European Railway Agency

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

Reference in ERA:	ERA/GUI/01-2008/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 3	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: *"Guide for the application of 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 0.2 03/09/2008	Dragan JOVICIC	All	Update of the document in compliance with: • the CSM Regulation of the European Commission {Ref. 2}; • 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. 2} 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

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. This guide provides information on 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 Directive 2004/49/EC of the European Parliament and the Council" {Ref. 2}. That regulation will be referred to in the present document as the "CSM Regulation".

0.1.2. This guide does not contain any legally binding advice. It contains explanatory information of potential 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 Regulation. It may serve as a clarification tool without however dictating in any manner compulsory procedures to be followed and without establishing any legally binding practice. The guide provides explanations on the provisions contained in the CSM Regulation and should be helpful for the understanding of the approaches and rules described therein. Actors may continue to use their own existing methods for the compliance with the CSM Regulation.

0.1.3. The guide needs to be read and used only as a non binding informative document and to help with the application of the CSM Regulation. It should be used in conjunction with the CSM Regulation to facilitate its application but it does not replace it.

0.1.4. The guide 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 guide to reflect the progress with the European standards, the changes to the CSM 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 the guide.

0.2. Outside the scope

0.2.1. The guide does not provide guidance on how to organise, operate or design (and manufacture) a railway system or parts of it. Neither does it define the contractual agreements and arrangements that can exist between some actors for the application of the risk management process. The project specific contractual arrangements are outside the scope of the CSM Regulation, as well as of the associated guide.

0.3. Principle for this guide

0.3.1. Although the guide may appear to be a standalone document for reading purposes, it does not substitute the CSM Regulation {Ref. 2}. For ease of reference, each article of the CSM Regulation is copied in the guide. Guidance is then provided in the following paragraphs to help provide understanding where this is considered necessary.

---

(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

0.3.2. The articles and their underlying paragraphs from the CSM Regulation are copied in a text box in the present guide 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 from the additional explanations provided in this document.

0.3.3. The structure of this document is mapped on to the structure of the CSM Regulation 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 guide and provides the list of reference documents;
(b) explanation of the articles of the CSM Regulation;
(c) Annex I: explanation of the process in the CSM Regulation;
(d) Annex II: the criteria that must be fulfilled by the assessment bodies.

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}	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. 3}	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. 4}	Safety Management System - Assessment Criteria for Railway Undertakings and Infrastructure Managers	SMS Assessment Criteria Part A Safety Certificates and Authorisations	31/05/2007
{Ref. 5}	Commission Decision on the adoption of a common safety method for the assessment of achievement of safety targets, as referred to in Article 6 of Directive 2004/49/EC of the European Parliament and of the Council	xxxx/yy/EC	voted by RISC on 25/11/2008
{Ref. 6}	/		

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

0.6. 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.

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 present "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. 2}

Table 4: Table of abbreviations.

Abbreviation	Meaning
CSM	Common Safety Method(s)
CST	Common Safety Targets
EC	European Commission
ERA	European Railway Agency
IM	Infrastructure Manager(s)
ISA	Independent Safety Assessor
MS	Member State
NOBO	Notified Body
NSA	National Safety Authority
ORR	(UK) Office of Rail Regulation
RISC	Railway Interoperability and Safety Committee
RU	Railway Undertaking(s)
RAC-TS	Risk Acceptance Criterion for Technical Systems
SMS	Safety Management System
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] Article 6(3)(a) of the Railway Safety Directive {Ref. 1} states that: "*The CSMs shall describe how the safety level, and the achievement of safety targets and compliance with other safety requirements, are assessed by elaborating and defining risk evaluation and assessment methods*".

[G 2] The CSM Regulation describes only how the safety levels and compliance with other safety requirements are assessed and met. The Railway Safety Directive {Ref. 1} mentions also the *"achievement of the safety targets"* in Article 6(3). The methods related to the assessment of the achievement of common safety targets (CST) at national level are based on a statistical evaluation of past safety performance of national systems and as such are different from the methods to assess the safety levels and the compliance with safety requirements. Those methods for assessing the achievement of the CST are subject of a separate "Commission Decision on the adoption of a common safety method for the assessment of achievement of safety targets, as referred to in Article 6 of Directive 2004/49/EC of the European Parliament and the Council" {Ref. 5}.

[G 3] The process of "risk evaluation" is considered, in both the CSM Regulation and the present guide, as being part of the overall "risk assessment process". Therefore, unless explicitly required (e.g. need for a quantitative risk evaluation), the words "risk evaluation" are not used in these two documents.

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] The risk management and risk assessment processes referred to in the CSM Regulation and in Figure 3 relate to the processes that are put in place for assessing the safety levels and the compliance with the safety requirements of a significant change. They are therefore only a part of the overall risk management and risk assessment process of the railway

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

undertakings' and infrastructure managers' safety management system. Section 1.1.1 in Annex I provides the overall risk management framework which is covered by the CSM Regulation. The CSM Regulation also sets out a harmonised decision process for assessing the significance of changes: see Article 4.

[G 2] By virtue of Article 2 (1), the risk management and risk assessment processes of the CSM cover safety risks related to technical, operational and organisational changes of railway systems. They do not deal with other project risks such as for example the management of financial risks or of risks to miss project deadlines.

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 helps the actors to meet the requirements in Annex III(2)(d) of the Railway Safety Directive {Ref. 1} related to the RU and IM safety management system. The relevant assessment criteria produced by the Safety Cert team of ERA for railway undertakings and infrastructure managers related to these requirements are set out below (*extracted from {Ref. 4}*):

ABSTRACT/DESCRIPTION
d.0 Railway organisations must have a system in place to control changes/new projects and manage related risks, taking into account also those relating to occupational safety[2]*.* *Changes can apply to* • *technique/technologies;* • *operational procedures/rules/standards;* • *organisational structure.* *The SMS needs to ensure that the CSMs on risk assessment, developed according to Article 6(3)(a) Safety Directive, are applied where appropriate.*
ASSESSMENT CRITERIA
d.1 The RU/IM has processes and criteria in place to recognise changes in equipment, procedures, organisation, staffing or interfaces.
d.2 The RU/IM has processes to assess the level of impact of changes to decide whether to apply the CSMs on risk assessment.
d.3 The RU/IM has processes to ensure risk assessment and identification of control measures.
d.4 The RU/IM has processes to monitor the implementation and effectiveness of control measures.
d.5 There are processes/measures in place to assess with other organisations (IM, other RUs, third parties, etc) interface risks introduced by changes.
d.6 The results of the risk analysis are visible to all relevant staff and there are processes in place to feed these results into other processes within the organisation.

(2) *Ref.: Directive 2004/49/EC, Recital (14)*

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 application of the CSM enables the railway undertakings and infrastructure managers to fulfil the assessment criteria d.2, d.3 and d.5. It does not address and does not deal with the fulfilment of the assessment criteria d.1, d.4 and d.6 (compliance with d.1 and d.6 criteria enables to demonstrate compliance with the SMS).

[G 3] When a change is categorised as significant, the risk assessment needs to focus only on the safety related functions and interfaces of the system under assessment that is or could be affected by the change. The analysis and assessment of what is not safety-related can be limited to the demonstration that it does not impact the safety related functions and interfaces of the system under assessment. This principle of focussing the risk assessment efforts on the safety related functions and interfaces can be extended to all further phases of the system development process.

[G 4] For the significant changes, the risk assessment is not limited only to the changes but includes also the assessment of all the interfaces with other sub-systems and/or components that could be affected by the change(s). The assessment does not need to be extended to the unchanged parts or functions of the existing system, as they are already proven to be safe in use. However, the CSM needs to demonstrate the correct integration of the system under assessment with the unchanged parts or unchanged functions of the existing railway system. The risk assessment enables then to provide evidence that the changes do not make the system under assessment less safe.

[G 5] The risk assessment process described in the CSM Regulation applies only to significant changes of the railway system. According to Article 2 (4) the CSM Regulation does not apply to systems and changes under implementation and safety acceptance at the date of entry into force of the CSM Regulation.
If a change is assessed to be non significant, based on the criteria in Article 4, the risk assessment process of the CSM Regulation does not need to be applied.

[G 6] By virtue of Article 5 (2) of the CSM Regulation, Article 4 and Annex III of the Railway Safety Directive {Ref. 1}, the CSM does not apply at the Member State level for changes to their internal organisation. The MS political decisions related to the railway system are put in place by infrastructure managers and railway undertakings. The IM and RU are responsible for applying the CSM Regulation and for putting in place the necessary risk control measures in cooperation with each other, where appropriate, that are needed to fulfil the MS decision.

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.

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] By virtue of Article 4 (2) of the Railway Safety Directive {Ref. 1} and Article 15(1) of the Railway Interoperability Directive {Ref. 3}, for a significant change a system approach and a risk assessment is necessary to ensure a safe integration and operation of the structural sub-systems covered by TSI within the system.

[G 2] The TSI sets out the technical requirements for the interoperability of the sub-system(s) but not necessarily all the safety requirements (see recital (7) of the Railway Safety Directive {Ref. 1}) which are needed for a safe integration of sub-systems or components within a complete railway system. A system based approach, supported by a harmonised risk assessment, enables the correct identification of all the additional (safety) requirements necessary for a safe integration.

