European Railway Agency	
Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation	
Reference in ERA:	ERA/GUI/02-2008/SAF
Version in ERA:	1.1
Date:	06/01/2009

Document elaborated by	European Railway Agency Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex France
Document Type:	Guide
Document Status:	Public

	Name	Function
Released by	Marcel VERSLYPE	Executive Director
Reviewed by	Anders LUNDSTRÖM Thierry BREYNE	Head of Safety Unit Head of Safety Assessment Sector
Written by (Author)	Dragan JOVICIC	Safety Unit - Project Officer

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

DOCUMENT INFORMATION

Amendment Record

Table 1 : Status of the document.

Version Date	Author(s)	Section Number	Modification Description
Old document title and structure: *"Guidance for use of the Recommendation on the 1st Set of CSM"*			
Guidance Version 0.1 15/02/2007	Dragan JOVICIC	All	First version of the "guidance for use" associated to the version 1.0 of the "1st set of the CSM recommendations". This is also the first version of the document transmitted to the CSM working group for Formal Review.
Guidance Version 0.2 07/06/2007	Dragan JOVICIC	All	Reorganisation of the document to match with the structure of version 4.0 of the CSM recommendation. Update vs. Formal Review Process by the CSM working group on version 1.0 of the recommendation.
		All	Update of the document with additional information collected during meetings internal to ERA, as well as with the requests from the CSM taskforce and working group to develop new points.
		Figure 1	Modification of the figure representing the "risk management framework for the first set of Common Safety Methods" in accordance with both the review comments and the ISO terminology.
Guidance Version 0.3 20/07/2007	Dragan JOVICIC	Appendices	Reorganisation of appendices and creation of new ones. New appendix for gathering all diagrams that illustrate and facilitate the reading and understanding of the Guide;
		All sections	Document updated in order: • to develop as much as possible existing x sections; • to develop further what the "demonstration of the system compliance with the safety requirements" refers to; • to make a link with the CENELEC V-Cycle (i.e. Figure 8 and Figure 10 of EN 50 126); • to develop further the need for collaboration and co-ordination between the different actors of the rail sector whose activities may impact the safety of the railway system; • to bring clarifications about the evidence (e.g. hazard log and safety case) expected to demonstrate to the assessment bodies the correct application of the CSM's risk assessment process; Document updated also according to a first review internal to the Agency.
Guidance Version 0.4 16/11/2007	Dragan JOVICIC	All sections	Document updated following the Formal Review Process according to the comments received on version 0.3 from the following CSM working group members or organisations and agreed with them during phone calls: • Belgian, Spanish, Finish, Norwegian, French and Danish NSA's; • SIEMENS (member of UNIFE); • Norwegian infrastructure manager (Jernbaneverket – EIM Member);
Guidance Version 0.5 27/02/2008	Dragan JOVICIC	All sections	Document updated according to the comments received on version 0.3 from the following CSM working group members or organisations and agreed with them during phone calls: • CER • Dutch NSA
		All sections	Document updated in compliance with the signed version of the CSM recommendation. Document updated according to Agency internal review comments from Christophe CASSIR and Marcus ANDERSSON
		All sections Appendices	Complete renumbering of paragraph in document vs. recommendation Examples of application of the CSM recommendation included.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 1 : Status of the document.

Version Date	Author(s)	Section Number	Modification Description
New document title and structure: *"Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation"*			
Guide Version 0.1 23/05/2008	Dragan JOVICIC	All	First version of the document resulting from the split of the "guidance for use" version 0.5 into two complementary documents.
Guide Version 02 03/09/2008	Dragan JOVICIC	All	Update of the document in compliance with: • the CSM Regulation of the European Commission {Ref. 3}; • comments from the workshop of 1 July 2008 with members of the Railway Interoperability and Safety Committee (RISC); • the comments from the CSM working group members (Norwegian NSA, Finnish NSA, UK NSA, French NSA,, CER, EIM, Jens BRABAND [UNIFE] and Stéphane ROMEI [UNIFE]
Guide Version 1.0 10/12/2008	Dragan JOVICIC	All	Update of the document in compliance with the European Commission CSM Regulation on risk evaluation and assessment {Ref. 3} adopted by the Railway Interoperability and Safety Committee (RISC) during their plenary meeting on 25 November 2008
Guide Version 1.1 06/01/2009	Dragan JOVICIC	All	Document update according to the comments on the CSM Regulation by the juridical and linguistic services of the European Commission.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table of Contents

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

List of Figures

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

List of Tables

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0. INTRODUCTION

0.1. Scope

0.1.1. The objective of this document is to provide further clarification on the "Commission Regulation 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 the Council" {Ref. 3}. The regulation will be referred to in the present document as the "CSM Regulation".

0.1.2. This document is not legally binding and its content must not be interpreted as the only way to achieve the CSM requirements. This document aims to supplement the guide for the application of the CSM Regulation {Ref. 4} on how the process of the CSM Regulation could be used and applied. It gives additional practical information, without dictating in any manner compulsory procedures to be followed and without establishing any legally binding practice. This information may be of use to all actors[(1)] whose activities may have an impact on the safety of railway systems and who directly or indirectly need to apply the CSM. The document provides examples of risk assessments and gives some possible tools that support the application of the CSM. These examples are given for advice and assistance only. Actors may use alternative methods or may continue to use their own existing methods and tools for the compliance with the CSM, if they consider them to be better suited.
Also, the examples and additional information given in this document are not exhaustive and do not cover all possible situations where significant changes are proposed, thus the document can only be seen as purely informative.

0.1.3. This informative document shall be read only as an additional help for the application of the CSM Regulation. When used, this document should be read in conjunction with the CSM Regulation {Ref. 3} and the associated guide {Ref. 4} to facilitate further the application of CSM but it does not replace the CSM Regulation.

0.1.4. The document is prepared by the European Railway Agency (ERA) with the support of railway association and national safety authority experts from the CSM working group. It represents a developed collection of ideas and information gathered by the Agency during internal meetings and meetings with the CSM working group and CSM taskforces. When necessary, ERA will review and update the document to reflect the progress with the European standards, the changes to the CSM Regulation on risk assessment and possible return from experience on the use of the CSM Regulation. As it is not possible to give a timetable for this revision process at the time of writing, the reader should refer to the European Railway Agency for information about the latest available edition of this document.

0.2. Outside the scope

0.2.1. This document does not provide guidance on how to organise, operate or design (and manufacture) a railway system or parts of it. Nor does it define the contractual agreements and arrangements that can exist between some actors for the application of the risk

(1) *The concerned actors are the contracting entities as defined in Article 2(r) of Directive 2008/57/EC on the interoperability of the rail system within the Community, or the manufacturers, all known in the regulation as the "proposer", or their suppliers and service providers.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

management process. The project specific contractual arrangements are outside the scope of the CSM Regulation, as well as of the associated guide and of the present document.

0.2.2. Although outside the scope of this document, the arrangements that are agreed between the relevant actors may be written down in the relevant contracts at the beginning of the project, however without prejudice to the provisions of the CSM. This could cover for example:

(a) the costs inherent to the management of safety related risks at the interfaces between the actors;
(b) the costs inherent to transfers of hazards and associated safety measures between the actors not yet known at the beginning of the project;
(c) how to manage conflicts that could arise during the project;
(d) etc.

Should disagreements arise or a conflict occurs between the proposer and his sub-contractors during the project development, reference may be made to the relevant contracts to help solving any conflict.

0.3. Principle for this document

0.3.1. Although this document may appear to be standalone for reading purposes, it does not substitute the CSM Regulation {Ref. 3}. For ease of reference, each article of the CSM Regulation is copied in this document. Where necessary, the relevant article is explained beforehand in the guide for the application of the CSM Regulation {Ref. 4}. Additional information is then provided in the following paragraphs to help understanding further the CSM Regulation where this is considered necessary.

0.3.2. The articles and their underlying paragraphs from the CSM Regulation are copied in a text box in the present document using the "Bookman Old Style" Italic Font, the same as the present text. That formatting enables to easily distinguish the original text of the CSM Regulation {Ref. 3} from the additional explanations provided in this document. The text from the guide for the application of the CSM Regulation {Ref. 4} is not copied in the present document.

0.3.3. The structure of this document is mapped on to the structure of the CSM Regulation and the associated guide to help the reader.

0.4. Document description

0.4.1. The document is divided into the following parts:

(a) chapter 0. that defines the scope of the document and provides the list of reference documents;
(b) Annex I and Annex II provide additional information for the corresponding sections of the CSM Regulation {Ref. 3} and of the associated guide {Ref. 4};
(c) new appendices develop further some specific aspects and provide examples.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.5. Reference documents

Table 2 : Table of reference documents.

{Ref. N°}	Title	Reference	Version
{Ref. 1}	Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive)	2004/49/EC OJ L 164, 30.4.2004, p. 44, as corrected by OJ L 220, 21.6.2004, p. 16.	-
{Ref. 2}	Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the Interoperability of the rail system within the Community	2008/57/EC OJ L 191, 18/7/2008, p.1.	-
{Ref. 3}	Commission Regulation (EC) N°.../.. of [...] 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	xxxx/yy/EC	voted by RISC on 25/11/2008
{Ref. 4}	Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the Interoperability of the rail system within the Community	2008/57/EC OJ L 191, 18/7/2008, p.1.	-
{Ref. 6}	Safety Management System - Assessment Criteria for Railway Undertakings and Infrastructure Managers	SMS Assessment Criteria Part A Safety Certificates and Authorisations	31/05/2007
{Ref. 7}	Railway Applications – Communication, Signalling and Processing Systems – Safety related Electronic Systems for Signalling	EN 50129	February 2003
{Ref. 8}	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: The Standard itself	EN 50126-1	September 2006
{Ref. 9}	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 2: Guide to the application of EN 50126-1 for Safety	EN 50126-2 (Guideline)	Final Draft (August 2006)
{Ref. 10}	Generic Guideline for the Calculation of Risk inherent in the Carriage of Dangerous Goods by Rail	OTIF guideline approved by the RID Committee of experts	24 November 2005.
{Ref. 11}	Risk Acceptance Criterion for Technical Systems	Note 01/08	1.1 (25/01/2008)
{Ref. 12}	ERA Safety Unit: Feasibility Study – "Apportionment of safety targets (to TSI sub-systems) and consolidation of TSI from a safety point of view" WP1.1 - Assessment of the feasibility to apportion Common Safety Targets	WP1.1	1.0
{Ref. 13}	"Railway Applications — Classification System for Rail Vehicles — Part 4: EN 0015380 Part 4: Function Groups".	EN 0015380 Part 4	

0.6. Standard definitions, terms and abbreviations

0.6.1. The general definitions, terms and abbreviations used in the present document can be found in a standard dictionary.

0.6.2. New definitions, terms and abbreviations in this guide are defined in the sections below.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.7. Specific definitions

0.7.1. See Article 3

0.8. Specific terms and abbreviations

0.8.1. This section defines the new specific terms and abbreviations that are used frequently in the present document.

Table 3 : Table of terms.

Term	Definition
Agency	the European Railway Agency (ERA)
guide	the "guide for the application of the Commission Regulation (EC) N°.../.. of [...] 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"
CSM Regulation	the "Commission Regulation (EC) N°.../.. of [...] 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" {Ref. 3}

Table 4 : Table of abbreviations.

Abbreviation	Meaning
CCS	Control Command and Signalling
CSM	Common Safety Method(s)
CST	Common Safety Targets
EC	European Commission
ERA	European Railway Agency
IM	Infrastructure Manager(s)
ISA	Independent Safety Assessor
OTIF	Intergovernmental Organisation for International Carriage by Rail
MS	Member State
NOBO	Notified Body
NSA	National Safety Authority
QMP	Quality Management Process
QMS	Quality Management System
RISC	Railway Interoperability and Safety Committee
RU	Railway Undertaking(s)
SMP	Safety Management Process
SMS	Safety Management System
SRT	Safety in Railway Tunnels
TBC	To be completed
TSI	Technical Specifications for Interoperability

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

EXPLANATION OF THE ARTICLES OF THE CSM REGULATION

Article 1. Purpose

Article 1 (1)

This Regulation establishes a common safety method on risk evaluation and assessment (CSM) as referred to in Article 6(3)(a) of Directive 2004/49/EC.

[G 1] Additional explanation is not judged necessary.

Article 1 (2)

The purpose of the CSM on risk evaluation and assessment is to maintain or to improve the level of safety on the Community's railways, when and where necessary and reasonably practicable. The CSM shall facilitate the access to the market for rail transport services through harmonisation of:

(a) the risk management processes used to assess the safety levels and the compliance with safety requirements;
(b) the exchange of safety-relevant information between different actors within the rail sector in order to manage safety across the different interfaces which may exist within this sector;
(c) the evidence resulting from the application of a risk management process.

[G 1] Additional explanation is not judged necessary.

Article 2. Scope

Article 2 (1)

The CSM on risk evaluation and assessment shall apply to any change of the railway system in a Member State, as referred to in point (2) (d) of Annex III to Directive 2004/49/EC, which is considered to be significant within the meaning of Article 4 of this Regulation. Those changes may be of a technical, operational or organisational nature. As regards organisational changes, only those changes which could impact the operating conditions shall be considered.

[G 1] The CSM applies to the whole railway system and covers the assessment of the following changes in railway systems if they are evaluated to be significant by the application of Article 4:

(a) construction of new lines or changes of existing lines,
(b) introduction of new and/or modified technical systems;
(c) operational changes (such as new or modified operational rules and maintenance procedures);
(d) changes within RU/IM organisations.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

The term "system" refers, in the CSM, to all aspects of a system including, among others its development, operation, maintenance, etc. till the de-commissioning or disposal

[G 2] The CSM covers the significant changes of both.

(a) "small and simple" systems that could be composed of few technical sub-systems or elements, and,
(b) "large and more complex" systems (e.g. that can include stations and tunnels).

Article 2 (2)

Where the significant changes concern structural sub-systems to which Directive 2008/57/EC applies, the CSM on risk evaluation and assessment shall apply:

(a) if a risk assessment is required by the relevant technical specification for interoperability (TSI). In this case the TSI shall, where appropriate, specify which parts of the CSM apply;
(b) to ensure safe integration of the structural subsystems to which the TSIs apply into an existing system, by virtue of Article 15(1) of Directive 2008/57/EC.

However, application of the CSM in the case referred to in point (b) of the first subparagraph must not lead to requirements contradictory to those laid down in the relevant TSIs which are mandatory.

Nevertheless if the application of the CSM leads to a requirement that is contradictory to that laid down in the relevant TSI, the proposer shall inform the Member State concerned which may decide to ask for a revision of the TSI in accordance with Article 6(2) or Article 7 of Directive 2008/57/EC or a derogation in accordance with Article 9 of that Directive.

[G 1] For example, in compliance with the Railway Safety Directive {Ref. 1} and Railway Interoperability Directive {Ref. 2}, a new type rolling stock for a high speed line must be compliant with the High Speed Rolling Stock TSI. Although the majority of the system under assessment is covered by the TSI, the key issue of human factors related to the driver's cab is not included in the TSI. Therefore, in order to ensure that all reasonably foreseeable hazards related to human factor issues (i.e. to the interfaces between the driver, the rolling stock and the rest of the railway system) are identified and adequately controlled, the CSM process shall be used.

Article 2 (3)

This Regulation shall not apply to:

(a) metros, trams and other light rail systems;
(b) networks that are functionally separate from the rest of the railway system and intended only for the operation of local, urban or suburban passenger services, as well as railway undertakings operating solely on these networks;
(c) privately owned railway infrastructure that exists solely for use by the infrastructure owner for its own freight operations;
(d) heritage vehicles that run on national networks providing that they comply with national safety rules and regulations with a view to ensuring safe circulation of such vehicles;
(e) heritage, museum and tourist railways that operate on their own network, including workshops, vehicles and staff.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 2 (4)

This Regulation shall not apply to systems and changes, which, on the date of entry into force of this Regulation, are projects at an advanced stage of development within the meaning of Article 2 (t) of Directive 2008/57/EC.

[G 1] Additional explanation is not judged necessary.

Article 3. Definitions

For the purpose of this Regulation the definitions in Article 3 of Directive 2004/49/EC shall apply.

The following definitions shall also apply:

(1) 'risk' means the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm (EN 50126-2)*;*

(2) 'risk analysis' means systematic use of all available information to identify hazards and to estimate the risk (ISO/IEC 73)*;*

(3) 'risk evaluation' means a procedure based on the risk analysis to determine whether the acceptable risk has been achieved (ISO/IEC 73)*;*

(4) 'risk assessment' means the overall process comprising a risk analysis and a risk evaluation (ISO/IEC 73)*;*

(5) 'safety' means freedom from unacceptable risk of harm (EN 50126-1)*;*

(6) 'risk management' means the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks (ISO/IEC 73)*;*

(7) 'interfaces' means all points of interaction during a system or subsystem life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks;

(8) 'actors' means all parties which are, directly or through contractual arrangements, involved in the application of this Regulation pursuant to Article 5 (2);

(9) 'safety requirements' means the safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) necessary in order to meet legal or company safety targets;

(10) 'safety measures' means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk;

(11) 'proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC, the contracting entities or the manufacturers when they invite a notified body to apply the "EC" verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles;

(12) 'safety assessment report' means the document containing the conclusions of the assessment performed by an assessment body on the system under assessment;

(13) 'hazard' means a condition that could lead to an accident (EN 50126-2)*;*

(14) 'assessment body' means the independent and competent person, organisation or entity which undertakes investigation to arrive at a judgment, based on evidence, of the suitability of a system to fulfil its safety requirements;

(15) 'risk acceptance criteria' means the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(16) 'hazard record' means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced;

(17) 'hazard identification' means the process of finding, listing and characterising hazards (ISO/IEC Guide 73)*;*

(18) 'risk acceptance principle' means the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable;

(19) 'code of practice' means a written set of rules that, when correctly applied, can be used to control one or more specific hazards;

(20) 'reference system' means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison;

(21) 'risk estimation' means the process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration (ISO/IEC 73)*;*

(22) '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; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;

(23) 'catastrophic consequence' means fatalities and/or multiple severe injuries and/or major damages to the environment resulting from an accident (Table 3 from EN 50126)*;*

(24) 'safety acceptance' means status given to the change by the proposer based on the safety assessment report provided by the assessment body;

(25) 'system' means any part of the railway system which is subject to a change;

(26) 'notified national rule' means any national rule notified by Member States under Council Directive 96/48/EC[4], Directive 2001/16/EC of the European Parliament and the Council[5] and Directives2004/49/EC and 2008/57/EC.

[G 1] Additional explanation is not judged necessary.

Article 4. Significant changes

Article 4 (1)

If there is no notified national rule for defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system.

When the proposed change has no impact on safety, the risk management process described in Article 5 does not need to be applied.

[G 1] If there is no notified national rule, the decision is under the proposer's responsibility. The significance of the change is based on expert judgment. For example, if the intended

(4) *OJ L 235, 17.9.1996, p. 6.*

(5) *OJ L 110 , 20.4.2001, p. 1.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

change in an existing system is complex, it can be evaluated as significant if the risk of impacting existing functions[6] of the system is high, although the change itself is not necessarily highly safety related.

Article 4 (2)

When the proposed change has an impact on safety, the proposer shall decide, by expert judgement, the significance of the change based on the following criteria:

(a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;

(b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;

(c) complexity of the change;

(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;

(e) reversibility: the inability to revert to the system before the change;

(f) additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Example of small changes:** after the system commissioning, increasing the maximum line speed once by 5 km/h could be not significant. However, if the maximum line speed continues to be increased by steps of 5 km/h, the sum of successive changes (evaluated individually as non significant changes) could become a significant change with respect to the initial system safety requirements.

[G 2] In order to evaluate whether a set of several successive (non significant) changes is significant, when taking them as a whole, all the hazard(s) and the associated risks linked to all the changes need to be assessed. The set of the considered changes can be considered as non significant if the resulting risk is broadly acceptable.

[G 3] The Agency work on significant changes has shown that:

(a) it is not possible to identify harmonised thresholds or rules from which, for a given change, the decision on the significance of the change can be taken, and;
(b) it is not possible to provide an exhaustive list of significant changes;
(c) the decision cannot be valid for all proposers and all technical, operational, organisational and environmental conditions

It is thus essential to leave the responsibility for the decision on the proposer's, who are responsible, in accordance with Article 4(3) of the Railway Safety Directive {Ref. 1}, of the safe operation and control of the risks associated with the their part of the system.

[G 4] To help the proposer, one example of "evaluation and use of criteria" is provided in section C.2. of Appendix C.

---

(6) *As the functions in a system are not always independent, changes of some functions can also impact other functions of the system although they could seem not to be directly concerned by the changes.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 5] The CSM must not be applied if a safety related change is not considered to be significant. But that does not mean that there is nothing to do. The proposer performs some kind of (preliminary) risk analyses to decide whether the change is significant. These risk analyses, as well as any justifications and arguments need to be documented in order to enable audits by the NSA. The evaluation of the significance of a change, and the decision that a change is not significant, must not be independently assessed by an assessment body.

Article 5. Risk management process

Article 5 (1)

The risk management process described in the Annex I shall apply:

(a) for a significant change as specified in Article 4, including the placing in service of structural sub-systems as referred to in Article 2(2)(b);
(b) where a TSI as referred to in Article 2 (2)(a) refers to this Regulation in order to prescribe the risk management process described in Annex I.

[G 1] Additional explanation is not judged necessary.

Article 5 (2)

The risk management process described in Annex I shall be applied by the proposer.

[G 1] Additional explanation is not judged necessary.

Article 5 (3)

The proposer shall ensure that risks introduced by suppliers and service providers, including their subcontractors, are managed. To this end, the proposer may request that suppliers and service providers, including their subcontractors, participate in the risk management process described in Annex I.

[G 1] Additional explanation is not judged necessary.

Article 6. Independent assessment

Article 6 (1)

An independent assessment of the correct application of the risk management process described in Annex I and of the results of this application shall be carried out by a body which shall meet the criteria listed in Annex II. Where the assessment body is not already identified by Community or national legislation, the proposer shall appoint its own assessment body which may be another organisation or an internal department.

[G 1] The required level of independence necessary for the assessment body depends on the safety level that is required for the system under assessment. Waiting for the harmonisation of this topic, the best practice on this matter can be found in IEC61508-1:2001 Clause 8 or in

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

§ 5.3.9. of the EN 50 129 standard {Ref. 7}. The degree of independence is dependent on both the consequence severity of the hazard associated with the equipment and its novelty. Section § 9.7.2 in EN 50 126-2 and EN 50129 define the level of independence for signalling systems. In principle this could also be used for other systems.

[G 2] The Agency is still working on the definition of the roles and responsibilities of the different assessment bodies (NSA, NOBO and ISA) as well as the necessary interfaces between them. That will define who (if possible) among those assessment bodies will do what and how it will do it. That will at the end enable to define how to:

(a) check, based on evidence, that the risk management and risk assessment processes covered by the CSM are correctly applied, and;
(b) support the proposer in its decision to accept the significant change within the system under assessment.

Article 6 (2)

Duplication of work between the conformity assessment of the safety management system as required by Directive 2004/49/EC, the conformity assessment carried out by a notified body or a national body as required by Directive 2008/57/EC and any independent safety assessment carried out by the assessment body in accordance with this Regulation, shall be avoided.

[G 1] Additional information will be brought by the Agency work the on roles and responsibilities of the assessment bodies.

Article 6 (3)

The safety authority may act as the assessment body where the significant changes concern the following cases:

(a) where a vehicle needs an authorisation for placing in service, as referred to in Articles 22(2) and 24(2) of Directive 2008/57/EC;

(b) where a vehicle needs an additional authorisation for placing in service, as referred to in Articles 23(5) and 25(4) of Directive 2008/57/EC;

(c) where the safety certificate has to be updated due to an alteration of the type or extent of the operation, as referred to in Article 10(5) of Directive 2004/49/EC;

(d) where the safety certificate has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 10(5) of Directive 2004/49/EC;

(e) where the safety authorisation has to be updated due to substantial changes to the infrastructure, signalling or energy supply, or to the principles of its operation and maintenance, as referred to in Article 11(2) of Directive 2004/49/EC;

(f) where the safety authorisation has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 11(2) of Directive 2004/49/EC.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 6 (4)

Where the significant changes concern a structural subsystem that needs an authorisation for placing in service as referred to in Article 15(1) or Article 20 of Directive 2008/57/EC, the safety authority may act as the assessment body unless the proposer already gave that task to a notified body in accordance with Article 18(2) of that Directive.

[G 1] Additional explanation is not judged necessary.

Article 7. Safety assessment reports

Article 7 (1)

The assessment body shall provide the proposer with a safety assessment report.

[G 1] Additional explanation is not judged necessary.

Article 7 (2)

In the case referred to in point (a) of Article 5(1), the safety assessment report shall be taken into account by the national safety authority in its decision to authorise the placing in service of subsystems and vehicles.

[G 1] Additional explanation is not judged necessary.

Article 7 (3)

In the case referred to in point (b) of Article 5(1), the independent assessment shall be part of the task of the notified body, unless otherwise prescribed by the TSI.
If the independent assessment is not part of the task of the notified body, the safety assessment report shall be taken into account by the notified body in charge of delivering the conformity certificate or by the contracting entity in charge of drawing up the EC declaration of verification.

[G 1] Additional explanation is not judged necessary.

Article 7 (4)

When a system or part of a system has already been accepted following the risk management process specified in this Regulation, the resulting safety assessment report shall not be called into question by any other assessment body in charge of performing a new assessment for the same system. The recognition shall be conditional on demonstration that the system will be used under the same functional, operational and environmental conditions as the already accepted system, and that equivalent risk acceptance criteria have been applied.

[G 1] This mutual recognition principle is already accepted by the CENELEC standards: see section § 5.5.2 in EN 50 129 and section § 5.9 in EN 50 126-2. In CENELEC, the cross-acceptance or mutual recognition principle is applied by proposers or independent safety

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

assessors to generic products and generic applications[7] provided the safety assessment and safety demonstration are performed in compliance with the CENELEC standard requirements.

[G 2] The mutual recognition has to be applied also for the acceptance of new or modified systems if their risk assessment and the demonstration of the system compliance with the safety requirements are performed in line with the provisions of the CSM Regulation {Ref. 3}

Article 8. Risk control management/internal and external audits

Article 8 (1)

The railway undertakings and infrastructure managers shall include audits of application of the CSM on risk evaluation and assessment in their recurrent auditing scheme of the safety management system as referred to in Article 9 of Directive 2004/49/EC.

