Agência Ferroviária Europeia
Exemplos de avaliações de risco e de algumas ferramentas possíveis para facilitar a aplicação do regulamento relativo ao Método Comum de Segurança (MCS)

Referência ERA	ERA/GUI/02-2008/SAF
Versão ERA	1.1
Data	06/01/2009

Documento elaborado por	Agência Ferroviária Europeia Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex França
Tipo de documento	Guia
Estatuto do documento	Público

	Nome	**Função**
Divulgação autorizada por	Marcel VERSLYPE	Director Executivo
Revisto por	Anders LUNDSTRÖM Thierry BREYNE	Chefe da Unidade de Segurança Chefe do Sector de Avaliação de Segurança
Escrito por (autor)	Dragan JOVICIC	Unidade de Segurança – Responsável do Projecto

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

INFORMAÇÕES SOBRE O DOCUMENTO

Histórico de alterações

Quadro 1: Estado do documento.

Versão Data	Autor(es)	Número de Secção	Descrição da modificação
Título e estrutura do documento antigo: *"Orientações de Utilização da recomendação relativa ao 1º Conjunto de MCS"*			
Orientações Versão 0.1 15/02/2007	Dragan JOVICIC	Todos	Primeira versão das "Orientações de Utilização" associadas à versão 1.0 do "primeiro conjunto de recomendações MCS". É igualmente a primeira versão do documento transmitida ao grupo de trabalho MCS para revisão formal.
Orientações Versão 0.2 07/06/2007	Dragan JOVICIC	Todos	Reorganização do documento para adequação à estrutura da versão 4.0 da recomendação MCS. Actualização por Processo Formal de Revisão pelo grupo de trabalho MCS sobre a versão 1.0 da recomendação.
		Todos	Actualização do documento com base em informações adicionais recolhidas em reuniões internas da ERA, no seguimento dos pedidos formulados pela *taskforce* e o grupo de trabalho MCS de desenvolver novos aspectos.
		Figura 1 :	Modificação do Figura que representa o "Quadro de gestão de riscos do primeiro conjunto de Métodos Comuns de Segurança" de acordo com os comentários de revisão e a terminologia ISO.
Orientações Versão 0.3 20/07/2007	Dragan JOVICIC	Apêndices	Reorganização de apêndices e criação de novos. Novo apêndice que junta todos os Figuras que ilustram e facilitam a leitura e compreensão do Guia;
		Todas as secções	Documento actualizado de modo a: • desenvolver tanto quanto possível as secções x existentes; • precisar o significado da "demonstração do cumprimento dos níveis e dos requisitos de segurança pelo sistema"; • criar uma ligação com o Ciclo em V CENELEC (Figura 8 e Figura 10 da norma EN 50 126); • precisar a necessidade de colaboração e de coordenação entre os diferentes actores do sector ferroviário cujas actividades possam ter um impacto na segurança do sistema ferroviário; • clarificar os dados (p. ex., registo de perigos e dossier de segurança) que irão provar junto dos organismos de avaliação a aplicação correcta do processo de avaliação dos riscos MCS; Documento igualmente actualizado de acordo com a primeira revisão na Agência.
Orientações Versão 0.4 16/11/2007	Dragan JOVICIC	Todas as secções	Documento actualizado no seguimento do Processo Formal de Revisão de acordo com os comentários recebidos sobre a versão 0.3 provenientes dos seguintes membros do grupo de trabalho dos MCS ou organizações e acordados com os mesmos em conversa telefónica: • Autoridades Nacionais de Segurança (ANS) da Bélgica, Espanha, Finlândia, Noruega, França e Dinamarca; • SIEMENS (membro da UNIFE); • Gestor de infra-estrutura da Noruega (Jernbaneverket – Membro da EIM);
Orientações Versão 0.5 27/02/2008	Dragan JOVICIC	Todas as secções	Documento actualizado de acordo com os comentários recebidos sobre a versão 0.3 provenientes dos seguintes membros do grupo de trabalho MCS ou organizações e acordados com os mesmos em conversa telefónica: • CER

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

Quadro 1: Estado do documento.

Versão Data	Autor(es)	Número de Secção	Descrição da modificação
			• ANS dos Países Baixos
		Todas as secções	Documento actualizado em conformidade com a versão assinada da recomendação MCS. Documento actualizado de acordo com os comentários da revisão interna da Agência formulados por Christophe CASSIR e Marcus ANDERSSON
		Todas as secções Apêndices	Renumeração de todos os artigos do documento de acordo com as recomendações Incluídos exemplos de aplicação das recomendações MCS.
Título e estrutura do novo documento: *"Exemplos de avaliações de risco e de algumas ferramentas possíveis para facilitar a aplicação do regulamento relativo ao Método Comum de Segurança (MCS)"*			
Guia Versão 0.1 23/05/2008	Dragan JOVICIC	Todos	Primeira versão do documento resultante da divisão da versão 0.5 das "Orientações de Utilização" em dois documentos complementares.
Guia Versão 0.2 03/09/2008	Dragan JOVICIC	Todos	Actualização do documento de acordo com: o Regulamento relativo ao MCS da Comissão Europeia {Ref. 3}; os comentários recolhidos no *workshop* de 1 de Julho de 2008 com os membros do Comité para Interoperabilidade e Segurança do Sistema Ferroviário (RISC); os comentários dos membros do grupo de trabalho MCS (ANS da Noruega, ANS da Finlândia, ANS do Reino Unido, ANS da França, CER, EIM, Jens BRABAND [UNIFE] e Stéphane ROMEI [UNIFE]
Guia Versão 1.0 10/12/2008	Dragan JOVICIC	Todos	Actualização do documento de acordo com o Regulamento da Comissão relativo ao MCS para a determinação e a avaliação dos riscos {Ref. 3} adoptado pelo RISC em reunião plenária de 25 de Novembro de 2008
Guia Versão 1.1 06/01/2009	Dragan JOVICIC	Todos	Actualização do documento de acordo com os comentários sobre o Regulamento relativo ao MCS formulados pelos serviços jurídicos e linguísticos da Comissão Europeia.

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

Índice

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

Lista de Figuras

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

Lista de Quadros

Nota : Devido a problemas de formatação as referências cruzadas e a numeração dos parágrafos estão alterados. Por favor não ter em conta este tipo de alterações porque não foram intencionais.

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. INTRODUÇÃO

0.1. Âmbito

0.1.1. O presente documento tem por objectivo clarificar o "Regulamento da Comissão relativo à adopção de um método comum de segurança para a determinação e a avaliação dos riscos, conforme referido no n.º 3, da alínea a) do artigo 6.º da Directiva 2004/49/CE do Parlamento Europeu e do Conselho" {Ref. 3}.No presente documento, o regulamento será designado "Regulamento relativo ao MCS".

0.1.2. O presente documento não é juridicamente vinculativo e o seu conteúdo não poderá ser interpretado como a única maneira de cumprir os requisitos do MCS. O presente documento visa completar o guia para a aplicação do Regulamento relativo ao MCS 0 no tocante à forma como o processo do Regulamento relativo ao MCS pode ser usado e aplicado. Fornece informações práticas adicionais, sem impor, de qualquer forma, procedimentos obrigatórios a serem seguidos e sem estabelecer práticas juridicamente vinculativas. Estas informações podem ser úteis para todos os actores(1) cujas actividades possam afectar a segurança dos sistemas ferroviários e que, de forma directa ou indirecta, têm de aplicar os MCS. O documento dá exemplos de avaliações de risco e fornece algumas ferramentas possíveis para ajudar na aplicação do MCS. Estes exemplos são dados apenas a título de exemplo e auxílio. Os actores poderão recorrer a métodos alternativos ou poderão continuar a usar os seus próprios métodos e ferramentas actuais para cumprirem o MCS, se os considerarem mais adequados.
De igual forma, os exemplos e as informações adicionais dados no presente documento não se esgotam em si mesmos e não cobrem todas as situações possíveis em que são propostas alterações significativas, por isso, o documento só pode ser considerado meramente informativo.

0.1.3. Este documento informativo deverá apenas ser lido como uma ajuda adicional na aplicação do Regulamento relativo ao MCS. Quando utilizado, este documento deve ser lido em conjunto com o Regulamento {Ref. 3} relativo ao MCS e com o guia associado 0, para facilitar a aplicação do MCS, mas em caso algum poderá substituir o Regulamento relativo ao MCS.

0.1.4. O documento foi elaborado pela Agência Ferroviária Europeia (ERA) com o apoio das associações ferroviárias e dos peritos das autoridades nacionais de segurança membros do grupo de trabalho MCS. Representa um conjunto desenvolvido de ideias e informações reunidas pela Agência em reuniões internas e reuniões com o grupo de trabalho MCS e as *taskforces* MCS. Sempre que necessário, a ERA procederá à revisão e actualização do guia para reflectir a evolução das normas europeias, as alterações aos MCS de avaliação dos riscos e a eventual experiência adquirida com a utilização do Regulamento relativo ao MCS. Dado que não é possível indicar um calendário para esse processo de revisão à altura de redacção do presente documento, o leitor deverá dirigir-se à ERA para obter informações sobre a última edição do presente documento.

