SLOVENSKI STANDARD
oSIST prEN 50126-2:2013

01-januar-2013

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 2. del: Sistemski pristop k varnosti

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems approach to safety

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Ta slovenski standard je istoveten z: **prEN 50126-2:2012**

ICS:

29.280	Električna vlečna oprema	Electric traction equipment
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50126-2:2013 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT prEN 50126-2

October 2012

ICS 45.020

Will supersede EN 50126-1:1999 (partially)

English version

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems approach to safety

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

This draft European Standard is submitted to CENELEC members for CENELEC enquiry. Deadline for CENELEC: 2013-03-29.

It has been drawn up by CLC/TC 9X.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Contents

Page

Foreword

This document [prEN 50126-2:2012] has been prepared by CLC/TC 9X "Electrical and electronic applications for railways".

This document is currently submitted to the Enquiry.

EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*" consists of the following parts:

– Part 1: Generic RAMS process;

– Part 2: Systems approach to safety;

– Part 4: Functional safety – Electrical/Electronic/Programmable electronic systems;

– Part 5: Functional safety – Software.

This new edition of EN 50126 (all parts) will supersede EN 50126-1:1999, CLC/TR 50126-2:2007, CLC/TR 50126-3:2008, EN 50128:2011 and EN 50129:2003.

This part of EN 50126 covers the systems approach to safety. It is mainly based on EN°50126-1:1999.

This part of EN 50126 will supersede EN 50126-1:1999 (together with prEN 50126-2:2012).

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

Introduction

EN 50126-1:1999 was produced to introduce the application of a systematic RAMS management process in the railway sector. For safety-related electronic systems for signalling EN 50128 and EN 50129 were produced. Through the application of these standards and the experiences gained over the last years, the need for revision and restructuring became apparent with a need to deliver a systematic and coherent approach to RAMS applicable to all the railway application fields Signalling, Rolling Stock and Electric power supply for Railways (Fixed Installations).

The revision work improved the coherency and consistency of the standards, the concept of safety management and the practical usage of EN 50126 and took into consideration the existing and related Technical Reports as well.

This European Standard provides railway duty holders and the railway suppliers, throughout the European Union, with a process which will enable the implementation of a consistent approach to the management of reliability, availability, maintainability and safety, denoted by the acronym RAMS.

Processes for the specification and demonstration of RAMS requirements are cornerstones of this standard. This European Standard promotes a common understanding and approach to the management of RAMS.

EN 50126 is the railways sector specific application of IEC 61508. Meeting the requirements in this European Standard is sufficient to ensure that additional compliance to IEC 61508 does not need to be evaluated.

With regard to safety EN 50126-1 provides a Safety Management Process which is supported by guidance and methods described in EN 50126-2.

EN 50126-1 and EN 50126-2 are independent from the technology used. EN 50126-4 and EN 50126-5 provide guidance specific to safety-related E/E/PE technology of railway applications. Their application is determined through the application of the general RAMS process of EN 50126-1 and through the outcome of the safety-related methods described in EN 50126-2. As far as safety is concerned, EN 50126 takes the perspective of functional safety. This does not exclude other aspects of safety. However, these are not the focus.

The aims set for revision of EN 50126 required a better understanding of the systems approach and improved methods for applying the safety management process described in EN 50126-1. EN 50126-2 provides this guidance.

The application of this standard should be adapted to the specific requirements of the system under consideration.

This European Standard can be applied systematically by the railway duty holders and railway suppliers, throughout all phases of the life-cycle of a railway application, to develop railway specific RAMS requirements and to achieve compliance with these requirements. The systems-level approach developed by this European Standard facilitates assessment of the RAMS interactions between elements of railway applications even if they are of complex nature.

This European Standard promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAMS and cost for railway applications. Adoption of this European Standard will support the principles of the European Single Market and facilitate European railway inter-operability.

The process defined by this European Standard assumes that railway duty holders and railway suppliers have business-level policies addressing Quality, Performance and Safety. The approach defined in this standard is consistent with the application of quality management requirements contained within the ISO 9001.

4196 In accordance with CENELEC editing rules [1)], mandatory requirements in this standard are
4197 indicated with the modal verb “shall”. Where justifiable, the standard permits process tailoring.
4198 Specific guidance on the application of this standard in the case of process tailoring is provided
4199 in 7.3 of EN 50126-1. EN 50126-2 provides various methods for use in the safety management
4200 process. Where a particular method is selected for the system under consideration, the
4201 mandatory requirements of this method are by consequence mandatory for the safety
4202 management of the system under consideration.