[G 1] Additional explanation is not judged necessary.

Article 8 (2)

Within the framework of the tasks defined in Article 16(2)(e) of Directive 2004/49/EC, the national safety authority shall monitor the application of the CSM on risk evaluation and assessment.

[G 1] Additional explanation is not judged necessary.

Article 9. Feedback and technical progress

Article 9 (1)

Each infrastructure manager and each railway undertaking shall, in its annual safety report referred to in Article 9(4) of Directive 2004/49/EC, report briefly on its experience with the application of the CSM on risk evaluation and assessment. The report shall also include a synthesis of the decisions related to the level of significance of the changes.

[G 1] Additional explanation is not judged necessary.

(7) *Refer to point [G 5] in section 1.1.5 and to the footnotes (9) and (10) at page 24, as well as to Figure 3, of this document for further explanation about the terminology "generic product and generic application" and the inherent principles.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 9 (2)

Each national safety authority shall, in its annual safety report referred to in Article 18 of Directive 2004/49/EC, report on the experience of the proposers with the application of the CSM on risk evaluation and assessment, and, where appropriate, its own experience.

[G 1] Additional explanation is not judged necessary.

Article 9 (3)

The European Railway Agency shall monitor and collect feedback on the application of the CSM on risk evaluation and assessment and, where applicable, shall make recommendations to the Commission with a view to improving it.

[G 1] Additional explanation is not judged necessary.

Article 9 (4)

The European Railway Agency shall submit to the Commission by 31 December 2011 at the latest, a report which shall include:

(a) an analysis of the experience with the application of the CSM on risk evaluation and assessment, including cases where the CSM has been applied by proposers on a voluntary basis before the relevant date of application provided for in Article 10;
(b) an analysis of the experience of the proposers concerning the decisions related to the level of significance of the changes;
(c) an analysis of the cases where codes of practice have been used as described in section 2.3.8 of Annex I;
(d) an analysis of overall effectiveness of the CSM on risk evaluation and assessment.

The safety authorities shall assist the Agency by identifying cases of application of the CSM on risk evaluation and assessment.

[G 1] Additional explanation is not judged necessary.

Article 10. Entry into force

Article 10 (1)

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 10 (2)

This Regulation shall apply from 1 July 2012.

However, it shall apply from 19 July 2010:

(a) to all significant technical changes affecting vehicles as defined in Article 2 (c) of Directive 2008/57/EC;

(b) to all significant changes concerning structural sub-systems, where required by Article 15(1) of Directive 2008/57/EC or by a TSI.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ANNEX I - EXPLANATION OF THE PROCESS IN THE CSM REGULATION

1. GENERAL PRINCIPLES APPLICABLE TO THE RISK MANAGEMENT PROCESS

1.1. General principles and obligations

1.1.1. The risk management process covered by this Regulation shall start from a definition of the system under assessment and comprise the following activities:

(a) the risk assessment process, which shall identify the hazards, the risks, the associated safety measures and the resulting safety requirements to be fulfilled by the system under assessment;
(b) demonstration of the compliance of the system with the identified safety requirements and;
(c) management of all identified hazards and the associated safety measures.

This risk management process is iterative and is depicted in the diagram of the Appendix (of the CSM Regulation)*. The process ends when the compliance of the system with all safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.*

[G 1] The risk management framework for the CSM and the associated risk assessment process are illustrated in Figure 1. When judged necessary, each box/activity of this figure is described further in a specific section of this document.

[G 2] CENELEC advises that the risk management and risk assessment processes are described in a safety plan. But if this is not convenient for the project, the associated description can be included in any other relevant document. Refer to section 1.1.6.

[G 3] The risk assessment process starts from a preliminary system definition. During the project development, the preliminary system definition is updated progressively and is replaced by the system definition. If there is no preliminary system definition, the formal system definition is used for performing the risk assessment. But then, it is useful that all the actors concerned by the significant change meet at the beginning of the project in order:

(a) to agree on the overall system principles, system functions, etc. In principle this could be described in a preliminary system definition;
(b) to agree on the project organisation;
(c) to agree on the sharing of the roles and responsibilities between the different actors already involved, including the NSA, NOBO and ISA where relevant.

Such a co-ordination, during the preliminary system definition for example, provides the opportunity to the proposer, the sub-contractors, NSA, NOBO and ISA, if relevant, to agree at an early stage regarding the codes of practice or reference systems that are acceptable to use within the project

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

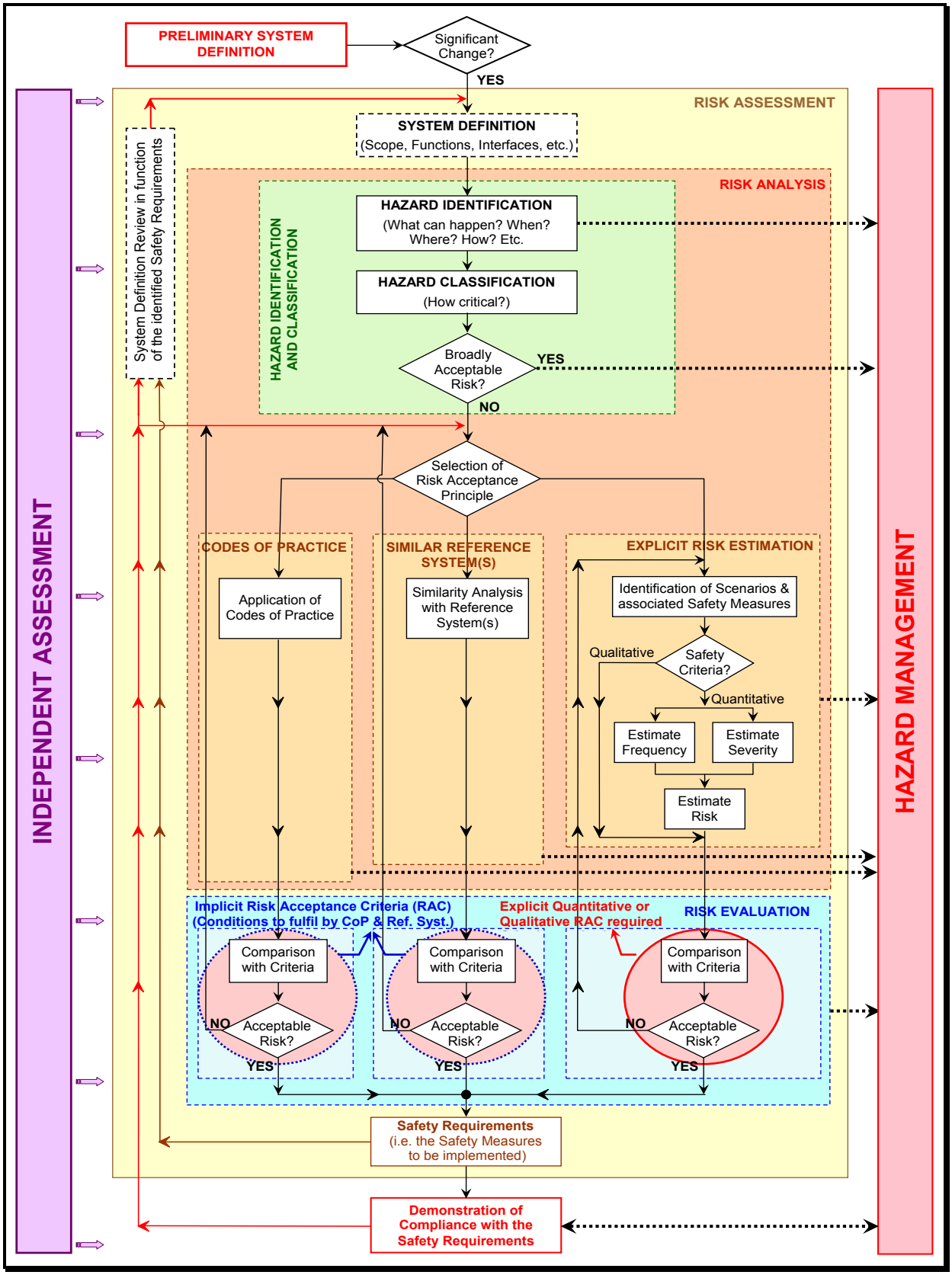

Figure 1 : Risk management framework in the CSM Regulation {Ref. 3}.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.2. This iterative risk management process:

(a) shall include appropriate quality assurance activities and be carried out by competent staff;
(b) shall be independently assessed by one or more assessment bodies.

[G 1] The railway undertaking and infrastructure manager safety management system (SMS) sets out the process and procedures that:

(a) monitor the system continues to be safe during its entire life-cycle (i.e. during its operation and maintenance);
(b) ensure a safe dismantling or replacement of the related system.

This process is not part of the CSM on risk assessment

[G 2] To implement the CSM, it is necessary that all parties involved are competent (i.e. have proper skills, knowledge and experience). There is a steady need for competence management within the organisations of the actors of the rail sector:

(a) for the infrastructure managers and railway undertakings, this is covered by their safety management system (SMS) under Annex III (2)(e) of the Railway Safety Directive {Ref. 1};
(b) for the other actors whose activities may impact the safety of the railway system, although the SMS is not obligatory, in general at least at the project level (see point [G 1] in section 5.1) they have a quality management process (QMP) and/or a safety management process (SMP) which covers that requirement.

[G 3] The following sections of the CENELEC EN 50 126-1 standard {Ref. 8} set out guidance on the competence:

(a) by virtue of § 5.3.5.(b): *"all personnel with responsibilities within the"* risk *"management process"* need to be *"competent to discharge those responsibilities"*;
(b) § 5.3.5.(d): the requirements of the risk management and risk assessment need to be *"implemented within business processes supported by a quality management system (QMS) compliant with the requirements EN ISO 9001, EN ISO 9002 or EN ISO 9003 appropriate for the system under"* assessment. An example of aspects controlled by the quality management system is given in section § 5.2. of EN 50 129 standard {Ref. 7}.

These cover the quality assurance activities, as well as the competence and training for the staff/persons, required for supporting the process covered by the CSM.

[G 4] Very often the risk assessment process is followed up by an assessment body from the very beginning of the project, but unless required by a national law in a Member State such an early involvement of the assessment body is not mandatory although it is advised. The opinion of the independent assessment body could be useful before switching over from one step of the risk assessment to the next one. Refer to Article 6 for further details on the independent assessment

1.1.3. The proposer in charge of the risk management process required by this Regulation shall maintain a hazard record according to section 4.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.4. The actors who already have in place methods or tools for risk assessment may continue to apply them as far as they are compatible with the provisions of this Regulation and subject to the following conditions:

(a) the risk assessment methods or tools are described in a safety management system which has been accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC, or;
(b) the risk assessment methods or tools are required by a TSI or comply with publicly available recognised standards specified in notified national rules.

[G 1] Figure 2 represents the relationship between the CSM and the "safety management systems and risk assessment processes".

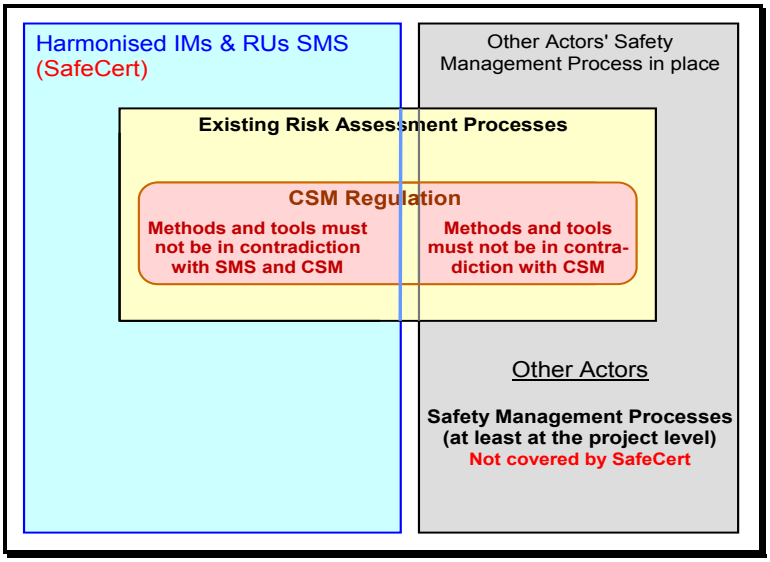

Figure 2 : Harmonised SMS and CSM.

1.1.5. Without prejudice to civil liability in accordance with the legal requirements of the Member States, the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment. This decision shall depend on the type of safety measures selected to control the risks to an acceptable level. The demonstration of compliance with the safety requirements shall be conducted according to section 3.

[G 1] If the proposer is an infrastructure manager or a railway undertaking, sometimes it may be necessary to involve other actors in the process [8] (see section 1.2.1). In some cases, the infrastructure manager or the railway undertaking might sub-contract, partly or completely, the risk assessment activities. The roles and responsibilities for each actor are usually agreed between the concerned actors at an early stage of the project.

(8) *This is compliant with the Appendix A.4 of CENELEC 50 129 standard {Ref. 7}.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] It is important to note that the proposer always remains responsible for the application of the CSM, for the acceptance of the risk and thus for the safety of the system. This will include ensuring that:

(a) there is full co-operation between the involved actors so that all the necessary information is provided, and;
(b) it is clear who needs to fulfil the particular CSM requirements (for example undertaking the risk analysis or managing the hazard record).

In case of disagreement between actors on safety requirements they have to fulfil, the NSA could be consulted for opinion. But the responsibility to find a solution remains on the proposer and cannot be transferred to the NSA: see also section 0.2.2.

[G 3] If the task is sub-contracted, there is no obligation for a sub-contractor to have its own safety organisation if this is not an infrastructure manager or railway undertaking, or especially if the sub-contractor's structure/size is small or if its contribution to the overall system is limited. The responsibility for the risk management, including the risk assessment and hazard management activities, can remain on the higher level organisation (i.e. on the sub-contractor's customer). However, the sub-contractor is always responsible to provide the right information related to its activities and necessary to the higher level organisation for building the risk management documentation.
Co-operating organisations can also agree to set up a common safety organisation for example in order to optimise the costs. In that case, only one organisation will manage the safety activities of all the involved organisations. The responsibility for the accuracy of the information (i.e. hazards, risks and safety measures), as well as the management of the implementation of the safety measures, remains under the organisation in charge of controlling the hazards that these safety measures are associated with.

[G 4] The proposer would normally set out the "safety levels" and "safety requirements" allocated to the actors involved in the project and to the different sub-systems and equipment of those actors:

(a) in the contracts between the proposer and the respective actors (sub-contractors);
(b) in a safety plan, or any other relevant document with the same purpose, with the description of the overall project organisation and responsibilities of each actor, including the proposer's ones: refer to section 1.1.6 ;
(c) in the proposer's hazard record(s): refer to section 4.1.1.

This allocation of the system "safety levels" and "safety requirements" down to the underlying sub-systems and equipment, and therefore to the respective actors including the proposer itself, can be refined/extended during the "demonstration phase of the system compliance with the safety requirements": refer to Figure 1. In comparison with the CENELEC V-Cycle (see section 2.1.1 and Figure 5 at page 33), this activity corresponds to Phase 5 dealing with the "apportionment of system requirements" down to the different sub-systems and components

[G 5] Article 5 (2) allows that other actors than RU and IM assume the overall responsibility of compliance with the CSM depending on their respective needs. For generic products or generic applications[9] for example, the manufacturer can perform the risk assessment on basis of a "generic system definition" in order to specify the safety levels and the safety requirements to be fulfilled by generic products and generic applications.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

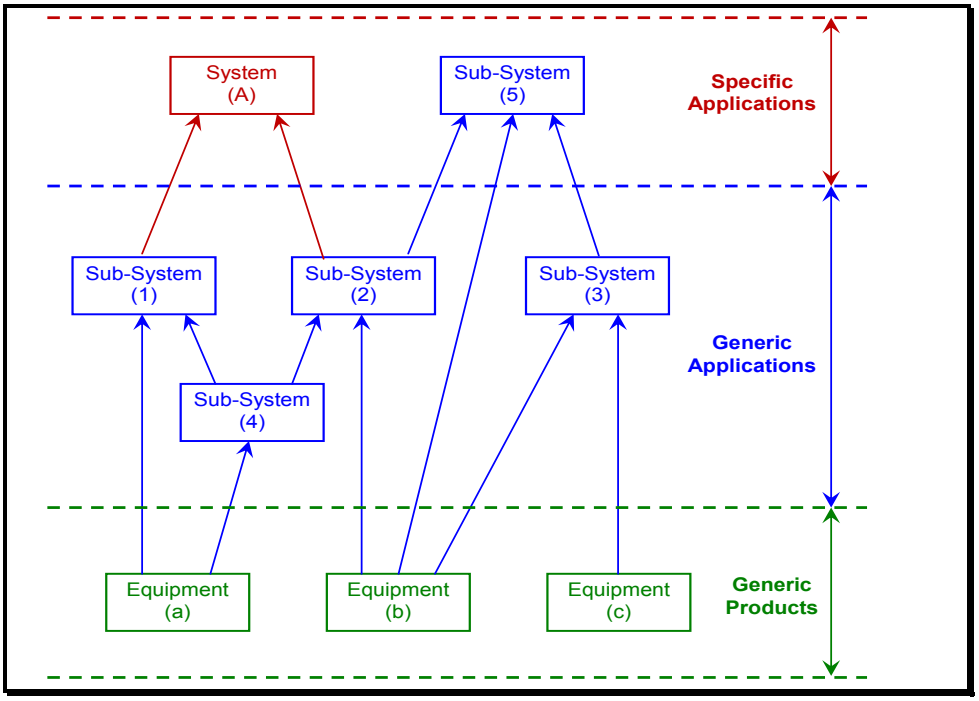

Figure 3 : Examples of dependencies between safety cases (drawn from Figure 9 in EN 50 129 standard).

[G 6] CENELEC advises that the manufacturer provides the documented evidence from the risk assessment in generic product (respectively generic application[9]) safety cases and hazard records. These safety cases and hazard records contain all the assumptions[10] and

---

(9) *The terminology "generic application" and "generic product safety cases" is reused from CENELEC where three different categories of safety cases can be considered (see Figure 3):*

(a) ***Generic product safety case*** *(independent of the application). A generic product can be re-used for different independent applications;*

(b) ***Generic application safety case*** *(for a class of application). A generic application can be re-used for a class/type of application with common functions;*

(c) ***Specific application safety case*** *(for a specific application). A specific application is used for only one particular installation.*

For more information about their interdependence, refer to section § 9.4. and Figure 9.1 of the CENELEC 50 126-2 Guideline {Ref. 9}.

(10) *These assumptions and restrictions of use determine the limits and the validity of the "safety assessments" and "safety analyses" associated to the related generic product and generic application safety cases. If they are not fulfilled by the considered specific application, it is necessary to update or replace the corresponding "safety assessments" and "safety analyses" (e.g. causal analyses) by new ones.*

> *This is in line with the following general safety principle: "Whenever a specific (sub-)system design is based on generic applications and generic products, it must be demonstrated that the specific (sub-)system complies with all the assumptions and restrictions of use (called safety related application conditions in CENELEC) that are exported in the corresponding generic application and generic product safety cases (see Figure 3)"*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

identified "restrictions of use" (i.e. safety related application conditions) that are applicable to the related generic products (respectively generic application). Therefore, whenever a generic product and a generic application are used in operation in a specific application, the compliance with all these assumptions[10] and "restrictions of use" (or safety related application conditions) needs to be demonstrated in each specific application.

1.1.6. The first step of the risk management process shall be to identify in a document, to be drawn up by the proposer, the different actors' tasks, as well as their risk management activities. The proposer shall coordinate close collaboration between the different actors involved, according to their respective tasks, in order to manage the hazards and their associated safety measures.

[G 1] Very often, unless it is differently agreed in the contracts at the beginning of the project, each project has a document that describes the risk management activities. The relevant document is updated and reviewed whenever significant modifications are made to the original system.

[G 2] Such a document sets out the organisational structure, the allocated staff responsibilities, the processes, procedures and activities which together ensure that the system under assessment satisfies the specified safety levels and safety requirements. The document needs to be compliant with the CSM as it supports and provides guidance to the assessment body. The CENELEC standards advise that this type of information is included in a safety plan or, in another document with a part dedicated to those topics.

[G 3] The proposer's safety plan in particular, or any other relevant document, presents the overall project organisation. It describes how the roles and responsibilities are shared between the involved actors. For detailed information, reference can be made to the safety plans or safety organisations of the different involved actors. Usually, the sharing of responsibilities between the different actors is discussed and agreed during the preliminary system definition (i.e. at the beginning of the project), if there is one.

[G 4] The safety plan is a living document that is updated when necessary during the project life.

[G 5] More details can be found in the EN 50 126-1 standard {Ref. 8} and its associated 50 126-2 Guideline {Ref. 9} about the content of a safety plan.

1.1.7. Evaluation of the correct application of the risk management process described in this Regulation falls within the responsibility of the assessment body.

[G 1] Additional explanation is not judged necessary.

Continuation of the footnote

If for a specific application, the compliance with some assumptions and restrictions of use cannot be achieved at a sub-system level (e.g. in case of operational safety requirements), the corresponding assumptions and restrictions of use can be transferred to a higher level (i.e. usually at system level). These assumptions and restrictions of use are then clearly identified in the "specific application safety case" of the related sub-system. This is essential to ensure in such examples of dependency that the safety related application conditions of each safety case are fulfilled in the higher-level safety case, or else are carried forward into the safety related application conditions of the highest-level safety case (i.e. system safety case).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2. Interface management

1.2.1. For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces. The management of shared risks at the interfaces shall be co-ordinated by the proposer.

[G 1] For example, if for operational reasons a railway undertaking needs an infrastructure manager to perform defined changes in the infrastructure, by virtue of the requirements in Annex III(2)(g) of the Railway Safety Directive {Ref. 1}, the RU also monitors the overall work in order to ensure that the expected changes are done correctly. However, the RU leadership does not remove the responsibility from the related IM to inform the other railway undertakings if they are also affected by the related change of the infrastructure. The IM may even have to carry out risk assessment, in accordance with the CSM, if the related change is significant from its point of view.

[G 2] Transfers of responsibilities between the different actors are possible and, in some circumstances even necessary. However, when several actors are involved in a system, very often one actor is pointed out as the responsible for the totality of the system. There are always dependencies between sub-systems and operations that require special efforts to identify. It is thus necessary that someone takes over the overall responsibility for the safety analyses and gets also full access to all relevant documentation. Obviously, the proposer who intends to introduce the significant change generally has the overall responsibility that the risk assessment is systematic and complete.

[G 3] The main criteria to be agreed on for the management of an interface between the concerned actors are:

(a) the leadership which is usually ensured by the proposer who intends to introduce the significant change;
(b) the required inputs;
(c) the methods for the hazard identification and the risk assessment;
(d) the required participants with the needed competence (i.e. combination of knowledge, skills and practical experience in the – see also definition of "staff competence" in point [G 2](b) of Article 3 in {Ref. 4});
(e) the expected outputs.

These criteria are described in the safety plans (or in any other relevant documents) of the companies dealing with the concerned interfaces.

[G 4] Examples of interfaces are provided in section C.3. of Appendix C, as well as an example of the application of those main criteria for the management of the interface between a train manufacturer and an infrastructure manager or a railway undertaking.

[G 5] The interface management is also to consider the risks that could arise at the interfaces with human operators (used during operation and maintenance) for designing those interfaces.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.2. When, in order to fulfil a safety requirement, an actor identifies the need for a safety measure that it cannot implement itself, it shall, after agreement with another actor, transfer the management of the related hazard to the latter using the process described in section 4.

[G 1] The process for transferring hazards and associated safety measures between actors is also applicable at lower levels of the CENELEC V-Cycle in Figure 5 at page 33. It can be applied whenever it is necessary to exchange such information between an actor and its sub-contractors for example. The difference with the same process at the system level is that the proposer needs not be informed about all transfers of hazards and associated safety measures at the sub-system level. The proposer is informed only when the transferred hazards and associated safety measures are related to high level interfaces (i.e. when impacting an interface with the proposer).

1.2.3. For the system under assessment, any actor who discovers that a safety measure is non-compliant or inadequate is responsible for notifying it to the proposer, who shall in turn inform the actor implementing the safety measure.

[G 1] The RU and IM safety management system (SMS) covers the arrangements and procedures for ensuring that non compliances or inadequacies of safety measures are managed correctly. Therefore, these arrangements and procedures are not part of the CSM.

[G 2] Similarly, arrangements and procedures[(11)] to put in place by the other actors[(12)] for ensuring that non compliances or inadequacies of safety measures are managed correctly and, if necessary, that the safety measures are transferred to all relevant actors are agreed between the relevant actors at the beginning of the project, and detailed in their safety plan: refer to section 0.2.

1.2.4. The actor implementing the safety measure shall then inform all the actors affected by the problem either within the system under assessment or, as far as known by the actor, within other existing systems using the same safety measure.

[G 1] That will thus enable to manage the possible non compliance or inadequacy of the safety measure within the system under assessment or within similar systems that use the same measure.

1.2.5. When agreement cannot be found between two or more actors it is the responsibility of the proposer to find an adequate solution.

[G 1] Additional explanation is not judged necessary.

---

(11) *In principle, these arrangements and procedures are covered by the quality management and/or the safety management process of these actors set out at least at the project level (see also Figure 2).*

(12) *The terminology "other actors" designates all concerned actors other than IM's and RU's.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.6.	*When a requirement in a notified national rule cannot be fulfilled by an actor, the proposer shall seek advice from the relevant competent authority.*

[G 1] Additional explanation is not judged necessary.

1.2.7.	*Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and the integration into the railway system as a whole.*

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2. DESCRIPTION OF THE RISK ASSESSMENT PROCESS

2.1. General description - Correspondence between the CSM risk assessment process and the CENELEC V-cycle

2.1.1. The risk assessment process is the overall iterative process that comprises:

(a) the system definition;
(b) the risk analysis including the hazard identification;
(c) the risk evaluation.

The risk assessment process shall interact with the hazard management according to section 4.1.