(1) *Os actores envolvidos são as entidades adjudicantes nos termos da alínea r) do artigo 2.º da Directiva 2008/57/EC relativa à interoperabilidade do sistema ferroviário na Comunidade, ou os fabricantes, todos designados no regulamento como "proponentes", ou os seus fornecedores e prestadores de serviços.*

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

0.2. Fora do âmbito

0.2.1. O presente documento não fornece orientações quanto à forma de organizar, operar ou conceber (e fabricar) um sistema ferroviário ou partes do mesmo. Não define tampouco as disposições contratuais ou acordos que possam existir entre actores no âmbito da aplicação do procedimento de gestão do risco. As disposições contratuais específicas do projecto não são abrangidas pelo âmbito do Regulamento relativo ao MCS estando, por isso, excluídas também do guia conexo e do presente documento.

0.2.2. Não obstante estarem fora do âmbito do presente documento, as disposições acordadas entre os actores pertinentes poderão ser reduzidas a escrito nos respectivos contratos no início do projecto, contudo, sem prejuízo das disposições do MCS. Isso pode abranger, por exemplo:

os custos inerentes à gestão de riscos relacionados com a segurança nas interfaces entre os actores;
os custos inerentes às transferências de perigos e medidas de segurança associadas entre os actores não conhecidos no início do projecto;
a forma de gerir conflitos que possam surgir durante o projecto;
etc.

Em caso de desacordo ou conflito entre o proponente e os seus subcontratantes durante o desenvolvimento do projecto, poderá ser feita referência aos respectivos contratos para ajudar a resolver o conflito.

0.3. Princípio do presente documento

0.3.1. Este documento, embora possa ser lido como documento independente, não substitui o Regulamento relativo ao MCS{Ref. 3}. Para uma maior facilidade de consulta, cada artigo do Regulamento relativo ao MCS foi transcrito para o presente documento. Nos casos necessários, o respectivo artigo é explicado previamente no guia para aplicação do Regulamento relativo ao MCS {Ref. 4}.. Nos números seguintes, são dadas mais informações para ajudar a compreender o Regulamento relativo ao MCS, sempre que se considere necessário.

0.3.2. The articles and their underlying paragraphs from the CSM Regulation are copied in a text box in the present document using the "Bookman Old Style" Italic Font, the same as the present text. That formatting enables to easily distinguish the original text of the CSM Regulation 0 from the additional explanations provided in this document. The text from the guide for the application of the CSM Regulation 0 is not copied in the present document.

0.3.3. De forma a ajudar o leitor, a estrutura do presente documento segue a estrutura do Regulamento relativo ao MCS e do guia associado.

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

0.4. Descrição do documento

0.4.1. O documento está dividido nas seguintes partes:

Capítulo 0.: define o âmbito do guia e fornece uma lista de documentos de referência;

o anexo I e anexo II dão informações adicionais às respectivas secções do Regulamento relativo ao MCS {Ref. 3} e do guia associado {Ref. 4};

os novos apêndices aprofundam alguns aspectos específicos e fornecem exemplos.

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

0.5. Documentos de referência

Quadro 2: Quadro de Documentos de Referência

{Ref. N°}	Título	Referência	Versão
	Directiva 2004/49/CE do Parlamento Europeu e do Conselho de 29 de Abril de 2004 relativa à segurança dos caminhos-de-ferro da Comunidade e que altera a Directiva 95/18/CE do Conselho relativa às licenças das empresas de transporte ferroviário e a Directiva 2001/14/CE relativa à repartição de capacidade da infra-estrutura ferroviária, à aplicação de taxas de utilização da infra-estrutura ferroviária e à certificação da segurança («Directiva relativa à segurança ferroviária»)	2004/49/CE JO L 164 de 30.04.04, p. 44 e rectificada no JO L 220 de 21.06.04, p. 16.	-
	Directiva 2008/57/CE do Parlamento Europeu e do Conselho de 17 de Junho de 2008 relativa à interoperabilidade do sistema ferroviário na Comunidade	2008/57/CE JO L 191 de 18.07.08, p.1	-
	Regulamento (CE) N°.../… da Comissão, de [...] relativo à adopção de um método comum de segurança para a determinação e a avaliação dos riscos, conforme referido no n.º 3, alínea a) do artigo 6.º da Directiva 2004/49/CE do Parlamento Europeu e do Conselho	xxxx/yy/CE	Votada pelo RISC a 25/11/2008
	Guia para a aplicação do Regulamento da Comissão relativo à adopção de um método comum de segurança para a determinação e avaliação dos riscos, conforme referido no n.º 3 da alínea a) do artigo 6.º da Directiva relativa à segurança ferroviária	ERA/GUI/01-2008/SAF	1.0
	Directiva 2008/57/CE do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, relativa à interoperabilidade do sistema ferroviário na Comunidade	2008/57/CE JO L 191 de 18.07.08, p.1	-
	Sistema de Gestão de Segurança – Critérios de Avaliação para as Empresas Ferroviárias e Gestores das infra-estruturas	Critérios de Avaliação SGS Parte A Certificados de Segurança e Autorizações	31/05/2007
	Aplicações Ferroviárias - Comunicação, Sinalização e Sistemas de Processamento - Sistemas Electrónicos de Segurança para a sinalização	EN 50129	Fevereiro 2003
	Aplicações Ferroviárias – Especificação e Demonstração de Fiabilidade, Disponibilidade, Manutenibilidade e Segurança (RAMS) – Parte 1: a norma	EN 50126-1	Setembro de 2006
	Aplicações Ferroviárias – Especificação e Demonstração de Fiabilidade, Disponibilidade, Manutenibilidade e Segurança (RAMS) Parte 2: Guia de aplicação da norma de Segurança EN 50126-1	EN 50126-2 (Guia)	Projecto Final (Agosto de 2006)
	Guia genérico para o Cálculo dos Riscos inerentes ao Transporte Ferroviário de Mercadorias Perigosas	Guia da OTIF aprovado pelo Comité de peritos RID	24 de Novembro de 2005.
	Critério de Aceitação de Risco para os Sistemas Técnicos	Nota 01/08	1.1 (25/01/2008)
	Unidade de Segurança da ERA: Estudo de viabilidade – “Repartição de objectivos de segurança (para os subsistemas ETI) e consolidação da ETI do ponto de vista da segurança” WP1.1 – Avaliação de viabilidade da repartição dos objectivos comuns de segurança	WP1.1	1.0
	"Aplicações Ferroviárias — Sistema de Classificação de Veículos Ferroviários — Parte 4: EN 0015380 Parte 4: Grupos funcionais”.	EN 0015380 Parte 4	

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

0.6. Definições normalizadas, termos e abreviaturas

0.6.1. As definições gerais, termos e abreviaturas usados no presente documento podem ser encontrados num dicionário normal.

0.6.2. As novas definições, termos e abreviaturas do presente guia são definidos nas secções que se seguem.

0.7. Definições específicas

0.7.1. Ver Artigo 3.º

0.8. Termos e abreviaturas específicos

0.8.1. Esta secção define os novos termos e abreviaturas específicos que são usados com frequência no presente documento.

Quadro 3: Quadro de termos.

Termo	Definição
Agência	Agência Ferroviária Europeia (ERA)
Guia	Guia para a aplicação do Regulamento (CE) N°.../.. da Comissão de [...] relativo à adopção de um método comum de segurança para a determinação e avaliação dos riscos, conforme referido no n.º 3 da alínea a) do artigo 6.º da Directiva 2004/49/CE do Parlamento Europeu e do Conselho
Regulamento relativo ao MCS	Regulamento (CE) n.º …/… da Comissão de […] relativo à adopção de um método comum de segurança para a determinação e avaliação dos riscos, conforme referido no n.º 3 da alínea a) do artigo 6.º da Directiva 2004/49/CE do Parlamento Europeu e do Conselho {Ref. 3}.

Quadro 4: Quadro de abreviaturas.

Abreviatura	Significado
ERA	Agência Ferroviária Europeia
AIS	Avaliador Independente de Segurança
ANS	Autoridade Nacional de Segurança
ASP	A ser preenchido
CCS	Comando/Controlo e Sinalização
CE	Comissão Europeia
EF	Empresa(s) Ferroviária(s)
EM	Estado-Membro
ETI	Especificações técnicas de interoperabilidade
GI	Gestor(es) de Infra-Estruturas
MCS	Método(s) Comum de Segurança
OCS	Objectivos Comuns de Segurança
ORNO	Organismo notificado
OTIF	Organização Intergovernamental para os Transportes Internacionais Ferroviários
PGQ	Processo de Gestão da Qualidade
PGS	Processo de Gestão da Segurança
RISC	Comité para a Interoperabilidade e Segurança do Sistema Ferroviário
SGQ	Sistema de Gestão de Qualidade
SGS	Sistema de Gestão da Segurança

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

Quadro 3: Quadro de termos.

Termo	**Definição**
STF	Segurança em Túneis Ferroviários

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

EXPLICAÇÃO DOS ARTIGOS DO REGULAMENTO RELATIVO AO MCS

Artigo 1.º Objectivo

Artigo 1.º (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.

Não são consideradas necessárias explicações adicionais.

Artigo 1.º (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] Não são consideradas necessárias explicações adicionais.

