



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

<https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012>

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[oSIST prEN 50126-2:2012](https://standards.iteh.ai/catalog/standards/sist/f166f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012)

<https://standards.iteh.ai/catalog/standards/sist/f166f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012>

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

iTeh STANDARD PREVIEW

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. [oSIST prEN 50126-2:2012](https://standards.iteh.ai/catalog/standards/sist/f166f08b-b546-4f65-bce8-43a018c1402a/pr-en-50126-2-2012)

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

4001	Contents	Page
4002	Foreword	5
4003	Introduction.....	6
4004	1 Scope.....	8
4005	2 Normative references	9
4006	3 Terms and definitions	9
4007	4 Abbreviations	9
4008	5 Tailoring the life-cycle	10
4009	5.1 The life-cycle Model	10
4010	5.2 The Hourglass Model	10
4011	5.3 Generic and specific safety acceptance processes	14
4012	5.3.1 Introduction	14
4013	5.3.2 Safety acceptance process.....	14
4014	5.3.3 After safety acceptance	16
4015	5.3.4 Dependency between safety cases.....	16
4016	5.3.5 Relationship between safety case dependencies and system architecture	17
4017	6 Avoidance of systematic failures.....	17
4018	6.1 General	17
4019	6.2 Independent safety assessment	17
4020	6.3 Prevention of systematic failure in the early phases of the life-cycle.....	18
4021	6.4 Detection and correction of systematic failure during the design and development	
4022	phases of the life-cycle.....	19
4023	6.5 Detection and correction of systematic failure during integration and following	
4024	phases of the life-cycle.....	19
4025	7 Guidance on system definition.....	21
4026	7.1 System definition in an iterative system approach	21
4027	7.2 Method for defining the structure of a system	21
4028	7.3 Parties/stakeholders/boundaries of systems	22
4029	7.4 Guidance on the content of a system definition.....	22
4030	8 Risk analysis and evaluation	23
4031	8.1 General	23
4032	8.2 Hazard identification - process and methods	23
4033	8.2.1 General	23
4034	8.2.2 Empirical hazard identification methods.....	23
4035	8.2.3 Creative hazard identification methods	24
4036	8.3 Hazard classification	24
4037	8.4 Consequence analysis.....	24
4038	8.4.1 General	24
4039	8.4.2 The risk model.....	25
4040	8.4.3 Techniques for the consequence analysis.....	26
4041	8.5 Risk evaluation and acceptance	27
4042	8.5.1 Introduction to the risk acceptance principles	27
4043	8.5.2 Use of code of practice.....	28
4044	8.5.3 Use of a similar system as reference	28

4045	8.5.4	Explicit risk estimation	29
4046	8.6	Guidelines to the explicit risk estimation	30
4047	8.6.1	Rationale	30
4048	8.6.2	Quantitative approach	30
4049	8.7	Qualitative approach	33
4050	9	Specification of system requirements	33
4051	9.1	General	33
4052	9.2	Functional safety requirements	34
4053	9.3	Technical safety requirements	34
4054	9.4	Operational and maintenance safety requirements	35
4055	10	Apportionment of System Safety Requirements	35
4056	10.1	Deriving and apportioning system safety requirements	35
4057	10.1.1	How to proceed with functions implemented by E/E/PE architectures	35
4058	10.1.2	How to proceed with functions implemented by non-E/E/PE architecture	35
4059	10.2	Functional safety integrity for E/E/PE	35
4060	10.2.1	Deriving functional safety requirements for E/E/PE systems from defined	
4061		hazards	35
4062	10.2.2	The safety integrity concept and its levels	36
4063	10.2.3	Random aspects of functional safety integrity	37
4064	10.2.4	Systematic aspect of functional safety integrity	37
4065	10.2.5	Combination of random and systematic aspects	37
4066	10.2.6	The SIL table	38
4067	10.2.7	SIL allocation	39
4068	10.2.8	Apportionment of TFFR	40
4069	10.2.9	Demonstration of quantified targets	40
4070	10.2.10	SIL0	41
4071	10.2.11	Prevention of misuse of SILs and warnings	41
4072	10.3	Safety Integrity for non-E/E/PE systems – Guidance on application of CoP	41
4073	11	Design and implementation	42
4074	11.1	Causal analysis	42
4075	11.2	Identification and treatment of additional hazards arising from design	42
4076	11.3	Techniques for causal analysis	43
4077	11.4	Functional Safety principles	43
4078	11.4.1	Functional composition	43
4079	11.4.2	Independence of functions	44
4080	11.4.3	Supporting rules for evaluating technical aspects of independence	44
4081	Annex A (informative)	Measures for the avoidance of systematic failures	46
4082	A.1	General remark	46
4083	A.2	Safety and quality management	46
4084	A.3	System requirements specification	46
4085	A.4	System architecture and design	47
4086	A.5	Integration and testing of the system	47
4087	A.6	Application, operation and maintenance	47
4088	Annex B (informative)	ALARP, GAME, MEM	48
4089	Annex C (informative)	Using failure and accident statistics to derive a THR	54
4090	Annex D (informative)	CoP on maintenance activities to preserve the safety integrity of non-	
4091		E/E/PE systems	55
4092	Annex E (informative)	Apportionment methods	57