[G 3] If the application of the CSM leads to a requirement non compliant with the TSI, the proposer could analyse at first if the system definition can be changed in order to allow compliance with the TSI. If and only if this cannot be done the provisions of Articles 6(2) or 7 and Article 9[i3i] of the Railway Interoperability Directive {Ref. 3} may be used to allow the Member States not to apply the TSI. The proposer shall then inform the Member State concerned which may decide:

(a) to ask for a revision of the relevant TSI in accordance with the Articles 6(2) or 7 of the Railway Interoperability Directive {Ref. 3}, or;
(b) to ask for a derogation in accordance with Article 9 of the Railway Interoperability Directive {Ref. 3}.

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] The CSM is applicable in a Member State as defined by the transposition of the Railway Safety Directive {Ref. 1} into national law.

[G 2] Although the networks or infrastructures listed in Article 2 (3) are be exempted from compliance with the CSM, the CSM must be applied to Rolling Stock that circulates both on those networks and on the same tracks as the conventional trains.

(3) Extract of text from the Article 9 of the Railway Interoperability Directive {Ref. 3}: *"for any proposed renewal, extension or upgrading of an existing line, when the application of"..."one or more TSIs"*, including those relating to rolling stock,*"..."would compromise the economic viability of the project and/or the compatibility of the rail system in the Member State", the "Member State need not apply"... "those TSIs"*

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] The CSM is not applicable to systems and changes already started and well advanced at the date of entry into force of the CSM Regulation: see CASE 3 in Figure 3. It is assumed that the proposer continues to apply their methods in place for risk assessment until these are superseded by the CSM Regulation (see Figure 2).

[G 2] Any change performed after the entry into force of the CSM needs to be assessed in compliance with the CSM Regulation (see Article 4 (2) including point (f) in Article 4 (2)).

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)*;*

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

(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;

(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] When a definition in the CSM Regulation refers to an existing standard, the link to the relevant standard is also provided in the definition in the present guide.

[G 2] In addition to those definitions from the CSM Regulation, the following definitions may be interesting for the understanding of the guide:

(a) 'contracting entity' in Article 2(r) from the Railway Interoperability Directive {Ref. 3} *"means any entity, whether public or private, which orders the design and/or construction or the renewal or upgrading of a subsystem. This entity may be a railway undertaking, an infrastructure manager or a keeper, or the concession holder responsible for carrying out a project"*;

(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

(b) 'staff competence' can be described as a combination of knowledge, skills and practical experience which a person has to have to be able to do a particular task properly. This includes not only the routine task, but also covers unexpected situations and changes:

In the scope of the CSM Regulation, this definition refers to the "ability of a person" or, when dealing with staff or team competence, the "ability of a team of persons" to carry out properly for the system under assessment the different tasks that are required by the CSM risk assessment and risk management process. This implies that in order to do properly a considered task, the person or the team of persons shall be competent both within:

(1) the technical, operational or organisational field the person is assessing, and;
(2) the risk assessment process, the methods and tools the person is using (e.g. PHA, HAZOP, Event Trees, Fault Trees, FMECA, etc.). Refer also to section 1.1.4 in Annex I.

For railway undertakings and infrastructure managers, the competence management system for the staff to perform properly their tasks are covered by the compliance with the requirements of the Annex III(2)(e) of the Railway Safety Directive {Ref. 1}.

The competence management system, as well as all the other basic elements of the RU and IM SMS, will be accepted by an NSA, in compliance with Articles 10(2)(a) and 11(1)(a) of the Railway Safety Directive {Ref. 1}. Therefore, in the scope of the check of the correct application of the CSM, the assessment body will take it into account.
For the other actors, the SMS is not obligatory. Therefore, they need to demonstrate to the assessment body their staff competence to carry out the safety assessment tasks for the part of the system under assessment that is under their responsibility.

(c) 'expert judgement" is where the considered expert is competent to make decisions that are suitable and sufficient for the situation or task that the expert is performing. Experts making judgements will need to be fully competent in the environment in which they operate, which means that they can make responsible and reasonable judgements, based on the information provided and the sources, expertise and knowledge available.

(d) 'sub-system' does not refer to the structural and functional sub-systems that are listed in Annex II of the Railway Interoperability Directive {Ref. 3}. By analogy with the definition 3.1.61 in the CENELEC EN 50129 standard, the term 'sub-system' designates in this Guide "a part of the system under assessment which fulfils a specialised function".

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] The first check should assess whether the change is safety related or not. If the change is safety related, the other criteria Article 4 (2) can then be used to evaluate whether the change is significant or whether it is not significant. This is illustrated in the flow chart in Figure 1. The failure consequence criterion could be used for example to check whether the consequences of any safety relevant failure of the change to the system under assessment are mitigated by existing safety measures outside the system under assessment. This

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

criterion, in combination with the other ones, may then allow the judgement that a safety related change could still be managed safely without using the CSM. It is the responsibility of the proposer to determine which importance should be given to each of these criteria for the assessed change.

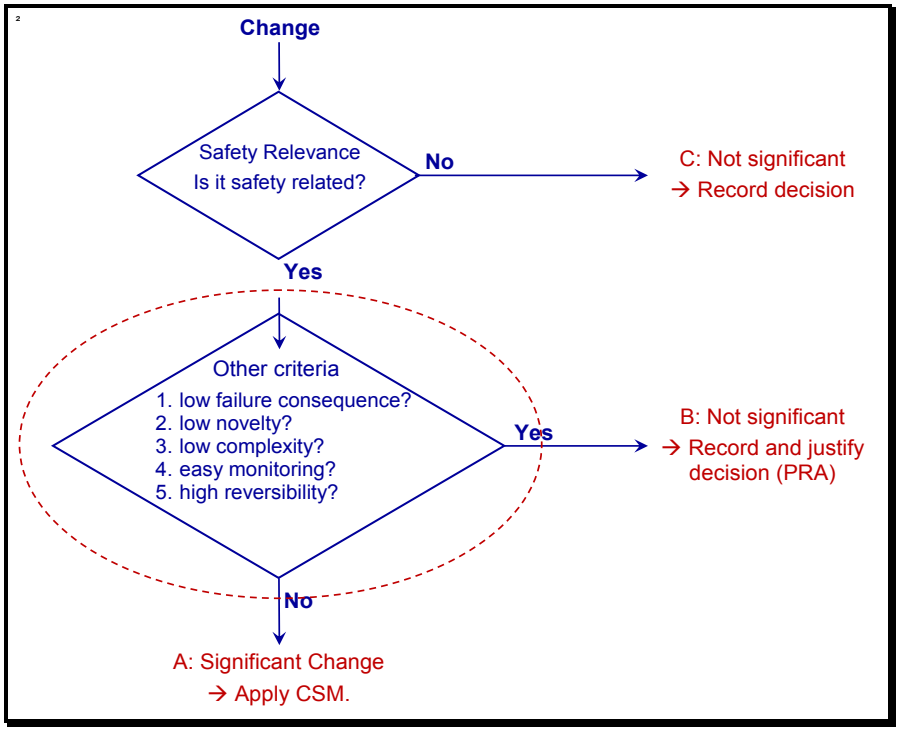

Figure 1 : Use of criteria in Article 4 for assessing the significance of a change

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.

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] All the criteria in Article 4 (2) for assessing the significance of a change should be analysed by the proposer but the proposer could take the decision based on only one or some of those criteria.

[G 2] Indeed, many safety-related changes, evaluated on basis of these criteria are likely to be categorised as non significant changes. But when looking at each change, it is important that all of the consecutive non significant changes "taken together" do not become a significant change that requires the application of the CSM process.

[G 3] When evaluating a set of several successive (non significant) changes, combinations of all types of changes made since the last safety acceptance need not be considered. Only the safety related changes that contribute to a same hazard in the risk analyses need to be taken into account.

[G 4] The reference point for evaluating the "sum of non significant changes" made to a system already in use is the latest date of the following (refer also to CASES 4 and 5 in Figure 2):

(a) either the entry into force of the CSM;
(b) or the last safety acceptance of the related system according to Article 7.

By virtue of Article 2 (4), the CSM is not retrospective: refer to CASES 1 and 2 in Figure 2. It does not require retrospective assessment of changes made prior to the CSM adoption. It is assumed that the proposer continues to apply the methods in place for risk assessment until those methods are superseded by the CSM.