Artigo 2.º Âmbito

Artigo 2.º (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 Artigo 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.

O MCS aplica-se à totalidade do sistema ferroviário e abrange a avaliação das seguintes alterações nos sistemas ferroviários caso sejam considerados significativos na acepção do Artigo 4.º:

(a) construção de linhas novas e alteração das existentes,
(b) introdução de sistemas técnicos novos e/ou modificados;

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) alterações operacionais (tais como regras operacionais novas ou modificadas e procedimentos de manutenção);
(d) mudanças nas organizações das EF/GI.

No MCS, o termo "sistema" refere-se a todos os aspectos de um sistema, incluindo, entre outros, o desenvolvimento, operação, manutenção, etc., até à desactivação ou eliminação.

O MCS abrange as alterações significativas introduzidas em:

sistemas "pequenos e "simples" que podem ser compostos por alguns elementos ou subsistemas técnicos e
sistemas "grandes e mais complexos" (p. ex., que podem incluir estações e túneis).

Artigo 2.º (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 Artigo 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 Artigo 6(2) or Artigo 7 of Directive 2008/57/EC or a derogation in accordance with Artigo 9 of that Directive.

Por exemplo, em conformidade com a Directiva 0 relativa à Segurança Ferroviária e a Directiva relativa à interoperabilidade ferroviária 0, um novo tipo de material circulante para uma linha de alta velocidade terá de estar em conformidade com as ETI do material circulante de alta velocidade. Não obstante a maior parte do sistema a ser avaliado estar abrangida pelas ETI , a questão crucial dos factores humanos relacionados com a cabina de condução não está coberta pela ETI. Por isso, de forma a garantir que todos os perigos relacionados com os factores humanos razoavelmente previsíveis (ou seja, as interfaces entre o condutor, material circulante e o resto do sistema ferroviário) são identificados e controlados de forma adequada, deverá ser usado o processo do MCS.

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

Artigo 2.º (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] Não são consideradas necessárias explicações adicionais.

Artigo 2.º (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 Artigo 2 (t) of Directive 2008/57/EC.

[G 1] Não são consideradas necessárias explicações adicionais.

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

Artigo 3.º Definições

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

The following definitions shall also apply:

'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)*;*

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

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

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

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

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

'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;

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

'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;

'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 accepQuadro level of risk;

'proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Artigo 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 Artigo 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles;

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

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

'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;

'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;

'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;

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

'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 accepQuadro;

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

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

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

'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)*;*

'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;

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

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

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

'notified national rule' means any national rule notified by Member States under Council Directive 96/48/EC[2], Directive 2001/16/EC of the European Parliament and the Council[3] and Directives2004/49/EC and 2008/57/EC.

[G 1] Não são consideradas necessárias explicações adicionais.

Artigo 4.º Alterações significativas

Artigo 4.º (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 Artigo 5 does not need to be applied.

[G 1] Caso não haja uma regra nacional notificada, a decisão é da responsabilidade do proponente. A avaliação da importância da alteração é baseada no parecer de peritos. Por exemplo, se a alteração prevista num dado sistema for complexa, pode ser avaliada como

(2) *JO L 235, 17.9.1996, p. 6.*

(3) *JO 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

significativa se o risco de impacto nas funções existentes[4] do sistema for elevado, apesar de a alteração em si não estar necessariamente estritamente relacionada com a segurança.

Artigo 4.º (2)

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

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

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

(c) complexity of the change;

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

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

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

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Exemplo de alterações menores**: depois da aceitação do sistema, poderá não ser significativo aumentar em 5 km/h a velocidade máxima permitida pela linha. Contudo, se a velocidade máxima permitida pela linha continuar a ser aumentada por fracções de 5 km/h, a soma das sucessivas alterações (avaliadas individualmente como não significativas) poderá corresponder a uma alteração significativa relativamente aos requisitos de segurança do sistema inicial.

[G 2] Para avaliar se uma série de alterações sucessivas (não significativas) se torna significativa no seu conjunto, é necessário avaliar todos os perigos e riscos associados relacionados com todas as alterações. O conjunto de alterações apreciadas pode ser considerado não significativo se o risco resultante for genericamente aceitável**.**

[G 3] O trabalho da Agência em matéria de alterações significativas demonstrou que:

(a) não é possível identificar limiares ou regras normalizados que permitam, para uma dada alteração, determinar a importância dessa alteração, e;
(b) não é possível indicar uma lista exaustiva de alterações significativas;
(c) a decisão não pode ser válida para todos os proponentes nem para todas as condições técnicas, operacionais, organizacionais e ambientais

Assim sendo, é essencial deixar a responsabilidade da decisão aos proponentes que são responsáveis, nos termos do n.º 3 do artigo 4.º da Directiva 0, relativa à segurança

(4) *Dado que as funções de um sistema nem sempre são independentes, as alterações de certas funções podem também afectar outras funções do sistema, mesmo que essas funções pareçam não ser afectadas directamente pelas alterações.*

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

ferroviária, pela segurança da operação e controlo dos riscos associados à sua parte do sistema.

[G 4] Para ajudar o proponente, é incluído um exemplo de “avaliação e utilização de critérios" na secção C.2. do Apêndice C.

[G 5] O MCS não deverá ser aplicado se uma alteração relacionada com a segurança não for considerada significativa. Porém, isso não quer dizer que não há nada a fazer. O proponente realiza análises de risco (preliminares) para decidir se a alteração é significativa. Estas análises de risco, bem como as eventuais justificações e razões terão de ser documentadas, para que as ANS as possam auditar. A avaliação do carácter significativo de uma alteração e a decisão que uma alteração não é significativa não deverão ser avaliadas de forma independente por um organismo de avaliação.

Artigo 5.º Processo de gestão dos riscos

Artigo 5.º (1)

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

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

Não são consideradas necessárias explicações adicionais.

Artigo 5.º (2)

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

[G 1] Não são consideradas necessárias explicações adicionais.

Artigo 5.º (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] Não são consideradas necessárias explicações adicionais.

Artigo 6.º Avaliação independente

Artigo 6.º (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

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

the criteria listed in Annex II. Where the assessment body is not already identified by Community or national legislation, the proposer shall appoint its own assessment body which may be another organisation or an internal department.

[G 1] O nível de independência necessário para o organismo de avaliação depende do nível de segurança requerido para o sistema que é objecto de avaliação. Enquanto se aguarda a harmonização desta questão, a melhor prática a seguir encontra-se identificada na cláusula 8 da norma IEC61508-1:2001 ou no n.º 5.3.9 da norma EN 50 129 0. O grau de independência depende da gravidade da consequência do perigo associado ao equipamento e ao grau de novidade. O n.º 9.7.2 da norma EN 50 126-2 e norma EN 50129 definem o nível de independência para os sistemas de sinalização. Este grau pode, em princípio, ser usado também noutros sistemas.

[G 2] A Agência ainda está a trabalhar na definição dos papéis e responsabilidades dos diferentes organismos de avaliação (ANS, ORNO e AIS), bem como as interfaces necessárias entre si. Assim, será definido (se possível) quem, de entre os organismos de avaliação, irá fazer o quê e de que forma o irá fazer. No final, isso irá permitir definir como:

(a) verificar, com base nas evidências disponíveis, que os processos de gestão de risco e avaliação de risco abrangidos pelo MCS são correctamente aplicados, e;
(b) apoiar o proponente na sua decisão de aceitar a alteração significativa dentro do sistema a ser avaliado.

Artigo 6.º (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] O trabalho da Agência relativo aos papéis e responsabilidades dos organismos de avaliação fornecerá informações complementares.

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

Artigo 6.º (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 Artigos 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 Artigos 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 Artigo 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 Artigo 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 Artigo 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 Artigo 11(2) of Directive 2004/49/EC.

Não são consideradas necessárias explicações adicionais.

Artigo 6.º (4)

Where the significant changes concern a structural subsystem that needs an authorisation for placing in service as referred to in Artigo 15(1) or Artigo 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 Artigo 18(2) of that Directive.

Não são consideradas necessárias explicações adicionais.

Artigo 7.º Relatórios de avaliação da segurança

Artigo 7.º (1)

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

[G 1] Não são consideradas necessárias explicações adicionais.

Artigo 7.º (2)

In the case referred to in point (a) of Artigo 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] Não são consideradas necessárias explicações adicionais.

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

Artigo 7.º (3)

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

[G 1] Não são consideradas necessárias explicações adicionais.

Artigo 7.º (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.

Este princípio de reconhecimento mútuo é aceite pelas normas do CENELEC: ver n.º 5.5.2 da norma EN 50 129 e n.º 5.9 da norma EN 50 126-2. No CENELEC, a aceitação cruzada ou princípio de reconhecimento mútuo é aplicado aos proponentes ou avaliadores independentes de segurança[5] desde que a avaliação de segurança e a demonstração de segurança sejam realizadas em conformidade com os requisitos das normas CENELEC.

O reconhecimento mútuo deve igualmente ser aplicado à aceitação de sistemas novos ou modificados se a respectiva avaliação de risco e a comprovação da conformidade do sistema com os requisitos de segurança forem realizadas de acordo com o disposto no regulamento relativo ao MCS {Ref. 3}.