4093	Annex F (informative) Safety Target Quantification Methods	61
4094	Annex G (informative) Common mistakes in quantification	67
4095	Annex H (informative) Techniques / methods for safety analysis	68
4096		
4097	Figure 1 – The Hourglass Model	11
4098	Figure 2 – Definition of hazards with respect to the system boundary	13
4099	Figure 3 – Generic and specific safety acceptance processes	15
4100	Figure 4 – Examples of dependencies between safety cases	16
4101	Figure 5 – Organisational structure for early phases	19
4102	Figure 6 – Organisational structure for integration and final phases	20
4103	Figure 7 – An example of risk model	25
4104	Figure 8 – Tolerable rates in an example of risk model	31
4105	Figure 9 – Safety requirements	34
4106	Figure 10 – Apportionment of functional safety requirements	36
4107	Figure 11 – Relationship between SILs and techniques	38
4108	Figure 12 – Impact of functional dependence in a fault-tree analysis.....	44
4109	Figure B.1 – Example of simple qualitative risk matrix for use within an ALARP framework.....	50
4110	Figure B.2 – Example of semi-quantitative risk matrix for use within an ALARP framework	50
4111	Figure B.3 – Differential risk aversion	53
4112	Figure E.1 – Functional breakdown	57
4113	Figure E.2 – Analysis of the scenario: functional independence	58
4114	Figure E.3 – 1st step of apportionment: analysis of the system	59
4115	Figure E.4 – Example of quantified apportionment	60
4116	Figure F.1 – Interpretation of failure and repair times.....	61
4117	Figure F.2 – Double channel failure with common cause.....	63
4118	Figure G.1	67
4119		
4120	Table 1 – Typical examples for a functional breakdown.....	22
4121	Table 2 – Examples of hazards	26
4122	Table 3 – SIL and SIL-measures	38
4123	Table A.1 – Safety planning and quality assurance activities	46
4124	Table A.2 – System requirements specification	46
4125	Table A.3 – System architecture and design	47
4126	Table A.4 – Integration and testing of the system.....	47
4127	Table A.5 – Application, operation and maintenance.....	47
4128	Table B.1	48
4129	Table D.1 – Measures to achieve the necessary safety integrity of non-E/E/PE systems.....	56
4130	Table H.1 – Techniques / Methods for safety analysis.....	68
4131		

4132 Foreword

4133 This document [prEN 50126-2:2012] has been prepared by CLC/TC 9X "Electrical and electronic
4134 applications for railways".

4135 This document is currently submitted to the Enquiry.

4136 EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability,
4137 Maintainability and Safety (RAMS)*" consists of the following parts:

- 4138 – Part 1: Generic RAMS process;
- 4139 – Part 2: Systems approach to safety;
- 4140 – Part 4: Functional safety – Electrical/Electronic/Programmable electronic systems;
- 4141 – Part 5: Functional safety – Software.