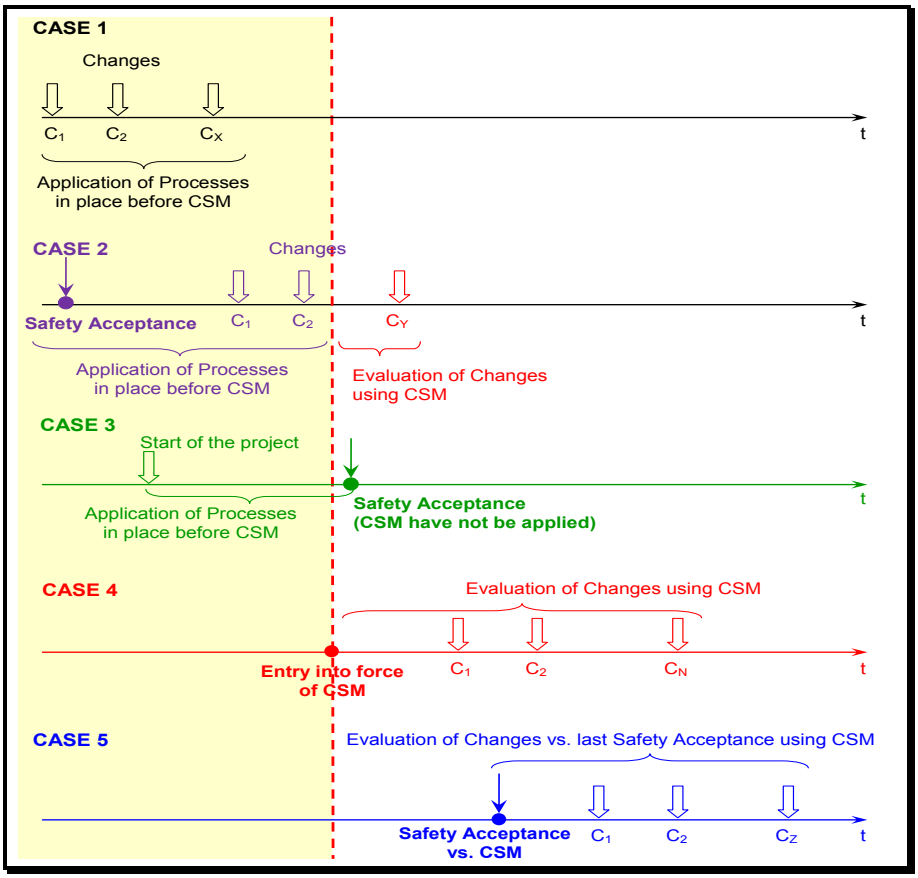

Figure 2: Safety related changes vs. entry into force of CSM.

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 5] The CSM does not require that the assessment body checks the evaluation of the significance of the change: refer also to points [G 1] and [G 2] in section 1.1.7. Nevertheless, the CSM requests to document the decisions on the significance of all changes in order to enable the NSA to fulfil their responsibility to monitor the application of the CSM Regulation: see Article 8 (2).

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] This paragraph summarises the different cases where the CSM process shall be applied. The articles referred to in Article 5 (1) request the proposer to apply the CSM process to significant changes and to keep adequate documentation to justify his decision: see also the explanations of Article 4 (2) above.

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. Definition (11) of the proposer in Article 3 explains who can be the proposer.

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.

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] Sections 1.1.2(b) and 1.1.7 in Annex I require that the correct application of the CSM is independently assessed by an assessment body before the acceptance by the proposer of a significant change. The activities of the assessment body in the CSM are identified in the relevant sections of the CSM Regulation.

[G 2] Without prejudice to contractual obligations (see section § 0.2.) or to the legal requirements(6) in the Member State, the proposer is free to appoint its own assessment body. The assessment bodies can be national safety authorities (NSAs), notified bodies (NOBOs) as well as external or in-house independent safety assessors (ISAs) if they fulfil the criteria in Annex II.

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] In the scope of management of the assessment body activities, the proposer, or its contractors, should take care to minimise the possible overlaps between the checks that can be performed by different assessment bodies, as well as to ensure, when necessary, an exchange of information between the relevant 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] This paragraph summarises the different cases from the Railway Safety Directive {Ref. 1} and Railway Interoperability Directive {Ref. 3} where the NSA is responsible to provide the needed authorisation or certificate.

(6) *In some Member States, legally some assessments are already to be carried out by defined actors, e.g. by the NSA. In such a case and for the relevant parts, the appointment of the assessment body is not free. The national rules are to be applied.*

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] Article 6 (1) allows the proposer to appoint any assessment body, who fulfils the criteria in Annex II, to check the correct application of the CSM process for the system under assessment. This is without prejudice to contractual obligations or to any relevant legal requirements in the Member State. In order to reduce duplication of checks and costs, if he so wishes, the proposer may decide to ask the NSA whether they would agree to act as the independent assessment body. This would be in addition to their tasks under Article 6 (3) of the CSM. The NSA is free to accept or refuse the task to act as an assessment body, unless it is required by Community or national legislation. If they refuse, the proposer will have to appoint another independent assessment body. The NSA will remain responsible for the tasks required under the Railway Safety Directive and Railway Interoperability Directive

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] In addition to the authorisation required for placing in service structural sub-systems, the NSA may also perform the checking of the correct application of the CSM process to the structural sub-system. By analogy with Article 6 (3) above, the same kind of explanation as the one already provided in that article are also valid for Article 6 (4).

Article 7. Safety assessment reports

Article 7 (1)

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

[G 1] The purpose of the safety assessment report is to support the proposer in the acceptance of the significant change. Without prejudice to the legal requirements in the Member State, the proposer remains nevertheless responsible for the acceptance of the change within the system under assessment.

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.

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] By virtue of Article 5 (1), TSI may request risk assessments to be performed. The notified bodies have the responsibility to assess the conformity of the system under assessment to the requirements of the applicable TSI. If notified bodies do not fulfil the criteria in Annex II of the CSM Regulation for performing the independent assessment of the correct application of the CSM, they could subcontract the assessment work to another assessment body who meets those criteria. In this case:

(a) the notified bodies will have to check that the tasks of that other assessment body are duly performed;
(b) the assessment body who performs the assessment work has to deliver its conclusions to the notified body or to the contracting entity within an independent safety assessment report. That report will support the notified body to provide its conclusions on the compliance with the considered TSI.

[G 2] By virtue of Article 6 (2), independently on whether the notified body will perform the work himself or whether he will subcontract it to an assessment body, duplication of work shall be avoided.

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] Member States and assessment bodies have to apply the principle of mutual recognition on the risk assessments that are evaluated in compliance with the CSM. Such a mutual recognition is to be based on the harmonised evidences that are produced during the risk management and risk assessment activities covered by the CSM.

[G 2] If for a railway system the following is done in a Member State:

(a) the risk assessment of the system is compliant with the CSM;
(b) the application of the CSM is assessed by an assessment body, and;
(c) the system is accepted by the proposer (see Article 7 (1));

assessment bodies in other Member States have to apply the principle of mutual recognition to this risk assessment. The system can therefore be used in other Member States without additional risk assessments and checks provided the related proposer demonstrates that:

(d) the system will be used under the same functional, operational and environmental conditions as the already accepted system in the original Member State, and;
(e) the same risk acceptance criteria are applied for controlling the identified hazard(s) as the ones that are applied in the concerned Member State for controlling the same hazard(s), or are considered as acceptable in that Member State.

[G 3] If a condition is not fulfilled in point [G 2] of Article 7 (4), the mutual recognition principle cannot be applied automatically; additional assessments by the proposer are therefore necessary. The difference needs to be considered as a deviation with respect to the system already accepted. If the application of Article 4 (2) shows that this deviation can be considered as a significant change when compared to the accepted system, the deviation shall be assessed in compliance with 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 4] Then the assessment body in the considered Member State is to:

(a) perform an independent assessment of the correct application of the CSM on the identified deviations with respect to the system already accepted;
(b) apply the principle of mutual recognition for the part of the system and its risk assessment which fulfils the conditions in point [G 2] of Article 7 (4).

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.

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] To support the NSA in this task and to provide advices on how to report the experience on the CSM Regulation, the Agency is revising the template of the annual report. The template will be given to the NSA.

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 (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] The Agency shall in relation to this matter collect information about the difficulties encountered by different actors who are applying the CSM. To do this, the Agency could consult, with the support of the NSA, the persons directly responsible for the CSM application. The purpose is to take into account in the future revision of CSM the difficulties that could be encountered during the first applications of the CSM.

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] The analysis of the overall effectiveness of the CSM Regulation will include among others the examination of the cases where the risk acceptance criterion for technical systems (RAC-TS) has been applied and the feedback from independent safety assessments.

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 CSM are applied at the beginning of the project to ensure that all applicable hazards are identified and managed using hazard records (see section 4).

[G 2] The risk management framework for the CSM and the associated risk assessment process are illustrated in Figure 3. Each box/activity of this figure is described in a specific section of this guide.

[G 3] The iterative risk management process covered by the CSM is completed when it is demonstrated (refer to section 3) and documented in the hazard record that the system under assessment complies with:

(a) the safety requirements that are issued from the risk assessment;
(b) the safety requirements that could be identified during the demonstration of the system compliance with the point (a) above.