[G 1] The risk management process covered by the CSM can be represented within a V-Cycle that starts with the (preliminary) system definition and that finishes with the system acceptance: see Figure 4. This simplified V-Cycle can be mapped then on the classical V-Cycle in Figure 10 of the EN 50 126-1 standard {Ref. 8}. In order to show the correspondence of the CSM risk management process in Figure 1, the CENELEC V-Cycle in Figure 10 is recalled in Figure 5:

(a) the "preliminary system definition" of the CSM in Figure 1 corresponds to the Phase 1 in CENELEC V-Cycle, i.e. to the definition of the system "concept" (see BOX 1 in Figure 5);
(b) the "risk assessment" of the CSM in Figure 1 includes the following phases of the CENELEC V-Cycle (see BOX 2 in Figure 5):

(1) Phase 2 in Figure 5: "system definition and application conditions";
(2) Phase 3 in Figure 5: "risk analysis";
(3) Phase 4 in Figure 5: "system requirements";
(4) Phase 5 in Figure 5: "apportionment of system requirements" down to the different sub-systems and components.

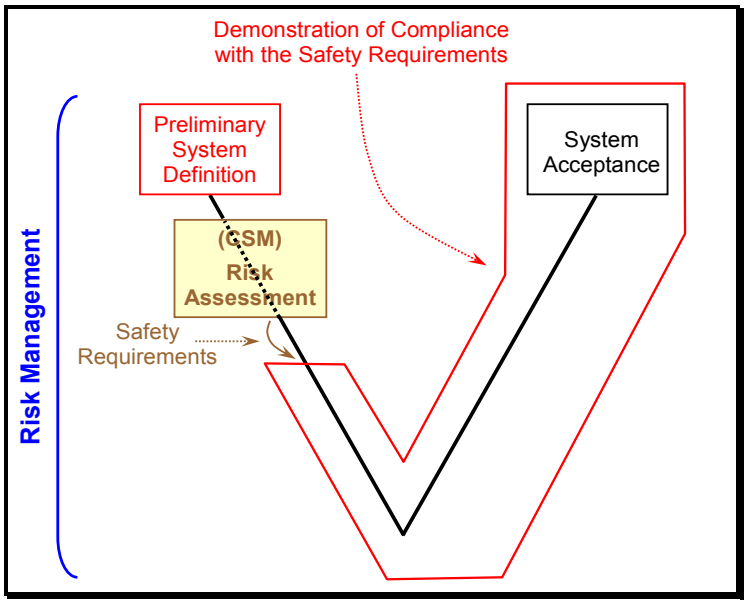

Figure 4 : Simplified V-Cycle of Figure 10 of EN 50 126 standard.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

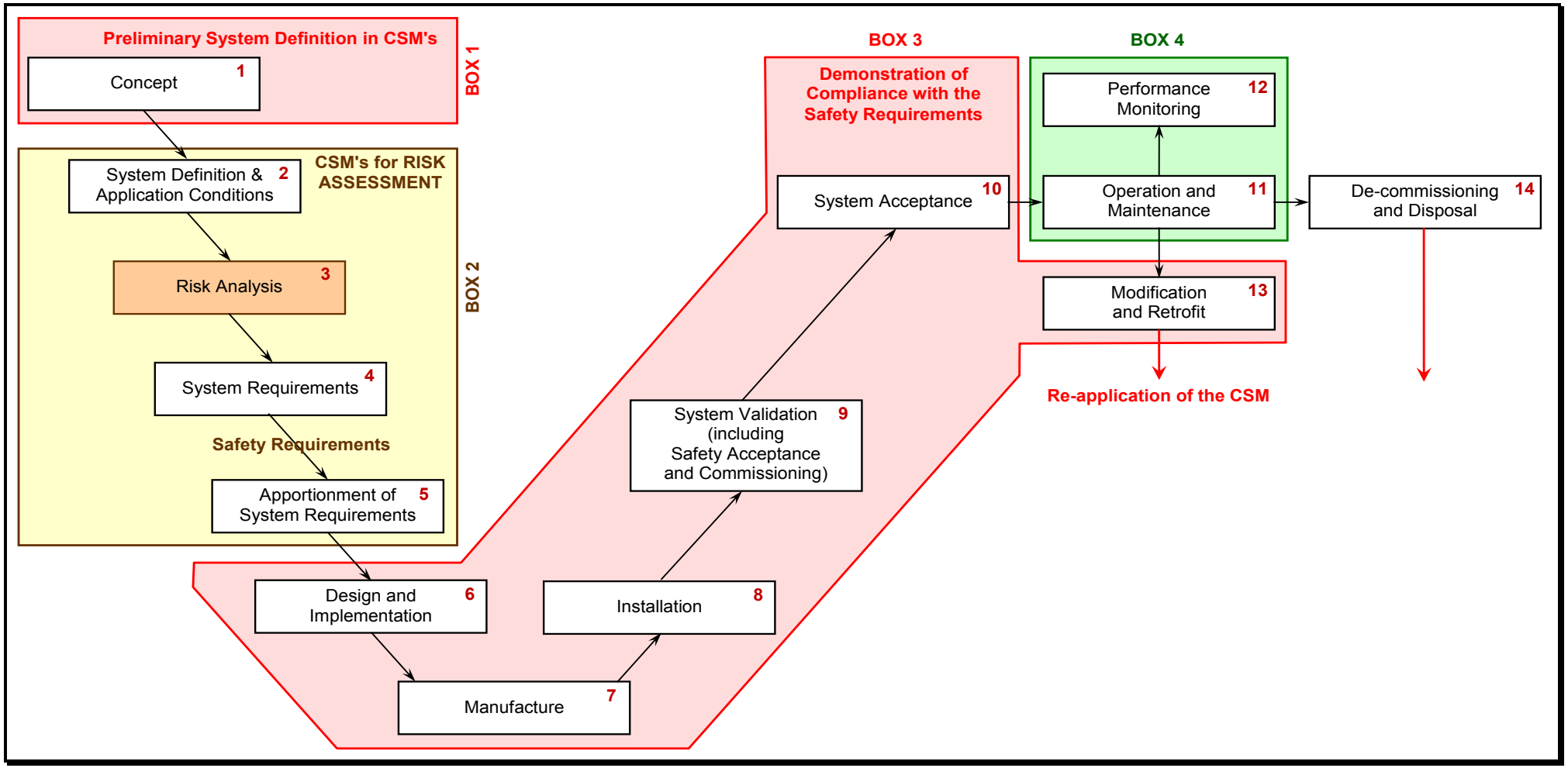

Figure 5 : Figure 10 of EN 50 126 V-Cycle (CENELEC system life-cycle).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] The outputs of the risk assessment process in the CSM are (after iterations - see Figure 1):

(a) the "system definition" updated with the "safety requirements" issued from the "risk analysis" and "risk evaluation" activities (see section 2.1.6);
(b) the "apportionment of system requirements" down to the different sub-systems and components (Phase 5 in Figure 5);
(c) the "hazard record" that registers:

(1) all the identified hazards and the associated safety measures;
(2) the resulting safety requirements;
(3) the assumptions taken into account for the system that determine the limits and validity of the risk assessment (see point (g) in section 2.1.2);

(d) and in general all the evidence resulting from the application of the CSM: see section 5.

These risk assessment outputs of the CSM correspond to the safety related outputs of the Phase 4 in the CENELEC V-Cycle, i.e. to the system requirement specification in Figure 5.

[G 3] The system definition updated with the results from the risk assessment and the hazard record constitute the inputs against which the system is designed and accepted. The "demonstration of the system compliance with the safety requirements" in the CSM corresponds to the following phases of the CENELEC V-Cycle (see BOX 3 in Figure 5):

(a) Phase 6 in Figure 5: "design and implementation";
(b) Phase 7 in Figure 5: "manufacture";
(c) Phase 8 in Figure 5: "installation";
(d) Phase 9 in Figure 5: "system validation (including safety acceptance and commissioning)";
(e) Phase 10 in Figure 5: "system acceptance".

[G 4] The demonstration of the system compliance with the safety requirements depends on whether the significant change is technical, operational or organisational. So, the different steps in the CENELEC V-cycle in Figure 5 may not be suitable for all significant changes of the given kind. The V-cycle in Figure 5 needs to be considered accordingly and used with appropriate judgement of what fits to each specific application (e.g. for operational and organisational changes, there is not manufacturing phase).

[G 5] This means that the "demonstration of the system compliance with the safety requirements" in the CSM does not include only the "verification and validation" activities by tests or simulation. In practice, it covers all the phases "6 to 10" (see list here above and Figure 5) in the CENELEC V-Cycle. They include the design, manufacture, installation, verification and validation activities, as well as the associated RAMS activities and the system acceptance.

[G 6] During the "demonstration of the system compliance with the safety requirements", the general principle is to focus the risk assessment only on the safety related functions and interfaces of the system. This means that whenever risk and safety assessment activities are required in the scope of one of the phases in the CENELEC V-Cycle in Figure 5, it focuses on:

(a) the safety related functions and interfaces;
(b) the sub-systems and/or components involved in the achievement of the safety related functions and/or interfaces assessed during the higher level risk assessment activities.

[G 7] It results then from the comparison with the classical CENELEC V-Cycle in Figure 5 that:

(a) the CSM covers the phases "1 to 10" and "13" of this V-Cycle. They include the set of activities required for the acceptance of the system under assessment;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) the CSM does not cover the phases "11", "12" and "14" of the system life-cycle:

(1) the phases "11" and "12" are respectively related to the "operation and maintenance" and "performance monitoring" of the system after its acceptance based on the CSM. These two phases are covered by the RU and IM safety management system (SMS) – (See BOX 4 in Figure 5). However, if during the operation, the maintenance or the performance monitoring of the system it appears necessary to modify and retrofit the system (Phase 13 in Figure 5), whereas it is already in operation, the CSM is applied again on the new required changes in compliance with the Article 2. Therefore, if the change is significant:

(i) the risk management and risk assessment processes in the CSM are applied to these new changes;
(ii) an acceptance is needed for these new changes in compliance with Article 6;

(2) the "de-commissioning and disposal" of a system already in operation (Phase 14) could also be considered as a significant change, and therefore, the CSM could be applied again in compliance with the Article 2 for the phase 14 in Figure 5

For more information about the scope of each phase or activity in the CENELEC V-Cycle recalled in Figure 5, refer to section § 6. of the EN 50 126-1 standard {Ref. 8}

2.1.2. The system definition should address at least the following issues:

(a) system objective, e.g. intended purpose;
(b) system functions and elements, where relevant (including e.g. human, technical and operational elements);
(c) system boundary including other interacting systems;
(d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;
(e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);
(f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process;
(g) assumptions which shall determine the limits for the risk assessment.

[G 1] Additional explanation is not judged necessary.

2.1.3. A hazard identification shall be carried out on the defined system, according to section 2.2.

[G 1] Additional explanation is not judged necessary.

2.1.4. The risk acceptability of the system under assessment shall be evaluated by using one or more of the following risk acceptance principles:

(a) the application of codes of practice (section 2.3);
(b) a comparison with similar systems (section 2.4);
(c) an explicit risk estimation (section 2.5).

In accordance with the general principle referred to in section 1.1.5, the assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] In general, the proposer will decide what risk acceptance principle is the most appropriate for controlling the identified hazards based on the specific requirements of the project, as well as on the proposer's experience with the three principles.

[G 2] It is not possible always to evaluate the risk acceptability at the system level through the use of only one of the three risk acceptance principles. The risk acceptance will often be based on a mix of these principles. If for a significant hazard, more than one risk acceptance principles need to be applied for controlling the associated risk, the related hazard needs to be divided into sub-hazards so that each individual sub-hazard is adequately controlled by only one risk acceptance principle.

[G 3] The decision for controlling a hazard by a risk acceptance principle needs to take into account the hazard and the causes of the hazard already identified during the hazard identification phase. Thus, if two different and independent causes are associated to the same hazard, the hazard needs to be sub-divided into two different sub-hazards. Each sub-hazard will then be controlled by a single risk acceptance principle. The two sub-hazards need to be registered and managed in the hazard record. For example, if the hazard is caused by a design error this can be managed by the application of a code of practice, whereas if the cause of the hazard is a maintenance error, the code of practice alone may not be sufficient; the application of another risk acceptance principle is then needed.

[G 4] The reduction of risk to an acceptable level might need several iterations between the risk analysis and risk evaluation phases until appropriate safety measures are identified.

[G 5] The present residual risk returned from experience on the field for the existing systems and for the systems based on the application of codes of practice is recognised to be acceptable. The risk resulting from explicit risk estimation is based on expert's judgement and different assumptions taken by the expert during the analyses, or on data bases related to accident or operational experience. Therefore the residual risk from explicit risk estimation cannot be confirmed immediately by return from the field. Such a demonstration requires time for operating, monitoring and getting a representative experience for the related system(s). In general, the application of codes of practice and comparison with similar reference systems has the advantage to avoid the over specification of unnecessarily strict safety requirements that can result from excessively conservative (safety) assumptions in explicit risk estimations. However it could happen that some safety requirements from codes of practice or similar reference systems need not to be fulfilled for the system under assessment. In that case, the application of explicit risk estimation would have the advantage to avoid an unnecessary overdesign of the system under assessment and would enable to provide a more cost effective design that has not been tried before.

[G 6] If the identified hazards and the associated risk(s) of the system under assessment cannot be controlled by the application of codes of practice or similar reference systems, an explicit risk estimation is performed, based on quantitative or qualitative analyses of hazardous events. This situation arises when the system under assessment is entirely new (or the design is innovative) or when the system deviates from a code of practice or a reference system. The explicit risk estimation will then evaluate whether the risk is acceptable (i.e. further analysis is not needed) or whether additional safety measures are needed to reduce the risk further.

[G 7] Guidance for risk reduction and risk acceptance can also be found in section § 8. of the EN 50 126-2 Guideline {Ref. 9}.

[G 8] The used risk acceptance principle and its application need to be evaluated by the assessment body.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.1.5. The proposer shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer shall also check that the selected risk acceptance principles are used consistently.

[G 1] For example, if for the software of a component the application of the SIL 4 development process of the EN 50 128 standard is specified as the safety requirement, the demonstration will need to prove that the process recommended by the standard is fulfilled. This includes for example the demonstration that:

(a) the requirements for independence in the organisation of the design, verification and validation of the software are fulfilled;
(b) the correct methods of the EN 50 128 standard for the SIL 4 safety integrity level are applied;
(c) etc.

[G 2] For example, if a dedicated code of practice is to be used for manufacturing emergency brake electro valves, the demonstration will need to prove that all requirements from the code of practice are fulfilled during the manufacturing process.

2.1.6. The application of these risk acceptance principles shall identify possible safety measures which make the risk(s) of the system under assessment acceptable. Among these safety measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with section 3.

[G 1] Two types of safety measures can be identified:

(a) "preventive safety measures" preventing the occurrence of hazards or their causes, and;
(b) "mitigation safety measures" preventing hazards to evolve into accidents or reducing the consequences of accidents after their occurrence (protection measures)

For the benefit of operability, prevention of causes is generally more efficient

[G 2] The proposer will consider as the most appropriate the safety measures that give the best compromise between the cost to achieve the risk reduction and the level of the residual risk. The chosen safety measures become the safety requirements for the system under assessment.

[G 3] It is important to check that the safety measures selected to control one hazard are not in conflict with other hazards. As represented in Figure 6, the following two cases may happen for example[13]:

(a) CASE 1: if the same safety measure (measure A on Figure 6) can control different hazards without creating conflicts between them, and if economically justified, the related safety measure could be chosen alone as the associated "safety requirement". The total number of safety requirements to fulfil is smaller than implementing both the measures B and C;

(13) *It must be noted that the guide does not list all the situations where safety measures could be in conflict with other identified hazards. Only a few illustrative examples are provided.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

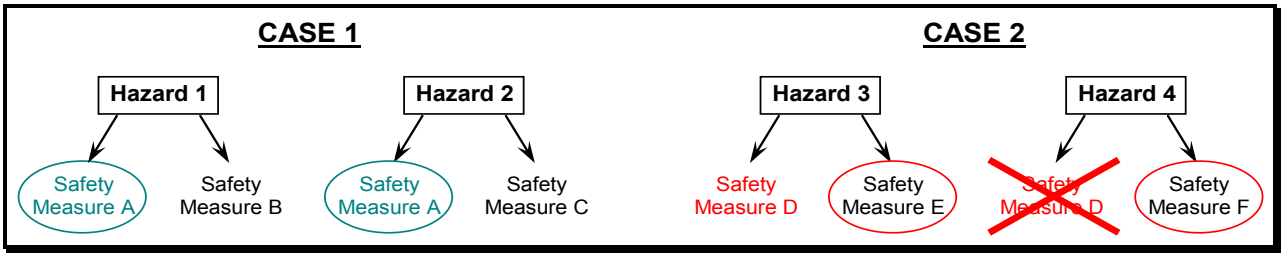

Figure 6 : Selection of adequate safety measures for controlling risks.

(b) CASE 2: reciprocally, if one safety measure can control one hazard but creates a conflict with another hazard (measure D on Figure 6), it cannot be chosen as "safety requirement". The other safety measures for the considered hazard need to be used (measures E and F on Figure 6):

(1) A typical example in the Control Command System is the use of the train location on the track either for controlling the brake application or for authorising the train acceleration. The use of the train front end as the train location (respectively of the train rear end) is not safe in all situations:

(i) when the ETCS control command system has to safely apply the emergency brakes, it uses the MAXIMUM SAFE FRONT END in order to guarantee that the train front actually stops before reaching the Danger Point;

(ii) reciprocally, when the train is authorised to accelerate after a speed limitation for example, the ETCS control command system uses the MINIMUM SAFE REAR END;

(2) Another example is a safety measure that could be valid for stopping a train in almost all circumstances to enter a fail-safe state except for a tunnel or a bridge. In this latter case, the measure D in CASE 2 of Figure 6 shall not be taken.

2.1.7. The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.

[G 1] Depending for example on technical choices for the design of a system, its sub-systems and equipment, new hazards could be identified during the "demonstration of compliance with the safety requirements" (e.g. use of certain painting could lead to toxic gases in case of fire). These new hazards and the associated risks need to be considered as new inputs for a new loop in the iterative risk assessment process. Appendix A.4.3 in EN 50 129 standard provides other examples where new hazards could be introduced and need to be controlled.

2.2. Hazard identification

2.2.1. The proposer shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces.

All identified hazards shall be registered in the hazard record according to section 4.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] The hazards are expressed as far as possible at the same level of detail. It can happen during preliminary hazard analyses that hazards of different levels of detail are identified (e.g. because during HAZOP's people with different experience are gathered).
The level of detail depends also on the risk acceptance principle that is selected to control the identified hazard(s). For example, if a hazard is controlled completely by a code of practice or a similar reference system, more detailed hazard identification will not be necessary.

[G 2] All the hazards identified during the risk assessment process (including the ones associated with broadly acceptable risks), the associated safety measures and the associated risks, need to be registered in the hazard record.

[G 3] Depending on the nature of the system to be analysed, different methods can be used for the hazard identification:

(a) empirical hazard identification can be used exploiting the past experience (e.g. use of checklists or generic hazard lists);
(b) creative hazard identification can be used for new areas of concern (proactive forecasting, e.g. structured "WHAT-IF" studies like FMEA or HAZOP).

[G 4] The empirical and creative methods for hazard identification can be used together to complement each other ensuring that the list of potential hazards and safety measures when applicable are comprehensive.

[G 5] As a preliminary step, the hazard identification could start with a brainstorming team where experts with different competence, covering all relevant aspects of the significant change, are present. When judged necessary by the experts' panel, empirical methods can be used to analyse a specific function or operational mode.

[G 6] The methods used for the hazard identification depend on the system definition. Some examples are given in Appendix B.

[G 7] More information on the hazard identification techniques and methods can be found in Annex A.2 & E of the EN 50 126-2 Guideline {Ref. 9}.

[G 8] An example of a generic hazard list is given in section C.17. of Appendix C.

2.2.2. To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.

[G 1] In order to help the risk assessment process, the significant hazards can be grouped further into different categories. For example, the significant hazards can be classified or ranked in function of their expected severity of risk, and frequency of occurrence. Guidance for such an exercise is given in CENELEC standards: see section A.2. in Appendix A.

[G 2] The risk analysis and evaluation described in section 2.1.4 are applied on a prioritised basis beginning with the highest-ranked hazards.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

[G 1] For example, a risk associated to a hazard can be considered as broadly acceptable:

(a) if the risk is less than a given percentage (e.g. x%) of the Maximum Tolerable Risk for this hazard type. The value of x% could be based on best practice and experience with several risk analysis approaches, e.g. the ratio between broadly acceptable risk and intolerable risk classifications in FN-curves or in risk matrices. This can be represented as shown in Figure 7;

(b) or if the loss associated to the risk is so small that it is not reasonable to implement any counter safety measure.

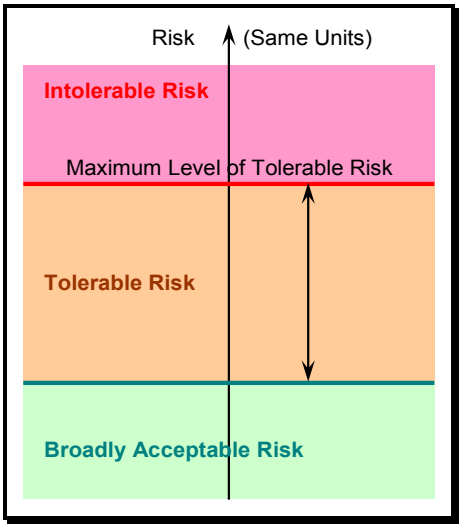

Figure 7 : Broadly acceptable risks

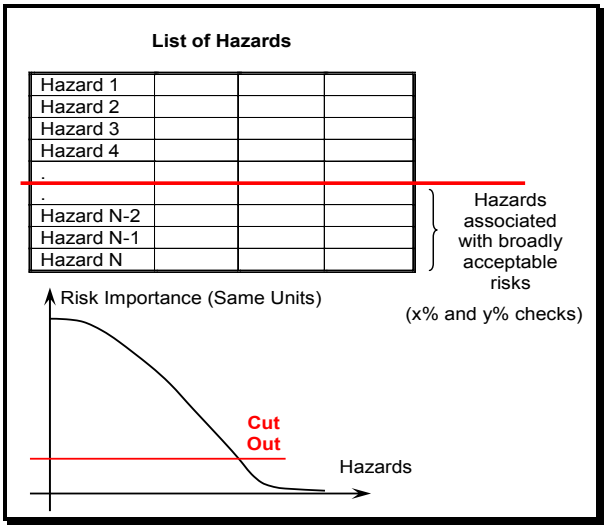

Figure 8 : Filtering out of hazards associated with broadly acceptable risk.

[G 2] In addition to that, if hazards with different levels of detail are identified (i.e. high level hazards on one hand, and detailed sub-hazards on the other hand), precautions need to be taken to avoid their wrong classification into hazards associated with broadly acceptable risk(s). The contribution of all hazards associated with broadly acceptable risk(s) cannot exceed a given proportion (e.g. y%) of the overall risk at the system level. This check is necessary in order to prevent that the rationale is hollowed out by subdividing the hazards into many low-level sub-hazards. Indeed, if one hazard is expressed as many different "smaller" sub-hazards, each of those can easily be classified as associated with broadly acceptable risk(s) if evaluating them independently, but associated with significant risk when evaluating them together (i.e. as one high level hazard). The value of the proportion (e.g. y%) depends on the risk acceptance criteria applicable at the system level. It can be based on and estimated from operational experience of similar reference systems.

[G 3] The two checks here above (i.e. against x % and y %) enable the focus of the risk assessment on the most important hazards, as well as to ensure that any significant risk is controlled (see Figure 8).
Without prejudice to the legal requirements in a Member State, the proposer is responsible to define, based on expert judgement, the values of x % and y % and to have them

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

independently assessed by the assessment body. An example of orders of magnitude can be x = 1% and y = 10%, if this is considered acceptable by the expert judgement

[G 4] Section 2.2.2 requests that the classification into "broadly acceptable risk(s)" is independently assessed by an assessment body.

2.2.4. During the hazard identification, safety measures may be identified. They shall be registered in the hazard record according to section 4.

[G 1] The main purpose of the activity is the identification of hazards that are linked to the change. If safety measures are already identified, they need to be registered in the hazard record. The nature of the measures depends on the change; they can be procedural, technical, operational or organisational.

2.2.5. The hazard identification only needs to be carried out at a level of detail necessary to identify where safety measures are expected to control the risks in accordance with one of the risk acceptance principles mentioned in point 2.1.4. Iteration may thus be necessary between the risk analysis and the risk evaluation phases until a sufficient level of detail is reached for the identification of hazards.

[G 1] Even if a risk is controlled to an acceptable level, the proposer may still decide that more detailed hazard identification is necessary. One reason for this could be that it is likely to find more cost effective risk control safety measures if performing more detailed hazard identification.

2.2.6. Whenever a code of practices or a reference system is used to control the risk, the hazard identification can be limited to:

(a) The verification of the relevance of the code of practices or of the reference system.
(b) The identification of the deviations from the code of practices or from the reference system.

[G 1] Additional explanation is not judged necessary.

2.3. Use of codes of practice and risk evaluation

2.3.1. The proposer, with the support of other involved actors and based on the requirements listed in point 2.3.2, shall analyse whether one or several hazards are appropriately covered by the application of relevant codes of practice.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.2. The codes of practice shall satisfy at least the following requirements:

(a) be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;
(b) be relevant for the control of the considered hazards in the system under assessment;
(c) be publicly available for all actors who want to use them.

[G 1] Additional explanation is not judged necessary.

2.3.3. Where compliance with TSIs is required by Directive 2008/57/EC and the relevant TSI does not impose the risk management process established by this Regulation, the TSIs may be considered as codes of practice for controlling hazards, provided requirement (c) of point 2.3.2 is fulfilled.

[G 1] Additional explanation is not judged necessary.

2.3.4. National rules notified in accordance with Article 8 of Directive 2004/49/EC and Article 17(3) of Directive 2008/57/EC may be considered as codes of practice provided the requirements of point 2.3.2 are fulfilled.

[G 1] Additional explanation is not judged necessary.

2.3.5. If one or more hazards are controlled by codes of practice fulfilling the requirements of point 2.3.2, then the risks associated with these hazards shall be considered as acceptable. This means that:

(a) these risks need not be analysed further;
(b) the use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.