Artigo 8.º Gestão do controlo dos riscos/ auditorias internas e externas

Artigo 8.º (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 Artigo 9 of Directive 2004/49/EC.

[G 1] Não são consideradas necessárias explicações adicionais.

---

(5) *Consulte o ponto 0 da secção 1.1.5 e as notas de rodapé (**Error! Bookmark not defined.**) e (**Error! Bookmark not defined.**) da página 27, bem como o Figura 3 do presente documento, para mais esclarecimentos sobre a terminologia de "produtos genéricos e aplicação genérica" e princípios inerentes. (ver os erros desta nota de rodapé)*

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

Artigo 8.º (2)

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

Não são consideradas necessárias explicações adicionais.

Artigo 9.º Feedback e progresso técnico

Artigo 9.º (1)

Each infrastructure manager and each railway undertaking shall, in its annual safety report referred to in Artigo 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] Não são consideradas necessárias explicações adicionais.

Artigo 9.º (2)

Each national safety authority shall, in its annual safety report referred to in Artigo 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] Não são consideradas necessárias explicações adicionais.

Artigo 9.º (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] Não são consideradas necessárias explicações adicionais.

Artigo 9.º (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 Artigo 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

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

2.3.8 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] Não são consideradas necessárias explicações adicionais.

Artigo 10.º Entrada em vigor

Artigo 10.º (1)

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

Não são consideradas necessárias explicações adicionais.

Artigo 10.º (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 Artigo 2 (c) of Directive 2008/57/EC;

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

[G 1] Não são consideradas necessárias explicações adicionais.

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

ANEXO I – EXPLICAÇÃO DO PROCESSO PREVISTO NO REGULAMENTO RELATIVO AO MCS

1. PRINCÍPIOS GERAIS APLICÁVEIS AO PROCESSO DE GESTÃO DOS RISCOS

1.1. Princípios gerais e obrigações

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] O quadro de gestão dos riscos do MCS e o processo associado de avaliação do risco são ilustrados no Figura 1.

[G 2] Nos casos considerados necessários, cada caixa/actividade da figura é descrita numa secção específica do documento.

[G 3] O CENELEC aconselha a que os processos de gestão e avaliação de risco sejam descritos num plano de segurança. Mas se isso não for adequado para o projecto, a descrição associada pode ser incluída em qualquer outro documento relevante. Consultar a secção 1.1.6.

[G 4] O processo de avaliação do risco começa com uma definição preliminar de sistema. Durante o desenvolvimento do projecto, a definição preliminar do sistema é actualizada progressivamente e é substituída pela definição do sistema. Se não existir uma definição preliminar do sistema, a definição formal de sistema é usada para realizar a avaliação do risco. É então aconselhável que os actores afectados pela alteração significativa se reúnam no início do projecto para:

(a) acordarem nos princípios gerais do sistema, nas funções do sistema, etc. Em princípio, isto pode ser descrito numa definição preliminar do sistema;
(b) acordarem na organização do projecto;
(c) acordarem na partilha de papéis e responsabilidades entre os diferentes actores já envolvidos, incluindo a ANS, ORNO e AIS, nos casos indicados.

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

Essa coordenação, durante a definição preliminar do sistema, confere a oportunidade ao proponente, aos subcontratados, à ANS, ORNO e AIS, se relevante, de chegarem a acordo, numa fase inicial, quanto aos códigos de práticas ou sistemas de referência cuja utilização é aceitável no quadro do projecto.

NOTA: Na figura 1 em algumas caixas algumas palavras não são visíveis devido ao tamanho da letra

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

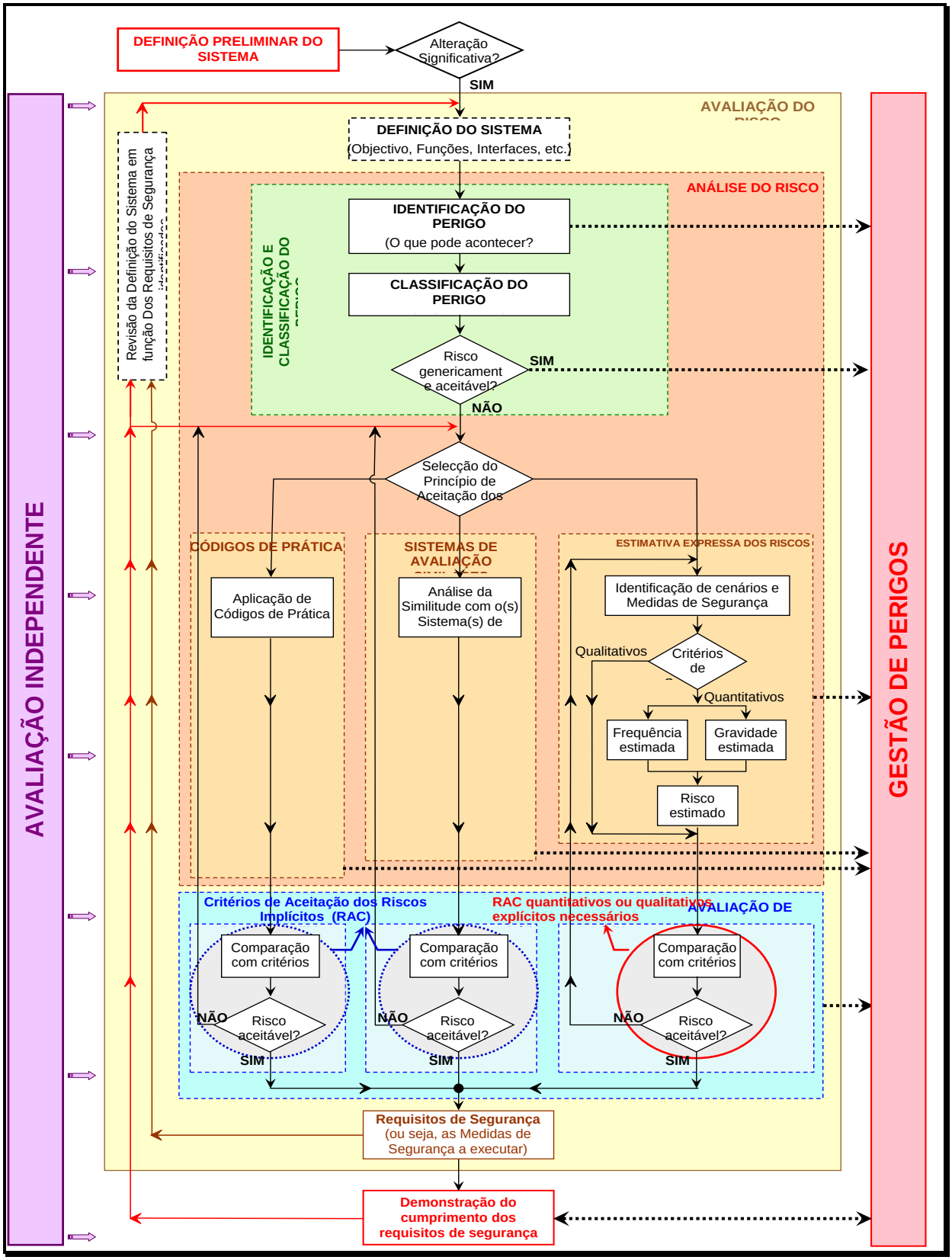

Figura 1 : Quadro de gestão do risco no regulamento relativo ao MCS. N

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] O sistema de gestão da segurança (SGS) da empresa ferroviária e gestor da infra-estrutura definem o processo e os procedimentos que:

(a) monitorizam o sistema para garantir que continua a ser seguro durante todo o ciclo de vida (ou seja, durante a operação e manutenção);
(b) garantem o seguro desmantelamento ou substituição do respectivo sistema.

Este processo não faz parte do MCS relativo à avaliação do risco

[G 2] Para implementar o MCS, é necessário que todas as partes envolvidas sejam competentes (ou seja, que tenham as competências, conhecimentos e experiência indicados). Os actores do sector ferroviário têm uma necessidade constante de gestão de competências:

(a) no caso dos gestores da infra-estrutura e empresas ferroviárias, isto é abrangido pelo seu sistema de gestão (SGS) ao abrigo da alínea e) do artigo 2.º do anexo III da Directiva relativa à segurança ferroviária 0;
(b) no caso dos restantes actores cujas actividades possam ter um impacto na segurança do sistema ferroviário, não obstante o SGS não ser obrigatório, no geral, pelo menos ao nível do projecto (ver ponto 0 na secção 0) existe um processo de gestão de qualidade (PGQ) e/ou um processo de gestão de segurança (PGS) que cobre esse requisito.

[G 3] As seguintes secções da norma EN 50 126-1 do CENELEC 0 estabelecem orientações sobre a competência:

(a) secção 5.3.5 b): "*todo o pessoal com responsabilidades no quadro do processo de gestão de riscos*" deve ser "*competente para assumir essas responsabilidades*";
(b) secção 5.3.5 d): os requisitos da gestão de riscos e da avaliação de riscos devem ser "*implementados no contexto de processos empresariais apoiados por um sistema de gestão de qualidade (SGQ) em conformidade com os requisitos das normas EN ISO 9001, EN ISO 9002 ou EN ISO 9003 apropriados para o sistema em avaliação".* Um exemplo dos aspectos controlados pelo sistema de gestão de qualidade é dado na secção 5.2. da norma da EN 50 129 0.