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

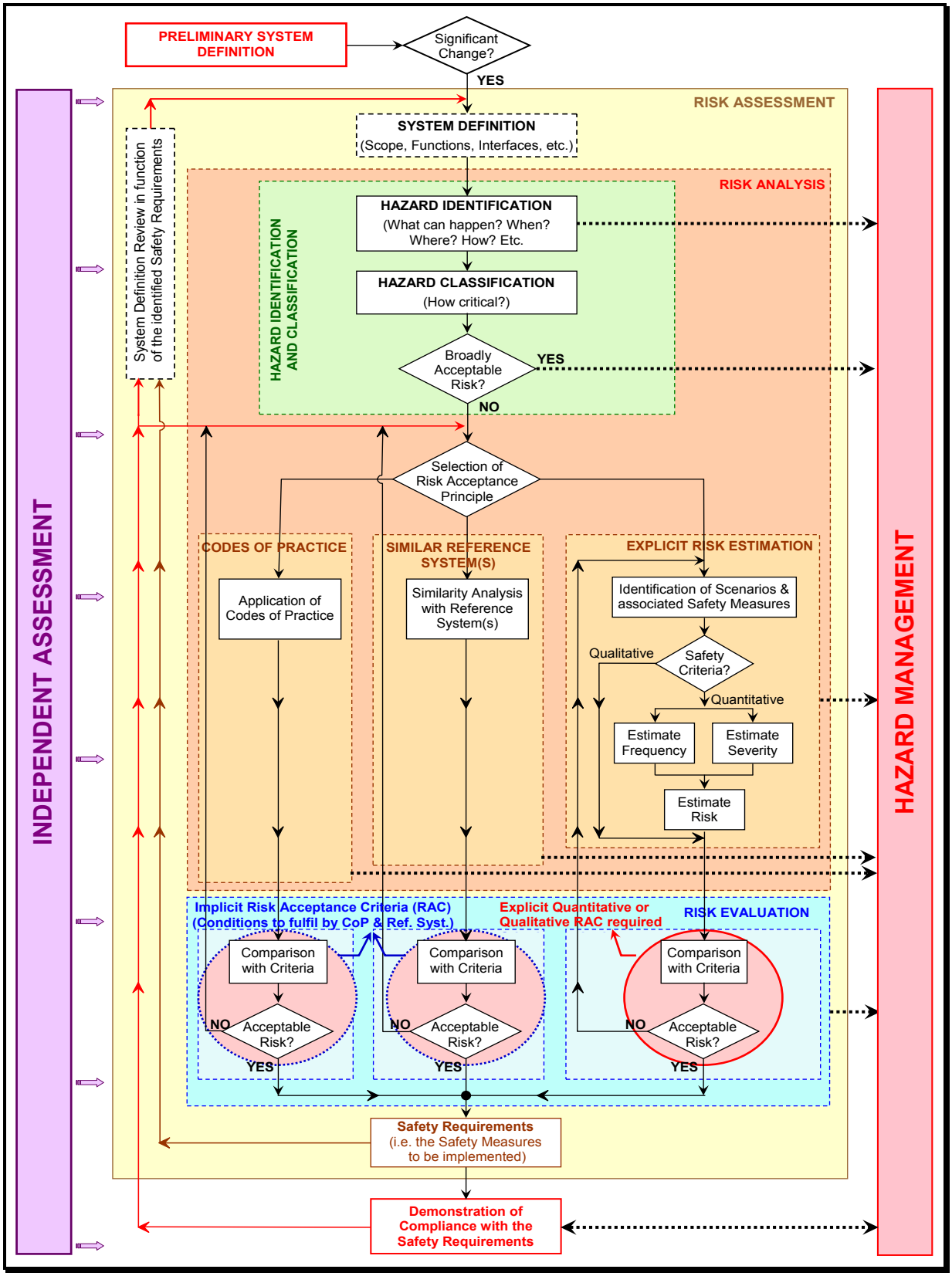

Figure 3: Risk management framework in the CSM Regulation {Ref. 2}.

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 application of the risk assessment process is triggered by a change that is categorised as significant (see Figure 3). The iterative risk management process finishes with the acceptance by the proposer of the significant change based on the safety assessment report provided by the assessment body for the system under assessment (see Article 7 (1)). After that, if during the system operation and maintenance another change appears necessary, the significance of the change needs to be considered. If the change is deemed significant, the CSM needs to be applied for that new change.

[G 2] A definition for "staff competence" is given in point [G 2](b) in the explanation of Article 3.

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.

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] According to recital (4) in the Railway Safety Directive {Ref. 1}, *"safety levels in the Community Rail System are generally high … It is important that safety is at the very least maintained during the current restructuring phase…"*. Actors who already have methods in place for risk assessment can continue to apply them as long as they are compatible with the provisions laid down in the CSM Regulation. Any risk assessment process already in place and not compliant with the CSM will need to be revised to ensure that it meets the requirements of the CSM.

[G 2] The terms "methods or tools" refers to "processes, techniques or tools" (e.g. HAZOP, PHA, Event Trees, Fault Trees, FMECA, etc.) which can be applied for meeting the requirements defined by the common process of the CSM. Therefore, as long as those processes, techniques and tools already in place are compatible with the provisions of the CSM they can continue to be used. Human factor analysis or human reliability analysis techniques and tools need also to be considered in this way.

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

1.1.5. 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] According to Article 5 (2), the proposer has to apply the risk management process described in the CSM. The definition (11) of the proposer in Article 3 explains who can be the proposer. By virtue of Article 5 (3), the proposer may request suppliers, service providers, including their sub-contractors, to participate in this risk management process as their activities may impact the safety of the railway system. Generally, the infrastructure managers and railway undertakings are the proposers, as they have the main responsibility for the operation of the railway system and the control of the associated risks. But contracting entities and manufacturers may also be considered as proposers:

(a) manufacturers may perform a risk assessment if they need an authorisation to place in service for a generic application or modifies significantly a rolling stock already authorised.
(b) maintenance suppliers may perform a risk assessment when changing their organisation or maintenance activities. This may include workshop activities where a maintenance certificate may be desired on a voluntary basis;
(c) keepers may need to perform risk assessment if they apply for a certificate for new rolling stock or if they modify significantly rolling stock already authorised.

[G 2] The other actors of the rail sector may also be concerned by the CSM as each of the actors referred to in point [G 1] of section 1.1.5 could ensure (via contractual arrangements) that the suppliers and service providers, including their sub-contractors, participate to the process described in the CSM.

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] The coordination of the safety activities at the interfaces between the collaborating actors is a key task to maintaining the safety level of the railway system.

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] For a significant change, section 1.1.2(b) requires the risk management process to be independently assessed by an assessment body in order to check that the process described in the CSM is correctly applied. The CSM does not require that the assessment body checks the evaluation of the significance of the change.

[G 2] If a change is assessed to be non significant, based on the criteria in Article 4:

(a) the risk assessment process of the CSM Regulation does not need to be applied;

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 correct application of the process described in the CSM does not need to be independently assessed by an assessment body.

[G 3] Without prejudice to contractual obligations (refer to section § 0.2.) or to legal requirements[7] in the Member State, each actor is free to appoint its own assessment body for the part of the system under assessment that the actor is responsible for. More than one assessment body can be involved in the same project. Depending on the project, there could be a need to coordinate the different assessment bodies. Usually, this is the responsibility of the proposer with the support of its assessment body.

[G 4] For the roles and responsibilities of the different assessment bodies, as well as the interfaces between them, refer to section 5 and Article 6 (1).

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] The separation of activities and/or functions between the various actors involved in the development and operation of railway systems (IM's, RU's, contractors, etc.) can result in residual risks at the interfaces. The management of these risks needs to be shared between all the actors involved at the related interfaces. This is necessary as residual interface risks are different from the type of risks which result from the activities carried out by the IM, RU or other actors (contractors; etc.) alone, who are directly responsible for their management and their control.

[G 2] Co-operation between all the involved actors is needed in order to ensure that the residual risks at the interfaces are addressed in a coherent way. This means that the hazards, the associated safety measures, and the resulting safety requirements are identified and agreed by all the concerned actors. The RU and IM have a key role in this process, as they have the system view and the responsibility for managing the environment in which trains operate. They are responsible for the overall control of the system risk. However, while the RU and IM can oversee and provide support to the other actors involved in managing the interfaces, each actor is responsible for carrying out correctly the activities and tasks in the CSM applicable to the sub-system(s) the actor is in charge of.

[G 3] The proposer who intends to introduce a significant change in the railway system needs to coordinate the management of shared risks at the interfaces. In particular the proposer will be in charge of allocating the responsibilities for the management of shared risks between the different actors concerned by the related interfaces.

(7) *In some Member States, legally some assessments are already to be carried out by defined actors, e.g. by the NSA. In such a case and for the relevant parts, the appointment of the assessment body is not free. The national rules are to be applied.*

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 described in sections 4, 4.1 and 4.2.

[G 2] According to section 4.2, the transfer of hazards and associated safety measures between those involved actors needs to be agreed by the relevant receiving actor. At the system level, as the proposer is responsible for the overall co-ordination and management of shared risks, the proposer needs to be kept informed about risk transfers between the different actors even if the proposer is not necessarily directly involved in controlling the related risks. This enables the proposer to communicate the information to other actors who could be impacted by the related risks through the interfaces.