[G 1] Additional explanation is not judged necessary.

2.3.6. Where an alternative approach is not fully compliant with a code of practice, the proposer shall demonstrate that the alternative approach taken leads to at least the same level of safety.

[G 1] Additional explanation is not judged necessary.

2.3.7. If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified applying one of the two other risk acceptance principles.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.8. When all hazards are controlled by codes of practice, the risk management process may be limited to:

(a) The hazard identification in accordance with section 2.2.6;
(b) The registration of the use of the codes of practice in the hazard record in accordance with section 2.3.5;
(c) The documentation of the application of the risk management process in accordance with section 5;
(d) An independent assessment in accordance with Article 6.

[G 1] Additional explanation is not judged necessary.

2.4. Use of reference system and risk evaluation

2.4.1. The proposer, with the support of other involved actors, shall analyse whether one or more hazards are covered by a similar system that could be taken as a reference system.

[G 1] More information on these principles can be found in section § 8 of the EN 50 126-2 guide {Ref. 9}.

2.4.2. A reference system shall satisfy at least the following requirements:

(a) it has already been proven in-use to have an acceptable safety level and would still qualify for acceptance in the Member State where the change is to be introduced;
(b) it has similar functions and interfaces as the system under assessment;
(c) it is used under similar operational conditions as the system under assessment;
(d) it is used under similar environmental conditions as the system under assessment.

[G 1] For example, an old Control Command System that is proven in-use to have an acceptable level of safety could be superseded by another system, with more recent technology and better safety performance. It is thus pertinent to check each time when applying a reference system whether it continues to qualify for acceptance.

[G 2] For example, as certain aspects of tunnel safety or the safety of dangerous good transport could be specific and could depend on operational and environmental conditions, it is necessary to check for each project that the system will be used under the same conditions.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.4.3. If a reference system fulfils the requirements listed in point 2.4.2, then for the system under assessment:

(a) the risks associated with the hazards covered by the reference system shall be considered as acceptable;
(b) the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;
(c) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.

[G 1] Additional explanation is not judged necessary.

2.4.4. If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

[G 1] More information about similarity analyses can be found in section § 8.1.3. of the EN 50 126-2 Guideline {Ref. 9}.

2.4.5. If the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

[G 1] Additional explanation is not judged necessary.

2.5. Explicit risk estimation and evaluation

2.5.1. When the hazards are not covered by one of the two risk acceptance principles described in sections 2.3 and 2.4, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5.2. The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.

If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.

[G 1] In order to evaluate whether the risks from the system under assessment are acceptable or not, risk acceptance criteria are needed (see "risk evaluation" boxes in Figure 1). The risk acceptance criteria can be either implicit or explicit:

(a) implicit risk acceptance criteria: according to sections 2.3.5 and 2.4.3, risks covered by application of codes of practice and by comparison with reference systems are considered implicitly as acceptable provided respectively that (see dotted circle in Figure 1):

(1) the conditions of application of codes of practice in section 2.3.2 are met;
(2) the conditions for use of a reference system in section 2.4.2 are met;

(b) explicit risk acceptance criteria: in order to evaluate whether the risk(s) controlled by the application of explicit risk estimation is acceptable or not, explicit risk acceptance criteria are needed (see plain line circle in Figure 1 for third principle). These can be defined at different levels of a railway system. They can be seen as a "pyramid of criteria" (see Figure 9) starting from the high level risk acceptance criteria (expressed for instance as societal or individual risk), going down to sub-systems and components (to cover technical systems) and including the human operators during operation and maintenance activities of the system and sub-systems. Although the risk acceptance criteria contribute to the achievement of the system safety performance, and thus are linked to CST and NRV, it is very difficult to build a mathematical model between them: see {Ref. 12} for more details about that.
The level at which the explicit risk acceptance criteria are defined needs to match with the importance and complexity of the significant change. For example, it is not necessary to evaluate the overall railway system risk when modifying a type of axle in rolling stocks. The definition of the risk acceptance criteria can focus on the rolling stock safety. Reciprocally, large changes or additions to an existing railway system should not be evaluated solely on the basis of the safety performance of individual functions or changes that are added. It should also be verified at the railway system level that the change is acceptable as a whole.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

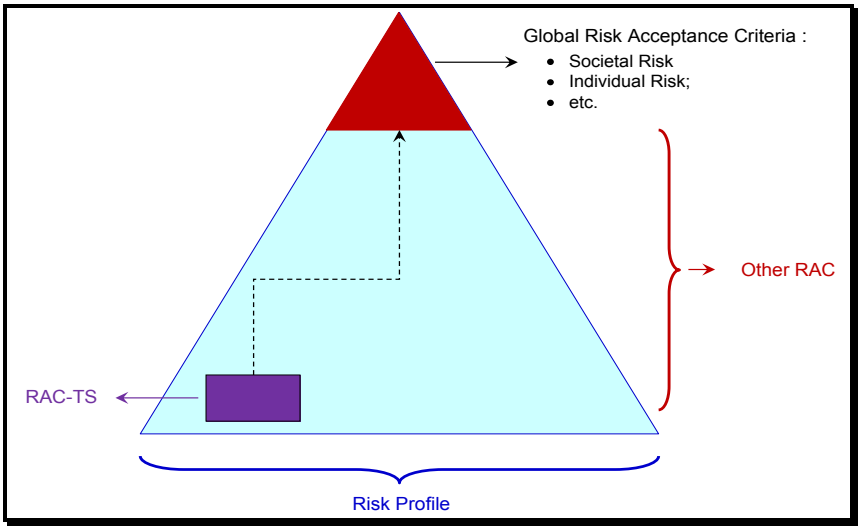

Figure 9 : Pyramid of risk acceptance criteria (RAC).

[G 2] The explicit risk acceptance criteria that are needed to support the mutual recognition will be harmonised between the Member States by the on-going Agency work on the risk acceptance criteria. When available, additional information will be included in this document.

[G 3] In the meantime risks can be evaluated using for example the risk matrix that can be found in section § 4.6 of the EN 50 126-1 standard {Ref. 8}. Other types of suitable criteria can also be used, given that these criteria are deemed to deliver an acceptable level of safety in the concerned case.

2.5.3. When the risk associated with one or a combination of several hazards is considered as acceptable, the identified safety measures shall be registered in the hazard record.

[G 1] Additional explanation is not judged necessary.

2.5.4. Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

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.

[G 1] Further details about the RAC-TS, as well as what aspects and functions of the technical system the criterion applies to, are provided in a separate Agency note associated to the present document: see section A.3. of Appendix A and reference document {Ref. 11}.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5.5.	*Without prejudice to the procedure specified in Article 8 of Directive 2004/49/EC, a more demanding criterion may be requested, through a national rule, in order to maintain a national safety level. However, in the case of additional authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.*

[G 1] Additional explanation is not judged necessary.

2.5.6.	*If a technical system is developed by applying the 10^{-9} criterion defined in point 2.5.4, the principle of mutual recognition is applicable in accordance with Article 7(4) of this Regulation.* *Nevertheless, if the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a rate of failure higher than 10-9 per operating hour, this criterion can be used by the proposer in that Member State.*

[G 1] Additional explanation is not judged necessary.

2.5.7.	*The explicit risk estimation and evaluation shall satisfy at least the following requirements:* *(a) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);* *(b) the results shall be sufficiently accurate to serve as robust decision support, i.e. minor changes in input assumptions or prerequisites shall not result in significantly different requirements.*

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. DEMONSTRATION OF COMPLIANCE WITH SAFETY REQUIREMENTS

3.1. Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

[G 1] As explained in points [G 3] to [G 6] in section 2.1.1, the "demonstration of the system compliance with the safety requirements" includes the phases "6 to 10" of the CENELEC V-Cycle (see BOX 3 in Figure 5). Refer to point [G 3] in section 2.1.1.

[G 2] Refer also to point [G 4] in section 2.1.1 of this document.

3.2. This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements, as decided in accordance with point 1.1.5.

[G 1] An example of safety assessments and safety analyses that can be performed at the sub-system level are causal analyses: see Figure 10. But any other method can be used to demonstrate the sub-system compliance with the input safety requirements.

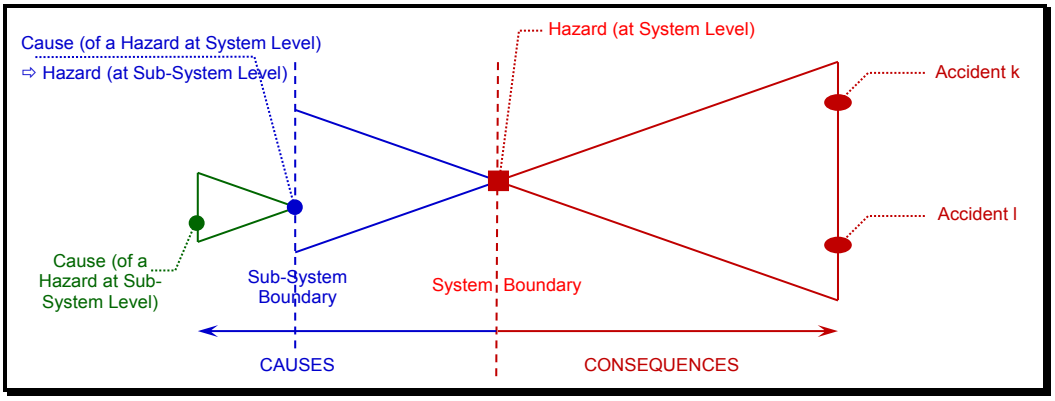

Figure 10 : Figure A.4 of EN 50 129: Definition of hazards with respect to the system boundary.

[G 2] The hierarchical structuring of hazards and causes, with respect to systems and sub-systems, can be repeated for each lower level phase of the CENELEC V-Cycle in Figure 5, The hazard identification and causal analysis activities (or any relevant method), as well as the use of codes of practice, similar reference systems and explicit analyses and evaluations, can also be repeated for each phase of the system development cycle in order to derive, from the safety measures identified at the sub-system level, the safety requirements to be fulfilled by the next phase. This is illustrated in Figure 11.

[G 3] Refer also to point [G 4] in section 2.1.1 of this document.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

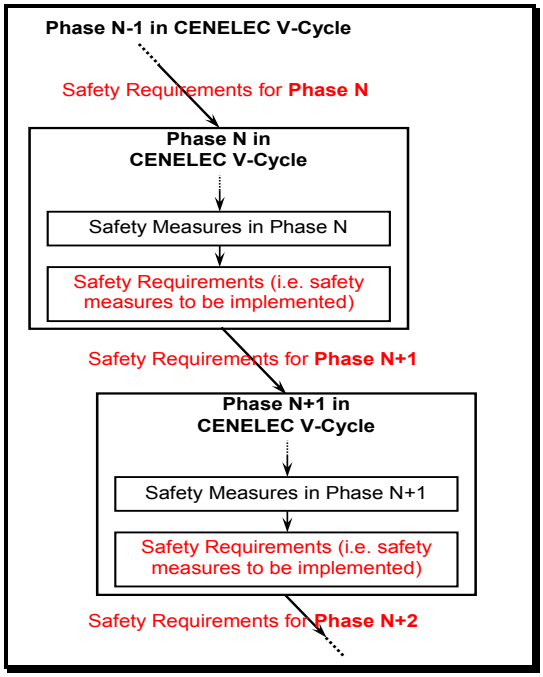

Figure 11 : Derivation of the safety requirements for lower level phases.

3.3.	*The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.*

[G 1] All the activities represented in BOX 3[14] of the CENELEC V-Cycle in Figure 5 are therefore also independently assessed.

[G 2] The kind and level of detail for the independent assessment that is carried out by the assessment bodies (i.e. detailed or macroscopic assessment) is dealt within the explanations of the Article 6.

3.4.	*Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer according to section 2. The new hazards shall be registered in the hazard record according to section 4.*

[G 1] For example, the way for extinguishing fire could lead to a new hazard (suffocation) that will impose new safety requirements (e.g. a specific procedure for the passenger evacuation). Another example is the use of toughened glass to avoid that windows are broken in crashes and that passengers are harmed by glass or even thrown out. The new hazard induced is

(14) *The correspondence of activities between the CSM's and Figure 5 (i.e. Figure 10 of CENELEC 50 126 V-Cycle) is described in section 2.1.1. In particular, point [G 3] in section 2.1.1 lists what CENELEC activities are included in the CSM's phase "demonstration of the system compliance with the safety requirements".*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

then that emergency evacuation from the wagons through windows is much more difficult, which may result in safety requirements that certain windows need to be specially designed to enable evacuation.

[G 2] Example of an operational change: it is required that all transports of dangerous goods are banned from running on a line through densely populated areas. Instead, it should therefore run through an alternative route with tunnels, therefore creating different types of hazards.

[G 3] Other examples of new hazards that could be identified during the demonstration of the system compliance with the safety requirements can be found in Appendix A.4.3 of the EN 50 129 standard.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. HAZARD MANAGEMENT

4.1. Hazard management process

4.1.1. Hazard record(s) shall be created or updated (where they already exist) by the proposer during the design and the implementation and till the acceptance of the change or the delivery of the safety assessment report. The hazard record shall track the progress in monitoring risks associated with the identified hazards. In accordance with point 2(g) of Annex III to Directive 2004/49/EC, once the system has been accepted and is operated, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment as an integrated part of its safety management system.

[G 1] The use of a hazard record for registering, managing and controlling safety relevant information is also recommended by the CENELEC 50 126-1 {Ref. 8} and 50 129 {Ref. 7} standards.

[G 2] For example, depending on the complexity of the system, an actor could have one or more hazard records. In both cases, the hazard record(s) is(/are) subject to independent assessment by the assessment body (-ies). For example, one possible solution could be to have:

(a) one "internal hazard record" for the management of all the internal safety requirements applicable to the sub-system the actor is responsible for. Its size and amount of management work depends on its structure and of course on the complexity of the sub-system. However, as it is used for internal management purposes, the hazard record does not need to be communicated to other actors. The internal hazard record contains all the identified hazards that are controlled, as well as the associated safety measures that are validated;
(b) one "external hazard record" for transferring to other actors hazards and the associated safety measures (that the actor cannot implement fully himself) in compliance with the section 1.2.2. Usually, this second hazard record is smaller and requires less management work (see example in section C.16.4. of Appendix C).

[G 3] If it seems complicated to manage several hazard records, another possible solution is to manage all hazards and the associated safety measures covered by the points (a) and (b) above in a single hazard record but with the possibility of two hazard record reports (see example in section C.16.3. of Appendix C):

(a) one internal hazard record report, which could even be not necessary if the hazard record is well structured in order to enable independent assessment;
(b) one external hazard record report for transferring hazards and the associated safety measures to other actors.

[G 4] As explained in section 4.2, at the end of the project when the system is accepted:

(a) all hazards that are transferred to other actors are controlled in the external hazard record of the actor who transfers them. As they are imported and managed in the internal hazard records of the other actors, they need not be managed further by the considered actor during the (sub-)system life-cycle;
(b) however all the associated safety measures should not be validated in the hazard record for the reasons that are explained in point [G 9] in section 4.2. Indeed, it is useful that the organisation exporting the restrictions of use clearly points out in its hazard record that the associated safety measures were not validated.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 5] Reciprocally, all internal hazard records are maintained throughout the whole (sub-)system life-cycle. That enables to track the progress on monitoring risks associated with the identified hazards during the (sub-)system operation and maintenance, i.e. even after its commissioning: see BOX 4 in the CENELEC V-Cycle in Figure 5.

4.1.2. The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. In particular, it shall contain a clear reference to the origin and to the selected risk acceptance principles and shall clearly identify the actor(s) in charge of controlling each hazard.

[G 1] The information on hazards and the associated safety measures that is received from other actors (see section 1.2.2) includes also all the assumptions(15) and restrictions of use(15) (also called safety related application conditions) applicable to the different sub-systems, generic application and generic product safety cases that are produced by the manufacturers, where relevant.

[G 2] A possible example of structure for the hazard record is described in section C.16. of Appendix C.

4.2. Exchange of information

All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution. The hazards registered in the hazard record of the actor who transfers them shall only be "controlled" when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.

[G 1] For example, for the odometry sub-system of the ETCS onboard equipment, the manufacturer can validate in laboratory the algorithms by simulating the theoretical signals that could be generated by the associated odometric sensing devices. However, the complete validation of the odometry sub-system requires the help of the RU and IM for carrying out the validation with the use of a real train and the real train wheel to rail contact.

[G 2] Other examples could be transfers by manufacturers to railway undertakings of operational or maintenance safety measures for technical equipment. These safety measures will need to be implemented by the railway undertaking.

[G 3] In order to enable these hazards, the associated safety measures and risks to be reassessed jointly by the involved organisations, it is helpful that the organisation having identified them provides all the explanations necessary to understand clearly the problem. It could be possible that the initial wording of the hazards, safety measures and risks needs to be changed to make them understandable without having to discuss them again jointly. The joint reassessment of the hazards could lead to identify new safety measures.

(15) *Refer to point [G 5] in section 1.1.5 and to the footnotes (9) and (10) at page 24 of this document for further explanation about the terminology "generic product and generic application" safety cases, "assumptions and restrictions of use".*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 4] The receiving actor responsible for the implementation, the verification and validation of the received or new safety measures registers in its own hazard record all the related hazards with the associated safety measures (both the imported and jointly identified ones).

[G 5] When a safety measure is not fully validated, a clear restriction of use (e.g. operational mitigation measures) needs to be elaborated and registered in the hazard record. Indeed, it is possible that technical/design safety measures are:

(a) not correctly implemented, or;
(b) not completely implemented, or;
(c) intentionally not implemented, for example because different safety measures are implemented instead of the ones registered in the hazard record (e.g. for cost purposes). As they are not validated, such safety measures need to be clearly identified in the hazard record. And evidence/justification needs to be provided why the safety measures implemented instead[16] are appropriate, as well as a demonstration that with the replacing safety measures the system complies with the safety requirements;
(d) etc.

In these cases the related technical/design safety measures cannot be verified and validated during the hazard management. The related hazard(s) and safety measures need then to remain open in the hazard record in order to avoid the misuse of the safety measures for other systems by the application of the "similar reference system" risk acceptance principle

[G 6] Usually the "not correctly" and/or "not completely" implemented safety measures are detected early in the system life-cycle and corrected before the system acceptance. However, if detected too late for a correct and complete technical safety measure implementation, the organisation responsible for the implementation and management needs to identify and register in the hazard record clear restrictions of use for the system under assessment. These restrictions of use are often operational application constraints for the system under assessment.

[G 7] It could also be useful to register in the hazard record whether the associated safety measures will be correctly implemented at a later stage of the system life-cycle or whether the system will continue to be used with the identified restrictions of use. It could be also useful to register in the hazard record the justification for not implementing correctly/completely the associated technical safety measures.

[G 8] The actor who receives the restrictions of use:

(a) imports all of them in its own hazard record;
(b) ensures that the conditions of use of the system under assessment are compliant with all the received restrictions of use;
(c) verifies and validates that the system under assessment complies with these restrictions of use

[G 9] Depending on the decisions agreed by the involved organisations:

(a) either the related technical safety measures are implemented correctly in the design at a later stage.
The organisation exporting the restrictions of use continues to track the correct technical implementation of the associated safety measures. Consequently, the related safety

(16) *If different safety measures are implemented instead of the initially specified ones, they need to be also registered in the hazard record.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

measures cannot be validated and the hazards associated to them not controlled in the hazard record of this organisation as long as the corresponding technical safety measures are not fully implemented. This needs to be ensured even if in the meantime the exported restrictions of use are put in place.

(b) or the related technical safety measures will not be implemented in the design at a later stage. The system will thus continue to be used during all its life-cycle with the associated restrictions of use. In this case, the following may be done:

(1) the organisation exporting the restrictions of use does not register the associated safety measures as "validated" in its hazard record. In this way, when using the related system as a reference system in other projects, the corresponding safety concerns will not be overlooked. So, even if another actor accepts to manage the associated risks differently, it is useful that the organisation exporting the restrictions of use clearly points out in its hazard record that the associated safety measures were not validated, or.

(2) the system description can be changed to include the restrictions of use in the scope of application of the system (i.e. assumptions for the system) and in the safety requirements. This will enable to control the hazards. Thus, if using the system as a reference system in another application:

(i) the new system will have to be used under the same conditions (i.e. to fulfil the restrictions of use associated to those assumptions), or;
(ii) additional risk assessment shall be done by the proposer for the deviations against those assumptions.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5. EVIDENCES FROM THE APPLICATION OF THE RISK MANAGEMENT PROCESS

5.1. The risk management process used to assess the safety levels and compliance with safety requirements shall be documented by the proposer in such a way that all the necessary evidence showing the correct application of the risk management process is accessible to an assessment body. The assessment body shall establish its conclusion in a safety assessment report.

[G 1] The infrastructure manager and railway undertaking safety management system (SMS) already addresses these requirements. For the other actors of the rail sector that are involved in the significant change, even if the SMS is not obligatory, in general at least at the project level they have a quality management process (QMP) and/or a safety management process (SMP). Both of these processes rely on a structured documentation hierarchy either within the company or at least within the project. They address also the RAMS management documentary needs. Such a structured documentation can be composed basically of the following (see also Figure 12):

(a) **Project plans** elaborated to describe the organisation to put in place for managing an activity within a project.
(b) **Project procedures** elaborated to describe in detail the way to achieve a dedicated task. Usually, procedures and instructions exist within the company and are used as such. New project procedures are only elaborated if there is a need to describe a specific task within the considered project.
(c) **Project development documents** elaborated along the system life-cycle represented in Figure 5.
(d) **Company or at least project templates** exist for the different types of documents to be produced.
(e) **Project records** elaborated along the project and necessary to demonstrate the compliance with the company quality management and safety management processes.

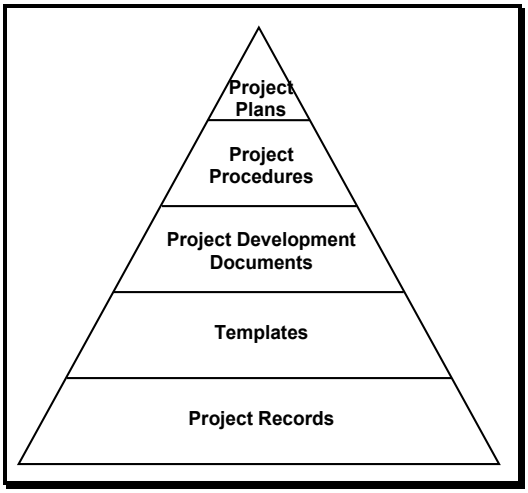

Figure 12 : Structured documentation hierarchy.

That is one way of achieving the needs of documented evidence. There may be other ways of doing this as long as it meets the criteria of the CSM.

[G 2] CENELEC standards advise to demonstrate the system compliance with the functional and safety requirements in a safety case document (or in a safety report). Even if it is not mandatory, the use of a safety case provides in a structured safety justification document:

(a) the evidence of quality management;
(b) the evidence of safety management;
(c) he evidence of functional and technical safety;

It has at the same time the advantage to support and guide the assessment body (-ies) in the independent assessment of the correct application of the CSM.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] The safety case describes and summarises how the project documents resulting from the application of the company or project quality and/or safety management processes interrelate within the system development process to demonstrate the system safety. Usually, the safety case does not include large volumes of detailed evidence and supporting documentation but provides precise references to such documents.

[G 4] **Safety case for technical systems:** CENELEC standards can be used as guidelines for writing and/or for the structure of safety cases:

(a) see EN 50 129 standard {Ref. 7} for "Railway Applications - "Communication, Signalling and Processing Systems & Safety related electronic Systems for Signalling"; Appendix H.2 of the EN 50 126-2 Guideline {Ref. 9} also proposes a structure for the safety case of signalling systems;
(b) see Appendix H.1 of the EN 50 126-2 Guideline {Ref. 9} for the structure of the safety case for rolling stock;
(c) see Appendix H.3 of the EN 50 126-2 Guideline {Ref. 9} for the structure of the safety case of infrastructures

As it appears in these references, the safety case structure for technical systems, as well as its content, depends on the system for which the demonstration of the safety compliance is to be provided.

The safety case outlined in Appendix H of the EN 50 126-2 Guideline {Ref. 9} provides only examples, and may not be suitable for all systems of the given kind. Therefore, the outline needs to be used with appropriate judgement of what fits to each specific application.

[G 5] **Safety case for organisational and operational aspects in railway systems:**

At present, there is not any dedicated standard providing the structure, the content and a guideline for writing the safety case for organisational and operational aspects of a railway system. However, as the safety case aims to demonstrate in a structured way the system compliance with its safety requirements, the same kind of safety case structure can be used as for technical systems. Indeed, the references in point [G 4] of section 5.1 provide advises and a checklist of items to address regardless the type of the system under assessment. The management of organisational and operational changes do require the same kind of quality management and safety management processes as the technical changes, with a demonstration of the system compliance with the specified safety requirements. Requirements from CENELEC standards not applicable to organisational and operational aspects are the ones purely related to technical system design facilities, as for example "inherent hardware fail-safety" principles, electromagnetic compatibility (EMC), etc.

5.2. The document produced by the proposer under point 5.1. shall at least include:

(a) description of the organisation and the experts appointed to carry out the risk assessment process,
(b) results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.

[G 1] Depending on the complexity of the system, these evidences can be gathered in one or several safety cases. Refer respectively to points [G 4] and [G 5] of section 5.1 for the structure of the safety case for technical systems and for operational and organisational aspects.

[G 2] Refer also to section A.4. in Appendix A for possible examples of evidences.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] The lifetimes of technical systems and subsystems in the railway sector are generally expected to be around 30 years. During such a long period of time it is plausible to also expect a number of significant changes to these systems. Further risk assessments could thus be conducted for these systems and their interfaces with the accompanying documentation that will need to be reviewed, supplemented and transferred between different actors and organisations using hazard records. This implies rather strict requirements on documentation control and configuration management.

[G 4] It is then helpful that the company which archives all the risk assessment and risk management information guarantees that the results/information are stored on a physical support that can be read/accessible during the complete system life(-cycle) (e.g. during 30 years).