Estas competências abrangem as actividades que garantem a qualidade, bem como as competências e formação da equipa/pessoal, necessárias para apoiar o processo abrangido pelo MCS.

[G 4] Frequentemente, o processo de avaliação do risco é acompanhado por um organismo de avaliação desde o início do projecto, mas, a não ser que isso seja exigido pela legislação nacional de um Estado-membro, tal envolvimento inicial do organismo de avaliação não é obrigatório, embora seja aconselhado. A opinião do organismo de avaliação independente pode ser útil antes de se passar de uma fase da avaliação de risco para a próxima. Ver o Artigo 6.º para mais detalhes sobre a avaliação independente

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

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

[G 1] Não são consideradas necessárias explicações adicionais.

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 Artigo 10(2)(a) or Artigo 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] O Figura 2: SGS e MCS harmonizados.

[G 2] representa a relação entre o MCS e os “sistemas de gestão de segurança e processos de avaliação do risco”.

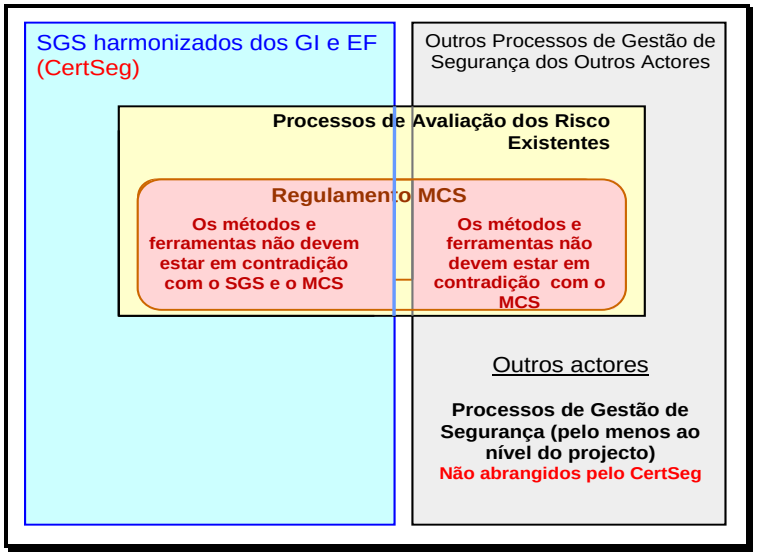

Figura 2: SGS e MCS harmonizados.

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 accepQuadro level. The demonstration of compliance with the safety requirements shall be conducted according to 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

[G 1] Se o proponente for um gestor de infra-estrutura ou empresa ferroviária, por vezes poderá ser necessário envolver outros actores no processo (6) (consultar a secção 1.2.1). Em alguns casos, o gestor de infra-estrutura ou a empresa ferroviária poderá subcontratar, de forma total ou parcial, as actividades de avaliação do risco. Os papéis e responsabilidades de cada actor são normalmente acordados entre os respectivos actores na fase inicial do projecto.

[G 2] É importante notar que o proponente é sempre responsável pela aplicação do MCS, pela aceitação do risco e, desta forma, pela segurança do sistema. Isto inclui garantir que:

(a) há plena cooperação entre os actores envolvidos, de modo a que todas as informações necessárias sejam fornecidas, e;
(b) é claro quem tem de cumprir os requisitos particulares do MCS (por exemplo, realizar a análise do risco ou gerir o controlo dos perigos).

Em caso de desacordo entre os actores quanto aos requisitos que têm de cumpridos, pode ser solicitado um parecer à ANS. Porém, a responsabilidade de encontrar uma solução continua a ser do proponente e não pode ser transferida para a ANS: ver também secção 0.2.2.

[G 3] Se a tarefa for subcontratada, o subcontratante não tem obrigação de ter a sua própria organização de segurança, caso não seja gestor de infra-estrutura ou empresa ferroviária ou, em especial, se a estrutura/dimensão do subcontratante for reduzida ou se a sua contribuição para o sistema global for limitada. A responsabilidade da gestão de riscos, incluindo a avaliação do risco e as actividades de gestão dos perigos, pode permanecer na organização de nível mais elevado, ou seja, no cliente do subcontratante. Contudo, o subcontratante é sempre responsável pela prestação das informações correctas relacionadas com as suas actividades e que são necessárias para que a organização de nível mais elevado possa elaborar a documentação relativa à gestão dos riscos.
As organizações cooperantes também podem acordar em criar uma organização de segurança comum, por exemplo, para optimizar os custos. Nesse caso, apenas uma organização irá gerir as actividades de segurança de todas as organizações envolvidas. A responsabilidade pela exactidão das informações (ou seja, dos perigos, riscos e medidas de segurança), bem como pela gestão da execução das medidas de segurança fica a cargo da organização encarregada do controlo dos perigos com os quais se relacionam essas medidas de segurança.

[G 4] Em geral, o proponente definirá os "níveis de segurança" e os "requisitos de segurança" atribuídos aos actores envolvidos no projecto e aos diferentes subsistemas e equipamentos desses actores:

(a) nos contratos entre o proponente e os respectivos actores (subcontratantes);
(b) num plano de segurança ou em qualquer outro documento relevante com a mesma finalidade e com a descrição da organização geral do projecto e responsabilidades de cada actor, incluindo as do proponente: consultar a secção 1.1.6;
(c) no registo(s) dos perigos do proponente: consultar a secção 4.1.1.

A repartição dos "níveis de segurança" e dos "requisitos de segurança" do sistema pelos subsistemas e equipamentos subjacentes e, concomitantemente, pelos respectivos actores, incluindo o próprio proponente, pode ser redefinida/alargada durante a "fase de demonstração da conformidade do sistema com os requisitos de segurança". Ver o Figura 1.

(6) *Em conformidade com o Apêndice A.4 da norma CENELEC 50 129 {Ref. 7}.*

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

Em comparação com o Ciclo CENELEC V (ver secção 2.1.1 e o Figura 5), esta actividade corresponde à Fase 5 relativa à "repartição dos requisitos do sistema".

[G 5] Artigo 5.º (2) permite que outros actores, com a excepção das EF e dos GI, assumam a responsabilidade geral da conformidade com o MCS, dependendo das suas necessidades respectivas. No caso de produtos ou aplicações genéricas [(9)], por exemplo, o fabricante pode realizar a avaliação de risco tendo por base uma "definição genérica do sistema", de modo a especificar os níveis de segurança e os requisitos de segurança a serem cumpridos pelos produtos e aplicações genéricos.

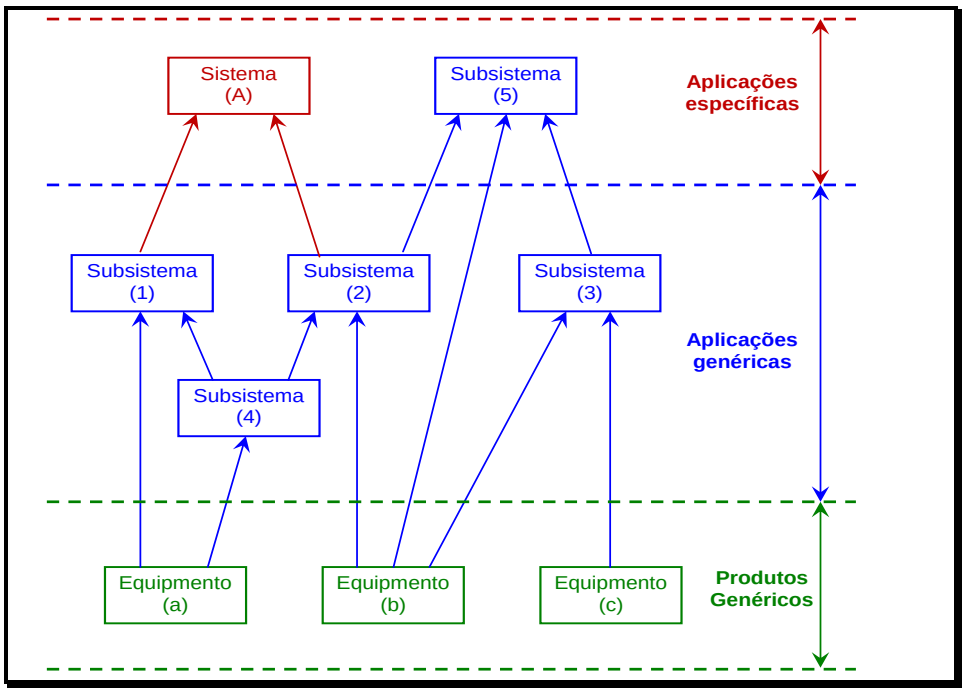

Figura 3: Exemplos de dependências entre casos de segurança (retirado do Figura 9 da norma EN 50 129).