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] During the assessment of the system, deviations from safety measures, or even inadequacy of safety measures, can be discovered. This means that the related safety measures (selected by the proposer according to section 2.1.6 to control the associated hazards and risks) are not adequate in controlling the associated risks. Section 3.4 explains that these deviations or inadequacies need to be considered as new inputs for a new loop in the iterative risk assessment process described in section 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] This paragraph relates to the detection of a non compliance or an inadequacy of a safety measure in controlling the associated hazard (see section 1.2.3). The actor responsible for the implementation of the related safety measure will need to inform all the other actors affected by this either within:

(a) the system under assessment. This enables another safety measure to be used to adequately control the associated hazard, or;

(b) within existing (reference) systems, provided the actor is aware that the same safety measure is used to control the same hazard. It is of prime importance that the RU and IM report to the manufacturers the safety related problems they encounter even after the warranty period of technical equipment. This information could enable the manufacturers to assess the related inadequacy on all other similar systems using the same safety measure, as well as to take appropriate actions for all other customers who could be impacted by this safety related problem.

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

1.2.5. 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.

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] The proposer who intends to introduce the significant change in the railway system is responsible for finding the adequate solution when agreement cannot be found either for sharing the risks at the interfaces or for transferring hazards and safety measures between actors.

[G 2] By analogy with the last paragraph in Article 2 (2), when a requirement in a notified national rule cannot be fulfilled by an actor, the proposer may ask the Member State for derogation.

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

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] See also section 2.2.5.

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] This article lists the minimum requirements to be addressed by the system definition. The assumptions that set out the limits for the system need to be exhaustively listed (see point (g)). These are registered in the hazard record in the same way as the safety requirements that are set out in the risk assessment. As the system assumptions determine the limits and the validity of the risk assessment, the risk assessment is updated or replaced by a new one if these assumptions are changed or revised.

[G 2] In order to enable the risk assessment to be done, the definition of the system needs also to take into account the context of the intended change:

(a) if the intended change is a modification of an existing system, the system definition needs to describe 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.

[G 3] The system definition is an important step in the risk assessment process. Initially, it specifies the system purpose, functions, interfaces and all the already existing safety measures inherent to the system. During the different iterations of the risk management and risk assessment processes, it is reviewed and updated with the additional safety requirements identified by the risk analyses.

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

2.1.3. 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.

[G 1] These three risk acceptance principles are already recognised as current possible practices for controlling hazards and the associated risks in railway systems.

[G 2] The possibility of using these three risk acceptance principles provides flexibility for the proposer to decide which one is the most appropriate depending on the specific requirements of the project. By virtue of Article 5 (1) and section 1.1.5 in Annex I, and without prejudice to the national law in the Member State, the proposer is free to use whichever of the three principles provided they are adequately applied to control the risks associated with the identified hazards. The assessment body could challenge the proposer, evaluate his choice of the risk acceptance principle for controlling an identified hazard (and the associated risk) and evaluate the correct application of the selected principle. But the assessment body should not call into question that choice if the risk is controlled to an acceptable level.

[G 3] The risk acceptance principles that are used need to be assessed by the assessment body.

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] This can be performed by the proposer at the end of the risk assessment process. The consistency check can consist in verifying that:

(a) the risk acceptance principles are correctly selected, i.e. that they can be used for controlling the corresponding hazards that are associated with risks that are not considered as broadly acceptable;
(b) the selected risk acceptance principles are correctly applied to the hazards that are associated with risks that are not considered as broadly acceptable. For example, if a standard is applied as a code of practice for controlling hazards, the compliance with the specific requirements from the standard needs to be checked;
(c) there is no contradiction or conflict between the safety measures being implemented by each individual actor involved in different aspects of the significant change;
(d) when the same risk acceptance principle is applied by different actors involved in the same project (e.g. the same code of practice), the principle is 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

2.1.6. 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] The risk assessment process will identify different possible safety measures that might be put in place either to eliminate the risk(s) or to control the risk(s) to an acceptable level (i.e. decrease the frequency of its occurrence or mitigate the consequences of the hazard). These safety measures could be technical, operational or organisational. The efficiency of the safety measures could be assessed quantitatively, where relevant, semi-quantitatively or qualitatively (e.g. use of trained drivers for controlling human factor errors). The proposer will decide the most appropriate ones to implement. The safety measures selected to control the identified hazards become the "safety requirements" and need to be included in an updated version of the "system definition": see section 2.1.2 and Figure 2.

[G 2] The coverage, the limits of validity and the efficiency of the safety measures chosen to control the identified hazards need to be clearly set out. Their wording needs to be clear and sufficient to understand the hazards and the associated risks they prevent/mitigate, without the need to go back into the related safety analyses.

[G 3] The demonstration that the system complies with the "safety requirements" issued from the risk assessment process is described in section 3.

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] The risk assessment can be considered as finished when the following conditions are fulfilled:

(a) all identified hazards and associated risks are evaluated;
(b) a consistency check is performed to ensure that the three risk acceptance principles have been correctly applied (see section 2.1.5);
(c) it has been verified that the safety measures taken to control the identified risks are adequate and that they do not create conflicts which could lead to new hazards that require reassessment;
(d) it is demonstrated that the system under assessment complies with the safety requirements": refer also to section 3;
(e) there are no additional safety relevant hazards that must be considered.

[G 2] If the demonstration shows that the system does not comply with all the safety requirements, i.e. some safety measures selected to control hazards are not implemented completely or correctly (see section 2.1.6), then:

(a) if another safety measure was identified for the related hazard, it can be selected as the new "safety requirement" for controlling the hazard, or;
(b) if there is a restriction of use, this is registered into the hazard record, or;
(c) if there was not any other identified restriction of use or safety measure, new safety measures need to be identified for controlling the associated risk to an acceptable level.

The system compliance with these new safety requirements needs also to be demonstrated as described in 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

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.

[G 1] It is very important that, at the considered level of detail[8], the hazard identification is complete and that hazards are neither forgotten nor wrongly classified to be associated with broadly acceptable risk(s)[9]. For the related level of detail, the following can be considered for the hazard identification:

(a) all the system modes of operation (i.e. nominal and degraded ones);
(b) the different circumstances of the system operation (main line, tunnel, bridge, etc.);
(c) the human factors;
(d) the environmental conditions;
(e) all relevant and foreseeable system failure modes;
(f) other potential factors that are safety relevant for the system under assessment.

This is of prime importance because if hazards are not identified, they are not mitigated and are not dealt with further in the risk management, risk assessment and hazard management processes.

[G 2] A definition for "staff competence" is given in point [G 2](b) in Article 3.

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] The classification of the identified hazards, at least into hazards associated with "broadly acceptable risk(s)" and hazards associated with risks that are not considered as broadly acceptable, enables the prioritisation of the risk assessment on those hazards that require risk management and risk control measures.

[G 2] The classification of hazards between these two categories is based on expert's judgement and will be done according to section 2.2.3.

[G 3] A definition for "expert judgement" is given in point [G 2](c) in Article 3.

---

(8) *As described in point [G 2] of section 2.2.5, the risk assessment is reiterated as many times as necessary until the (individual and/or the overall) risk(s) associated to all the identified (sub-)hazards of the last considered level of detail is(/are) acceptable with respect to the associated risk acceptance criteria.*

(9) *Refer to section 2.2.3 for the definition of "broadly acceptable 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

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] It is the responsibility of the proposer to evaluate whether the risk associated with each identified hazard is broadly acceptable, as well as to ensure that the assessment is performed by competent experts (see definitions in points [G 2](b) and (c) in Article 3).

[G 2] Given that a detailed risk quantification cannot always be possible during the hazard identification phase, in practice an expert judgement can enable to decide whether the considered hazard could be associated with a broadly acceptable risk in the following cases:

(a) either if the hazard frequency of occurrence is judged to be sufficiently low due to e.g. physical phenomena(10) (such as fall of meteorites on the track) regardless of the potential severity;
(b) or/and if the potential severity of the hazard consequence is judged to be sufficiently low, regardless of the hazard frequency of occurrence.

[G 3] 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), the proposer will take action to ensure that they are correctly classified at least into hazards associated with broadly acceptable risk and hazards associated with risks that are not considered as broadly acceptable. This will include measures to ensure that the contribution of all hazards associated with broadly acceptable risk(s) does not exceed a given proportion of the overall risk at the system level.

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] Additional explanation is not judged necessary.

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] The level of detail required for the hazard identification depends on the system to be assessed.

[G 2] As set out in Figure 3, the iterative risk assessment process starts with the system definition (see section 2.1.2) that is used as the basis for the hazard identification phase. "High level hazards", associated with "high level functions", can be considered first. Then:

(a) if the risks associated with these "high level hazards" are controlled to an acceptable level by safety measures covered within the system definition or by new identified

(10) *If the reason for the low frequency is that the hazard is incredible due to laws of physics, then the hazard and the argument for low frequency needs to be 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

ones[11], the hazard identification does not need to be continued further below this level, or;

(b) if some aspects of these "high level hazards" are not controlled either by safety measures existing in the system definition or by any new identified one, the hazard identification needs to be extended to a deeper level of detail[12] for the non controlled aspects.