[G 5] The main reasons for this requirement are among others:

(a) to ensure that all the safety analyses and safety records of the system under assessment are accessible during the complete system life. Thus:

(1) in case of further significant changes to the same system, the latest system documentation is available;
(2) in case of any problem during the system life, it is useful to be able to go back into the associated safety analyses and safety records;

(b) to ensure that the safety analyses and the safety records of the system under assessment are accessible in case it is used in another application as a similar reference system.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ANNEX II TO THE CSM REGULATION

Criteria which must be fulfilled by the Assessment Bodies

1. *The assessment body may not become involved either directly or as authorised representatives in the design, manufacture, construction, marketing, operation or maintenance of the system under assessment. This does not exclude the possibility of an exchange of technical information between that body and all the involved actors.*
2. *The assessment body must carry out the assessment with the greatest possible professional integrity and the greatest possible technical competence and must be free of any pressure and incentive, in particular of a financial type, which could affect their judgement or the results of their assessments, in particular from persons or groups of persons affected by the assessments.*
3. *The assessment body must possess the means required to perform adequately the technical and administrative tasks linked with the assessments; it shall also have access to the equipment needed for exceptional assessments.*
4. *The staff responsible for the assessments must possess:*
   - *proper technical and vocational training,*
   - *a satisfactory knowledge of the requirements relating to the assessments that they carry out and sufficient practice in those assessments,*
   - *the ability to draw up the safety assessment reports which constitute the formal conclusions of the assessments conducted.*
5. *The independence of the staff responsible for the independent assessments must be guaranteed. No official must be remunerated either on the basis of the number of assessments performed or of the results of those assessments.*
6. *Where the assessment body is external to the proposer's organisation must have its civil liability ensured unless that liability is covered by the State under national law or unless the assessments are carried out directly by that Member State.*
7. *Where the assessment body is external to the proposer's organisation its staff are bound by professional secrecy with regard to everything they learn in the performance of their duties (with the exception of the competent administrative authorities in the State where they perform those activities) in pursuance of this Regulation.*

[G 1] Additional explanation is not judged necessary.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APPENDIX A: ADDITIONAL CLARIFICATIONS

A.1. Introduction

A.1.1. The purpose of this appendix is to facilitate the reading of the present document. Instead of providing wide amount of information within the document, more complex subjects are explained further in the present appendix.

A.2. Hazard classification

A.2.1. A guideline is provided in section § 4.6.3. of the EN 50 126-1 standard {Ref. 8}, as well as in Appendix B.2 of the EN 50 126-2 Guideline {Ref. 9}, for the hazard classification/ ranking.

A.3. Risk acceptance criterion for technical systems (RAC-TS)

A.3.1. Upper Limit of Risk Acceptability for Technical Systems

A.3.1.1. The RAC-TS is described in section 2.5.4. of {Ref. 4}.

A.3.1.2. The purpose of the RAC-TS is to specify an upper limit of risk acceptability for technical systems for which the safety requirements can neither be derived by the application of codes of practice nor by comparison to similar reference systems. Consequently it defines a reference point, from which the risk analysis methods for the technical systems can be calibrated. As described in section A.3.6. of Appendix A of this document, this reference point or upper limit of risk acceptability could also be used to determine the risk acceptance criteria for other functional failures of technical systems that do not have a credible direct potential for a catastrophic consequence (i.e. for other severities). But the RAC-TS is not a method for risk analysis.

A.3.1.3. The RAC-TS is a semi-quantitative criterion. It applies both to the random hardware failures and the systematic failures/errors of the technical system. The systematic failures/errors of the technical system potentially resulting from human errors during the development process of the technical system (i.e. specification, design, implementation and validation) are thus also covered. But the human errors during the operation and maintenance of the technical systems are not covered by the RAC-TS.

A.3.1.4. According to appendices A.3 and A.4 of the CENELEC 50 129 standard, the systematic failures/errors are not quantifiable and thus the quantitative target needs to be demonstrated for random hardware failures only, while the systematic failures/errors are addressed by qualitative methods[17]. *"Because it is not possible to assess systematic failure integrity by quantitative methods, safety integrity levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realisation of a system to a stated integrity level."*

---

(17) *According to the CENELEC 50 126, 50 128 and 50 129 standards, the quantitative figure dealing with random hardware failures must be always linked to a safety integrity level to manage the systematic failures/errors. Therefore, the $10^{-9}\,h^{-1}$ figure of the RAC-TS also requires that an adequate process is put in place to correctly manage also the systematic failures/errors. But to facilitate the reading of the note, it often refers to only the random hardware failures of the technical system.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.1.5. Similarly, according to the CENELEC standards, the integrity of the software of technical systems is not quantifiable. The CENELEC 50 128 standard, provides guidance for the development process of safety related software in function of the requested safety integrity level. That includes the design, verification, validation and quality assurance processes for the software.
According to the CENELEC 50 128 standard; for a programmable electronic control system, implementing safety functions, the highest possible safety integrity level for the software development process is SIL 4, which corresponds to a quantitative tolerable hazard rate of $10^{-9}\ h^{-1}$.

A.3.1.6. Therefore, as the systematic failures/errors cannot be quantified, they need instead to be managed qualitatively by putting in place a quality and safety process that are compatible with the safety integrity level required for the system under assessment.

(a) the purpose of the quality process is *"to minimise the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system"*;
(b) the purpose of the safety process is *"to reduce further the incidence of safety related human errors throughout the life-cycle and thus minimise the residual risk of safety related systematic faults."*

A.3.1.7. Guidance for managing the incidence of systematic failures/errors, as well as guidance for possible design measures to protect against Common Cause/Mode Failures (CCF/CMF) and to ensure that the technical system enters a fail-safe state in case of such failures/errors, is provided in standards:

(a) the CENELEC 50 126-1 standard {Ref. 8} and its Guide 50 126-2 {Ref. 9} list the CENELEC 50 129 clauses and their applicability for documented evidence to systems other than signalling: see Table 9.1 in Guide 50 126-2 {Ref. 9}. This list provides reference to the guidance on how to address both the faults coming from the system itself and the effect of the environment on the system under assessment;

For example, techniques/measures for design features are given in *"Table E.5: Design features (referred to in 5.4)"* of the CENELEC 50 129 standard {Ref. 7}, *"for the avoidance and control of faults caused by:*

(1) *"any residual design faults";*
(2) *"environmental conditions";*
(3) *"misuse or operating mistakes";*
(4) *"any residual faults in the software";*
(5) *"human factors";*

Appendices D and E of the CENELEC 50 129 standard {Ref. 7} give techniques and measures for the avoidance of systematic faults and the control of random hardware and systematic failures/errors for safety related electronic systems in signalling. Many of them can be extended to systems other than signalling via a reference to these guidelines in Table 9.1 of Guide 50 126-2 {Ref. 9}.

(b) the CENELEC 50 128 standard provides guidance for the development process of safety related software in function of the safety integrity level (SIL 0 to SIL 4) that is requested for the software of the system under assessment.

A.3.1.8. The RAC-TS represents also the highest level of integrity that can be required according to both the CENELEC and IEC standards. For ease of reference the requirements from IEC 61508-1 and CENELEC 50 129 are quoted:

(a) IEC 61508-1: *"This standard sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed. These are specified as the lower*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

limits for safety integrity level 4. It may be possible to achieve designs of safety-related systems with lower values for the target failure measures for noncomplex systems, but it is considered that the figures in the table represent the limit of what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time."

(b) EN 50129: *"A function having quantitative requirements more demanding than 10^{-9} h^{-1} shall be treated in one of the following ways:*

(1) *if it is possible to divide the function into functionally independent sub-functions, the THR can be split between those sub-functions and a SIL assigned to each sub-function;*

(2) *if the function cannot be divided, the measures and methods required for SIL 4 shall, at least, be fulfilled and the function shall be used in combination with other technical or operational measures in order to achieve the necessary THR."*

A.3.1.9. All technical systems need then to limit the quantitative safety requirement to that figure. If there is a need for a higher level of protection, it cannot be achieved with only one system. The architecture of the system needs to be changed, for example using two independent systems in parallel that cross-check between them for generating safe outputs. But this definitely increases the costs of the technical system development.

Remark: if there are existing functions, e.g. purely mechanical systems that, based on operational experience, may have achieved a higher level of integrity, then the safety level may be described by a particular code of practice or the safety requirements may be set by similarity analysis with the existing system. In the scope of the CSM, the RAC-TS needs only to be applied, if no code of practice and no reference system exist.

A.3.1.10. The following can then be summarised:

(a) according to the CENELEC 50 126, 50 128 and 50 129 standards, the systematic failures/errors in the development are not quantifiable;

(b) the incidence of systematic failures/errors, as well as their residual risk, needs to be controlled and managed by the application of appropriate quality and safety process that are compatible with the safety integrity level requested for the system under assessment;

(c) the highest achievable safety integrity level is SIL 4 both for the random hardware failures and the systematic failures/errors of technical systems;

(d) this SIL 4 safety integrity level limit implies that the maximum tolerable hazard rate (THR) (i.e. the maximum failure rate) for technical systems needs to be limited also to 10^{-9} h^{-1}.

A.3.1.11. A tolerable hazard rate of 10^{-9} h^{-1} can be achieved by the technical system with either a "failsafe architecture" (which by definition meets such a safety performance) or a "redundant architecture" (e.g. two independent processing channels cross-checking each other).

For a redundant architecture, it can be shown that the overall wrong side failure (Λ_{WSF}) of the technical system is proportional to $\lambda^{2}*T$ where:

(a) λ^2 represents the square of the wrong side failure rate of one channel;

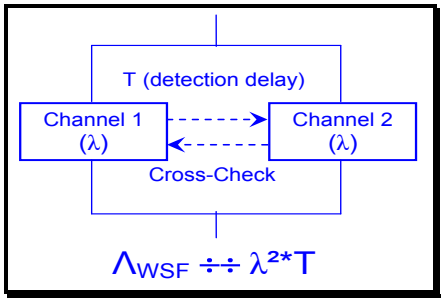

Figure 13 : Redundant Architecture for a Technical System.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) T represents the time necessary for one channel to detect the wrong side failure(s) of the other channel. This is usually a multiple of the processing time/cycle of a channel. Usually T is much less than 1 second.

A.3.1.12. Based on this formula (λ^2*T), theoretically it can be demonstrated (considering only the random hardware failures of the technical system – see also point A.3.1.13. in Appendix A) that a 10^{-9} h^{-1} quantitative requirement for the RAC-TS can be achieved. The systematic failures/errors must be managed by a process: refer to point A.3.1.6. in Appendix A. For example:

(a) with an MTBF of 10 000 hours for the reliability figure a channel, and the conservative assumption that any channel failure is unsafe, the wrong side failure of the channel is 10^{-4} h^{-1};
(b) even with a time of 10 minutes (i.e. $\approx 2*10^{-3}$ hours) to detect the wrong side failure(s) of the other channel, which is also a conservative assumption;

The overall wrong side failure $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}

A.3.1.13. In practice, for such a redundant architecture the evaluation of the quantitative overall wrong side hardware failures needs to consider the measures that are taken in the design to protect against the Common Cause/Mode Failures (CCF/CMF) and to ensure that the technical system enters a fail-safe state in case of a CCF/CMF failure/error. This evaluation of overall wrong side failure (Λ_{WSF}) needs thus also to consider:

(a) the components common to all channels, e.g. single or common inputs to all channels, common power supply, comparators, voters, etc.;
(b) the time required to detect the dormant or latent failures. For complex technical systems, this time can be higher by several orders of magnitude than 1 second;
(c) the impact of the Common Cause/Mode Failures (CCF/CMF).

Guidance on these topics can be found in standards that are recalled in point A.3.1.7. of Appendix A of this document.

A.3.2. Flow chart for the applicability test of the RAC-TS

A.3.2.1. The way to apply the RAC-TS to hazards that arise from failures of technical systems can be represented as shown in Figure 14.

A.3.2.2. The application of that flow chart on an example is provided in section C.15. of Appendix C.

A.3.3. Definition of a Technical System from the CSM

A.3.3.1. The RAC-TS applies to technical systems only. The following definition is provided for "technical system" in Article 3(22) of the CSM Regulation:

'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. Although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system. The maintenance process is described in the maintenance manuals but is not itself part of the technical system.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

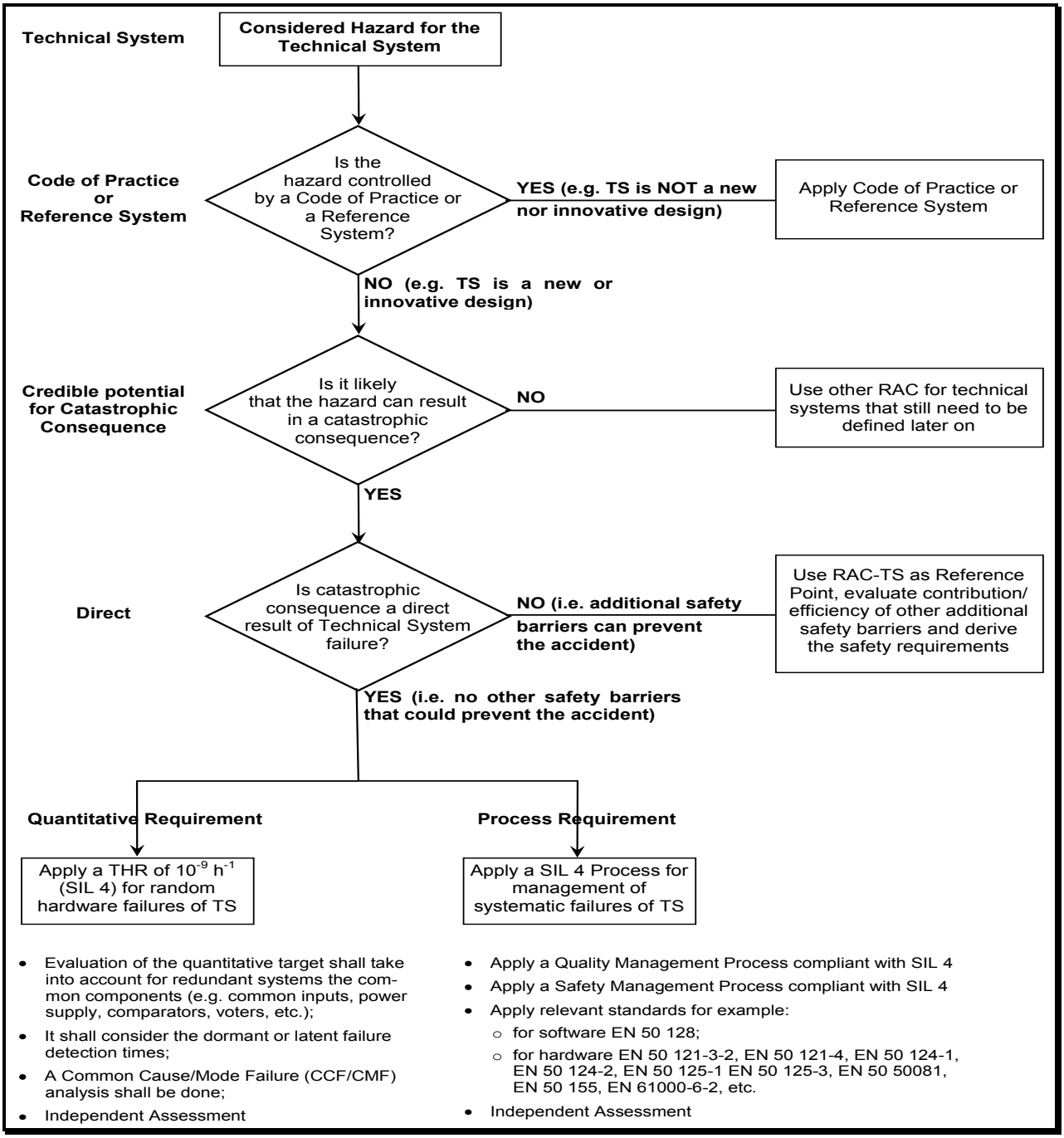

Figure 14 : Flow Chart for the Applicability Test of the RAC-TS.

A.3.4. Explanation of the "Technical System" Definition

A.3.4.1. This definition of a technical system describes the scope of the technical system: *"technical system means a product or an assembly of products including the design, implementation, and support documentation."* Accordingly, it consists of and includes:

(a) the physical parts constituting the technical system;
(b) the associated software (if any);

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) the design and the implementation of the technical system, including if applicable the configuration or parameterisation of a generic product to specific requirements of the specific application;
(d) the supporting documentation necessary for:

(1) the development of the technical system;
(2) the operation and maintenance of the technical system;

A.3.4.2. The notes associated to this definition specify further the scope of the technical system:

(a) *"The development of a technical system starts with its requirements specification and ends with its safety approval".* It includes the phases 1 to 10 of the V-Cycle represented in Figure 10 of the CENELEC 50 126-1 Standard {Ref. 8};

(b) *"It shall consider the design of relevant interfaces with human behaviour. Human operators and their actions are however not included in a technical system."* Although the human factor errors during the operation and the maintenance of the technical system are not part of the technical system itself, the design of the interfaces with the human operators needs to take them into account. The purpose is to minimise the probability of human errors due to a poor design of the relevant interfaces with the human operators;

(c) *"Maintenance is not included in the definition, but is included in maintenance manuals."* This means that the RAC-TS needs not be applied to the operation and maintenance of the technical system; these rely strongly on processes and actions performed by human personnel.
However, in order to support the maintenance of technical systems, the technical system definition must include any relevant requirements (e.g. periodic preventive maintenance, or corrective maintenance in case of failures), with a sufficient level of details. But how the maintenance needs to be organised and achieved on the related technical system is not part of the technical system definition but in the corresponding maintenance manuals.

A.3.4.3. See also section A.3.1. in Appendix A.

A.3.5. Functions of Technical Systems to which RAC-TS applies

A.3.5.1. According to the definition of the RAC-TS, it applies to wrong side failures of the functions to be fulfilled by the technical system if they have *"a credible **direct** potential for a catastrophic consequence"*: see section 2.5.4. in {Ref. 4}.

A.3.5.2. The RAC-TS can also be applied to functions that involve technical systems but whose failures **do not have a *"direct*** *potential for a catastrophic consequence"*. In this case, the RAC-TS needs to be applied as an overall target for the set of events that leads to the catastrophic consequence. Based on this overall target, the actual contribution of each event, and thus of the functional failures of the technical system that is involved in the considered scenario, need to be derived according to section A.3.6. in Appendix A.
Such a use of the RAC-TS needs still to be discussed and agreed on with the CSM working group.

A.3.5.3. To what functions of the technical system does the RAC-TS apply? According to the IEC 61226:2005 standard:

(a) a function is defined in this context as a *"specific purpose or objective to be accomplished that can be specified or described without reference to the physical means of achieving it"*;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) a function (considered as a black-box) transfers input parameters (e.g. material, energy, information) into aim related output parameters (e.g. material, energy, information);
(c) the analysis of the function is independent of its technical realisation.

A.3.5.4. The RAC-TS is applicable to the following types of functions:

(a) examples for the ETCS on-board sub-system :

(1) "provide the Driver with information to allow him to drive the train safely and enforce a brake application in case of over-speed". Based on information received from the trackside (permitted speed) and on the train speed computation by the on-board ETCS, the Driver and the on-board ETCS are able to supervise that train does not exceed the permitted speed limit. The RAC-TS applies to the evaluation of the train speed by the on-board since:

(i) there is no additional barrier (direct) as the information provided to the Driver is also under evaluated;
(ii) the train over speed could lead to derailment which is an accident with potential for catastrophic consequences;

(2) "provide the Driver with information to allow him to drive the train safely and enforce a brake application in case of violation of the permitted movement authority";

(b) example for a track circuit: "detect the occupation of the track section". The RAC-TS will be applicable as such to this function only if there is no "sequence monitoring" function implemented in the Interlocking;
(c) example for a point: "control the point position";

A.3.5.5. Some standards also define functions to which the RAC-TS could be applicable. For example:

(a) the prEN 0015380-4 standard {Ref. 13} (ModTrain Work) defines in its normative part three hierarchical function levels (extended in informative annexes up to five levels). In total prEN 0015380-4 defines several hundred functions related to trains;
(b) in general it is recommended to select the functions from the first three levels of prEN 0015380-4 (but not below), taking also into account the product breakdown structure;
(c) for functions, which are not in the scope of prEN 0015380-4, the appropriate functional level needs to be decided by comparison using an expert judgment.

These examples of functions from prEN 0015380-4 need still to be worked on by the Agency in the scope of the work on broadly acceptable risks and risk acceptance criteria.

A.3.5.6. The RAC-TS is applicable also for example to the following function of prEN 0015380-4: *"control tilting"* (code = CLB). The function could be used at the system level in the following two ways:

(a) first case: the train is to tilt in curves for passenger comfort and must monitor the train gauge compliance with the trackside infrastructure;
(b) second case: the train is to tilt in curves only for passenger comfort but needs not to monitor the train gauge compliance with the trackside infrastructure;

In the first case the RAC-TS will be applied but not in the second case as the failure of the tilting function does not have catastrophic consequence.

A.3.5.7. The example (b) in point A.3.5.4. and the examples in point A.3.5.6. in Appendix A show clearly that it will not be feasible to build a predefined list of functions on which the RAC-TS applies in all cases. This will always depend on how the system will use these sub-system functions.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.5.8. An example of application of the RAC-TS is provided in section C.15. of Appendix C.

A.3.6. Application examples for RAC-TS

A.3.6.1. Introduction

(a) this chapter shows examples how to determine the failure rate for the other hazard severities and how lower safety requirements than $10^{-9}\,h^{-1}$ can be derived. This document does not prefer nor mandates any particular method. It only shows for information how the RAC-TS can be used to calibrate some widely used methods. It needs to be developed further in the Agency work on broadly acceptable risks and risk acceptance criteria.

(b) indeed, the RAC-TS may be applied directly only to a small number of cases as in practice, not many functional failures of technical systems lead directly to accidents with potentially catastrophic consequences. Therefore, in order to apply the criterion to hazards with non-catastrophic consequences and to determine the target failure rate, it is possible to perform trade-offs (e.g. by calibrating a risk matrix by this criterion) between different parameters, e.g. severity vs. frequency.

A.3.6.2. Example 1: Direct Risk Trade-off

(a) the RAC-TS can be applied easily to scenarios which differ only by a few independent parameters from the reference conditions defined in the RAC-TS in section 2.5.4. of the CSM Regulation {Ref. 3};

(b) assume that for a particular parameter p the relationship with risk is multiplicative. Assume that in the reference condition p* is present while in the alternative scenario p‘ is applicable. In this case only the parameter ratio p*/p’ is relevant and the rate of occurrence may be reduced. This procedure may be iterated if the parameters are independent.

(c) Example:

(1) assume that the actual potential of the catastrophic consequence has been assessed by expert judgment to be ten times less than the potential under reference conditions in section 2.5.4 of the CSM Regulation {Ref. 3}. Then the requirement would be $10^{-8}\,h^{-1}$ instead of $10^{-9}\,h^{-1}$.

(2) assume an additional safety barrier by another technical system (independent of the consequences), which is effective in 50% of cases, is identified;

(3) then the safety requirement would be $5*10^{-7}\,h^{-1}$ (i.e. $0.5*10^{-8}\,h^{-1}$) instead of $10^{-9}\,h^{-1}$.

A.3.6.3. Example 2: Risk Matrix Calibration

(a) in order to use properly the RAC-TS in a risk matrix, the matrix has to relate to the correct system level (comparable to that provided in section A.3.5. in Appendix A).

(b) the RAC-TS defines one field in the risk matrix as tolerable which corresponds to the coordinate (catastrophic severity; $10^{-9}\,h^{-1}$ frequency of occurrence): see red field in Table 5. All fields that relate to a higher frequency have to be labelled "intolerable". It is to note that only in case of credible direct potential for a catastrophic consequence the frequency of accidents is the same as the functional failure frequency.

(c) then the rest of the matrix can be filled out, but effects like risk aversion or scaling of the categories have to be taken into account. In the simplest case of linear decadal scaling (as shown in the Table 5 by the arrow) the field that way labelled "acceptable" by the RAC-TS is extrapolated in a linear way to the rest of the matrix. This means that all fields in the same diagonal (or below the diagonal) are also labelled "acceptable". The fields below can also be labelled "acceptable".

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 5 : Typical Example of a calibrated Risk Matrix.

Frequency of occurrence of an accident (caused by a hazard)	Risk Levels			
Frequent (10^{-4} per hour)	Intolerable	Intolerable	Intolerable	Intolerable
Probable (10^{-5} per hour)	Intolerable	Intolerable	Intolerable	Intolerable
Occasional (10^{-6} per hour)	Acceptable	Intolerable	Intolerable	Intolerable
Remote (10^{-7} per hour)	Acceptable	Acceptable	Intolerable	Intolerable
Improbable (10^{-8} per hour)	Acceptable	Acceptable	Acceptable	Intolerable
Incredible (10^{-9} per hour)	Acceptable	Acceptable	Acceptable	Acceptable
	Insignificant	Marginal	Critical	Catastrophic
	Severity Levels of Hazard Consequence (i.e. of accident)			

Risk Evaluation	Risk Reduction/Control
Intolerable	The risk shall be eliminated.
Acceptable	The risk is acceptable. Independent Assessment is required.

(d) once the matrix is filled out, it can be applied also to non-catastrophic hazards. If for example another functional failure has the severity classified "critical" then by the calibrated risk matrix the tolerable frequency of accidents should be no more than "improbable" (or even less).

(e) it is to remark that the use of the risk matrix may lead to overly conservative results, when applying to functional failure frequencies (i.e. for functional failures which do not lead directly to accidents).

A.3.6.4. Principle for calibrating other Risk Analysis Methods

Other risk analysis methods, for example the proposed risk priority number scheme or the risk graph from VDV 331 or IEC 61508 can be also calibrated by a similar procedure as outlined for the risk matrix:

(a) first step: classify the reference point from the RAC-TS as tolerable and points with higher frequency or higher severity as an intolerable RAC-TS.
(b) second step: use the trade-off mechanisms of the particular method to extrapolate the risk tolerability to non-catastrophic hazards (using linear risk trade-off as a starting point).
(c) third step: for the non-catastrophic hazards, the RAC-TS can then be derived from the calibrated risk analysis method by comparing the (frequency; severity) coordinate to the so obtained FN-curve.

