk analyses in railway automation* (in German). Hamburg, Eurailpress.

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

[5] Braband, J. (2011). *Semi-quantitative Risk Assessment of Technical Systems on European Railways*. RSRS 2011.

[6] Braband, J. & Lennartz, K. *A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications*. Signal+Draht, 9/99.

[7] CENELEC (1997). EN 50126 Railway applications –The specification and

demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

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

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

[10] 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.

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