[G 6] O CENELEC recomenda que o fabricante forneça as evidências documentais da avaliação de riscos nos produtos genéricos (respectivamente a aplicação genérica[(9)] em casos de segurança e registos de perigos. Estes casos de segurança e registos de perigos contêm todos os pressupostos[(7)] e as "restrições de utilização" identificadas (ou seja, condições da

7 *Estes pressupostos e restrições de utilização determinam os limites e a validade das "avaliações de segurança" e "análises de segurança" associadas ao produto genérico associado e dossiê de segurança de aplicação genérica. Se não forem cumpridos pela aplicação específica considerada, é necessário actualizar ou substituir as "avaliações de segurança" e "análises de segurança" correspondentes (por exemplo, análises causuais) por outras novas.*

Isto está de acordo com o seguinte princípio geral de segurança: "Sempre que o design de um dado subsistema for baseado em aplicações genéricas e produtos genéricos, terá de ser provado que esse (sub)sistema está em conformidade com todos os pressupostos e restrições de utilização (designados condições de aplicação relacionadas no CENELEC)

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

aplicação relacionadas com a segurança) que se aplicam aos produtos genéricos relacionados (respectivamente, a aplicação genérica). Por isso, sempre que um produto genérico e uma aplicação genérica forem usados em operação numa aplicação específica, a conformidade com estes pressupostos(10) e "restrições de utilização" (ou condições de aplicação relacionadas com a segurança) deve ser demonstrada em cada aplicação específica.

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] Não raro, salvo disposição contratual acordada na fase inicial do projecto, cada projecto tem um documento que descreve as actividades de gestão dos riscos. O respectivo documento é actualizado e revisto sempre que o sistema original sofrer alterações significativas.

[G 2] Esse documento fixa a estrutura organizacional, as responsabilidades atribuídas ao pessoal, os processos, procedimentos e as actividades que, no seu todo, garantem que o sistema em avaliação cumpre os níveis de segurança especificados e os requisitos de segurança. O documento terá de estar em conformidade com o MCS, dado que apoia e proporciona orientações ao organismo de avaliação. Os padrões do CENELEC aconselham a que este tipo de informação seja incluído num plano de segurança ou noutro documento com uma parte dedicada a esse tema.

Nota: Verificar as notas de rodapé de todo o texto porque algumas faltam e outras estão desalinhadas.

[G 3] O plano de segurança do proponente, em especial, ou quaisquer outros documentos relevantes, apresenta a organização geral do projecto. O plano descreve a forma como os papéis e responsabilidades são partilhados entre os actores envolvidos. Para mais

---

Continuation of the footnote

exportados na aplicação genérica correspondente e nos dossiês de segurança de produtos genéricos (ver Figura 3: Exemplos de dependências entre casos de segurança (retirado do Figura 9 da norma EN 50 129).

).

Se, numa aplicação específica, a conformidade com certos pressupostos e restrições de utilização não puder ser alcançada ao nível do subsistema (por exemplo, no caso de requisitos operacionais de segurança), os pressupostos e restrições de utilização correspondentes podem ser transferidos para um nível superior (por exemplo, geralmente ao nível do sistema). Estes pressupostos e restrições de utilização são então claramente identificados no "dossiê de segurança da aplicação específica" do subsistema respectivo. É essencial garantir, nesses exemplos de dependência, que as condições de aplicação relacionadas com a segurança de cada dossiê de segurança são cumpridas no dossiê de segurança de nível superior, ou que sejam considerados nas condições de aplicação relacionadas com a segurança do dossiê de segurança de nível mais alto (ou seja, o dossiê de segurança de sistema).

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

informações pormenorizadas, poderá ser feita referência aos planos de segurança ou organizações de segurança dos vários actores envolvidos. Normalmente, a partilha de responsabilidades entre os vários actores é discutida e acordada durante a definição preliminar do sistema (ou seja, no início do projecto), se existir.

[G 4] O plano de segurança é um documento em constante mutação que é actualizado durante a vida do projecto.

[G 5] Poderão ser encontrados mais pormenores sobre os conteúdos do plano de segurança na norma EN 50 126-1 0 e no guia associado 50 126-2 0.

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] Não são consideradas necessárias explicações adicionais.

1.2. Gestão das interfaces

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] Por exemplo, se por razões operacionais uma empresa ferroviária precisar que um gestor de infra-estrutura realize alterações na infra-estrutura, por força dos requisitos da alínea g) do n.º 2 do anexo III da Directiva relativa à segurança ferroviária 0, a EF monitoriza de igual forma todo o trabalho, de modo a garantir que as alterações esperadas são feitas de forma correcta. Contudo, a liderança da EF não exonera de responsabilidade o respectivo GI quanto a informar as restantes empresas ferroviárias, caso estas também sejam afectadas pela alteração relacionada da infra-estrutura. O GI poderá até ter de realizar uma avaliação de risco, em conformidade com o MCS, caso a alteração relacionada seja no seu entender significativa.

[G 2] É possível, e em algumas circunstâncias até necessário, transferir responsabilidades entre os vários actores. Contudo, quando há vários actores envolvidos num sistema, é frequente nomear-se um actor como responsável por todo o sistema. Há sempre relações de dependência entre os subsistemas e operações que necessitam de esforços especiais para serem identificadas. Desta forma, é necessário que haja alguém que assuma a responsabilidade pelas análises de segurança e que também tenha pleno acesso a toda a documentação relevante. É claro que o proponente que pretende introduzir a alteração significativa tem a responsabilidade geral de garantir que a avaliação do risco seja sistemática e completa.

[G 3] Os principais critérios a serem acordados quanto à gestão de uma interface entre os actores envolvidos são:

(a) a direcção, que é normalmente garantida pelo proponente que pretende introduzir a alteração significativa;

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) os *inputs* necessários;
(c) os métodos da identificação de perigos e de avaliação do risco;
(d) os participantes necessários com as competências exigidas (ou seja, a combinação de conhecimento, competências e experiência prática em – ver também a definição de "competência do pessoal" na alínea b) do ponto [G 2] do artigo 3.º) {Ref. 4};
(e) os *outputs* esperados.

Estes critérios são descritos nos planos de segurança (ou noutros documentos relevantes) das empresas que lidam com as interfaces envolvidas.

[G 4] A secção C.3. do Apêndice C contém exemplos de interfaces, bem como um exemplo da aplicação dos critérios principais da gestão da interface entre um fabricante de comboios e um gestor de infra-estrutura ou empresa ferroviária.

[G 5] A gestão das interfaces irá considerar igualmente os riscos que podem surgir nas interfaces com os operadores humanos (usados durante a operação e manutenção) na concepção dessas interfaces.

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] O processo de transferência de perigos e medidas de segurança associadas entre os actores aplica-se também aos níveis inferiores do Ciclo CENELEC V ilustrado na Figura 5: Figura 10 do Ciclo em V da norma EN 50 126 (ciclo de vida CENELEC do sistema).

[G 2] da página 37. Pode ser aplicado sempre que for necessário trocar informações entre um actor e os subcontratantes, por exemplo. A diferença relativamente ao mesmo processo ao nível do sistema é que o proponente não necessita de ser informado sobre todas as transferências de perigos e medidas de segurança associadas ao nível do subsistema. O proponente apenas é informado quando os perigos transferidos e medidas de segurança associadas estão relacionados com as interfaces de nível alto (ou seja, quando se afecta uma interface no proponente).

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] A EF e o sistema de gestão de segurança do GI (SMS) abrangem as regras e procedimentos para garantir que as não conformidades ou inadequações das medidas de segurança são geridas de forma correcta. Por isso, as regras e os procedimentos não fazem parte do MCS.

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] De igual forma, as propostas e procedimentos [8] a realizar pelos outros actores[9] para garantir que as não conformidades ou inadequações das medidas de segurança são geridas de forma correcta e, se necessário, que as medidas de segurança são transferidas para todos os actores relevantes são acordadas entre os actores no início do projecto e pormenorizadas no plano de segurança: consulte a secção 0.2.

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

[G 1] Desta forma, será então possível gerir a possível não conformidade ou inadequação da medida de segurança dentro do sistema a ser avaliado ou dentro dos sistemas semelhantes que usam a mesma medida.

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] Não são consideradas necessárias explicações adicionais.

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] Não são consideradas necessárias explicações adicionais.

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] Não são consideradas necessárias explicações adicionais.

---

(8) Em princípio, estas disposições e procedimentos são abrangidas pelo processo de gestão de qualidade e/ou processo de gestão de segurança destes actores identificados pelo menos ao nível do projecto (ver também Figura 2: SGS e MCS harmonizados.

).

(9) O termo "outros actores" designa todos os intervenientes envolvidos que não os GI's e EF's.

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

2. DESCRIÇÃO DO PROCESSO DE AVALIAÇÃO DO RISCO

2.1. Descrição geral – correspondência entre o processo de avaliação do risco previsto no MCS e o Ciclo V CENELEC

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] O processo de gestão dos riscos abrangido pelo MCS pode ser representado sob a forma de ciclo em V que começa com a definição (preliminar) do sistema e que termina com a aceitação do sistema: ver a Figura 4. Este ciclo em V simplificado pode ser relacionado com o ciclo em V clássico da Figura 10 da norma EN 50 126-1 0. De modo a identificar a correspondência com o processo de gestão dos riscos do MCS na Figura 1 : ,o ciclo em V CENELEC da Figura 10 é reproduzido na Figura 5:

(a) a definição preliminar do sistema" do MCS na Figura 1 corresponde à Fase 1 do Ciclo em V CENELEC, ou seja, à identificação do “conceito” do sistema (ver CAIXA 1 da Figura 5.