A.3.7. Conclusions for RAC-TS

A.3.7.1. In the general risk assessment framework proposed by the CSM, risk acceptance criteria are necessary to determine when the residual level of risk(s) becomes acceptable and thus when to stop the explicit risk estimation.

A.3.7.2. The RAC-TS is a design target (10^{-9} h^{-1}) for technical systems.

A.3.7.3. The main purposes of the RAC-TS are:

(a) to specify an upper limit of risk acceptability, and consequently a reference point, from which the risk analysis methods for the technical systems can be calibrated

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) to enable the mutual recognition of technical systems since the associated risk and safety assessments will be evaluated against the same risk acceptance criterion in all the MS;
(c) to save cost as it does not require unnecessarily high quantitative safety requirements;
(d) to facilitate the competition between the manufacturers. The use of different risk acceptance criteria in function of either the proposer or Member State would lead the industry to perform a lot of different demonstrations on the same technical systems. That would consequently jeopardize the competitiveness of manufacturers and render products unnecessarily expensive.

A.3.7.4. The semi-quantitative requirement contained in the RAC-TS is not always to be demonstrated for technical systems. Indeed, in the scope of the CSM, the RAC-TS needs only to be applied to technical systems for which the identified hazards can neither be adequately controlled by the use of codes of practice nor by comparison with reference systems. This allows to setting out lower safety requirements provided the global safety level can be maintained.

A.3.7.5. Only when no code of practice exists and also no reference system, a harmonised semi-quantitative risk acceptance criterion for technical systems is necessary.

A.3.7.6. As the safety integrity level for systematic failures/errors is limited to SIL 4, the safety integrity level for the random hardware failures of technical systems needs also to be limited to SIL 4. This corresponds to a maximum tolerable hazard rate (THR) of $10^{-9}\,h^{-1}$ (i.e. the maximum failure rate). According to CENELEC 50 129 standard, if more demanding safety requirements are required, it cannot be achieved with only one system; the architecture of the system needs to be changed, for example using two systems which unavoidably increases the costs of the technical system drastically. For more details, refer to section A.3.1. in Appendix A.

A.3.7.7. Finally, section A.3.6. in Appendix A outlines how the RAC-TS can be used as a reference point for calibrating particular risk analysis methods when technical systems have a potential for less severe consequences than catastrophic.

A.4. Evidence from safety assessment

A.4.1. This section provides a guidance of evidences which are usually provided to an assessment body in order to allow the independent assessment and to get the safety acceptance without prejudice to the national requirements in a Member State. This can be used as a check list to verify that all associated aspects are covered and documented, when relevant, during the application of the CSM.

A.4.2. Safety plan: CENELEC advises that a safety plan is produced at the beginning of the project, or if this is not convenient for the project that the associated description is included in any other relevant document. If assessment bodies are appointed at the beginning of the project, the safety plan can also be submitted for their opinion. In principle, the safety plan describes:

(a) the organisation put in place and the competence of people involved in the development and in the risk assessment;
(b) all the safety related activities that are planned along the various phases of the project, as well as the expected outputs;

A.4.3. Evidences required from system definition phase:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) description of system:

(1) definition of system scope/boundaries;
(2) description of functions;
(3) description of system structure;
(4) description of operating and environmental conditions;

(b) description of external interfaces;
(c) description of internal interfaces;
(d) description of life cycle phases;
(e) description of safety principles;
(f) description of the assumptions defining the limits for the risk assessment;

A.4.4. In order to enable the risk assessment to be done, the context of the intended change is taken into account in the system definition:

(a) if the intended change is a modification of an existing system, the system definition describes both the system before the change and also the intended change:
(b) if the intended change is the construction of a new system, the description is limited to the definition of the system as there is no description of any existing system.

A.4.5. Evidences required from hazard identification phase:

(a) description and justification (including limitations) of methods and tools for hazard identification (top down method, bottom up, HAZOP, etc.);
(b) results:

(1) lists of hazards:
(2) system (boundary) hazards;
(3) sub-system hazards;
(4) interface hazards;
(5) the safety measures that could be identified during this phase;

A.4.6. The following evidences is also needed from risk analysis phase:

(a) when codes of practice are used for controlling hazards, demonstration that all relevant requirements from the codes of practice are fulfilled for the system under assessment. This includes the demonstration of the correct application of the relevant codes of practice;

(b) when similar reference systems are used for controlling hazards:

(1) definition for the system under assessment of the safety requirements from the relevant reference systems;
(2) demonstration that the system under assessment is used under similar operational and environmental conditions as the relevant reference system. If this cannot be done demonstration that the deviations from the reference system are correctly assessed;
(3) evidence that the safety requirements from reference systems are correctly implemented in the system under assessment;

(c) when explicit risk estimation is used for controlling hazards:

(1) description and justification (including limitations) of method and tools for risk analysis (qualitative, quantitative, semi-quantitative, non-regression analysis, ...);
(2) identification of existing safety measures and risk reduction factors for each hazard (including human factor aspects);
(3) evaluation and ranking of risk for each hazard:

(i) estimation of consequences of hazard and justification (with assumption and conditions);

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(ii) estimation of frequency of hazard and justification (with assumption and conditions);
(iii) ranking of hazards according to their criticality and frequency of occurrence;

(4) identification of additional appropriate safety measures leading to acceptable risks for each hazard (iterative process after the risk evaluation phase);

A.4.7. Evidences required from the risk evaluation:

(a) when explicit risk estimation is performed:

(1) definition and justification of risk evaluation criteria for each hazard;
(2) demonstration/justification that the safety measures and safety requirements cover each hazard to an acceptable level (according to above risk evaluation criterion);

(b) in virtue of sections 2.3.5 and 2.4.3 in the CSM Regulation, risks covered by application of codes of practice and by comparison with reference systems are considered implicitly as acceptable provided respectively that (see dotted circle in Figure 1):

(1) the conditions of application of codes of practice in section 2.3.2 are met;
(2) the conditions for use of a reference system in section 2.4.2 are met;

The risk acceptance criteria are implicit for these two risk acceptance principles.

A.4.8. Evidences from hazard management:

(a) registration of all hazards in a hazard record, containing the following elements:

(1) identified hazard;
(2) safety measures preventing occurrence of hazard or mitigating its consequences;
(3) safety requirements on the measures;
(4) relevant part of the system;
(5) actor responsible for safety measures;
(6) status of hazard (e.g. open, solved, deleted, transferred, controlled, etc.);
(7) date of registration, review and control of each hazard;

(b) description on how hazards will be managed effectively during the whole life-cycle;
(c) description of the information exchange between parties for hazards at the interfaces and allocation of responsibilities.

A.4.9. Evidences relating to the quality of the risk evaluation and assessment process:

(a) description of persons involved in the process and their competence;
(b) for explicit risk estimations, description of information, data and other statistics used in the process, and justification for their adequacy (e.g. sensitivity study on the used data).

A.4.10. Evidences of compliance with safety requirements:

(a) list of standards used;
(b) description of design and of operational principles;
(c) evidences of application of a good quality and safety management system for the project: refer to point [G 3] in section 1.1.2;
(d) summary of safety analysis reports (e.g. hazard cause analysis) demonstrating the fulfilment of safety requirements;
(e) description and justification of methods and tools (FMECA, FTA, …) that are used for the hazard cause analysis;
(f) summary of safety verification and validation tests.

A.4.11. Safety case: CENELEC advises that all previously mentioned evidences are regrouped and summarised in one document that is submitted to the assessment body: refer to points [G 4] and [G 5] in section 5.1.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APPENDIX B: EXAMPLES OF TECHNIQUES AND TOOLS SUPPORTING THE RISK ASSESSMENT PROCESS

B.1. Examples of techniques and tools for carrying out the risk assessment activities covered by the CSM can be found in Annex E of the EN 50126-2 guide {Ref. 9}. A summary of techniques and tools is given in Table E.1. Each technique is described, and when necessary, a reference to other standards is provided for more information.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APPENDIX C: EXAMPLES

C.1. Introduction

C.1.1. The purpose of this appendix is to facilitate the reading of the present document. It gathers all the collected examples which aim to facilitate the application of the CSM.

C.1.2. The examples of risk or safety assessments that are given in this appendix do not result from the application of the CSM process as they were carried out before the existence of CSM Regulation. The examples can be classified into:

(a) examples, with reference to their origin, received from experts in the CSM working group
(b) examples, intentionally without reference to their origin, also received from experts in the CSM working group. The related experts requested the origin to remain confidential;
(c) examples, whose origin is not mentioned, and which were produced by members from the Agency staff based on their earlier personal professional experience.

For each example, a traceability is given between the applied process and the one required by the CSM, as well as the argumentation and added value to perform the additional steps (if any) requested by the CSM.

C.2. Examples of application of significant change criteria in Article 4 (2)

C.2.1. The Agency is working on the definition of what can be considered as a "significant change". One example from that work is provided in this section how to apply the criteria in Article 4 (2).

C.2.2. The change consists to modify at a manually operated level crossing the way signalmen communicate the information about the direction of a coming train to the level crossing operator. The change is represented in Figure 15.

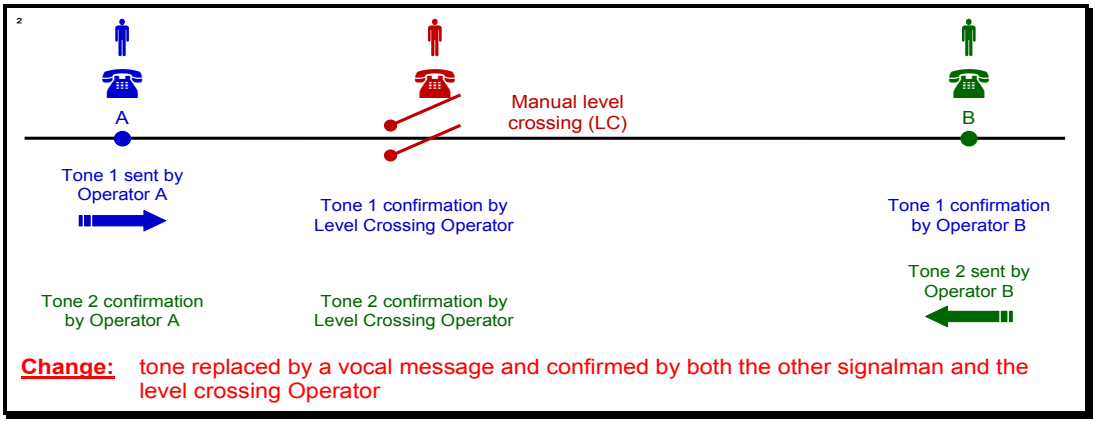

Figure 15 : Example of a not significant change Telephone message for controlling a level crossing.

C.2.3. Existing system: before making the intended change, the information about the direction of a coming train was automatically indicated to the level crossing operator by the ringing tone of the telephone. The tone was different depending on where the call was coming from.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.2.4. Intended change: as the old telephone system becomes obsolete and must be replaced by a new digital one, technically the relevant information cannot be included any more in the tone. The tone is exactly the same regardless which signalman it is coming from. It is thus decided to achieve the same function by an operational procedure:

(a) on train departure, the signalman informs verbally the level crossing operator on the direction of the coming train;
(b) the information is checked against the timetable and acknowledged by both the level crossing operator and the other signalman in order to avoid misunderstanding from the operator.

The intended change and associated operational procedure are illustrated in Figure 15.

C.2.5. Although the change appears to have a potential safety impact (risk of not closing the level crossing barrier in time), other criteria in Article 4 (2) like:

(a) low complexity;
(b) lack of innovation, and;
(c) easy monitoring;

may suggest that the intended change is not a significant one.

C.2.6. In this example, some safety analysis or argument is anyway necessary to show that, for this safety critical task, replacing an old technical system by an operational procedure (with personnel cross-checking each other) would lead to a similar level of safety. The question is whether this would require the application of the full CSM process, with hazard record, independent assessment by an assessment body, etc. In this case, it is questionable whether this would bring any added value, implying that such a change could then not be qualified as significant.

C.3. Examples of interfaces between rail sector actors

C.3.1. Here are some examples of interfaces and reasons for cooperation between actors of the rail sector:

(a) IM – IM: for example both infrastructures shall foresee safety measures for ensuring a safe transition of trains from one infrastructure to the other one;

(b) IM – RU: for example there could be specific operational rules dependent on the infrastructure that must be observed by the train driver;

(c) IM – Manufacturer: for example manufacturer's sub-systems could have restrictions of use that must be fulfilled by the IM;

(d) IM – Service Provider: for example there could be specific maintenance constraints for the infrastructure that must be fulfilled by the subcontractor of the maintenance activities;

(e) RU – Manufacturer: for example manufacturer's sub-systems could have restrictions of use that must be fulfilled by the RU;

(f) RU – Service Provider: for example there could be specific maintenance constraints for the infrastructure that must be fulfilled by the subcontractor of the maintenance activities;

(g) RU – Keepers: for example there could be vehicle specific restrictions of use that must be fulfilled by the railway undertaking operating those vehicles;

(h) Manufacturer – Manufacturer: for example the management of safety related technical interfaces between sub-systems from two different manufacturers;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(i) Manufacturer – Service Provider: for example the management by the manufacturer of the hazard record when sub-;contracting some work to a company whose size is too small for having a safety organisation on the considered project;

(j) Service Provider – Service Provider: similar example as in point (j) here above;

C.3.2. Service providers are covering all activities sub-contracted by either the IM or RU or manufacturer like maintenance, ticketing, engineering services, etc.

C.3.3. In order to illustrate the interface management and the associated hazard identification, the following example is given. It considers an interface between a train manufacturer and an proposer (RU). It describes then how the main criteria requested in point [G 3] of section 1.2.1 could be fulfilled:

(a) Leadership: the proposer (RU);

(b) Inputs:

(1) list(s) of relevant hazards coming from similar projects;
(2) description of all inputs and outputs (I/O) for the interface, including the performance characteristics;

(c) Methods: refer to Appendix A.2 of the EN 50 126-2 Guideline {Ref. 9};

(d) Required Participants:

(1) proposer (RU) safety assurance manager;
(1) train manufacturer safety assurance manager;
(2) train proposer design authority;
(3) train manufacturer design authority;
(4) train proposer maintenance staff (partially depending of the analysed I/O);
(5) train drivers (partially depending of the analysed I/O);

(e) Outputs:

(1) common agreed hazard identification report;
(2) safety measures for the hazard record with a clear description of the responsibility.

C.4. Examples of methods for determining broadly acceptable risks

C.4.1. Introduction

C.4.1.1. Broadly acceptable risks are defined in the CSM regulation as risks that are *"so small that it is not reasonable to implement any additional safety measure (to reduce the risk further)"*. In the hazard identification, classifying some hazards as associated with broadly acceptable risks allows not to analyse those hazards further in the risk assessment process. The definition of broadly acceptable risks quoted above does leave some room for interpretation. This is why it is indicated in the regulation that the decision for classifying hazards with broadly acceptable risks is left to expert judgment.

C.4.1.2. It is indeed difficult to define commonly a more explicit criterion for broadly acceptable risks that would apply to all the different possible system levels where such hazards might be identified, and which also account for the different risk aversion factors that may prevail for different applications. However, since it is important to ensure that the judgments of experts are easily understood and traceable, some guidance on how to define risks as broadly acceptable is useful. Criteria for defining broadly acceptable risks can be quantitative, qualitative or semi-qualitative. Below are some examples on how to derive criteria which allows the evaluation of broadly acceptable risks in a quantitative or semi quantitative manner.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.4.1.3. The examples below illustrate that principle. They are taken from the paper: *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Derivation of quantitative criterion

C.4.2.1. One could define broadly acceptable risks as risks that are much smaller than the acceptable risk for a given class of hazards. Using statistical data it might be possible to calculate what is the current level of risk for railway systems, and thus to declare that calculated level as acceptable. Dividing that level of risk by the number (N) of hazards (for example arbitrarily one can assume that there are about N = 100 main categories of hazards in the railway system), gives an acceptable level of risk per category of hazard. One could then state that a hazard with a risk which is two orders of magnitude lower than the acceptable level of risk per hazard (this is the parameter x % in point [G 1] of section 2.2.3) would be considered as a broadly acceptable risk.

C.4.2.2. It shall be checked however that the contribution of all hazards associated with broadly acceptable risk(s) does exceed a given proportion (e.g. y%) of the overall risk at the system level: refer to section 2.2.3 and the explanation in point [G 2] of section 2.2.3.

C.4.3. Evaluation of broadly acceptable risks

C.4.3.1. The limit values for broadly acceptable risks, as derived in the examples above, can then be used to calibrate qualitative tools, like a risk matrix, a risk graph, or risk priority numbers, in order to help the expert to make its decision to classify risk as broadly acceptable. It is important to stress that having quantitative values as criteria for broadly acceptable risks, does not imply that it is necessary to make a precise risk estimation or analysis in order to decide about the broad acceptability of the risk. Here this is where the judgment of the expert applies for making this rough estimation in the hazard identification phase

C.4.3.2. It is also important to checked that the contribution of all hazards associated with broadly acceptable risk(s) does exceed a given proportion (e.g. y%) of the overall risk at the system level: refer to section 2.2.3 and the explanation in point [G 2] of section 2.2.3.

C.5. Risk assessment example of an organisational significant change

C.5.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.5.2. The example is related to an organisational change. It was considered significant by the related proposer. A risk assessment based approach was applied to evaluate the change.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.5.3. A branch of the infrastructure manager organisation, that was performing until the change some maintenance activities (other than signalling and telematic), had to be put in competition with other companies working in the same field. The direct impact was a need for downsizing and redistribution of staff and tasks within the detached branch of the IM organisation put in competition.

C.5.4. Concerns for the impacted infrastructure manager:

(a) the IM staff affected by the change was in charge of emergency maintenance and repairs required by sudden errors on the infrastructure. Staff was also performing some planned or project based maintenance activities such as track packing, ballast cleaning, vegetation control;
(b) these tasks were considered critical for the safety and punctuality of the operation. They had thus to be analysed in order to find the right measures which ensure that the situation does not deteriorate as many of the people in charge of safety matters are leaving the IM organisation.
(c) the same level of safety and train punctuality need to be maintained during and after the change of the organisation.

C.5.5. In comparison to the CSM process, the following steps were applied (see also Figure 1):

(a) system description [section 2.1.2]:

(1) description of the tasks performed by the existing organisation (i.e. by the IM organisation before the change);
(2) description of the changes planned in the IM organisation.
(3) the interfaces of the "branch to be detached" with other surrounding organisations or with the physical environment could only be briefly described. The boundaries could not be 100 % clearly presented;

(b) hazard identification [section 2.2]:

(1) brainstorming by group of experts:

(i) to find all hazards, with a relevant influence on risk brought on by the intended organisational change;
(ii) to identify possible actions to control the risk;

(2) hazard classification:

(i) in function of the severity of the associated risk: high, medium, low risk;
(ii) in function of the impact of the change: increased, unchanged, decreased risk;

(c) use of a reference system [section 2.4]:

The system before the change was judged to have an acceptable level of safety. It was thus used as "reference system" to derive the risk acceptance criteria (RAC) for the change of organisation;

(d) explicit risk estimation and evaluation [section 2.5]:

For each hazard with increased risk due to the change of organisation, risk reduction measures are identified. The residual risk is compared against RAC from the reference system to check whether additional measures need to be identified;

(e) demonstration of the system compliance with safety requirements [section 3]:

(1) the risk analysis and hazard record shown that hazards cannot be controlled until they are verified and until it is demonstrated that the safety requirements (i.e. selected safety measures) are implemented;
(2) the risk analysis and hazard record were living documents. The efficiency of the decided actions was monitored at regular intervals in order to check if the

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

conditions were changed and if the risk analysis and risk evaluation need to be updated;
(3) if the implemented measures were not enough efficient, the risk analysis, risk evaluation and hazard record were updated and monitored again;

(f) hazard management [section 4.1]:

The identified hazards and safety measures were registered and managed in a hazard record. One of the conclusions of the example was to continuously update the risk analysis and the hazard record as decisions and actions were taken during the change of the organisation. The risk at interfaces with for example sub-contractors and entrepreneurs were also covered by the risk analysis.

The structure and fields used for the hazard record, as well as an extract of some lines, are given in section C.16.2. of Appendix C.

(g) independent assessment [Article 6]:

An independent assessment by a third party was also carried out in order:

(1) to check that the risk management and risk assessment were correctly done;
(2) to check that the organisational change is suitable and will enable to maintain the same level of safety as before the change.

C.5.6. The example shows that the principles required by the common safety method are existing methods in the railway sector already applied for assessing the risks for organisational changes. The risk assessment in the example fulfils all the requirements from the CSM. It uses two out of three risk acceptance principles allowed by the harmonised approach of the CSM:

(a) a "reference system" is applied to determine the risk acceptance criteria necessary for evaluating the risk acceptance of the organisational change;
(b) "explicit risk estimation and evaluation":

(1) to analyse the deviations of the change from the reference system;
(2) to identify risk reduction measures for increased risk arising from the change;
(3) to evaluate whether an acceptable level of risk is reached.

C.6. Risk assessment example of an operational significant change – Change of driving hours

C.6.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.6.2. The example is an operational change where the railway undertaking wanted to assign new routes and potentially new working hours (including rotations and shift patterns) to the drivers

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.6.3. In comparison to the CSM process, the following steps were applied (see also Figure 1):

(a) significance of the change [Article 4]:

The railway undertaking performed a preliminary risk assessment which concluded that the operational change was significant. As the drivers had to run on new routes, and possibly outside their usual working hours, the potential of passing signals at danger, of over speeding or of ignoring temporary speed restrictions could not be neglected.

When comparing this preliminary risk assessment with the criteria in Article 4 (2) of the CSM Regulation, the change could be also categorised as significant based on the following criteria:

(1) safety relevance: the change is safety related as the impact of modifying the drivers' way of working could be catastrophic;
(2) failure consequence: the drivers' errors mentioned here above have the potential to lead to a catastrophic consequences;
(3) novelty: potentially the RU could be introducing new ways of working for the drivers;
(4) complexity of the change: modifying the driving hours could be complex as this could require a complete assessment and modification to existing working conditions;

(b) system definition [section 2.1.2]:

The system definition initially described:

(1) the existing working conditions: working hours, shift patterns, etc.;
(2) the changes of the working hours;
(3) the interface issues (e.g. with the infrastructure manager)

During the different iterations, the system definition was updated with the safety requirements resulting from the risk assessment process. Key staff representatives were involved in this iterative process for the hazard identification and system definition update.

(c) hazard identification [section 2.2]:

The hazards and possible safety measures were identified by a brainstorming of a group of experts, including drivers' representatives, for the new routes and shift patterns. The drivers' tasks for the new conditions were looked at in order to assess whether they were affecting the drivers, their workload, the geographical scope and the time of the work shift system.
The RU also consulted the worker unions to see if they could provide additional information and reviewed the risk of fatigue and sickness levels that could be induced by a possible increase of overtime due to extended journeys on unknown routes.
Each of the hazards was assigned a level of severity of risk and consequences (high, medium, low) and the impact of the proposed change reviewed against them (increased, unchanged, decreased) risk.

(d) use of codes of practice [section 2.3]:

Codes of practice related to working hours and human fatigue risks were used to revise the existing working conditions and to determine the new safety requirements. The necessary operational rules were written according to the codes of practice for the new work shift system. All necessary parties were involved in the revised operational procedures and in the agreement to proceed with the change.

(e) demonstration of the system compliance with the safety requirements [section 3]:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

The revised operational procedures were introduced in the RU safety management system. They were monitored and a review process was put in place to ensure that the identified hazards continue to be correctly controlled during the operation of the railway system.

(f) hazard management [section 4.1]:

See point here above as for the railway undertakings the hazard management process can be part of their safety management system for recording and managing risks. The identified hazards were registered in a hazard record with the safety requirements (i.e. reference to the revised operational procedures) controlling the associated risk.
The revised procedures were monitored, and reviewed when needed, to ensure that the identified hazards continue to be correctly controlled during the operation of the railway system.

(g) independent assessment [Article 6]:

The risk assessment and risk management process were assessed by a competent person within the RU's company who was independent from the assessment process. The competent person assessed both the process and the results, i.e. the identified safety requirements.

The RU has based its decision to put the new system into effect on the independent assessment report produced by the competent person.

C.6.4. The example shows that the principles and process used by the railway undertaking are in line with the common safety method. The risk management and risk assessment process fulfilled all the requirements from the CSM.

C.7. Risk assessment example of a technical significant change (CCS)

C.7.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.7.2. The example is related to a technical change of the control command system. It was considered significant by the related manufacturer. A risk assessment based approach was applied to evaluate the change.

C.7.3. Description of the change: the change consists to replace a trackside loop located before a signal by a "radio infill + GSM " sub-system (see Figure 16).

C.7.4. Concern: maintain the safety level of the system after the change.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

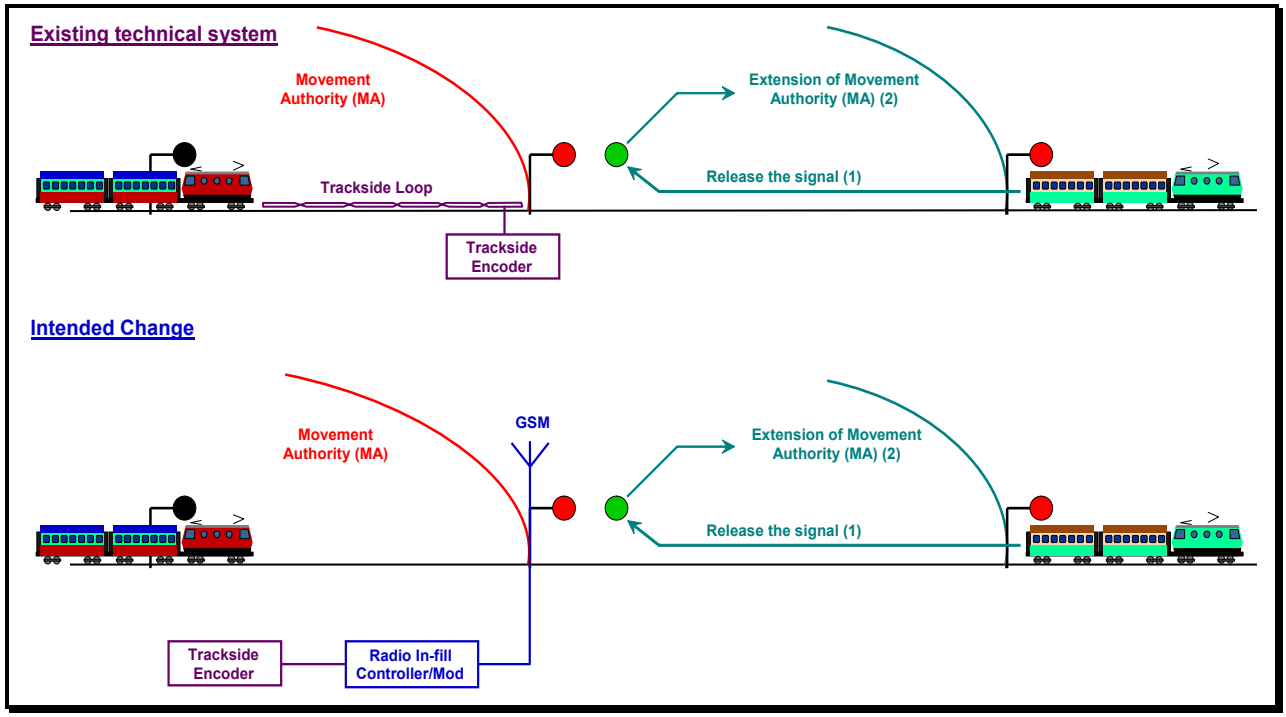

Figure 16 : Change of a trackside loop by a radio in-fill sub-system.