4142 This new edition of EN 50126 (all parts) will supersede EN 50126-1:1999,
4143 CLC/TR 50126-2:2007, CLC/TR 50126-3:2008, EN 50128:2011 and EN 50129:2003.

4144 This part of EN 50126 covers the systems approach to safety. It is mainly based on
4145 EN°50126-1:1999.

4146 This part of EN 50126 will supersede EN 50126-1:1999 (together with prEN 50126-2:2012).

4147 This document has been prepared under a mandate given to CENELEC by the European
4148 Commission and the European Free Trade Association, and supports essential requirements of
4149 EU Directive(s).

ITEH STANDARD PREVIEW
(standards.iteh.ai)

[oSIST prEN 50126-2:2012](https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012)

<https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012>

4150 Introduction

4151 EN 50126-1:1999 was produced to introduce the application of a systematic RAMS management
4152 process in the railway sector. For safety-related electronic systems for signalling EN 50128 and
4153 EN 50129 were produced. Through the application of these standards and the experiences
4154 gained over the last years, the need for revision and restructuring became apparent with a need
4155 to deliver a systematic and coherent approach to RAMS applicable to all the railway application
4156 fields Signalling, Rolling Stock and Electric power supply for Railways (Fixed Installations).

4157 The revision work improved the coherency and consistency of the standards, the concept of
4158 safety management and the practical usage of EN 50126 and took into consideration the existing
4159 and related Technical Reports as well.

4160 This European Standard provides railway duty holders and the railway suppliers, throughout the
4161 European Union, with a process which will enable the implementation of a consistent approach to
4162 the management of reliability, availability, maintainability and safety, denoted by the acronym
4163 RAMS.

4164 Processes for the specification and demonstration of RAMS requirements are cornerstones of
4165 this standard. This European Standard promotes a common understanding and approach to the
4166 management of RAMS.

4167 EN 50126 is the railways sector specific application of IEC 61508. Meeting the requirements in
4168 this European Standard is sufficient to ensure that additional compliance to IEC 61508 does not
4169 need to be evaluated.

4170 With regard to safety EN 50126-1 provides a Safety Management Process which is supported by
4171 guidance and methods described in EN 50126-2.

4172 EN 50126-1 and EN 50126-2 are independent from the technology used. EN 50126-4 and
4173 EN 50126-5 provide guidance specific to safety-related E/E/PE technology of railway
4174 applications. Their application is determined through the application of the general RAMS
4175 process of EN 50126-1 and through the outcome of the safety-related methods described in
4176 EN 50126-2. As far as safety is concerned, EN 50126 takes the perspective of functional safety.
4177 This does not exclude other aspects of safety. However, these are not the focus.

4178 The aims set for revision of EN 50126 required a better understanding of the systems approach
4179 and improved methods for applying the safety management process described in EN 50126-1.
4180 EN 50126-2 provides this guidance.

4181 The application of this standard should be adapted to the specific requirements of the system
4182 under consideration.

4183 This European Standard can be applied systematically by the railway duty holders and railway
4184 suppliers, throughout all phases of the life-cycle of a railway application, to develop railway
4185 specific RAMS requirements and to achieve compliance with these requirements. The systems-
4186 level approach developed by this European Standard facilitates assessment of the RAMS
4187 interactions between elements of railway applications even if they are of complex nature.

4188 This European Standard promotes co-operation between the stakeholders of Railways in the
4189 achievement of an optimal combination of RAMS and cost for railway applications. Adoption of
4190 this European Standard will support the principles of the European Single Market and facilitate
4191 European railway inter-operability.