[G 3] Therefore, the risk assessment process is repeated as many times as necessary until the overall system risk is controlled to an acceptable level and/or the risk associated with each identified hazard of the last considered level of detail[12] is acceptable with respect to the applied risk acceptance criteria or risk acceptance principles. Each time the risk assessment process is repeated, it could identify:

(a) either more detailed sub-hazards and related safety measures to put in place for accepting the associated risk(s);
(b) or new safety measures when the risk acceptance criteria are not met with the already identified safety measures.

[G 4] The safety requirements identified by the risk analyses are included in the system definition as additional (safety requirement) specification: see sections 2.1.2(f) and 2.1.6.

[G 5] The hazard identification phase is also necessary for the systems where (all) the hazards can be controlled either by the application of codes of practice or by comparison to similar reference systems. This enables:

(a) to check that the identified hazards can actually be controlled by the related codes of practice or similar reference systems;
(b) to support the mutual recognition of risk assessments as the safety requirements derived from the three risk acceptance principles are linked with the hazards they control;
(c) transparency in the use of codes of practice and in the assessment of their ability to control the identified hazards.

The hazard identification can be limited to high level hazards if relevant codes of practice or reference systems completely control the associated hazards.

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.

---

(11) *If the considered hazards can be controlled completely by the application of codes of practice or similar reference systems, further hazard identification is not needed. Demonstration of compliance with these newly identified safety measures (i.e. with the codes of practice or with the safety requirements derived from the reference systems) is sufficient for accepting the risk(s).*
In general deeper hazard identification is performed only for the hazards that cannot be fully addressed by these two risk acceptance principles: see point [G 5] in section 2.2.5.

(12) *In some literature, the terminology "indenture level" is used to designate the level of detail that is being considered within a structural approach. For example, the number of indenture levels in an assembly relates to how far in detail the considered assembly can be broken down.*

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] This requirement needs to be considered in the overall context of section 2.2 related to the hazard identification phase. It tells that when using codes of practice and reference systems, by virtue of sections 2.2.1 and 2.2.5, the hazard identification is necessary but it can be considered as complete, and thus the hazard identification needs not to be extended to a deeper level of detail, if the identified hazards are all controlled to an acceptable level by the selected codes of practice or reference systems.

[G 2] When using codes of practice and reference systems, the risk assessment consists then:

(a) to verify the relevance of the selected code of practice or reference system to adequately control the identified hazards;

(b) to identify possible deviations from the selected code of practice or reference system. Only if deviations are identified, the hazard identification will need to be extended to a deeper level of detail as explained in section 2.2.5. There will then be need of additional loop(s) in the iterative risk assessment process for controlling the hazards and the risks associated with those deviations.

[G 3] The requirement in section 2.2.6 does not permit to skip the hazard identification phase neither the next ones in the risk assessment process following the hazard identification phase. Compliance with the complete CSM process, including thus the fulfilment of the requirements in sections 2.3.8 and 2.4.3, has still to be demonstrated.

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] The evaluation of whether or not a code of practice controls one or several hazards may include:

(a) the check that the relevant part of the definition of the system under assessment is within the scope of the related code[(13)] of practice;
(b) the scrutiny of the gaps or differences between the definition of the system under assessment and the scope of the related code of practice by using other codes of practice or one of the other two risk acceptance principles;
(c) the comparison of design parameters for the system under assessment with the requirements of the considered code of practice. If the design parameters fulfil the requirements of the related code of practice, the associated risk(s) can be deemed acceptable;
(d) the registration of the application of a code of practice to controlling a hazard in the hazard record as the safety requirement for the related hazard.

[G 2] For any design parameter of the system not satisfying the requirements of the code of practice:

(a) if the design parameter can be changed to fit with the requirements of the code of practice, the system definition will need to be reviewed and the design parameter change assessed in compliance with the CSM;

(13) *For example, codes of practice used for controlling hazards identified on the mainline could differ from codes of practice used for "tunnel safety" or for "safety of dangerous good transport".*

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) if the design parameter cannot be changed, that needs to be considered as a deviation that will be dealt in compliance with section 2.3.6.

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] It is important that the "codes of practice" are composed of documents acceptable to the relevant assessment body.

[G 2] Codes of practice from other fields (e.g. nuclear power, military and aviation) can also be applied to railway systems for certain technical applications provided the concerned actor demonstrates that the related codes of practice are effective at controlling the related railway hazards.

[G 3] In the framework of the Railway Safety Directive {Ref. 1} and the CSM Regulation, the following may be considered as codes of practice:

(a) TSI and mandatory European standards;
(b) Notified National Safety Rules;
(c) Notified National Technical Rules (technical standards or statutory documents) and if relevant non mandatory European standards;
(d) provided the conditions in section 2.3.2 are fulfilled, internal rules or standards that are issued by an actor of the railway sector.

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] If it can be demonstrated for the system under assessment that the applicable TSI also enables the adequate control of one or more of the identified hazards, further risk analysis and safety measures are not needed for those related hazards.

[G 2] If the relevant TSI cannot fully control the identified hazards, other codes of practice or another risk acceptance principle need to be applied for controlling these hazards.

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.

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

2.3.5. 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] The hazards and associated risks that are covered by the application of codes of practice are implicitly considered as acceptable, provided the conditions of application of codes of practice in section 2.3.2 are fulfilled. This means that explicit risk acceptance criteria need not be defined for the hazards controlled by this principle.

[G 2] The demonstration that the system under assessment complies with the related codes of practice is performed according to section 3.

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] If one or more conditions from the code of practice are not fulfilled by the system under assessment, the related code of practice can still be used for controlling hazards provided the proposer demonstrates that at least the same level of safety is achieved.

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] This may also occur when it is discovered that the related code of practice does not sufficiently cover the identified hazards, e.g. the code of practice is not applicable to the full range of hazards. Then for these hazards either other codes of practice or one of the other two risk acceptance principles needs to be used for controlling the associated risks (see also point [G 1] in section 2.3.1).

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] This text summarises in one section the different requirements in the CSM Regulation that are to be fulfilled when all hazards of the system under assessment are controlled by codes of practice.

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. 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] Recital (4) of the Railway Safety Directive {Ref. 1} also encourages the application of similar reference systems for maintaining the safety levels of the Community rail system.

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] This sets out the conditions necessary in order to enable the control of one or several hazards of the system under assessment by the comparison with similar reference systems.

[G 2] Hazards could be identified where "similar reference systems" exist but, under specific circumstances, the comparison with those may not be sufficient to ensure the safety of the system under assessment. Therefore, it is of prime importance to ensure that the system under assessment is used under similar functional, operational and environmental conditions as the similar reference system. If this is not the case, another "similar reference system" or one of the other two risk acceptance principles can be used for controlling the risk to an acceptable level.

[G 3] If the safety requirements from a reference system are used for the system under assessment, it is necessary to check also that the reference system still *"qualifies for acceptance"* in the Member State where the intended change is being introduced. It can happen, for example, that the safety performance of the considered reference system is not appropriate for the system under assessment because it is based on out of date technology (i.e. old fashioned technology).

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] The hazards and associated risks that are covered by reference systems are implicitly considered as acceptable, provided the conditions of application of reference systems in section 2.4.2 are fulfilled. This means that explicit risk acceptance criteria need not to be defined for the hazards controlled by this principle.

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] Further risk analysis and risk evaluation are not required for the related hazards.

[G 3] The demonstration that the system under assessment complies with the safety requirements derived from reference systems is performed according to section 3.

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] In case of deviation from the reference system, the safety requirements for the hazards that are covered by the reference system can still be used. But it is necessary to demonstrate that the system under assessment reaches at least the same safety performance as the reference system. This may require also explicit risk estimation in order to show that the level of risk is at least as good as that of the reference system.

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] If the same level of safety cannot be demonstrated, or if the requirements in section 2.4.2 are not fulfilled, the safety measures derived for the system under assessment will be insufficient. The corresponding hazards need then to be considered as deviations from the reference system. These become new inputs for a new loop in the iterative risk assessment process described in sections 2.1.1 and 2.2.5. Additional safety measures can be identified by applying one of the other two risks acceptance principles.

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] In general explicit risk estimation and evaluation is used (see also point [G 2] in section 2.1.4):

(a) when codes of practice or reference systems cannot be applied to control fully the risk to an acceptable level. This situation will typically arise when the system being assessed is entirely new or where there are deviations from a code of practice or from a similar reference system;
(b) or when a design strategy is chosen that does not allow the use of codes of practice or similar reference systems because for example there is a wish to produce a more cost effective design that has not been tried before.

[G 2] The explicit risk estimation is not necessarily always quantitative. The estimation of risks can be quantitative (if sufficient quantitative information is available in terms of frequency of their occurrence and severity), semi-quantitative (if such quantitative information is not sufficiently

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

available) or even qualitative (e.g. in terms of process for management of systematic errors/failures, when quantification is not possible).

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] Points [G 1] in section 2.3.5 and [G 1] in section 2.4.3 explain that the risk acceptance criteria for the risks that are covered by the application of codes of practice and by comparison with similar reference systems are implicit.

[G 2] Explicit risk acceptance criteria will therefore only be needed for evaluating the risk acceptability when applying the explicit risk estimation.

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] This is one risk acceptance criterion for technical systems (RAC-TS) that could be used in explicit risk estimation. The CSM Regulation does not require the use of the 10^{-9} h^{-1} value in the RAC-TS for operational and organisational changes.

[G 2] Explanation of the RAC-TS terminology in section 2.5.4:

(a) *"Where hazards arise from failures of technical systems"* means that among the whole set of the scenarios identified by the explicit risk estimation, the RAC-TS applies only to the wrong side failures of technical systems that could potentially lead to catastrophic consequences.

(b) *"not covered by codes of practice or the use of a reference system"* mean that this is not a standalone criterion but is integrated into the risk assessment framework of the CSM. The RAC-TS applies to technical systems for which the identified hazards can neither be adequately controlled by the use of codes of practice nor by comparison with similar reference systems. For example, usually the RAC-TS will not need to be applied for mechanical parts or for the catenary sub-system where appropriate codes of practice enable to control 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) *"the following risk acceptance criterion shall apply for the design of the technical system"* means that the criterion will be a design target. It does not mean that this will be the actual safety performance of the related technical system on the field;

(d) *"For technical systems where a functional failure has a credible"* means that it must be likely that the particular failure of the technical system can result in an accident with catastrophic consequences;

(e) *"direct"* means in this context that no effective barriers exist that may prevent an accident due to the failure of the technical system. If the consequence does not directly result from the technical system failure, the impact of mitigating effects or safety barriers (e.g. a human action or another technical system preventing the accident) could be taken into account in the safety analysis;

(f) *"potential for"* means that when the failure of the technical system occurs, it can credibly result in a catastrophic consequence. This is a conservative assumption. In practice, when a failure of a technical system occurs the consequence (e.g. a train derailment) is not necessarily catastrophic;

(g) *"a catastrophic consequence,"* means an accident that causes more than one fatality;

(h) *"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."* Provided all the conditions here above are fulfilled and, the frequency of occurrence of the technical system failure demonstrated during the design is less than or equal to 10^{-9} per operating hour, then the associated risk is acceptable. Consequently, the risk does not have to be reduced further.
The operating hour relates directly to the function, which causes the failure mode. This relates to the cumulative operating times of the considered technical system.

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] A Member State who wants to apply a more demanding risk acceptance criterion than the one in section 2.5.4 shall notify a national safety rule in compliance with the provisions in Article 8 of the Railway Safety Directive {Ref. 1}. According to Article 8(7) of that directive, *"the Member State shall submit the draft rule to the Commission for examination, stating the reasons for introducing it"*.

[G 2] Article 8 of the Railway Safety Directive {Ref. 1} foresees that the justifications of the reasons for requesting a more demanding risk acceptance criterion and the draft safety rule are analysed by the Commission (which can ask the Agency for technical advice) in order to check whether *"the draft safety rule"* does not constitute *"a means of arbitrary discrimination or a disguised restriction on rail transport operations between Member States"*. A decision is then *"addressed to the Member State concerned ... in accordance with the procedure referred to in Article 27(2)"* of the Railway Safety Directive {Ref. 1}.

[G 3] The additional criteria that may be requested by the NSA in case of additional authorisations for placing in service vehicles have to be compliant with the Articles 23 and 25 of the Railway Interoperability Directive {Ref. 3}. Consequently, if a vehicle is already authorised in a Member State based on the risk acceptance criterion in section 2.5.4, the same vehicle shall not be refused in another Member State if it does not comply with the more demanding national safety rule in section 2.5.5: see also section 2.5.6.

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

2.5.6. 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] In order to fulfil these requirements, the following may be considered:

(a) the explicit risk analysis considers all relevant operational modes (both the nominal and degraded modes of operation) of the system under assessment;
(b) the results are presented in a format compatible to the risk acceptance criteria to enable the comparison of the assessed risk with the criteria;
(c) a demonstration is provided to show that all significant risk model parameters related to considered risks are taken into account;
(d) a "method" "capable" of performing a trade-off / impact analysis, based on expert judgement and review, with respect to the different "significant risk model parameters" is used for the explicit risk estimation and evaluation;
(e) all parameter choices and results are "comprehensively" documented and justified;
(f) the results are provided together with a sensitivity analysis for the main risk "contributors" in order to demonstrate that a moderate modification of the input parameters does not result in significantly different safety requirements;
(g) the results are documented with a sufficient level of detail to allow for cross-checks;
(h) where quantitative criteria are used the tolerable accuracy of the overall results is within one order of magnitude or all parameters used for the quantification are conservative.

[G 2] The way to determine the quantitative parameters for the system under assessment need to be supported by a well documented justification with appropriate arguments.

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] The application of the CSM specifies the safety requirements that are expected to control the hazards, and the associated risks, identified during the risk analysis phase in Figure 2. The system is then designed, validated and accepted against those safety requirements.

[G 2] Before the system safety can be accepted (see Article 7 (1)), the proposer needs to demonstrate that:

(a) the three risk acceptance principles are correctly applied for controlling the identified hazards and associated risks to an acceptable level: see section 2.1.5;
(b) the system is actually compliant with all specified safety requirements;

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] The proposer has the overall responsibility for coordinating and managing the demonstration of the system compliance with the safety requirements. However, the proposer does not necessarily carry out all the demonstration activities. In practice, each actor, including the proposer where relevant, demonstrates the compliance of the sub-system[(14)] it is responsible for with the following relevant safety requirements:

(a) the safety requirements allocated to the sub-system by the proposer as described in section 1.1.5;
(b) the safety requirements associated with the safety measures related to interfaces and transferred to the relevant actor by other actors in compliance with the section 1.2.2;
(c) the additional internal safety requirements identified in the scope of the safety assessments and safety analyses carried out at the sub-system level: see point [G 2] in section 3.2.

[G 2] In order to fulfil the safety requirements allocated to each sub-system in points (a) and (b) above, each related actor carries out safety assessments and safety analyses in order:

(a) to identify systematically all reasonably foreseeable causes contributing to the hazards at the level of the system under assessment which are associated with the safety requirements for the relevant sub-system.

These causes of hazards at the level of the system under assessment may then be considered as hazards at the sub-system level (with respect to the sub-system boundary).

(b) to identify safety measures at the sub-system level and resulting safety requirements expected to control these sub-system level hazards and the associated risks to an acceptable level. In practice, the considered actor can also use codes of practice,

(14) *At the system level, the proposer is responsible for demonstrating the system compliance with the safety requirements issued from the risk 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

similar reference systems or explicit analyses and evaluations at the sub-system level. The related actor will also demonstrate the compliance of its sub-system with these additional safety requirements identified at the sub-system level (see section 3.2).

[G 3] Therefore, each actor is responsible for both implementing the sub-system safety requirements and demonstrating the sub-system compliance with these safety requirements.

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] Sections 1.1.2(b) and 1.1.7 require that the risk management and risk assessment processes are independently assessed by assessment bodies. This needs to include the independent assessment of the demonstration of the system compliance with the safety requirements. The assessment body provides the results of the independent assessment to the relevant actor within an assessment report: see Article 7 (1).

[G 2] Without prejudice to point [G 3] in section 1.1.7, each actor will appoint an assessment body for the part of the system under its responsibility. This assessment body will independently assess the demonstration of the sub-system compliance with the safety requirements set out in section 3.2 as well as the approach chosen by the actor for that demonstration. Depending on the project, there could be a need to coordinate the different assessment bodies. Usually, this is the responsibility of the proposer with the support of its assessment body.

[G 3] The concerned actors will provide the evidence set out in section 5 to the assessment bodies.

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] If safety measures are found to be inefficient or inadequate, the associated risk is not controlled sufficiently (i.e. not controlled to an acceptable level). In such a case, there is not necessarily new hazard but the requirements in point [G 3] of section 3.4 are to be applied.

[G 2] New hazards may arise from the implementation of safety measures expected to fulfil the safety requirements: This could be due for example to the choice of a technical solution, not foreseen by the safety requirements, for the design of the system and its underlying sub-systems.

[G 3] These deviations and/or new hazards with the associated risks are to be considered as new inputs for a new loop in the iterative risk assessment process described in section 2.

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 requirement in section 4.1.1 identifies two steps for the hazard management process:

(a) until the acceptance of the system under assessment, the hazard record has to be managed by the proposer or other actors if so contractually arranged (refer to definition (8) of the actors in Article 3, as well as to point [G 2] in section 4.1.1;

(b) once the system has been accepted, the hazard record has to be maintained and managed further by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment. As explained below, the IM and RU hazard management process will be an integrated part of their safety management system.

[G 2] According to Article 5 (2), Article 5 (3) and the definition (11) of the proposer in Article 3, suppliers and service providers, including their subcontractors, could also ensure hazard record management if so required by contractual arrangements between them and the proposer. In that case, those actors will have and will manage their own hazard record for the part of the system under assessment that is under their responsibility. Independently on whether they or the proposer are managing the hazard record, the responsibility for the correctness of the information to be registered in the hazard record rests with the actor controlling the considered hazard.

[G 3] The basic element in Annex III(2)(g) of the Railway Safety Directive {Ref. 1} requires that the RU and IM safety management system contains *"procedures and formats for how safety information is to be documented and designation of procedure for configuration control of vital safety information"*. The assessment criteria produced by the ERA Safety Cert team in relation to this matter are set out below (extracted from {Ref. 4}):

ABSTRACT/DESCRIPTION

g.0 Organisations must define document and data control procedures, based on existing management systems; documents and records must be readily available for consultation and/or verification.

Measures to control vital safety information are important to maintain and improve safety performance within an organisation and also to allow for corrective actions to be taken promptly and efficiently.

RUs and IM, operating on a same network system, should have arrangements in place to ensure the correct exchange, duly documented, of all relevant safety information. They should develop and support the use of standardised protocols for formal communications concerning operation (train logs, traffic/operating restrictions etc.) as a useful means of harmonisation.

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

ASSESSMENT CRITERIA

g.1 The SMS has adequate processes to ensure that all relevant safety information are accurate, complete, appropriately updated and duly documented.

g.2 The SMS has adequate processes to:

- *format, generate, distribute and manage the control of changes to all relevant safety documentation;*
- *receive, collect and store/archive all relevant documentation/information on paper or by other means/registration systems;*
- *ensure that staff are formerly given all relevant and updated documentation and act upon it as necessary;*

g.3 The SMS has adequate processes to ensure consistency, coherence and comprehension of language/content.

g.4 RUs and IMs have arrangements in place to ensure that communication barriers don't arise, or are minimised; evidence should be provided of the use of standardised protocols/formats for safety related information and to document all relevant data.

[G 4] In relation to the requirements in Annex III(2)(g) of the Railway Safety Directive {Ref. 1}, the CSM Regulation identifies what information from the risk assessment process is to be considered as safety relevant and therefore is to be registered in the hazard record. The CSM hazard management process enables then the RU and IM to meet their SMS requirements for the safety relevant information issued by the CSM risk assessment process. The recording, management and control of other safety relevant information will be covered by other processes or procedures of the RU and IM SMS.

[G 5] By virtue of Article 2 (1), the hazard management is required in the CSM Regulation for technical, operational and organisational significant changes. If the change is not significant, the hazard management process is not required.

[G 6] A hazard management process based on hazard records enables therefore:

(a) the control of the exchange of safety requirements between the different actors involved in the significant change, as well as;
(b) the management of the status of the hazards under the actor's responsibility.

[G 7] For a significant change to an existing system already accepted but for which the hazard record did not exist, the hazard record needs to be created, updated and maintained for the part of the system that is changed.

[G 8] In general, when the organisation responsible for the system under assessment subcontracts an activity to another organisation, it may be asking too much to that organisation to keep a hazard record, especially if the subcontractor's structure/size is small or if its contribution to the overall system is limited. In such cases the concerned actors may agree at the beginning of the project who is the most appropriate to take on the responsibility for the overall management of the hazard record.
The use of one single hazard record enables also flexibility among co-operating organisations since at least one of them is responsible for the management of the common hazard record for 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 9] The hazard management process for railway undertakings and infrastructure managers can be part of their safety management system for recording and managing risks that occur

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

throughout the lifecycle of technical equipment, the operation and organisation of the railway system. It does not have to be an additional and separate process.

[G 10] Concerning the other actors, by virtue of the requirements in Annex III(2)(g) of the Railway Safety Directive {Ref. 1}, the RU and IM shall ensure that their sub-contractors maintain their safety related information or that the RU and IM do it by themselves. Therefore, the requirements for hazard management by those actors may be reflected in the contracts between the RU/IM and those other actors. If those actors have an existing hazard management system, this could be adapted to meet the requirements of the CSM Regulation.

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 hazard record shall contain at least the following information:

(a) all the hazards that the considered actor is responsible for, the associated safety measures, and the resulting safety requirements issued from the risk assessment process (see section 2.1.6);
(b) all the assumptions taken into account within the definition of the system under assessment (see point [G 1] in section 2.1.2). These assumptions determine the limits and the validity of the risk assessment. If they are changed or revised, the risk assessment needs to be updated or replaced by a new risk assessment;
(c) all the hazards and the associated safety measures received from other actors in compliance with the point [G 1] in section 2.1.2. These include all the assumptions and restrictions of use (also called safety-related application conditions) applicable to the underlying sub-systems, generic application and generic product safety cases that are produced by the manufacturers;
(d) the status of the hazards (i.e. controlled or open) and of the associated safety measures (i.e. validated or open).

All this information needs to be clearly registered in the hazard record with a sufficient level of accuracy for enabling the management of the hazard record.

[G 2] The tools and format that can be used for the hazard record are not imposed by the CSM Regulation. It is up to the proposer to decide how to fulfil the requirements in section 4 of the CSM Regulation.

[G 3] The hazard record is not simply a development tool. It needs to be updated and maintained by the IM/RU whenever necessary during the whole system life-cycle, in particular:

(a) whenever a significant change is made;
(b) whenever a new hazard is discovered or a new safety measure is identified;
(c) whenever a new hazard is identified during the operation and maintenance of the system after its commissioning, so that the hazard can be assessed in compliance with the CSM as to whether it represents a significant change;
(d) whenever it could be necessary to take into account accident and incident data;
(e) whenever the safety requirements, or the assumptions about the system, are changed.

[G 4] The validity of the information registered in the hazard record needs also to be checked whenever changes are made during the system operation and maintenance. With reference to point [G 1] in section 4.1.2, if a safety requirement, or an assumption or a restriction of use, is not fulfilled any more, it needs to be considered as a change. The change will need

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

to be evaluated according to Article 4 in order to determine whether it is significant. If the change is significant, it shall be handled in compliance with the CSM.

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] During the hazard management, it is possible that some hazards cannot be controlled, and the associated safety measures cannot be validated, in the hazard record by one actor alone. In such cases a process or procedure may be necessary in order to identify how these hazards can be controlled by the actors that are involved in the project. This may involve either:

(a) the various actors discussing and agreeing the outcome in order to control the related hazards and to validate the associated safety measures in the hazard record, or.
(b) the transfer of the related hazards and the associated safety measures into the hazard record of the actor responsible for implementing, verifying and validating them. For example, an operational procedure could be needed for mitigating a risk when there is not technical/design measure possible. This exchange of safety information complies with the requirement in the last paragraph of the abstract g.0 of the assessment criteria which is set out in point [G 2] of section 4.1.1.

[G 2] When a safety measure is not fully validated:

(a) a clear restriction of use (e.g. operational mitigation measures) needs to be elaborated and registered in the hazard record;
(b) as this restriction of use is a further or an alternative safety measure, its appropriateness to control adequately the risk needs to be justified;
(c) the restriction of use and the associated hazard and risk need to be exported or transferred to the actor responsible for implementing, verifying and validating that restriction of use (for example to RU if it is an operational constraint).

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 number of documents the proposer may produce for documenting the risk management process is not imposed by the CSM. It is up to the proposer to decide how to structure this documentary evidence: see point [G 1] in section 5.2. The purpose of the evidence from the risk management and risk assessment activities is to enable:

(a) the development of the change under assessment;
(b) independent assessment by assessment bodies;
(c) in case of any problem during the system life-cycle, to be able to go back into the associated safety analyses and safety records for understanding the reasons having lead to decisions: see point [G 4] in section 5.2;
(d) the reuse of the system under assessment as a reference system for other applications.

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] The term "document" in section 5.2 of the CSM is to be read as the documentary evidence produced by the application of the risk management process in the CSM rather than a "single physical document". Section 5.2 tells what the minimum documentary evidence is necessary to enable the assessment body (-ies) to check the correct application of the CSM. How to fulfil this requirement is not imposed. Freedom is left to each actor involved in the system under assessment to use its own structure for the documentation, specified by their internal quality management and safety management system/process (where relevant), provided that at least:

(a) the organisation put in place to carry out the risk assessment process is clearly set out beforehand;
(b) the experts involved in the risk assessment process have the proper competence. A definition for "staff competence" and "expert judgement" is given in points [G 2](b) and [G 2](c) in Article 3;
(c) the results of the different phases of the risk assessment process are clearly documented;
(d) the list of all the necessary safety requirements to be fulfilled, in order to control the risk at an acceptable level, is established.

[G 2] When evidence is not available, justifications need to be provided to and assessed by the assessment body.

[G 3] Once a project is completed, the outcomes of the risk management and risk assessment process will either be incorporated into the system or, if necessary, will become part of the risk control system for the RU and IM under their safety management 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

[G 4] During the system life cycle or the system operation, a number of significant changes may occur which would require the accompanying documentation to be reviewed, supplemented and/or transferred between different actors and organisations using hazard records. It is thus advised to keep and update, where necessary, the documentary evidence (see point [G 1] in section 5.2) resulting from the application of the CSM process in order to enable those further risk assessments to be conducted for the railway systems and their interfaces. Where relevant, the results of each system configuration used in operation will need to be put into the proposer's archives at least during the system life-time. Unless agreed differently in the contracts at the beginning of the project, the other involved actors could also have themselves to archive their respective risk and safety analysis results.

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