C.7.5. In comparison to the CSM process, the following steps are applied (see also Figure 1):

(a) assessment of the significance of the change [Article 4]

The criteria in Article 4 (2) are used to assess the significance of a change. Mainly the complexity and the novelty were used to decide that the change is significant.

(b) system description [section 2.1.2]:

(1) description of the existing system: loop and its functions in the control command system;
(2) description of the change planned by the proposer and the manufacturer;
(3) description of the functional and physical interfaces of the loop with the rest of the system;

The function of the "loop+encoder" in the existing system is to release the signal on approach of a train when the section behind the signal (i.e. in front of the approaching train) becomes unoccupied: see Figure 16.

(c) hazard identification [section 2.2]:

The iterative risk assessment process and hazard identification (see section 2.1.1) is applied, based on a brainstorming by a group of experts in order:

(1) to identify the hazards, with a relevant influence on risk brought on by the intended change;
(2) to identify possible actions to control the risk;

As the loop, and thus the radio infill, releases the signal, there is a risk to provide an unsafe movement authority to the approaching train whereas the preceding train still occupies the section in front of the signal. The risk must be controlled to an acceptable level.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) use of a reference system [section 2.4]:

The system before the change (loop) is judged to have an acceptable level of safety. It is thus used as "reference system" to derive the safety requirements for the radio infill sub-system.

(e) explicit risk estimation and evaluation [section 2.5]:

(1) the differences between the "loop" and "radio infill+GSM" sub-systems are analysed by explicit risk estimation and evaluation. The following new hazards are identified for the "radio infill + GSM" sub-system:

(i) transmission by hackers of unsafe information in the air gap since the "radio infill+GSM" is an open transmission sub-system;
(ii) delayed transmission or transmission of memorised data packets in the air gap;

(2) explicit risk estimation and use of RAC-TS for the Radio Infill Controller part;

(f) use of codes of practice [section 2.3]:

(1) the EN 50159-2 standard (*"Railway Applications: Part 2: Safety related communication in open transmission systems"*) provides the safety requirements for controlling the new hazards to an acceptable level, e.g.:

(i) data encrypting and protection;
(ii) message sequencing and time stamping;

(2) use for example of EN 50 128 standard for the software development of the Radio Infill Controller;

(g) demonstration of the system compliance with safety requirements [section 3]:

(1) follow up of the implementation of the safety requirements through the development process of the "radio infill + GSM" sub-system;
(2) verification that the system, as designed and installed, is compliant with the safety requirements;

(h) hazard management [section 4.1]:

The identified hazards, the safety measures and the resulting safety requirements issued from the risk assessment and the application of the three risk acceptance principles are registered and managed in a hazard record.

(i) independent assessment [Article 6]:

An independent assessment by a third party is also carried out in order:

(1) to check that the risk management and risk assessment are correctly done;
(2) to check that the technical change is suitable and will maintain the same level of safety as before the change.

C.7.6. The example shows that the three risk acceptance principles required by the common safety method are used in a complementary way to define the safety requirements for the system under assessment. The risk assessment in the example fulfils all the requirements from the CSM summarised in Figure 1, including the hazard record management and independent safety assessment by a third party.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.8. Example of Swedish BVH 585.30 guideline for risk assessment of railway tunnels

C.8.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.8.2. The purpose of the example is to compare the process in the CSM with the BVH 585.30 guideline used by the Swedish infrastructure manager Banverket to design and verify the achievement of a sufficient safety level in the planning and construction of new railway tunnels. The common points and differences with the CSM are listed here after; the detailed risk assessment requirements can be found in the guideline BVH 585.30.

C.8.3. In comparison to the CSM process in Figure 1:

(a) the BVH 585.30 guideline presents the following common points:

(1) system description [section 2.1.2]:

The guideline demands a detailed system description containing:

(i) a description of the tunnel;
(ii) a description of the track;
(iii) a description of the rolling stock type (including on board staff);
(iv) a description of the traffic and intended operations;
(v) a description of the external assistance (including rescue services);

(2) hazard identification [section 2.2]:

The guideline does not explicitly demand hazard identification. It demands risk identification and an "accident catalogue" containing the types of identified potential accidents that are deemed to have a significant impact on the risk level of the tunnel and that have to be covered by the subsequent assessment. Examples of accidents:

(i) "derailment of passenger train";
(ii) "derailment of goods train";
(iii) "accident involving dangerous goods";
(iv) "fire in vehicle";
(v) "collision between passenger train and light/heavy object";
(vi) etc.

(3) there is no provision for the application of codes of practice or similar reference systems. It is considered that risk analysis should be carried out in any case;

(4) explicit risk estimation and evaluation [section 2.5]:

(i) generally, the guideline recommends performing for each type of accident a full Event Tree, based on quantitative risk analysis. But, as the intention of the risk

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

analysis is to analyse the global safety level of the tunnel rather than to analyse the safety individually at more detailed levels, the consequences of all scenarios are summed to get the overall risk level for the tunnel;

(ii) the acceptability of this global risk level for the tunnel is to be compared with the following explicit quantitative risk acceptance criterion. *"railway traffic per kilometer in tunnels shall be as safe as railway traffic per kilometer on open air tracks, excluding level crossings"*. This criterion is transformed into an F-N curve based on historic data of railway accidents in Sweden and is extrapolated to cover also consequences that are not present in the statistics;

(iii) beside this criterion for the global risk level of the tunnel, there are also additional requirements to be fulfilled specifically for evacuation in tunnels and possibilities for the rescue services:

- verify that self rescue is possible in the case of fire in a train for a "credible worst case" (criteria for this assessment are also given);
- the tunnel should be planned to allow rescue efforts to be possible for a given set of scenarios;

(5) output from the risk assessment [section 2.1.6]:

The outputs of the risk assessment are:

(i) a list of safety measures from the minimum standard based on TSI-SRT and national rules to be used for the design of the tunnel, and;

(ii) all additional safety measures identified as necessary by the risk analysis, indicating their purpose. It is stated that measures should be decided upon according to the following priority order:

- prevent accidents;
- reduce consequences of accidents;
- facilitate evacuation;
- facilitate rescue efforts;

(6) hazard management [section 4.1]:

The guideline does not explicitly demand to keep a hazard record. This is related to the fact that the level of the assessment is global and therefore, hazards are not evaluated and controlled individually. The acceptability of the global risk of the tunnel is evaluated, without any apportionment of the global risk acceptance criterion down to the different types of accidents or underlying hazards.

There is however a list of all the safety measures, both those resulting from the "minimum standard" and those identified as necessary by the risk analysis: see point (a)(5)(ii) here above. It should be indicated in the list of safety measures whether they concern the tunnel infrastructure, the track, the operations or the rolling stock and also what their intended effect are according to the numbered list in point (a)(5)(ii). But the guideline does not request to explicitly state what hazards the safety measures are controlling and who is responsible for which measures.

(7) independent assessment [Article 6]:

An independent assessment by a third party is mandatory in order:

(i) to check that the risk assessment process recommended by the BVH 585.30 guideline is correctly done;

(ii) to consider the risk analysis acceptable;

(iii) to check that it is clearly indicated how the future safety management should be performed in the project;

The final risk analysis document is signed by the independent assessor and also by safety coordinator within the project.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) the BVH 585.30 guideline differs in the following aspects:

(1) demonstration of the system compliance with safety requirements [section 3]:

The BVH 585.30 guideline does neither demand to trace how the identified safety requirements are implemented nor to verify that the final tunnel design fulfils the stated safety requirements. It only describes how this requirement should be transferred to make sure that they are implemented in the construction phase.

The guideline provides the safety requirements to be used to verify that the risk analysis has been performed in an appropriate and transparent way, and that it can be accepted by the project.

C.8.4. In conclusion, the comparison with the CSM shows that:

(a) the BVH 585.30 guideline fulfils the relevant parts of the CSM even though their scope and purpose are not exactly the same;
(b) the BVH 585.30 guideline assesses the overall risk level of the railway tunnel;
(c) the hazards are not controlled individually and there is thus less focus on hazard management;
(d) the demonstration of compliance and verification of the correct implementation of all the safety measures is not so explicitly stated. The guideline states however that the role of the safety coordinator within the project (a role and competency that is required by the BVH 585.30) is to verify that the conclusions of the risk analysis are implemented in the design documents and drawings and also to control that they are correctly implemented in the construction phase;

C.8.5. The CSM are more general than the BVH 585.30 guideline in that sense they offer the application of three different risk acceptance principles. However, applying the BVH 585.30 guideline within the CSM does not pose any problems, as it is compatible with using the third principle of explicit risk estimation.

C.9. Example of risk assessment at a system level for Copenhagen Metro

C.9.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.9.2. The example is related to a complete and complex driverless metro system, including underlying technical sub-systems (e.g. Automatic Train Protection and Rolling Stock) as well as the system operation and maintenance. A risk assessment based approach was applied to evaluate the system and the underlying sub-systems. The project covered also the certification of the SMS of the company that had to operate the system. This relates to the RU and IM ability to operate and maintain safely the overall system throughout the system life-cycle.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.9.3. In comparison to the CSM process, the following steps were applied (see also Figure 1):

(a) system description [section 2.1.2]:

(1) description of the system performance requirements;
(2) description of the operational rules;
(3) clear description of the interfaces and responsibilities between the different actors, especially between the technical sub-systems;
(4) definition of high level system requirements (in terms of acceptable frequency of accidents and definition of an ALARP region);

(b) hazard identification [section 2.2]:

(1) a preliminary system level hazard analysis;
(2) system level functional analysis highlighting all sub-systems, and not only those obviously safety critical (e.g. Automatic Train Protection and Rolling Stock) which participate to safety functions and have an active role in ensuring passengers' and staff safety;
(3) intense coordination between the actors (contractors, sub-system suppliers of the technical sub-systems and of the civil works):

(i) to identify systematically all reasonably foreseeable hazards;
(ii) to identify possible actions to control all the risks associated to the identified hazards to an acceptable level;

(c) use of codes of practice [section 2.3]:

Different codes of practice, standards and regulations were used, e.g.:

(1) BOStrab regulation for the construction and operation of street cars (German regulation applicable to urban railway systems) and on the operation without driver;
(2) VDV papers (German codes of practice) related to requirements on equipment for ensuring passenger safety in stations for driverless operation;
(3) CENELEC standards for railway systems (EN 50 126, 50 128 and 50 129). These standards address technical railway systems in particular. But as they contain a methodological approach which has general validity, they have been widely adopted for the Copenhagen metro:

(i) EN 50 126 was used for the safety management and risk assessment activities of the complete railway system;
(ii) EN 50 129 was used for the complete signalling system;
(iii) EN 50 128 was used for software development (including their verification and validation) of the technical sub-systems;

(4) fire protection standards for tunnels (NEPA 130);
(5) standards for civil engineering and civil works (Euro Codes);

(d) use of a reference system [section 2.4]:

The metro had to achieve the safety level of corresponding modern installations in Germany, France or Great Britain. These existing systems were used as similar reference systems to derive the risk acceptance criteria in terms of acceptable frequencies of accidents for the Copenhagen metro;

(e) explicit risk estimation and evaluation [section 2.5]:

(1) for estimation of risks related to specific hazards;
(2) for emergency tunnel ventilation control (including human factors involving the fire brigades);
(3) for identifying risk reduction measures;
(4) for evaluating whether an acceptable level of risk is reached for the complete system;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(f) demonstration of the system compliance with safety requirements [section 3]:

(1) managerial and technical efforts compliant with the complexity of the system for demonstrating the system safety;
(2) apportionment of system safety requirements down to technical sub-systems and civil works, as well as to all safety related metro functions;
(3) demonstration that each sub-system fulfils, as constructed, its safety requirements,;
(4) for safety functions performed by more than one sub-system, the demonstration of compliance to the safety requirements could not be concluded at sub-system level. It was performed at the system level by integrating the different sub-systems, tools and procedures;
(5) demonstration that the overall system complies with the high level safety requirements;

(g) hazard management [section 4.1]:

The identified hazards, the associated safety measures and the resulting safety requirements were registered and managed through a central hazard record. The overall safety manager of the project was responsible for this hazard record. The operational hazards raised during design and installation, as well as hazards related to operation and maintenance were included in the hazard record;

(h) evidences from risk management and risk assessment [section 5]:

The risk assessment results were formally documented and supported by a safety case in compliance with the requirements of the CENELEC standards:

(1) overall system safety case;
(2) safety case for each technical sub-system (including signalling sub-systems and civil works);
(3) safety case for civil works (stations, tunnels, viaducts, embankments);
(4) installation safety case;
(5) vehicles safety case;
(6) operator safety case (supporting the RU and IM SMS certification, i.e. demonstration of the proposer ability to operate and maintain safely the system);

(i) independent assessment [Article 6]:

The overall process was followed up and assessed by an independent safety assessor, acting with a delegation from the Technical Supervisory Authority (i.e. Danish Ministry of Transportation). The roles of the independent safety assessor are outlined in a relevant code of practice. This included:

(1) the check of correct risk management and risk assessment;
(2) the check that that the system is suitable for purpose, and that it will be operated and maintained safely during the complete life-cycle;
(3) recommendation of approval to the Technical Supervisory Authority.

C.9.4. The complete project was supported by an appropriate quality management process.

C.9.5. In the project, the evidences from the suppliers (i.e. safety cases and detailed supporting documentation for the technical sub-systems and civil work) were provided to the proposer safety manager. These evidences were then reviewed by the safety management organisation, as well as by the independent safety assessor whose conclusions were reported in an assessment report.
The independent safety assessment report was reviewed by the proposer safety management and submitted to proposer who forwarded all the files to Technical Supervisory Authority (i.e. Danish Ministry of Transportation) for final approval.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.9.6. The example shows that the principles required by the common safety method are existing methods in the railway sector. The risk assessment in the example fulfils all the requirements from the CSM. In particular, it uses all three risk acceptance principles allowed by the harmonised approach of the CSM.

C.10. Example of OTIF guideline for the calculation of risk due to railway transport of dangerous goods

C.10.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.10.2. The overall OTIF guideline philosophy is in line with the purpose of the CSM, but the guideline has a reduced scope. The objective of the OTIF *"guideline is to obtain a more uniform approach for the risk assessment of transport of dangerous goods in the COTIF Member States and consequently make individual risk assessments comparable"*. It supports thus the cross acceptance, between the COTIF member states, of risk assessments of the transport of dangerous goods by rail.

C.10.3. Compared with the CSM and the flowchart in Figure 1:

(a) the OTIF guideline presents the following common points:
  (1) it is a common approach for risk assessment, nevertheless only based on explicit risk estimation (i.e. the third CSM risk acceptance principle);
  (2) the OTIF risk assessment is composed of:
    (i) a risk analysis phase that includes:
      - a hazard identification phase;
      - a risk estimation phase;
    (ii) a risk evaluation phase based on risk (acceptance) criteria which are not yet harmonised. Indeed, a lot of national specificities can influence those criteria;

(b) the OTIF guideline differs in the following aspects:
  (1) the scope of application is different. Whereas the CSM have to be applied only for significant changes to the railway system, the OTIF guideline should be applied for assessing the risks of transporting dangerous goods by rail, whether this constitutes a significant change or not to the railway system;
  (2) there is no possibility to chose among three risk acceptance principles for controlling the risk(s). The third principle, i.e. explicit risk estimation, is the only allowed one. Furthermore, is must be based exclusively on a quantitative estimation rather than on a qualitative one. The qualitative risk analysis may only be suitable for comparing options of (safety) measures for risk reduction;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) the application of the ALARP principle is requested in order to determine if additional safety measures could reduce the assessed risk further at a reasonable price;
(4) there is no concept of "hazards associated with broadly acceptable" allowing to focus the risk assessment effort on the most contributing hazards. Nevertheless, it recommends to reduce the number of potential accident scenarios to a reasonable number of basic scenarios (see section § 3.2 in {Ref. 10});
(5) the process concentrates on risk assessment but does not include:

(i) the process for the selection and implementation of (safety) measures to modify the risk;
(ii) the process for risk acceptance;
(iii) the process for demonstrating the system compliance with the safety requirements;
(iv) the process for communicating the risk to other concerned actors (see point here after);

(6) it does not give directives about the evidence to be provided by the risk assessment process;
(7) there is no request for hazard management;
(8) there is no request for independent assessment by a third party of the correct application of the common approach.

C.10.4. The comparison between the OTIF guideline and the CSM shows that both are compatible even though their scope and purpose are not exactly the same. The CSM is more general than the OTIF guideline, in that sense it is more flexible. On the other hand the CSM covers also more risk management activities:

(a) it allows to use three risk acceptance principles that are based on existing practices in railways: refer to section 2.1.4;
(b) its application is requested only for significant changes and further risk analysis is requested only for hazards that are not associated with a broadly acceptable risk;
(c) it includes the selection and implementation of the safety measures expected to control the identified hazards and the associated risks;
(d) it harmonises the risk management process, including:

(1) the harmonisation of the risk acceptance criteria that is dealt within the scope of the Agency work on broadly acceptable risks and risk acceptance criteria,
(2) the demonstration of the system compliance with the safety requirements;
(3) the results and evidence from the risk assessment process;
(4) the exchange of safety related information between the actors involved at interfaces;
(5) the management in a hazard record of all identified hazards and associated safety measures;
(6) the independent assessment by a third party of the correct application of the CSM.

C.10.5. Applying the OTIF guideline within the CSM (in case transporting dangerous goods constitutes a significant change for an IM or RU) does however not pose any problems, as it is compatible with using the third principle of explicit risk estimation.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.11. Risk assessment example of an application for approval of a new rolling stock type

C.11.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.11.2. This example of risk assessment is related to an application for approval of a new type of rolling stock. A risk analysis was performed to evaluate the risks related to the introduction of a new freight wagon.

C.11.3. The purpose of the change was to increase the efficiency, capacity, performance and reliability for the transport of bulk goods on a specific freight line. As the wagons were intended for cross border traffic, an approval by two different NSAs was also needed. The proposer was the freight operator which is in turn owned by the company producing the goods to be transported.

C.11.4. The project development comprised the construction, manufacturing, montage, putting in to service and verification of the new rolling stock. The risk analysis was performed to verify that the new design fulfilled the safety requirements for each of the sub-systems as well as for the complete system.

C.11.5. In the risk analysis, reference is made to the CENELEC EN 50126 procedures and definitions and the risk evaluation is performed according to this standard.

C.11.6. In comparison to the CSM process, the following steps were applied:

(a) system description [section 2.1.2]:

For each of the design phases, there were requirements on the safety verification documentation and description of the system design:

(1) conceptual phase: preliminary description of the operating demands of the operator;
(2) specification phase: functional specification, applicable technical standards, plan for testing and verification. Requirements from the operator on the use and maintenance of the wagon were also included;
(3) manufacturing phase: technical documentation of the manufacturer, including drawings, standards, calculations, analysis etc. In depth risk analysis for new or innovative designs or new areas of use;
(4) verification phase:

(i) the manufacturer's verification of the technical performance of the wagon (test reports, calculations, verifications in compliance with standards and functional requirements);

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(ii) documentation of risk reducing measures and test reports to prove the wagons compatibility with the rail infrastructure;
(iii) maintenance and training documents, user's manuals, etc.

(5) acceptance phase:

(i) the manufacturer's safety declaration and safety evidence (safety case);
(ii) the acceptance by the operator of both the freight wagon and its documentation;

(b) hazard identification [section 2.2]:

this was performed continuously in all the design phases. First a "bottom-up" approach is used where the different manufacturers evaluated risk sequences arising from failure of components within their sub-system. The division into sub-systems was as follows:

(1) chassis;
(2) braking system;
(3) central coupling;
(4) etc.

A complementary "top-down" approach was then applied to look for gaps or missing information. Risks that could not immediately be accepted were transferred into the hazard record for further treatment and classification.

(c) use of risk acceptance principles [section 2.1.4]:

Explicit risk estimation was performed on the system as a whole. However codes of practice or similar reference systems could be used to assess individual hazards. The principle is that every new sub-system should be at least as safe as the sub-system it is replacing, thus leading to a new complete system with a higher safety level than the previous one. The EN50126 risk matrix was used to plot the identified hazards. Different additional risk acceptance criteria were also applied, among others:

(1) single failure should not lead to a situation where people, materiel or the environment may be seriously affected;
(2) if this cannot be avoided by technical construction means, it should be prevented by operational rules or maintenance requirements. This was only applicable for hazards where it was possible to identify the occurred failure before it creates a hazardous situation;
(3) for components with a high probability of failure, or where failures cannot be detected beforehand or prevented through maintenance of operational rules, additional safety functions and barriers should be considered;
(4) redundant systems with components that may develop undetectable failures during operations should be protected by maintenance measures to prevent reduced redundancy;
(5) the resulting final safety level was a management decision, which was based on quantitative and qualitative risk analysis;

(d) demonstration of the system compliance with safety requirements [section 3]:

All identified risks and hazards were registered, and the list was continuously consulted and updated. Remaining hazards were registered in the hazard record together with the corresponding list of risk reducing measures to be taken in construction, operation and maintenance. Based on this a final safety report was produced with the verification that the safety requirements have been implemented;

(e) hazard management [section 4.1]:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

As stated above, the hazards and their related safety measures were registered in a hazard record keeping track of all identified hazards and safety measures. Hazards related to risks that were acceptable without measures were however not included in the hazard record;

(f) independent assessment [Article 6]:

There was no mention of an independent assessment within the documents received related to this significant change.

C.11.7. The risk assessment example is based on the CENELEC EN 50126 standard and thus corresponds well with the CSM process. The risk assessment in the example fulfils all the requirements from the CSM, with the exception of the requirement for independent assessment which was not explicitly clarified within the documents received. Explicit risk acceptance criteria were used and clearly indicated.

C.12. Risk assessment example of an operational significant change – Driver only operation

C.12.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.12.2. The example is an operational change where the railway undertaking decided that the train had to be operated by the driver alone (Driver Only Operated – DOO) on a route where previously there was an onboard guard to assist the driver with the train dispatching.

C.12.3. In comparison to the CSM process, the following steps were applied (see also Figure 1):

(a) significance of the change [Article 4]:

The railway undertaking performed a preliminary risk assessment which concluded that the operational change was significant. As the driver had to operate alone, without assistance, the potential that passengers could be caught between the doors or fall down on to the track (e.g. if doors are opened on the wrong side) could not be neglected.

When comparing this preliminary risk assessment with the criteria in Article 4 of the CSM Regulation, the change could be also categorised as significant based on the following criteria:

(1) safety relevance: the change is safety related as the impact of requiring a completely different way of managing the operation of the train service could be catastrophic;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) failure consequence: the potential effect of the driver performance could lead to catastrophic consequences if the operation is not effectively controlled;
(3) novelty: the driver only operation could require innovative ways of operating trains whose risks must be assessed;

(b) system definition [section 2.1.2]:

The system definition described:

(1) the existing system, explaining clearly which tasks were performed by the driver and which other ones were carried out by the onboard staff (or guard) to assist the driver;
(2) the change of the driver's responsibilities due to the removal of the onboard assisting staff;
(3) the technical requirements of the system to cover changes in operation;
(4) the existing interfaces between the onboard assisting staff, the driver and the trackside staff of the infrastructure manager;

During the different iterations, the system definition was updated with the safety requirements resulting from the risk assessment process. Key persons (including drivers, staff representatives and the infrastructure manager) were involved in this iterative process for the hazard identification and system definition update.

(c) hazard identification [section 2.2]:

The hazards and possible safety measures were identified by a brainstorming of a group of experts, including among others:

(1) drivers' and staff's representatives for their operational experience;
(2) IM representatives as the infrastructure could be also affected by the change, implying for example changes to stations (e.g. installation of mirrors/closed circuit television [CCTV] at platforms);

The additional tasks to be performed by the driver were scrutinised in order to identify all foreseeable hazards that might occur consecutively to the removal of the onboard assisting staff. Particularly, the hazard identification looked at what the key operational hazards could be at stations, on the existing routes where there was assistance from on board or trackside staff including the safe dispatch of the trains, specific issues related to the driver, the rolling stock (e.g. door opening/closure check), maintenance requirements, etc.

Each of the identified hazards was assigned a level of severity of risk and consequences (high, medium, low) and the impact of the proposed change reviewed against them (increased, unchanged, decreased) risk.

(d) use of codes of practice [section 2.3] and use of similar reference systems [section 2.4]:

Both codes of practice (i.e. a set of standards for Driver Only Operation) and similar reference systems were used to define the safety requirements for the identified hazards. These safety requirements included:

(1) the revised operational procedures for the driver that are required to operate safely the trains without onboard assistance;
(2) any additional equipment necessary onboard or on the track to ensure safe and reliable means of train dispatch;
(3) a checklist for ensuring that the driver's cab was suitable, taking into account the interface between the railway system (both onboard and trackside) and the driver;

The necessary operational rules were revised in compliance with the requirements from the applicable codes of practice and the relevant reference systems. All necessary

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

parties were involved in the revised operational procedures and in the agreement to proceed with the change.