1) CENELEC “Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2009-08), Annex H.

1 Scope

This part of EN 50126

- considers the safety-related generic aspects of the RAMS life-cycle. The guidance in this part is still applicable in the application of specific standards;
- defines methods and tools which are independent of the actual technology of the systems and subsystems, whilst following EN 50126-4 and EN 50126-5 are related to E/E/PE internal systems/subsystems;
- provides:
  - the user of the standard with the understanding of the system approach to safety which is a key concept of EN 50126;
  - methods to derive the safety requirements and their safety integrity requirements for the system and to apportion it to the subsystems, be it for hardware or software;
- provides guidance and methods for the following areas:
  - system life-cycles as applicable to generic and specific applications, and to the generic products;
  - systems safety assurance;
  - risk assessment process;
  - risk management process;
  - application of risk acceptance principles and criteria;
  - safety integrity concept.
- provides the user with the methods to assure safety with respect to the system under consideration and its interactions. Examples are guidance on safety integrity by the apportionment amongst the various parts of a system or a method to derive the safety-related role of software as a precondition to apply EN 50126-5;
- enables the user to define the system under consideration, to identify the interfaces and the interactions of this system with its subsystems or other systems and to conduct the risk analysis;
- addresses railway specifics;
- does not define:
  - RAMS targets, quantities, requirements or solutions for specific railway applications;
  - rules or processes pertaining to the certification of railway products against the requirements of this standard;
  - an approval process by the safety authority.
- does not specify requirements for ensuring system security.

This part 2 of EN 50126 is applicable

- to all systems under consideration - as regards safety - within the entire railway system and the stakeholders involved;
- to the specification and demonstration of safety for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major systems and to individual and combined sub-systems and components within these major systems, including those containing software; in particular:
  - to new systems;
  - to new systems integrated into existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system;
  - for modifications of existing systems in operation prior to the creation of this standard, although it is not generally applicable to other aspects of the existing system;
  - at all relevant phases of the life-cycle of an application;
  - for use by railway duty holders and the railway suppliers.

It is not required to apply this standard to existing systems including those systems already compliant with any version of former EN 50126, EN 50128 or EN 50129, which remain unmodified. Railway applications mean Command, Control & Signalling, Rolling Stock and Electric Power Supply for Railways (Fixed Installations).

In this standard the term hardware refers to E/E/PE components or systems. If non-E/E/PE hardware is meant, this is specifically mentioned.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 501261:2012, *Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process*

ISO 9001, *Quality management systems – Requirements*

ISO/IEC GUIDE 51, *Safety aspects – Guidelines for their inclusion in standards*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in prEN 50126-1:2012 apply.

4 Abbreviations

ALARP	As Low As Reasonable Practicable
CBA	Cost Benefit Analysis
CCF	Common Cause Failure (Analysis)
CoP	Code of Practice
DCCA	Deductive Cause-Consequence Analysis
DRA	Differential Risk Aversion
E/E/PE	Electrical/electronic/programmable electronic systems
ERE	Explicit Risk Estimation
EMC	Electromagnetic capability
ETA	Event Tree Analysis
FCA	Failure Consequence Analysis
FMECA	Failure Mode Effect & Criticality Analysis
FTA	Fault Tree Analysis
GA, GASC	Generic Application, Generic Application Safety Case
GP, GPSC	Generic Product, Generic Product Safety Case
GAME	Globalement Au Moins Equivalent
HAZOP	Hazard and Operability study
ISA	Independent Safety Assessment
MEM	Minimum Endogenous Mortality
RAC	Risk Acceptance Criterion
RAMS	Reliability, Availability, Maintainability, Safety
RBD	Reliability Block Diagram
RRA	Rapid Ranking Analysis
SA, SASC	Specific Application, Specific Application Safety Case
SDR	Safe Down Rate
SDT	Safe Down Time
SIL	Safety Integrity Level
SRAC	Safety-related Application Conditions
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
VPF	Value of Preventing a Fatality

5 Tailoring the life-cycle

5.1 The life-cycle Model

The model described in EN 50126-1 covers general RAMS aspect of the whole life-cycle.

From the perspective of safety methods, with the aim of

- achieving a clear definition of responsibilities and interfaces between the operator and the supplier, and
- facilitating reuse of existing systems and their related acceptance,

the following subclauses are introducing the concept of hourglass model (see 5.2) and the distinction between generic product, generic application and specific application processes (see 5.3).