4192 The process defined by this European Standard assumes that railway duty holders and railway
4193 suppliers have business-level policies addressing Quality, Performance and Safety. The
4194 approach defined in this standard is consistent with the application of quality management
4195 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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[oSIST prEN 50126-2:2012](https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012)

<https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012>

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

4203 1 Scope

4204 This part of EN 50126

- 4205 • considers the safety-related generic aspects of the RAMS life-cycle. The guidance in this
- 4206 part is still applicable in the application of specific standards;
- 4207 • defines methods and tools which are independent of the actual technology of the systems
- 4208 and subsystems, whilst following EN 50126-4 and EN 50126-5 are related to E/E/PE internal
- 4209 systems/subsystems;
- 4210 • provides:
 - 4211 – the user of the standard with the understanding of the system approach to safety which
 - 4212 is a key concept of EN 50126;
 - 4213 – methods to derive the safety requirements and their safety integrity requirements for
 - 4214 the system and to apportion it to the subsystems, be it for hardware or software;
- 4215 • provides guidance and methods for the following areas:
 - 4216 – system life-cycles as applicable to generic and specific applications, and to the generic
 - 4217 products;
 - 4218 – systems safety assurance;
 - 4219 – risk assessment process;
 - 4220 – risk management process;
 - 4221 – application of risk acceptance principles and criteria;
 - 4222 – safety integrity concept.
- 4223 • provides the user with the methods to assure safety with respect to the system under
- 4224 consideration and its interactions. Examples are guidance on safety integrity by the
- 4225 apportionment amongst the various parts of a system or a method to derive the safety-
- 4226 related role of software as a precondition to apply EN 50126-5;
- 4227 • enables the user to define the system under consideration, to identify the interfaces and the
- 4228 interactions of this system with its subsystems or other systems and to conduct the risk
- 4229 analysis; <https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715c1f42/osist-pren-50126-2-2012>
- 4230 • addresses railway specifics;
- 4231 • does not define:
 - 4232 – RAMS targets, quantities, requirements or solutions for specific railway applications;
 - 4233 – rules or processes pertaining to the certification of railway products against the
 - 4234 requirements of this standard;
 - 4235 – an approval process by the safety authority.
- 4236 • does not specify requirements for ensuring system security.

4237 This part 2 of EN 50126 is applicable

- 4238 • to all systems under consideration - as regards safety - within the entire railway system and
- 4239 the stakeholders involved;
- 4240 • to the specification and demonstration of safety for all railway applications and at all levels
- 4241 of such an application, as appropriate, from complete railway systems to major systems and
- 4242 to individual and combined sub-systems and components within these major systems,
- 4243 including those containing software; in particular:
 - 4244 – to new systems;
 - 4245 – to new systems integrated into existing systems in operation prior to the creation of this
 - 4246 standard, although it is not generally applicable to other aspects of the existing system;
 - 4247 – for modifications of existing systems in operation prior to the creation of this standard,
 - 4248 although it is not generally applicable to other aspects of the existing system;
 - 4249 – at all relevant phases of the life-cycle of an application;
 - 4250 – for use by railway duty holders and the railway suppliers.

4251 It is not required to apply this standard to existing systems including those systems already
 4252 compliant with any version of former EN 50126, EN 50128 or EN 50129, which remain
 4253 unmodified. Railway applications mean Command, Control & Signalling, Rolling Stock and
 4254 Electric Power Supply for Railways (Fixed Installations).

4255 In this standard the term hardware refers to E/E/PE components or systems. If non-E/E/PE
4256 hardware is meant, this is specifically mentioned.

4257 **2 Normative references**

4258 The following documents, in whole or in part, are normatively referenced in this document and
4259 are indispensable for its application. For dated references, only the edition cited applies. For
4260 undated references, the latest edition of the referenced document (including any amendments)
4261 applies.

4262 prEN 501261:2012, *Railway applications – The Specification and Demonstration of Reliability,*
4263 *Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process*

4264 ISO 9001, *Quality management systems – Requirements*

4265 ISO/IEC GUIDE 51, *Safety aspects – Guidelines for their inclusion in standards*

4266 **3 Terms and definitions**

4267 For the purposes of this document, the terms and definitions given in prEN 50126-1:2012 apply.

4268 **4 Abbreviations**

4269	ALARP	As Low As Reasonable Practicable
4270	CBA	Cost Benefit Analysis
4271	CCF	Common Cause Failure (Analysis)
4272	CoP	Code of Practice
4273	DCCA	Deductive Cause-Consequence Analysis
4274	DRA	Differential Risk Aversion
4275	E/E/PE	Electrical/electronic/programmable electronic systems
4276	ERE	Explicit Risk Estimation
4277	EMC	Electromagnetic capability
4278	ETA	Event Tree Analysis oSIST prEN 50126-2:2012
4279	FCA	Failure Consequence Analysis https://standards.iteh.ai/catalog/standards/sist/fl66f08b-b546-4f65-bce8-45e5715e1f42/osist-pren-50126-2-2012
4280	FMECA	Failure Mode Effect & Criticality Analysis
4281	FTA	Fault Tree Analysis
4282	GA, GASC	Generic Application, Generic Application Safety Case
4283	GP, GPSC	Generic Product, Generic Product Safety Case
4284	GAME	Globalement Au Moins Equivalent
4285	HAZOP	Hazard and Operability study
4286	ISA	Independent Safety Assessment
4287	MEM	Minimum Endogenous Mortality
4288	RAC	Risk Acceptance Criterion
4289	RAMS	Reliability, Availability, Maintainability, Safety
4290	RBD	Reliability Block Diagram
4291	RRA	Rapid Ranking Analysis
4292	SA, SASC	Specific Application, Specific Application Safety Case
4293	SDR	Safe Down Rate
4294	SDT	Safe Down Time
4295	SIL	Safety Integrity Level
4296	SRAC	Safety-related Application Conditions
4297	TFFR	Tolerable Functional Failure Rate
4298	THR	Tolerable Hazard Rate
4299	VPF	Value of Preventing a Fatality
4300		

4301 **5 Tailoring the life-cycle**

4302 **5.1 The life-cycle Model**

4303 The model described in EN 50126-1 covers general RAMS aspect of the whole life-cycle.

4304 From the perspective of safety methods, with the aim of

- 4305 • achieving a clear definition of responsibilities and interfaces between the operator and the
- 4306 supplier, and
- 4307 • facilitating reuse of existing systems and their related acceptance,

4308 the following subclauses are introducing the concept of hourglass model (see 5.2) and the
4309 distinction between generic product, generic application and specific application processes (see
4310 5.3).

4311 **5.2 The Hourglass Model**

4312 In this subclause, the so-called Hourglass Model is introduced: it offers a simplified approach
4313 that although not containing all aspects implied in the life-cycle model helps to clarify some
4314 issues.

4315 The Hourglass Model provides an overview of the major safety-related activities that are needed
4316 to ensure an acceptable safety level for a technical system, including the corresponding
4317 responsibility areas.

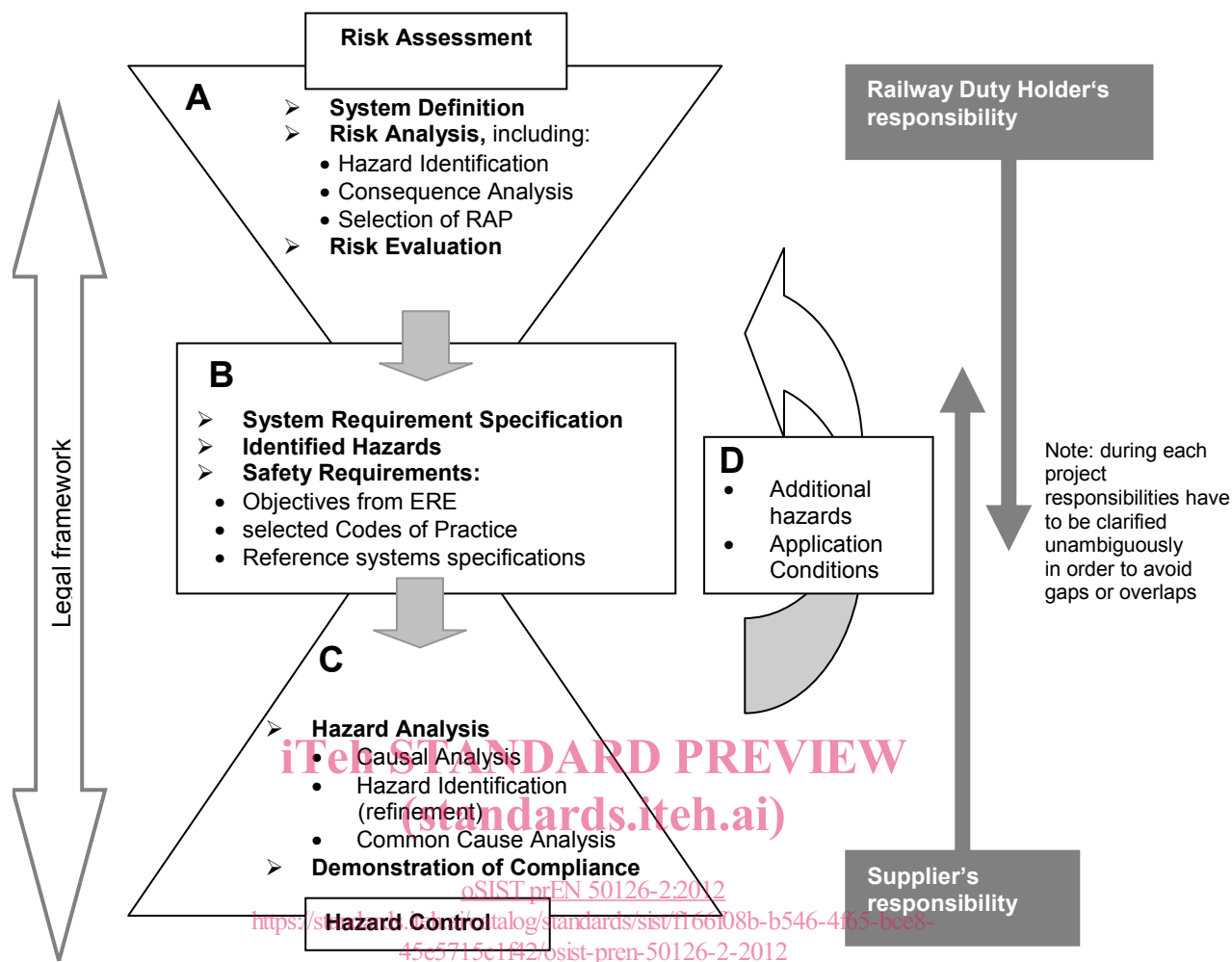
4318 Technical system means a product or an assembly of products including the design,
4319 implementation and support documentation. The development of a technical system starts with
4320 its requirements specification and ends with its acceptance. The design of relevant interfaces
4321 with human behaviour is considered, while human operators and their actions are not included in
4322 a technical system. Both the maintenance process (described in the maintenance manuals) and
4323 the operation are specified but are not considered parts of the technical system itself. They can
4324 be restricted in "application conditions"

4325 The purpose of this model is to highlight the separation between risk analysis (at the railway
4326 system level) from hazard analysis (at the level of the system under consideration).

4327 This enhances co-operation between the relevant stakeholders, clarifying responsibilities and
4328 interfaces and has the advantages of reducing complexity and facilitating modularization.

4329 The Hourglass Model describes two main aspects:

- 4330 • "risk assessment", i.e. deriving high-level safety requirements for operational and technical
- 4331 issues (including maintenance), and
- 4332 • "hazard control", i.e. design and implementation of the safety-related system under
- 4333 consideration by determining and analysing causes internal to the system and implementing
- 4334 control measures on the basis of the given safety requirements.



4335
4336
4337

Figure 1 – The Hourglass Model

4338 **A Risk assessment**

4339 Risk assessment is performed at the railway system level.

4340 It covers system definition, risk analysis, risk evaluation.

4341 It defines the high level system safety requirements, in particular safety requirements for the
4342 system under consideration from the perspective of operator. It takes into account safety-related
4343 operational aspects, previous experience and the regulatory requirements of the railway
4344 application.

4345 The main task for this activity is the risk analysis, which is derived from the system definition.
4346 The risk analysis includes hazard identification, consequence analysis, and selection of risk
4347 acceptance principles ("RAP" in the picture) and associated criteria.

4348 The specification of safety requirements is the final result of risk assessment; in Figure 1 it is
4349 allocated in box B, because it has an interface function (together with system requirement
4350 specifications and the list of identified hazards) between different responsibilities.