(e) demonstration of the system compliance with the safety requirements [section 3]:

The system was implemented in compliance with the identified safety requirements (additional equipment and revised procedures). These were verified as appropriate means to ensure a sufficient level of safety for the system under assessment.

The revised operational procedures were introduced in the RU safety management system. They were monitored and reviewed, when needed, to ensure that the identified hazards continue to be correctly controlled during the operation of the railway system.

(f) hazard management [section 4.1]:

See point here above as for the railway undertakings the hazard management process can be part of their safety management system for recording and managing risks. The identified hazards were registered in a hazard record with the safety requirements controlling the associated risk, i.e. reference to additional onboard and trackside equipment as well as to the revised operational procedures.
The revised procedures were monitored, and reviewed when needed, to ensure that the identified hazards continue to be correctly controlled during the operation of the railway system.

(g) independent assessment [Article 6]:

The risk assessment and risk management process were assessed by a competent person within the RU's company who was independent from the assessment process. The competent person assessed both the process and the results, i.e. the identified safety requirements.

The RU has based its decision to put the new system into effect on the independent assessment report produced by the competent person.

C.12.4. The example shows that the principles and process used by the railway undertaking are in line with the common safety method. The risk management and risk assessment process fulfilled all the requirements from the CSM.

C.13. Example of the use of a reference system for deriving safety requirements to new electronic interlocking systems in Germany

C.13.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.13.2. In order to derive standard safety requirements for future electronic interlocking systems, Deutsche Bahn had conducted a risk analysis of an already approved electronic system. The latter system had been previously approved according to German codes of practice (Mü 8004).

C.13.3. The risk analysis was done in accordance with the CENELEC standards (EN 50126 and EN 50129), and included the following steps:

(a) system definition;
(b) hazard identification;
(c) hazard analysis and quantification.

C.13.4. For the system definition, care had been taken to define the boundaries of the system, its functions and its interfaces. The main challenge there was to define the system in such a way that it is independent from the internal architecture of an interlocking system while remaining compatible with existing interlocking systems. Particular attention was thus given in defining very clearly the interfaces with outside systems interacting with the interlocking, without detailing the inner functions of the interlocking.

C.13.5. The hazards were then identified only at the interfaces in order to remain generic (i.e. to avoid any dependency with specific architectures). Only hazards arising from technical faults were considered. For each interface, two generic hazards were thus identified:

(a) wrong output from interlocking transmitted to the interface
(b) (correct) Input is corrupted at the interface

C.13.6. More specific characteristics were then given to these generic hazards for each interface.

C.13.7. In the following phase, the contributions of the existing system's components to each identified hazards were analysed and assembled in a fault tree. This allowed, based on the estimated failure rates of the components, to calculate a rate of occurrence for each hazard, and use those rates as Tolerable Hazard Rates (THR) for future generations of electronic interlocking.

C.13.8. The risk analysis was followed up and assessed by the national safety authority (EBA).

C.13.9. As part of the risk analysis, an analysis for the control and display functions in electronic system was also conducted. Again an existing approved electronic interlocking system was taken as a reference in order to derive safety requirements of the Man-Machine-Interface (MMI) functions for controlling both random failures and faults and for controlling systematic faults. As a result the safety integrity levels (SILs) for different functions were determined: for MMI functions in standard operation, for MMI functions in Command-Release operation (degraded mode), and for display functionality.

C.13.10. This risk analysis was also followed up and assessed by the national safety authority (EBA).

C.13.11. Those risk assessment examples illustrate how the second risk acceptance (reference system) of the CSM can be used for deriving safety requirements for new systems. Furthermore they were based on the CENELEC standards and thus correspond well with the CSM process. The risk assessment in the examples fulfils the requirements from the CSM related to the phases that are covered. But as no design activity is included, there is neither a reference to hazard record management nor to the demonstration of compliance of the system under assessment with the identified safety requirements.

C.13.12. Further information on these risk analyses can be found in:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15, and;

(b) Bock, H., Braband, J., and Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

C.14. Example of an explicit Risk acceptance criterion for FFB Radio-based Train Operation in Germany

C.14.1. **Remark:** this example of risk assessment was not produced as a result of the application of the CSM process; it was carried out before the existence of CSM. The purpose of the example is:

(a) to identify the similarities between the existing risk assessment methods and the CSM process;
(b) to give traceability between the existing process and the one requested by the CSM;
(c) to provide justification of the added value of performing the additional steps (if any) required by the CSM.

It must be stressed that this example is given for information only. Its purpose is to help the reader understanding the CSM process. But the example itself shall not be transposed to or used as a reference system for another significant change. The risk assessment shall be carried out for each significant change in compliance with the CSM Regulation.

C.14.2. A risk analysis in accordance with the CENELEC standards was carried out for a totally new operating procedure that had been envisaged (but never introduced) in Germany for conventional railway lines. The concept consisted in operating trains safely only through radio-based (route and train) control. As there were not existing codes of practice (acknowledged engineering rules) and reference systems for such a new system, explicit risk estimation was conducted in order to demonstrate the safety of the new procedure. It was necessary to show that the level of risk to a passenger due to the new system would not exceed an acceptable risk value (explicit risk acceptance criterion).

C.14.3. This explicit risk acceptance criterion was estimated on the basis of statistics of accidents in Germany that had been attributable to signalling and control systems, and its plausibility was also checked against the MEM criterion. Such demonstration of safety conforms with the German EBO requirement of having "the same level of safety" in case of deviations from engineering rules. The risk analysis also was followed up and assessed by the national safety authority (EBA).

C.14.4. This risk assessment example shows how a global explicit criterion (for the third risk acceptance principle in the CSM) can be derived for new systems with no applicable codes of practice nor any reference system. The risk analysis that was subsequently carried out for the new system is based on the CENELEC standards and thus corresponds well with the CSM process. The risk assessment in the example fulfils the requirements from the CSM, but there is no reference to hazard record management neither to demonstration of the compliance of the system under assessment with the identified safety requirements.

C.14.5. Further information on this risk analysis can be found in: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, 10-15

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.15. Example of applicability test of the RAC-TS

C.15.1. The purpose of this appendix is to show on an example of the ETCS on-board sub-system function how to use the criterion in section 2.5.4 and how to determine whether the RAC-TS is applicable.

C.15.2. The ETCS on-board sub-system is a technical system. The following function is considered: *"provide the Driver with information to allow him to drive the train safely and enforce a brake application in case of over-speed"*.

Description of the function: based on information received from the trackside (permitted speed) and on the train speed computed by the on-board ETCS sub-system:

(a) the Driver drives the train and ensures that the train speed does not exceed the permitted one;
(b) in parallel, the on-board ETCS sub-system supervises that the train never exceeds the permitted speed limit. In case of over speed, it applies automatically the brakes.

Both the Driver and the ETCS on-board sub-system are using the evaluation of the train speed that is computed by the on-board ETCS sub-system.

C.15.3. Question: "Does the RAC-TS apply to the evaluation of the train speed by the on-board sub-system?"

C.15.4. Application of the flow chart in Figure 14 and answers to the different questions:

(a) Considered hazard for the technical system:

"Exceedance of the safe speed as advised to ETCS" (see UNISIG SUBSET 091).

(b) Can the hazard be controlled by a code of practice or by a reference system?

NO. It is assumed that the ETCS system is a new and innovative design. Therefore, there are no codes of practice or reference systems that can enable to control the hazard to an acceptable level of risk.

(c) Is it likely that the hazard can result in a catastrophic consequence?

YES since an *"exceedance of the safe speed as advised to ETCS"* can result in a train derailment that can potentially lead to *"fatalities and/or multiple severe injuries and/or major damage to the environment"*.

(d) Is the catastrophic consequence a direct result of the Technical System failure?

YES if there are no additional safety barriers. The same evaluation of the train speed that is computed by the on-board ETCS sub-system is provided to both the Driver and the brake control function of the on-board ETCS sub-system. Therefore, assuming the Driver is driving the train (for performance reasons) at the maximum speed permitted by the trackside, then neither the Driver nor the on-board ETCS sub-system will detect that the train is over speeding in case of under estimation of the train speed. That has a potential to lead to a train derailment with catastrophic consequences.

(e) Conclusions:

(1) for the quantitative requirements: apply a THR of 10^{-9} h^{-1} for the random hardware failures of the on-board ETCS sub-system, ensuring that:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(i) the evaluation of this quantitative target takes into account for redundant systems the common components (e.g. single or common inputs to all channels, common power supply, comparators, voters, etc.);
(ii) the dormant or latent failure detection times are covered;
(iii) a Common Cause/Mode Failure (CCF/CMF) analysis is done;
(iv) an Independent Assessment is carried out;

(2) for the process requirements: apply a SIL 4 process for the management of the systematic failures/errors of the on-board ETCS sub-system. This requires the application of:

(i) a quality management process compliant with SIL 4;
(ii) a safety management process compliant with SIL 4;
(iii) the relevant standards, e.g.:

- for the software development use the EN 50 128 standard;
- for the hardware development use the EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2, etc. standards;

(3) an Independent Assessment of the process(es).

C.16. Examples of possible structures for the hazard record

C.16.1. Introduction

C.16.1.1. The minimum requirements to be registered in the hazard record are identified in section 4.1.2 of the CSM Regulation. These are indicated with a shaded background in the examples hereafter of hazard records.

C.16.1.2. There may be different ways to structure a hazard record, as well as any additional information that could characterise the hazards and the associated safety measures. For example, the hazards and associated safety measures can be fitted with one field per piece of information. However, whatever structure is used, it is important that the hazard record provides clear links between the hazards and the associated safety measures. One possible solution is that the hazard record contains, for each hazard and for each safety measure, at least a field with:

(a) a clear description including references of its origin and of the risk acceptance principle selected to control the associated hazard. This field enables to understand the hazard and the associated safety measures, as well as to know in which safety analyses they are identified.

As the hazard record is used and maintained during the whole system life-cycle (i.e. during the system operation and maintenance), a clear traceability, or link, is helpful between each hazard and:

(1) the associated risk;
(2) the hazard causes when already identified;
(3) the associated safety measures, as well as the assumptions defining the limits of the system under assessment;
(4) the associated safety analyses where the hazard is identified;

Furthermore, the wording of safety measures (especially the ones to transfer to other actors such as to a proposer), the wording of the associated hazards and risks needs to be clear and sufficient. "Clear and sufficient" mean that the safety measures and the

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

associated hazards can be understood what risks they are expected to control, without the need to go back into the related safety analyses.

(b) the risk acceptance principle used to control the hazard in order to support the mutual recognition and help the assessment body to assess the correct application of the CSM;

(c) a clear information on its status: this field indicates whether the related hazard/safety measure is still open or controlled/validated.

(1) an open hazard/safety measure is tracked until it is controlled/validated;
(2) reciprocally, the controlled/validated hazards/safety measures are not tracked anymore unless significant changes in operation or in maintenance of the system occur: see point [G 6](b) in section 2.1.1. If this happens:

(i) the CSM is applied again on the required changes in compliance with the Article 2. See also point [G 6](b)(1) in section 2.1.1;
(ii) all controlled hazards and safety measures are reconsidered in order to check that they are not impacted by the changes. If impacted, the related hazards and associated safety measures are re-opened and managed again in the hazard record;

It could happen that different safety measures are implemented instead of the ones registered in the hazard record (e.g. for cost purposes). The implemented safety measures are then registered in the hazard record with the evidence/ justification why they are appropriate and the demonstration that with these measures the system complies with the safety requirements.

(d) the reference to the associated evidence controlling a hazard or validating a safety measure. This field enables to find later the evidence having permitted to control the hazard and to validate the associated safety measure(s);

A hazard could be controlled in the hazard record only when all the associated safety measures, linked to the hazard, are validated beforehand;

(e) the organisation(s) or entity (ies) responsible to manage it.

C.16.1.3. Another example of possible content of a hazard record is given in the Appendix A.3. of the EN 50126-2 guideline {Ref. 9}.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.2. Example of the hazard record for the organisational change in section C.5. in Appendix C

Table 6 : Example of the Hazard Record for the organisation change in section C.5. in Appendix C.

Hazard Description	Safety Measures	Priority/ Safety Punctuality	Imple-mentation(18)	Notes	Respon-sibility(18)	Origin	Used Risk Acceptance Principle	Responsi-bility for verification	Way of veri-fication	Status xx.xx.xx
Reduced motivation among employees remaining in Company. Hence staff continuing to leave without stop. Demotivated / worn out managers	New round of motivational work for the staff, to be performed in smaller groups Reallocation of funds so that the Company gets meaningful tasks to perform More frequent inspections by track manager. Allocate funds to make sure that key staff stays throughout the process. Give special attention to make sure that information and knowledge is transferred between leaving employees and those who take over the tasks. etc.	High/High	Coordinated by XYZ. Regions must look at measures to increase control of tracks, over-lap of emp-loyees and follow up by line manager	Increased inspections need to be included in the contracts. Etc.	Company Manager	Brain-storming HAZID report R_X	N/A			Change of conditions of circumstances have reduced this risk significantly Work environ-ment analysis performed and some training of staff.
Subcontractors of the entrepreneurs lacking skill, competency and quality control	Increased demand for documented competence. Systematic control of performed tasks	High/ Medium	IM must coordinate. Regions must implement measures for requiring competence and controlling the work	Implemented by contract follow up. Input to revision planning.	Infra-structure manager	Brain-storming HAZID report R_X	N/A	Safety manager		Increased focus on routines for control (2 operative controls per month and operative area)
Uncertainty of roles and responsibilities in the interface between Company and IM (Track manager).	Define roles and responsibilities. Map all interfaces and define who is responsible for the interfaces.	Medium/ Medium	In each region separately	Implemented by maintenance contract and the strategy plan for the reorganisation	Regional directors	Brain-storming HAZID report R_X	N/A	Safety Manager		Regions have presented their strategy.

(18) *These two columns relate to the information/field about the actors in charge of controlling the identified hazards.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.3. Example of a complete hazard record for an onboard control command sub-system

C.16.3.1. This section gives in an example a single hazard record (refer to point [G 3] in section 4.1.1) for managing both:

(a) all the internal safety requirements applicable to the sub-system the actor is responsible for; and,
(b) all identified hazards and associated safety measures that the actor cannot implement and that must be transferred to other actors.

Table 7 : Example of a Manufacturer's hazard record for an onboard control command sub-system.

N° HZD	Origin	Hazard description	Additional information	Actor in charge	Safety Measure	Used Risk Acceptance Principle	Exported	Status
1	HAZOP report R_X	Maximum speed of train set too high (Vmax)	Wrong specific configuration of the onboard sub-system (maintenance staff). Wrong Data Entry onboard (driver)	Railway Undertaking	• Define a procedure for the approval of the onboard sub-system configuration data; • Define an operational procedure for the Data Entry Process by the Driver;	Explicit Risk Estimation	Yes	Controlled (exported to RU) Refer also to section C.16.4.2. in Appendix C
2	HAZOP report R_X	Braking curves (i.e. Movement Authority) in onboard sub-system configuration data too permissive	The procedure for the specific configuration of the onboard sub-system depends on: • the safety margins taken for the train braking system; • the reaction delay of the train braking system (this one is directly dependent on the train length, especially for fret trains)	Railway Undertaking	• Specify correctly the system requirements in the System Definition; • Take sufficient safety margins for the braking system of the specific train;	Explicit Risk Estimation	Yes	Controlled (exported to RU) Refer also to section C.16.4.2. in Appendix C
3	HAZOP report R_X	• Maximum speed of train set too high (Vmax) • Braking curves (i.e. Movement Authority) in onboard sub-system configuration data too permissive	Failure to update the train wheel diameter in the specific configuration of the onboard sub-system (maintenance staff).	Railway Undertaking	• Define a procedure for the measure of the train wheel diameter by the maintenance staff; • Define a procedure for the regular update of the train wheel diameter in the onboard sub-system;	Explicit Risk Estimation	Yes	Controlled (exported to RU) Refer also to section C.16.4.2. in Appendix C
			Failure in manufacturer procedure for the preparation and the upload of the configuration data into the onboard sub-system	Manufacturer	Define a procedure for updating the train wheel diameter in the onboard configuration data	Explicit Risk Estimation	Yes	Controlled by Procedure P_X
4	HAZOP report R_X	Entry of the train at a high speed (160 km/h if line side signal free) on	Could be controlled only by the driver's vigilance. The entry into a trackside ATP fitted area relies on an acknowledgment procedure by the driver before the	Infrastructure Manager	Infrastructure Manager to ensure that trains that are not fitted with an active onboard control command	Explicit Risk Estimation	Yes	Controlled (exported to IM) Refer also to

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 7 : Example of a Manufacturer's hazard record for an onboard control command sub-system.

N° HZD	Origin	Hazard description	Additional information	Actor in charge	Safety Measure	Used Risk Acceptance Principle	Exported	Status
		the track without the onboard sub-system active and without line side signalling	transition location. In case of absence of acknowledgement, there is an automatic application of the train brakes by the onboard control command sub-system.		sub-system do not enter the relevant track. Define a procedure for the traffic management.			section C.16.4.2. in Appendix C
				Railway Undertaking	Ensure the driver training for entering a trackside ATP fitted area	Explicit Risk Estimation	Yes	Ccontrolled (exported to RU) Refer also to section C.16.4.2. in Appendix C
5	HAZOP report R_X	Maximum speed of train set displayed to the driver too high (Vmax)	The information displayed on the driver's interface is monitored by the SIL 4 onboard control command sub-system that applies the emergency brakes in case of discrepancy between display and expected value. In case of non compliance of with the movement authority the onboard sub-system control command sub-system applies the emergency brakes	Manufacturer	Develop a SIL 4 onboard control command sub-system	Explicit Risk Estimation	Yes	Safety Case demonstrating a SIL 4 sub-system assessed by an Independent Safety Assessor
6	HAZOP report R_X	Train is leaving without driver machine interface	Loss of redundant architecture of onboard sub-system	Manufacturer	Develop a SIL 4 onboard control command sub-system	Explicit Risk Estimation	Yes	Safety Case demonstrating a SIL 4 sub-system assessed by an Independent Safety Assessor
etc.								

C.16.4. Example of a hazard record for transferring information to other actors

C.16.4.1 This section gives in an example a hazard record for transferring to other actors the identified hazards and associated safety measures that a considered actor cannot implement. Refer to point [G 1] in section 4.1.1.
This example is the same one as the example in section C.16.3. in Appendix C. The only difference is that all the internal hazards and safety measures that could be controlled by the considered actor are removed.

C.16.4.2. The last column in Table 8 is used to fulfil the requirement in section 4.2 of the CSM Regulation. There are different solutions to achieve it. One way may be to refer to the evidence used by the actor receiving the exported safety information. Another way could be to have a meeting between the two

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

actors in order to find jointly the adequate solution for controlling the associated risk(s). The results of such a meeting could be reported in an agreed document (for example a minutes of meeting) to which the actor exporting the safety related information can refer for closing the associated hazards in his hazard record.

Table 8 : Example of a hazard record for transferring safety related information to other actors.

N° HZD	Origin of Hazard		Hazard description	Additional information	Actor in charge	Safety measure	Comment from receiver
	N° in Table 7	Other					
1	N°1	HAZOP report R_X	Maximum speed of train set too high (Vmax)	Wrong specific configuration of the onboard sub-system (maintenance staff). Wrong Data Entry onboard (driver)	Railway Undertaking	• Define a procedure for the approval of the onboard sub-system configuration data; • Define an operational procedure for the Data Entry Process by the Driver;	• The configuration data of the onboard control command sub-system depends on physical characteristics of the rolling stock. • Safety margins are then applied on this data in coordination between Infrastructure Manager and Railway Undertaking. • This data is then uploaded in the onboard sub-system in compliance with the appropriate manufacturer's procedure during the installation, integration into the rolling stock and acceptance of the control command sub-system. • The drivers are trained and evaluated against the procedure D_P. • Drivers are also evaluated by the IM against the rules applicable on the IM infrastructure.
2	N°2	HAZOP report R_X	Braking curves (i.e. Movement Authority) in onboard sub-system configuration data too permissive	The procedure for the specific configuration of the onboard sub-system depends on: • the safety margins taken for the train braking system; • the reaction delay of the train braking system (this one is directly dependent on the train length, especially for fret trains)	Railway Undertaking	• Specify correctly the system requirements in the System Definition; • Take sufficient safety margins for the braking system of the specific train;	Refer comment for line 1 here above.
3	N°3	HAZOP report R_X	• Maximum speed of train set too high (Vmax) • Braking curves (i.e. Movement Authority) in onboard sub-system configuration data too permissive	Failure to update the train wheel diameter in the specific configuration of the onboard sub-system (maintenance staff).	Railway Undertaking	• Define a procedure for the measure of the train wheel diameter by the maintenance staff; • Define a procedure for the regular update of the train wheel diameter in the onboard sub-system;	• The maintenance of the onboard control command sub-system is done in compliance with the "Maintenance Procedure MP_Z". • The train wheel diameter is updated at defined intervals according to the procedure P_W. • For the Data Entry Process, the train drivers are trained and evaluated against the "Procedure P_{DE}".
4	N°4	HAZOP report	Entry of the train at a high speed (160	Could be controlled only by the driver's vigilance.	Infrastructure Manager	Infrastructure Manager to ensure that trains that are not	The traffic management on the IM infrastructure is ruled by the set of rules R_{TM}

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 8 : Example of a hazard record for transferring safety related information to other actors.

N° HZD	Origin of Hazard		Hazard description	Additional information	Actor in charge	Safety measure	Comment from receiver
	N° in Table 7	Other					
		R_X	km/h if line side signal free) on the track without the onboard sub-system active and without line side signalling	The entry into a trackside ATP fitted area relies on an acknowledgment procedure by the driver before the transition location. In case of absence of acknowledgement, there is an automatic application of the train brakes by the onboard control command sub-system.		fitted with an active onboard control command sub-system do not enter the relevant track. Define a procedure for the traffic management.	
					Railway Undertaking	Ensure the driver training for entering a trackside ATP fitted area	• The drivers are trained at regular intervals against the IM procedure P_{IM_DP}. • Drivers are also evaluated by the IM against the set of rules (S_R) applicable on the IM infrastructure.
etc.							

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.17. Example of a generic hazard list for railway operation

C.17.1. ROSA (Rail Optimisation Safety Analysis), a project in the framework of DEUFRAKO (French-German cooperation) attempted to establish a generic and comprehensive hazard list covering standard railway operation. The aim and challenge was to define these hazards at a maximum level of detail possible while not reflecting the specificities of the French and German railways. The list was established using currently existing hazard lists from both countries (SNCF and DB) and was also cross-checked with hazard lists from other countries. In spite of the declared objective to be comprehensive and generic, the list is only given here as an indicative example that may serve as a help for the actors when they have to identify hazards for a particular project. It is expected that the hazards given in this list would probably need to be refined or complemented to reflect any specificities of a project.

C.17.2. The hazards in the draft list below are called "starting point hazards" (SPH), meaning hazards from which both a consequence analysis and a causal analysis could be carried out in order to determine safety measures/barriers and safety requirements for controlling the hazards.

C.17.3. ROSA project hazard list:

SPH 01	Initial wrong Determination of speed limit (related to infrastructure)
SPH 02	Wrong Determination of speed limit (train related)
SPH 03	Wrong braking distance determined /wrong speed profile / wrong braking curves
SPH 04	Insufficient deceleration (physical causes)
SPH 05	Wrong/ inappropriate speed/ brake command
SPH 06	Wrong speed registered (wrong speed train)
SPH 07	Failure of speed limit communication
SPH 08	Train rolls away
SPH 09	Wrong travel direction/ intentional backwards moving - (combination of SPH 08 and SPH 14)
SPH 10	Wrong absolute/ relative position registered
SPH 11	Train detection failure
SPH 12	Loss of train integrity
SPH 13	Possible wrong route for train
SPH 14	Failure in transmission/communication of timetable/MA (movement authority)
SPH 15	Guideway structural failure
SPH 16	Broken switch component
SPH 17	Wrong switch command
SPH 18	Wrong switch status
SPH 19	System object on guideway/ within CE (clearance envelope) (excl. Ballast)
SPH 20	Foreign object on guideway/ within CE
SPH 21	Road traffic user on LC
SPH 22	Slipstream effects on ballast
SPH 23	Aerodynamic forces impact on train
SPH 24	Train equipment/ element/ loading infringes CE of train
SPH 25	Inappropriate CE dimension for train (wayside)
SPH 26	Wrong distribution of loading
SPH 27	Broken wheel, broken axle
SPH 28	Hot axle/ wheel/ bearing
SPH 29	Failure of bogie/ suspension, damping
SPH 30	Failure of vehicle frame/ car body
SPH 31	Trespassing (security-aspect)
SPH 32	Authorised person crosses track

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

SPH 33	Staff working on track
SPH 34	Unauthorised person intrudes track (negligence)
SPH 35	Person falls from platform edge onto track
SPH 36	Slipstream/ person too close to platform edge
SPH 37	Staff working near track e.g. neighbouring track
SPH 38	Person leaves train intentionally (excl. passenger exchange)
SPH 39	Person falls out of (side) door
SPH 40	Person falls out of door in end wall
SPH 41	Train leaves/ rolls with open doors (uninfringed CE)
SPH 42	Person falls in gangway area between two cars
SPH 43	Passenger leans out of door
SPH 44	Passenger leans out of window
SPH 45	Staff/ train attendant leans out of door
SPH 46	Staff/ train attendant leans out of window
SPH 47	Shunting staff on vehicle leaning out from step
SPH 48	Person falls/climbs from platform into gap between vehicle and platform
SPH 49	Person falls out of/ leaves train without presence of platform
SPH 50	Person falls in door area at passenger exchange
SPH 51	Train doors close with person in door area
SPH 52	Train moves during passenger exchange
SPH 53	Possibility of person hurt in train
SPH 54	Fire/ explosion hazard (in/ at train) - accident category, Consequence of SPH 55, SPH 56)
SPH 55	Inappropriate temperature (in train)
SPH 56	Intoxication/ asphyxiation (in/ at train)
SPH 57	Electrocution (in/ at train)
SPH 58	Person falls on platform (excluding passenger exchange)
SPH 59	Inappropriate temperature (on platform)
SPH 60	Intoxication/ asphyxiation (on platform)
SPH 61	Electrocution (on platform)

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu