한국철도학회논문집 제16권 제2호 ▌pp. 104-109 (2013년 4월)
JOURNAL OF THE KOREAN SOCIETY FOR RAILWAY VOL.16, NO.2 ▌pp. 104-109 (April 2013)
ISSN 1738-6225(Print)
ISSN 2288-2235(Online)

Determination of THRs – A Practical Approach for Manufacturers According to EN50129

Ulrich Weber*

Abstract The paper will outline how hazard identification and risk evaluation can effectively be performed to obtain Tolerable Hazard Rates (THR). As a target group manufacturers are addressed, who face the situation, that for a generic application THRs are needed for compliance with EN 50129 [1]. Focusing on functional hazards this paper shows a possible hazard log and the relevant analysis methods. The terms safety barrier and barrier function will be introduced and used instead of the term "safety function". As functional hazards and barrier functions depend on each other, emphasis will be put on a comprehensive and detailed definition of barrier functions and the usage of function lists. By using detailed and complete hazard and barrier function definitions THRs can be obtained while at the same time the approach becomes clear how the hazard rates (HR) will be established.

Keywords : Risk Analysis, THR, Safety Barrier, Hazard Log, Functional Failure

1. Introduction

For the following considerations it is assumed that a manufacturer wants to design a generic application, but safety requirements given by a railway undertaking or railway duty holder do not include THRs or have to be specified by the manufacturer, because for applications first invitations to bid have to be won. In these cases the supplier has to determine safety barriers and their functions together with the THRs. Without THRs it is impossible to prove compliance with EN50129 [1]. In the following text we will outline a risk analysis, which a manufacturer can carry out, and by which he can identify hazards together with barrier functions and specify their corresponding THRs. Established suppliers of railway systems have the knowledge and will give back the safety responsibility to the railway duty holder by a safety relevant application condition.

This paper will focus on the perspective of suppliers of electrical/electronic/programmable electronic systems (E/E/PE) and outline typical activities of a risk analysis: system definition, hazard identification, consequence analysis and risk estimation. Important is to follow a systematic procedure to assure and allow to judge qualitative requirements. THRs which are lower than necessary, but could be used as a selling argument, must be avoided, because the risk based approach of EN 50129 [1] is intended to reduce costs and such THRs would be contradictory.

*Corresponding author.
Tel.: +49-(0)531-3802-390, E-mail : Ulrich.Weber@tuev-sued.de

http://dx.doi.org/10.7782/JKSR.2013.16.2.104

2. Principles of Railway Operation

Control systems (or elements) and (railway) safety barriers shall ensure safe operation of trains. Control functions can be carried out by humans, e.g. drivers or train dispatchers, or technical systems, e.g. traffic control center. As defined by Sklet: "Safety barriers are physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents" [2]. Examples are: brakes, train control and protection systems, point controllers, signals, traffic lights, regulations, fences, flood warning system, operational rules or regulations. Safety Barriers usually include a barrier function, which is defined as "a function planned to prevent, control or mitigate undesired events or accidents" [2]. Examples are: apply train service brake, show red signal aspect or supervise turnout position.

For a hazardous situation usually control and protection functions must fail, but EN 50129 only concerns barrier functions of E/E/PE systems. The basic model (Fig. 1) shows the connection between the functional failure of a barrier function of a technical safety barrier (hazard), other safety barriers and the possible accident (based on model from [3]). At least one technical safety barrier is nearly always in place. Despite of a

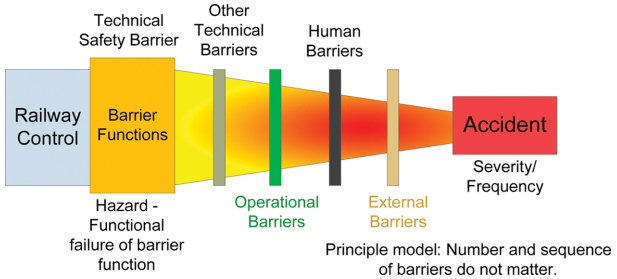

Fig. 1 Basic model (based on model from [3])

safety critical failure of a safety barrier, e.g. a signal controller, it depends on other barriers and further events or circumstances whether an accident occurs. As safety barriers can prevent or mitigate consequences also the severity of the accident depends on them.

3. System Definition

The results of a risk analysis always depend on a correct and complete system definition. A suitable system definition is the prerequisite for a meaningful risk analysis.

According to [4] the following aspects have to be covered by a system definition:

a) The intended purpose of the system;

b) Functions and components of the system (including e.g. human, technical and operational items/operational modes);

c) System boundaries, including external interfaces;

d) Definition of the physical interfaces (of those systems, with which interfaces exist) and functional interfaces (functional in- and output);

e) System environment (e.g., shock, vibration, EMC, operation);

f) Existing protection and mitigation measures – herein called 'safety barriers';

g) Assumptions determining boundaries of the risk estimation.

For the definition of operation modes IEC 62267 [6] should be used:

- On-Sight train Operation TOS;
- Non-automated train operation NTO;
- Semi-automated train operation STO;
- Unattended Train Operation UTO;
- Driverless Train Operation DTO.

A Block Diagram is an important part of a system definition. The following figure (Fig. 2) shows an example:

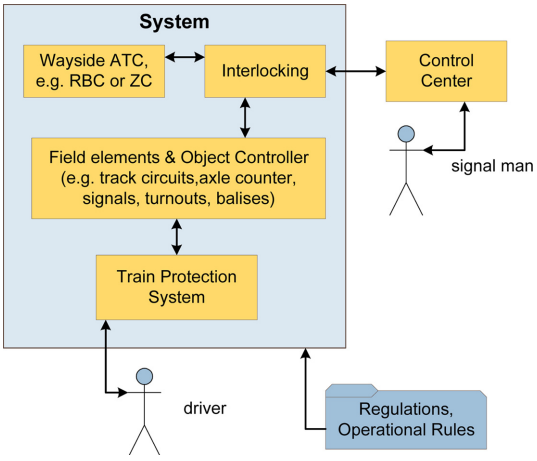

Fig. 2 System block diagram

The following example of operational conditions could further contribute to the system definition: Light Rail, speed 120 km/hours, mixed traffic, 2 trains per hour and STO.

Most of the above requirements can be fulfilled by use of a standardized function list, which implicitly defines the above aspects. The author suggests to combine function list and hazard list to form the intended hazard log. Function lists are available e.g. in prEN 15380-4 [8] or VDE 0831-101 [3]. Also several generic hazard lists have been created, see e.g. IEC 62267 [6] or refer to the project "ModUrban" [11].

Function lists can be grouped by basic railway functions, as suggested e.g. in IEC 62267 [6] and prEN 15380-4 [8]. Basic railway functions like "Ensure safe route", "Prevent collision with obstacles", "Ensure safe separation of trains" and "Ensure safe speed" are e.g. defined in IEC 62267 [6]. The author suggests to group the barrier functions instead by means of safety barriers. It is further recommended to create an extensive function definition, which gives a clear and complete picture and covers all architecture elements. Such a definition shows the way forward how the HR will be calculated e.g. by means of fault trees. A complete definition of functions should follow the scheme: Inputs – Processing – Outputs.

Barrier functions should be defined on system level in such a way that their functional failure can lead to an accident. The same hint coming from the Norway Petroleum Authority is stated in Skled [2]: "It shall be known what barriers have been established and which functions they are intended to fulfil. This means that a barrier should be well defined or formalised and be related to a specific hazard." For generic products, e.g. vital computer platforms, a risk analysis makes no or little sense. For such products THRs can be derived for the intended applications and then the THRs apportioned to subsystems and components (generic products).

As an example we consider a barrier function of a Platform Screen Door Control Unit: Instead of "Jam protection" a completer definition would look like this: "Detect an obstacle by measuring the motor drive current and in case of exceeding the predefined limit stop the motor drive, move the door leaves back and repeat this 2 times."

In case that several THRs of a railway system are to be considered it has to be taken into account that barrier functions shall be independent from each other.

4. Hazard Identification

4.1 Selection of Risk Acceptance Criteria

The principle procedure is shown in the following data flow diagram. If the risk is not broadly acceptable then a certain risk acceptance criteria has to be selected, which also is a matter of national laws, regulations and cultural aspects.

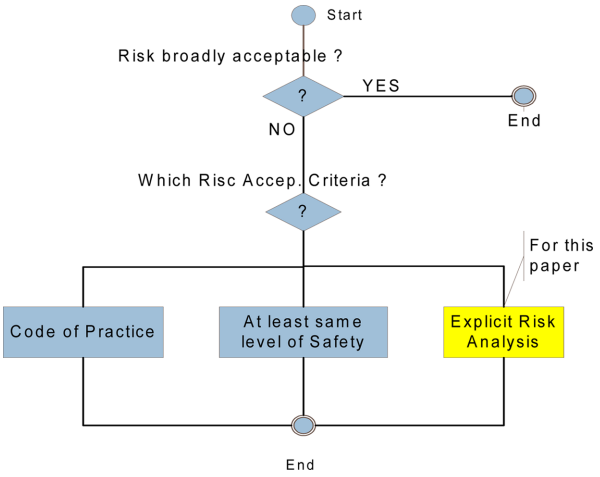

Fig. 3 Selection of risk acceptance criteria

Broadly acceptable risk: In principle risks resulting from hazards can be classified as acceptable, if the risk is so low, that it is not appropriate to introduce further safety barriers.

Code of practice:

Let us assume the following hazard:

H1: Fire can break out due to use of *easy flammable material.*

To this hazard belongs the function:

F1: *Protect against fire (from [8])*

EU CSM-RA states [4]: *"On the basis of the selected risk acceptance principles safety requirements can refer to Code of Practice (CoP), to similar systems or give explicit targets derived from an explicit risk estimation ('ERE').* 'Code of practice' means a written set of rules that, when correctly applied, can be used to control one or more specific hazards".

Hazards related to fire will be covered by Code of Practice, which would be managed in a complete hazard log with a corresponding column to provide for each hazard the risk acceptance criteria. As the focus in this paper is related to THRs only ERE has to be considered and hazards falling under CoP can be skipped in our hazard log. Following the CSM-RA regulation and taking the goal (chapt. Introduction) into account in the here suggested hazard log all non functional hazards can be excluded from the hazard list.

4.2 Hazards and Functions

Because functional hazards and barrier functions can be derived from each other, they should be considered together. The example in Table 1 shows how the negation of a barrier function results into the corresponding hazard. It works also in the other way round: for hazards barrier functions can be identified or specified.

5. Consequence Analysis

For the consequence analysis **accident classes** should be used as Braband states in [5]: "In order to reach an unambiguous and easy-to-use classification, accidents instead of severities should be classified". Table 2 shows an example of a classification matrix with letters A to E ranking the severity.

Table 1 Connection of hazard and failure of barrier function

Barrier Function	Hazard
Detect Service Brake demand (signal via MVB), control valves to generate the required brake cylinder pressure with jerk limitation depending on the current dynamic brake effort (signal via MVB) and actual car load.	Critical loss of braking capacity of one bogie (or axle or car) (unrecognized insufficient brake effort) caused by • undetected brake command • vehicle load falsely considered • falsely calculated values (wrong brake blending)

Table 2 Accident classification matrix (from [5])

Severity ranking	Collision	Derailment	Impact	Personal Accidents
E	Passenger train at high speed	Passenger train on a main line		-
D	Passenger train at medium speed	At a level crossing	Train with work gang	Passenger falling out of a train at high speed
C	Passenger train at low speed			Passenger falling out of a train at low speed or at a stop
B	In shunting operation		Train into buffer at low speed	Passenger hit by a door Passenger falling during embarkment.
A				

The table may be used e.g. in case that the method risk matrix is applied for risk evaluation.

6. Risk Estimation

For risk estimation the semi-quantitative methods risk matrix, risk graph or BP-risk are suitable and except for BP-Risk, which is quite new, are widely used. They have to be carefully calibrated e.g. be using the "Risk acceptance criteria - Technical Systems" - RAC-TS, which has been defined in [4].

RAC-TS: *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.*

RAC-TS shall be applied where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system. The next version of the CSM-RA regulation [4] will contain additional figures for events with less severe consequences (see [12]).

6.1 Example Hazard Log

On the next page (page 6) an example of a hazard log is shown (Table 6). Usually it will be realized within a spreadsheet program, which allows to obtain directly a THR after entering or changing the parameters of the used risk estimation method. The following tables show the parameters of the corresponding method and one table could replace the column "risk estimation" in the example table (Table 6).

The example in Table 3 shows that certain values can be applied to the parameters of the risk graph and then by means of some simple formulas in a spreadsheet calculation the corresponding THR of 10^{-7}/h is calculated. In brackets are the ranges of the values listed (for example the parameter consequence may have a value between 1 and 4). Due to the limited size of this paper more details cannot be provided here.

Table 5 Parameters of risk matrix

Risk matrix		
S[1..6]	F[1..9]	
Severity	Frequency	THR
4	4	0,5 10E-8

The examples in Table 4 and 5 just show how defined parameter values result in a THR if the mathematical formulas of the corresponding method are realized in a spreadsheet software.

All defined parameters shall be justified by outlining all assumptions and considerations in the risk analysis report thus allowing the reader to understand the reasons for certain parameter values.

7. Conclusions

Ongoing research and analyses are taking care that in some years lists with generic railway system functions, generic hazards and corresponding THRs will be available. Until this time an effective risk analysis should follow these instructions: derive hazards from barrier functions, structure the hazard log by safety barriers and their barrier functions, define barrier functions completely (no shortened definitions) and explain all assumptions and considerations in a report. The examples of function definitions in this paper shall demonstrate approach and benefit of completely defined functions. In this manner the complete process of determining THRs and the calculation of the HRs becomes more transparent.

Table 3 Parameters of risk graph

Risk Graph				
C[1..4]	F[1..2]	P[1..2]	W[1..3]	THR
(Consequence)	(Frequency)	(People affected)	(Defense)	
2	1	4	3	10E-7

Table 4 Parameters of BP-Risk

BP Risk								
Severity				Defence			Occurrence	
T (Train category)	V (Velocity)	A (People affected)	S (Severity) T+V+A	B (Density)	M (Human action)	G (Defence) B+M	O (S+G)	THR
1	3	1	5	3	5	8	13	3×10^{-9}/h

Table 6 Example Hazard log (extract – more barrier functions and hazards exist for each safety barrier)

Haz ID	Barrier Function	Hazard	Causes	Operation mode	Other barriers	Accident/ consequence	Risk estimat.				THR
	Brake control system										
H101	Detect Service Brake demand (signal via MVB), control valves to generate the required brake cylinder pressure with jerk limitation depending on the current dynamic brake effort (signal via MVB) and actual car load	Critical loss of braking capacity of the train (unrecognized insufficient brake effort) caused by • undetected Brake command • false car load considered • wrongly calculated brake blending values	Failure of brake control system	STO, DTO	• low speed allowed • daily brake test • additional eddy current brake • redundant brakes on each car	Impact, Derailment-[C] (see table 2)					
	Point controller (Object controller)										
H201	Detect and notify position of switch to interlocking and supervise end position	Switch end position notified despite switch had not entered end position	Failure of point controller or point machine	TOS	• driver can notice • trains run with low speed	Collision, Derailment [D]					
H202		Switch changes untimely its position.	Failure of point controller or point machine	TOS	• driver can notice hazard	Derailment [D]					
H203		Wrong switch position notified to interlocking	Failure of point controller or point machine	TOS	• driver can notice • point position signal	Collision, Derailment [D]					
	PSD control system										
H301	Ensure that Platform Screen Doors are only opened if a train has stopped at the correct position (doors are aligned)	Platform Screen Doors are opened despite there is no train in front of them	Failure of train position detection or ATP interface	UTO, Passenger exchange	• white line on platform • speaker announcement	1 - 3 passengers can fall on the track and be hit by a train					
H302	Detect speed/kinetic energy of closing door and stop motor drive in case of too high speed.	A Platform Screen Door is closing with too high speed.	Failure of motor drive or door control unit	TOS, Passenger exchange	• alarm sound • white line on platform	Passenger jammed					

References

[1] EN 50129:2003, Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling.

[2] S. Sklet (2006) Safety barriers: definition, classification, and performance, *Journal of Loss Prevention in the Process Industries*, 19(5), pp. 494-506.

[3] DIN VDE 0831-101, 5:2010, Elektrische Bahn-Signalanlagen -Teil 101: Semi-quantitative Verfahren zur Risikoanalyse technischer Funktionen in der Eisenbahnsignaltechnik.

[4] Commission Regulation (EC) No. 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment (acc. Directive 2004/49/EC).

[5] J. Braband (2010) On the justification of a risk matrix for technical systems in European railways, *Proceedings of the 8th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems*, Braunschweig, Germany, pp. 185-193.

[6] IEC 62267:2009 Railway application - Automated guided urban transport (AUGT) - Safety Requirements.

[7] E DIN VDE 0831-102, Version 0.5, 29.02.2012: Elektrische Bahn-Signalanlagen - Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik im Geltungsbereich der VO(EG) Nr. 352/2009.

[8] prEN 15380-4:2007, CENELEC, Railway applications - Classification system for rail vehicles - part 4.

[9] IEC 62290-1:2007 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts.

[10] IEC 62290-2:2011: Railway applications - Urban guided transport management and command/control systems - Part 2: Functional requirements specification.

[11] http://www.modurban.org/

[12] ERA Safety Unit - CSM Team, 13.07.2012, Agency report on the experience with the existing regulation (EC) N° 352/2009 on a common safety method on risk evaluation and assessment and on the revision of that regulation, Version: 1.0.

접수일(2013년 3월 19일), 게재확정일(2013년 3월 25일)

Ulrich Weber: Ulrich.Weber@tuev-sued.de
TUEV SUED Rail GmbH, Braunschweig, 38106, Germany