4351 **Gaining and sharing system knowledge**

4352 All the knowledge gained during the process and the documented analyses, resulting from the
4353 risk assessment, should be considered as relevant information together with the specification of
4354 safety requirements.

4355 This knowledge should be shared and distributed among the stakeholders involved in the system
4356 process. It will provide significant potential benefits in terms of improved awareness of hazards
4357 and risk of accidents in the given operational and maintenance context, and will also help to
4358 understand the scope and limits of the risk reduction measures.

4359 **Conducting risk assessment**

4360 The level of detail in a risk assessment should be adequate to the risk. The purpose is not to
4361 catalogue every trivial hazard, nor is it expected that hazards beyond the limits of current
4362 knowledge will always be identified. A suitable and sufficient risk assessment should reflect a
4363 reasonable analysis of hazards and their associated risks within the railway operation and within
4364 the applied technology itself. Where reasonably practicable, risk assessments should be
4365 correlated with historical records of accidents and the records of causes.

4366 When possible, consideration of technical implementation/architecture should be avoided in this
4367 first stage i.e. the system to be developed should be considered as a black box, of which
4368 functions and hazards are evaluated only at the boundaries. These boundaries are well defined
4369 interfaces between the operational environment and the system under consideration.

4370 As an example, an “unintentional train motion” is a hazard for a train. It can be observed as an
4371 abstraction at the boundary of the “system train” and it could lead to different accidents
4372 depending on the operational context (e.g. collision in context with over-speeding while running
4373 or fall of persons in connection with a train moving in a station while expected to stand still, etc.).

4374 Assumptions defined during the risk assessment have to be checked and updated throughout the
4375 life-cycle phases.

4376 **B Outcomes of the risk assessment**

4377 The results of the first stage of the risk assessment are a set of safety requirements attached to
4378 clearly-identified functions, systems or operating rules. They are part of the System Requirement
4379 Specification that establishes the technical interface between the stakeholders.

4380 NOTE The project organisational structure and responsibilities are another factor to consider in understanding and
4381 controlling risk. For organisational aspects and requirements see EN 50126-1, 5.3 and EN 50126-1, 7.1.1.3

4382 On the basis of the selected risk acceptance principles, safety requirements can refer to Codes
4383 of Practise, to similar systems, or give explicit targets derived from an explicit risk estimation
4384 (“ERE” in the picture).

4385 Safety requirements include required efficiency of safety functions , that could be assessed
4386 quantitatively (e.g. maximum rates of hazards), semi-quantitatively or qualitatively (e.g. use of
4387 trained drivers for controlling human factor errors).

4388 Safety requirements should be assessed with a holistic approach, i.e. the residual risk should be
4389 evaluated as acceptable taking into consideration the identified hazards.

4390 **C Hazard control**

4391 The hazard control stage in the hourglass model is dedicated to ensuring that the system under
4392 consideration is compliant with the safety requirements: hence hazard control is performed for a
4393 specific system architecture.

4394 NOTE Hazard control as here defined has a narrow meaning and is limited to the design and implementation phase.

4395 The major impacts of human factors, operational and general maintenance rules as well as
4396 procedures are part of the preceding risk analysis and should have already been taken into
4397 account in the safety requirements. Therefore, during hazard control, the designer of the system
4398 under consideration can focus on the internal causes of the identified hazards, that can be
4399 considered as hazards at the system level.