5.2 The Hourglass Model

In this subclause, the so-called Hourglass Model is introduced: it offers a simplified approach that although not containing all aspects implied in the life-cycle model helps to clarify some issues.

The Hourglass Model provides an overview of the major safety-related activities that are needed to ensure an acceptable safety level for a technical system, including the corresponding responsibility areas.

Technical system means a product or an assembly of products including the design, implementation and support documentation. The development of a technical system starts with its requirements specification and ends with its acceptance. The design of relevant interfaces with human behaviour is considered, while human operators and their actions are not included in a technical system. Both the maintenance process (described in the maintenance manuals) and the operation are specified but are not considered parts of the technical system itself. They can be restricted in “application conditions”.

The purpose of this model is to highlight the separation between risk analysis (at the railway system level) from hazard analysis (at the level of the system under consideration).

This enhances co-operation between the relevant stakeholders, clarifying responsibilities and interfaces and has the advantages of reducing complexity and facilitating modularization.

The Hourglass Model describes two main aspects:

- “risk assessment”, i.e. deriving high-level safety requirements for operational and technical issues (including maintenance), and
- “hazard control”, i.e. design and implementation of the safety-related system under consideration by determining and analysing causes internal to the system and implementing control measures on the basis of the given safety requirements.

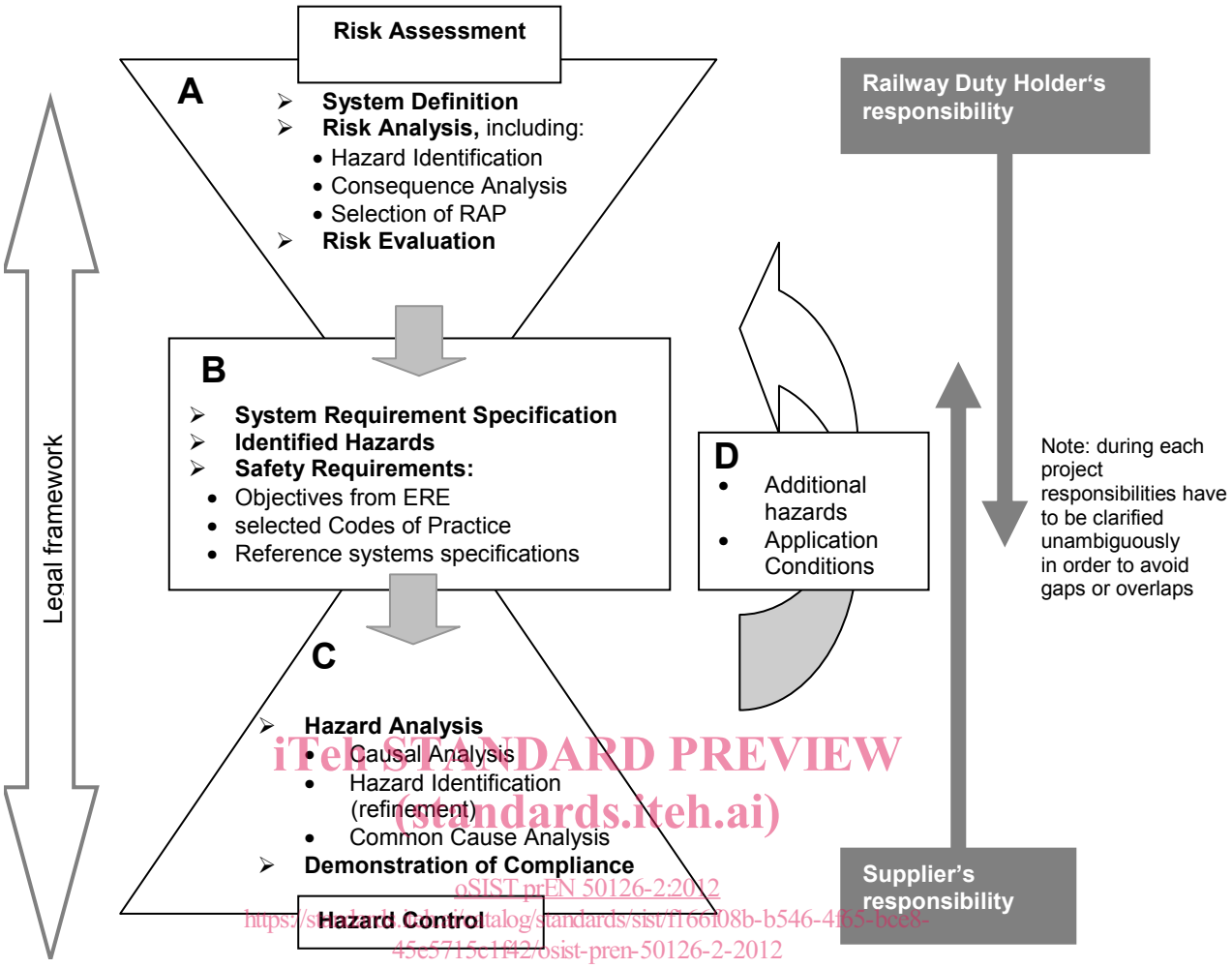

Figure 1 – The Hourglass Model

A Risk assessment

Risk assessment is performed at the railway system level.

It covers system definition, risk analysis, risk evaluation.

It defines the high level system safety requirements, in particular safety requirements for the system under consideration from the perspective of operator. It takes into account safety-related operational aspects, previous experience and the regulatory requirements of the railway application.

The main task for this activity is the risk analysis, which is derived from the system definition. The risk analysis includes hazard identification, consequence analysis, and selection of risk acceptance principles ("RAP" in the picture) and associated criteria.

The specification of safety requirements is the final result of risk assessment; in Figure 1 it is allocated in box B, because it has an interface function (together with system requirement specifications and the list of identified hazards) between different responsibilities.

Gaining and sharing system knowledge

All the knowledge gained during the process and the documented analyses, resulting from the risk assessment, should be considered as relevant information together with the specification of safety requirements.

This knowledge should be shared and distributed among the stakeholders involved in the system process. It will provide significant potential benefits in terms of improved awareness of hazards and risk of accidents in the given operational and maintenance context, and will also help to understand the scope and limits of the risk reduction measures.

Conducting risk assessment

The level of detail in a risk assessment should be adequate to the risk. The purpose is not to catalogue every trivial hazard, nor is it expected that hazards beyond the limits of current knowledge will always be identified. A suitable and sufficient risk assessment should reflect a reasonable analysis of hazards and their associated risks within the railway operation and within the applied technology itself. Where reasonably practicable, risk assessments should be correlated with historical records of accidents and the records of causes.

When possible, consideration of technical implementation/architecture should be avoided in this first stage i.e. the system to be developed should be considered as a black box, of which functions and hazards are evaluated only at the boundaries. These boundaries are well defined interfaces between the operational environment and the system under consideration.

As an example, an “unintentional train motion” is a hazard for a train. It can be observed as an abstraction at the boundary of the “system train” and it could lead to different accidents depending on the operational context (e.g. collision in context with over-speeding while running or fall of persons in connection with a train moving in a station while expected to stand still, etc.).

Assumptions defined during the risk assessment have to be checked and updated throughout the life-cycle phases.

B Outcomes of the risk assessment

The results of the first stage of the risk assessment are a set of safety requirements attached to clearly-identified functions, systems or operating rules. They are part of the System Requirement Specification that establishes the technical interface between the stakeholders.

NOTE The project organisational structure and responsibilities are another factor to consider in understanding and controlling risk. For organisational aspects and requirements see EN 50126-1, 5.3 and EN 50126-1, 7.1.1.3

On the basis of the selected risk acceptance principles, safety requirements can refer to Codes of Practise, to similar systems, or give explicit targets derived from an explicit risk estimation (“ERE” in the picture).

Safety requirements include required efficiency of safety functions , that could be assessed quantitatively (e.g. maximum rates of hazards), semi-quantitatively or qualitatively (e.g. use of trained drivers for controlling human factor errors).

Safety requirements should be assessed with a holistic approach, i.e. the residual risk should be evaluated as acceptable taking into consideration the identified hazards.

C Hazard control

The hazard control stage in the hourglass model is dedicated to ensuring that the system under consideration is compliant with the safety requirements: hence hazard control is performed for a specific system architecture.

NOTE Hazard control as here defined has a narrow meaning and is limited to the design and implementation phase.

The major impacts of human factors, operational and general maintenance rules as well as procedures are part of the preceding risk analysis and should have already been taken into account in the safety requirements. Therefore, during hazard control, the designer of the system under consideration can focus on the internal causes of the identified hazards, that can be considered as hazards at the system level.

The main task for this activity is the “hazard analysis” comprising:

– causal analysis;

– a dedicated hazard identification focusing on the system under consideration, and;

– a Common Cause Analysis.

Hazard identification is a recurring task that can appear on several iteration levels for subsets of the system under consideration. In order to distinguish these different tasks (and related documents) the hazard identification has been quoted twice in Figure 1:

1. during risk assessment, it focuses on high level hazards derived from the system functions (black box) and related operation of the system as well as its environment;
2. within the hazard control, a refined/iterated hazard identification focuses on hazards and their causes derived from the technical solutions, i.e. from defined architecture and internal interfaces of the system under consideration, and potential new hazards introduced by the system itself.

Figure 2 shows that the cause of a hazard at the railway system level may be considered as a hazard on level of the system under consideration, with respect to its boundary. The boundary for a hazard identification is always given in the system definition that limits the scope of the task. This implies that the hazards are structured hierarchically hence a hierarchical approach to hazard analysis and hazard logging should be used.

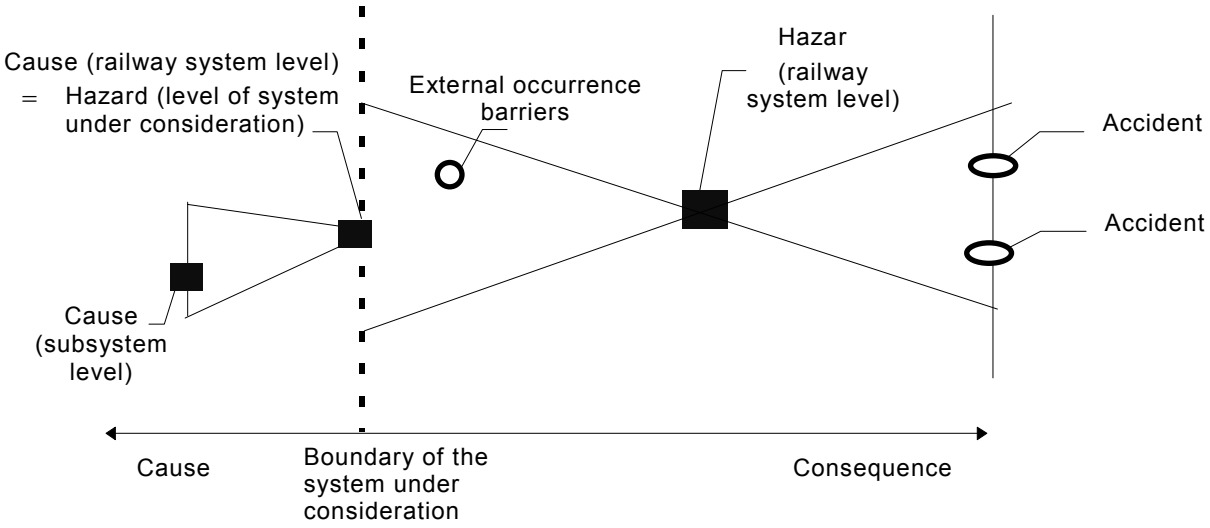

Figure 2 – Definition of hazards with respect to the system boundary

The picture is hazard-oriented and shows a “bow-tie” shape, suggesting that several causes may lead to the same hazard and one hazard may lead to several different accidents.

The demonstration of compliance with the safety requirements of the system under consideration can be performed in various forms. These forms depend on the nature of the underlying requirements set at the beginning of the hazard control.

D Revision of risk assessment

During the hazard control stage, fulfilment of safety targets may not be reached at the first iteration:

– additional hazards may be identified at the level of the system under consideration;

– a need of new operational rules may arise;

– additional external safety measures may be required to fulfil the safety objectives.

In all these cases, a revision of the risk assessment is necessary.

This revision should also take account of the application conditions that could rise at the level of the system under consideration.

Responsibilities

Risk assessment is mainly within the responsibility of the railway duty holders and operators.

The roles and responsibilities may however be contracted to other parties in relation to their accountabilities, provided that they have a documented and suitable range of competencies to consider the whole operational context in detail. They need to take into account safety-related operational aspects, previous experience and regulatory requirements. In any case the railway duty holders should approve the results of the risk assessment.

The hazard control, for hazards associated purely with the technical system, is the responsibility of the supplier of the technical system.

Railway duty holder and supplier need to comply with the prevailing legal requirements.