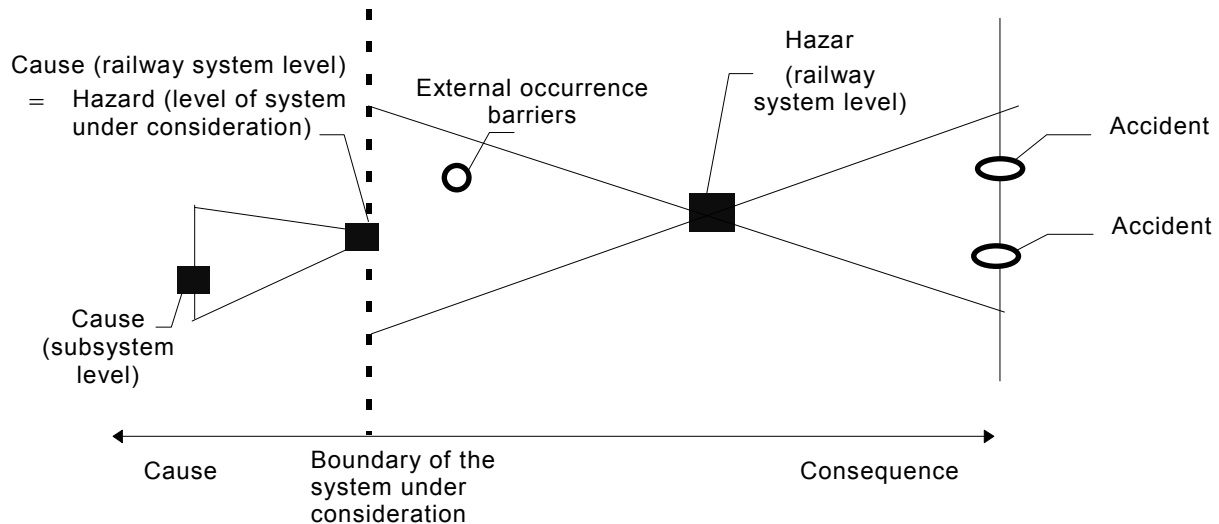
4400 The main task for this activity is the “hazard analysis” comprising:

- 4401 – causal analysis;
- 4402 – a dedicated hazard identification focusing on the system under consideration, and;
- 4403 – a Common Cause Analysis.

4404 Hazard identification is a recurring task that can appear on several iteration levels for subsets of
4405 the system under consideration. In order to distinguish these different tasks (and related
4406 documents) the hazard identification has been quoted twice in Figure 1:

- 4407 1. during risk assessment, it focuses on high level hazards derived from the system functions
4408 (black box) and related operation of the system as well as its environment;
- 4409 2. within the hazard control, a refined/iterated hazard identification focuses on hazards and
4410 their causes derived from the technical solutions, i.e. from defined architecture and internal
4411 interfaces of the system under consideration, and potential new hazards introduced by the
4412 system itself.

4413 Figure 2 shows that the cause of a hazard at the railway system level may be considered as a
 4414 hazard on level of the system under consideration, with respect to its boundary. The boundary
 4415 for a hazard identification is always given in the system definition that limits the scope of the
 4416 task. This implies that the hazards are structured hierarchically hence a hierarchical approach to
 4417 hazard analysis and hazard logging should be used.
 4418



4419
 4420
 4421
 4422

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

4423 The picture is hazard-oriented and shows a “bow-tie” shape, suggesting that several causes may
 4424 lead to the same hazard and one hazard may lead to several different accidents.
 4425 The demonstration of compliance with the safety requirements of the system under consideration
 4426 can be performed in various forms. These forms depend on the nature of the underlying
 4427 requirements set at the beginning of the hazard control.

4428 **D Revision of risk assessment**

4429 During the hazard control stage, fulfilment of safety targets may not be reached at the first
 4430 iteration:

- 4431 – additional hazards may be identified at the level of the system under consideration;
- 4432 – a need of new operational rules may arise;
- 4433 – additional external safety measures may be required to fulfil the safety objectives.

4434 In all these cases, a revision of the risk assessment is necessary.

4435 This revision should also take account of the application conditions that could rise at the level of
 4436 the system under consideration.

4437 **Responsibilities**

4438 Risk assessment is mainly within the responsibility of the railway duty holders and operators.

4439 The roles and responsibilities may however be contracted to other parties in relation to their
 4440 accountabilities, provided that they have a documented and suitable range of competencies to
 4441 consider the whole operational context in detail. They need to take into account safety-related
 4442 operational aspects, previous experience and regulatory requirements. In any case the railway
 4443 duty holders should approve the results of the risk assessment.

4444 The hazard control, for hazards associated purely with the technical system, is the responsibility
 4445 of the supplier of the technical system.

4446 Railway duty holder and supplier need to comply with the prevailing legal requirements.