(b) a "avaliação do risco" do MCS na Figura 1 inclui as fases seguintes do Ciclo em V CENELEC (ver CAIXA 2 da Figura 5)

(1) Fase 2 da Figura 5: "definições do sistema e condições de aplicação";
(2) Fase 3 da Figura 5: : "análise de risco";
(3) Fase 4 da Figura 5: : "requisitos de sistema"; "distribuição dos requisitos de sistema” até aos vários subsistemas e componentes.

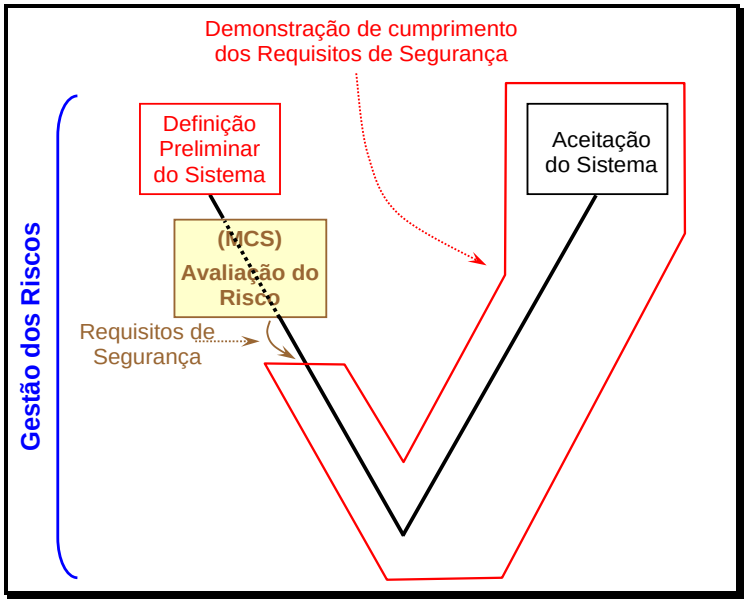

Figura 4: Ciclo em V simplificado da Figura 10 da norma EN 50 126.

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

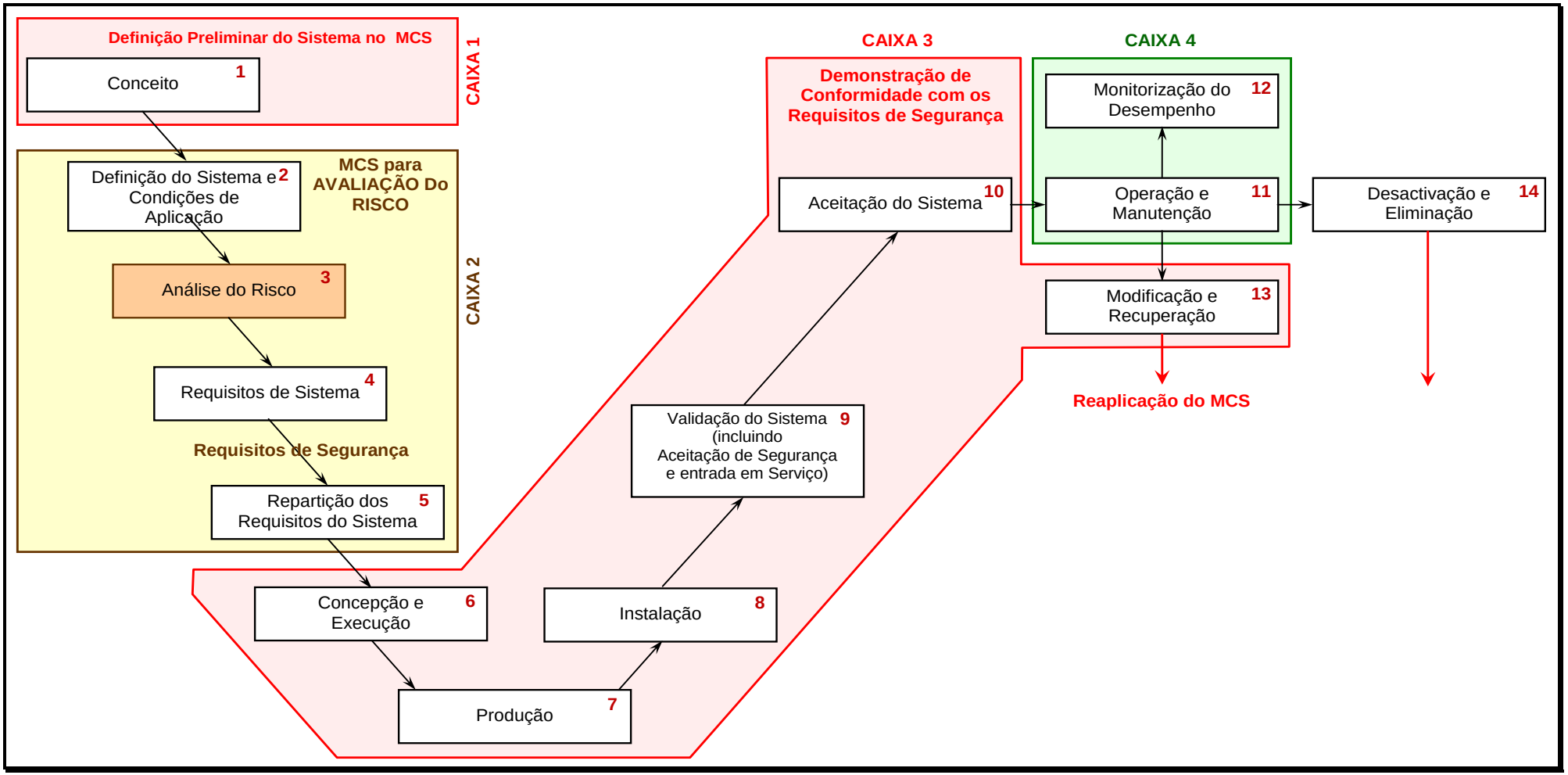

Figura 5: Figura 10 do Ciclo em V da norma EN 50 126 (ciclo de vida CENELEC do sistema).

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] Os outputs do processo de avaliação do risco no MCS são os seguintes (depois das iterações - ver Figura 1

(a) a “definição do sistema” actualizada com os "requisitos de segurança” resultantes da "análise do risco" e das actividades de "avaliação do risco" (ver secção 2.1.6);
(b) a "repartição dos requisitos do sistema" em subsistemas e componentes diferentes (Fase 5 da Figura 5);
(c) o “registo dos perigos” que documenta:

(1) todos os perigos identificados e as medidas de segurança associadas;
(2) os requisitos de segurança resultantes;
(3) os pressupostos tidos em consideração no sistema e que determinam os limites e a validade da avaliação do risco (ver alínea (g) da secção 2.1.2);

(d) e, no geral, todos os dados resultantes da aplicação do MCS: ver secção 5.

Estes outputs de avaliação do risco do MCS correspondem aos outputs relacionados com a segurança da Fase 4 do Ciclo em V CENELEC, ou seja, à especificação dos requisitos do sistema da Figura 5.

[G 3] A definição do sistema actualizada com os resultados da avaliação do risco e do registo de perigos constitui os inputs a partir dos quais o sistema é concebido e aceite. A "demonstração da conformidade do sistema com os requisitos de segurança" no MCS corresponde às seguintes fases do Ciclo em V CENELEC (ver CAIXA 3 do Figura 5.

[G 4]):
( ) fase 6 da Figura 5: "design e implementação";
(a) fase 7 da Figura 5: :"produção";
(b) fase 8 da Figura 5: “instalação”;
(c) fase 9 da Figura 5: “validação do sistema incluindo a aceitação de segurança e a activação)";
(d) fase 10 da Figura 5: "aceitação do sistema".

A demonstração da conformidade do sistema com os requisitos de segurança depende do facto de a alteração significativa ser técnica, operacional ou organizacional. Por isso, as várias etapas do Ciclo em V CENELEC da Figura 5 poderão não ser adequados a todas as alterações significativas do tipo mencionado. O ciclo em V da Figura 5 deve ser considerado em conformidade e usado com o critério adequado naquilo que se adequa a cada aplicação específica (por exemplo, nas alterações operacionais e organizacionais não existe uma fase de produção).

[G 5] Isto significa que a “demonstração da conformidade do sistema com os requisitos de segurança” do MCS não inclui apenas a “verificação e validação” das actividades mediante testes ou simulações. Na prática, abrange todas as fases de “6 a 10” (ver lista supra e o Figura 5) do Ciclo em V CENELEC. Essas fases incluem o design, produção, instalação, verificação e actividades de validação, bem como as actividades RAMS associadas e a aceitação do sistema.

[G 6] Durante a “demonstração da conformidade do sistema com os requisitos de segurança” o principio geral é concentrar a avaliação do risco apenas nas funções relacionadas com a segurança e na interface do sistema. Isto significa que sempre que as actividades de

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

avaliação de segurança e de risco forem necessárias no âmbito de uma das fases do Ciclo em V CENELEC do Figura 5, as mesmas devem-se centrar:

(a) nas funções e interfaces relacionadas com a segurança;
(b) nos subsistemas e/ou componentes envolvidos na realização das funções relacionadas com a segurança e/ou interfaces avaliadas durante as actividades de avaliação do risco de nível mais alto

[G 7] Da comparação entre o Ciclo em V CENELEC clássico e Figura 5 resulta que:

(a) o MCS abrange as fases de "1 a 10" e "13" do presente Ciclo em V. Inclui-se o conjunto de actividades necessárias à aceitação do sistema em avaliação;

(b) o MCS não abrange as fases "11", "12" e "14" do ciclo de vida do sistema:

(0) As fases “11” e “12” estão respectivamente relacionadas com a “operação e manutenção” e “monitorização do desempenho” do sistema após a sua aceitação com base no MCS. Estas duas fases são abrangidas pelo sistema de gestão de segurança (SGS) da EF e do GI – (ver CAIXA 4 do Figura 5. Contudo, se durante a operação, manutenção ou monitorização do desempenho do sistema for necessário modificar e readaptar o sistema (Fase 13 do Figura 5), apesar de já estarem em funcionamento, o MCS é aplicado de novo nas alterações exigidas, em conformidade com o Artigo 2.º. Por isso, se a alteração for significativa:

(i) os processos de gestão dos riscos e de avaliação do risco do MCS são aplicados nestas novas alterações;
(ii) é necessário que estas novas alterações sejam aceites, em conformidade com o Artigo 6.º;

(1) a “desactivação e eliminação” de um sistema já em operação (Fase 14) também pode ser considerada uma alteração significativa e, por essa razão, o MCS pode ser novamente aplicado em conformidade com o Artigo 2.º da Fase 14 do Figura 5.

.

Para mais informações sobre o âmbito de cada fase ou actividade no Ciclo em V CENELEC ilustrados no Figura 5, ver a secção 6 da norma EN 50 126-1 0.

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.

Não são consideradas necessárias explicações adicionais.

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] Não são consideradas necessárias explicações adicionais.

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] Regra geral, o proponente irá decidir sobre qual é o princípio de aceitação do risco mais adequado para controlar os perigos identificados com base nos requisitos específicos do projecto, bem como na experiência do proponente com os três princípios.

[G 2] Nem sempre é possível avaliar a aceitação do risco ao nível do sistema, usando apenas um dos três princípios de aceitação de risco. A aceitação do risco será frequentemente baseada numa mistura destes princípios. Se, para um perigo significativo, tiverem de ser aplicados mais do que um princípio de aceitação do risco de modo a controlar o risco associado, o perigo relacionado deve ser dividido em subperigos, para que cada subperigo individual seja adequadamente controlado por apenas um princípio de aceitação do risco.

[G 3] A decisão de controlar um perigo com um princípio de aceitação do risco terá de contemplar o perigo e as causas do perigo já identificadas durante a fase de identificação dos perigos. Desta forma, se existirem duas causas diferentes e independentes associadas ao mesmo perigo, o perigo terá de ser subdividido em dois subperigos diferentes. Cada subperigo será, em seguida, controlado por um único princípio de aceitação do risco. Os dois subperigos têm de ser registados e geridos no registo de perigos. Por exemplo, se o perigo for causado por um erro de design, isto pode ser gerido com a aplicação de um código de práticas, ao passo que se a causa do perigo for um erro de manutenção, o código de práticas poderá ser por si só insuficiente; é necessário, nesse caso, aplicar outro princípio de aceitação do risco.

[G 4] A redução do risco para um nível aceitável poderá exigir várias iterações entre as fases da análise do risco e da avaliação do risco até serem identificadas as medidas de segurança adequadas.

[G 5] Reconhece-se que é aceitável o risco residual actual obtido pelo retorno da experiência no terreno relativamente aos sistemas existentes e aos sistemas com base na aplicação de códigos de práticas. O risco resultante da estimativa expressa dos riscos baseia-se no parecer de peritos e nos diferentes pressupostos adoptados pelos peritos durante as análises ou nas bases de dados relacionadas com experiência operacional ou acidentes. Por isso, o risco residual resultante da estimativa expressa dos riscos não pode ser confirmado imediatamente pelo retorno da experiência do terreno. Essa confirmação exige tempo para operar, monitorizar e obter uma experiência representativa do sistema(s) relacionados. De um modo geral, a aplicação de códigos de práticas e comparação com sistemas de referência semelhantes tem como vantagem evitar a especificação em excesso

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

de requisitos de segurança desnecessariamente estritos que podem resultar dos pressupostos (de segurança) excessivamente conservadores nas estimativas expressas dos riscos. Contudo, pode acontecer que certos requisitos de segurança dos códigos de práticas ou de sistemas de referência semelhantes não necessitem de ser cumpridos no sistema a ser avaliado. Nesse caso, a aplicação de uma estimativa expressa dos riscos teria a vantagem de evitar uma concepção em excesso e desnecessária do sistema que está a ser avaliado e permitiria uma concepção mais eficiente do ponto de vista dos custos que ainda não foi experimentada.

[G 6] Se os perigos identificados e o(s) risco(s) associado(s) do sistema a ser avaliado não puderem ser controlados pela aplicação de códigos de prática ou de sistemas de referência semelhantes, é realizada uma estimativa expressa dos riscos, com base em análises quantitativas ou qualitativas de acontecimentos perigosos. Esta situação surge quando o sistema em avaliação é completamente novo (ou de design for inovador) ou quando o sistema se desvia de um código de práticas ou de um sistema de referência. A estimativa expressa dos riscos irá então avaliar se o risco é aceitável (ou seja, não é necessário uma análise mais aprofundada) ou se são necessárias medidas adicionais de segurança para continuar a reduzir o risco.

[G 7] Na secção 8 do Guia EN 50 126-2 0 poderá encontrar critérios orientadores a respeito da redução e aceitação de riscos.

[G 8] O princípio de aceitação do risco usado e a sua aplicação deverão ser avaliados pelo organismo de avaliação.

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] Por exemplo, se, no caso do software de um componente, a aplicação do processo de desenvolvimento SIL 4 da norma EN 50 128 for especificado como requisito de segurança, a demonstração terá de provar que o processo recomendado pela norma é cumprido. Isso inclui, por exemplo, a demonstração que:

(a) os requisitos de independência na organização do design, verificação e validação do software são cumpridos;
(b) os métodos correctos da norma EN 50 128 para o nível de integridade de segurança do SIL 4 são aplicados;
(c) etc.

[G 2] Por exemplo, se um designado código de práticas vai ser usado na produção de electroválvulas de freio de emergência, a demonstração terá de provar que todos os requisitos do código de práticas são cumpridos durante o processo de produção.

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 accepQuadro. 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] Podem ser identificados dois tipos de medidas de segurança:

(a) "medidas preventivas de segurança" que previnem a ocorrência de perigos ou as suas causas e;
(b) "medidas de mitigação de segurança", evitando que os perigos se transformem em acidentes ou reduzindo as consequências dos acidentes após a sua ocorrência (medidas de protecção).

Em benefício da operacionalidade, a prevenção das causas é, regra geral, mais eficiente.

[G 2] O proponente irá considerar como mais apropriadas as medidas de segurança que oferecem o melhor compromisso entre o custo ligado à redução do risco e o nível de risco residual. As medidas de segurança escolhidas tornam-se nos requisitos de segurança para o sistema que está a ser avaliado.

[G 3] É importante verificar que as medidas de segurança seleccionadas para controlar um perigo não entrem em conflito com outros perigos. Tal como representado no Figura 6, poderão acontecer, por exemplo, os dois casos seguintes(10):

(a) CASO 1: se a mesma medida de segurança (medida A do Figura 6) pode controlar vários perigos sem criar conflitos entre si, e se justificado do ponto de vista económico, a medida de segurança relacionada pode ser escolhida por si só como "requisito de segurança" associado. O número total de requisitos de segurança a cumprir é inferior à implementação de ambas as medidas B e C;

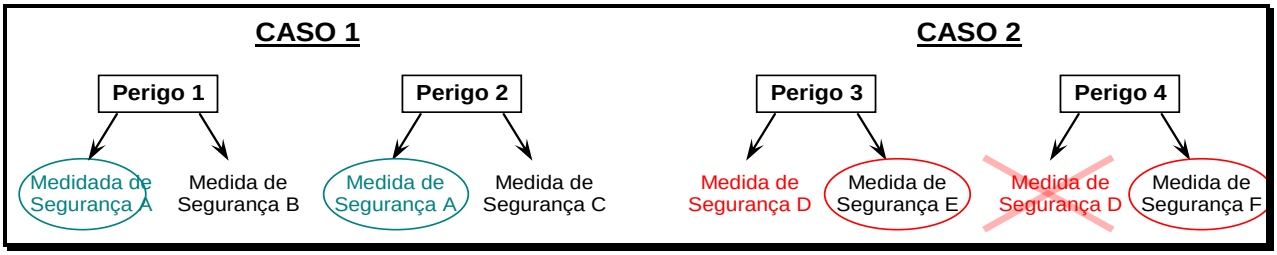

Figura 6: Escolha de medidas adequadas para controlar os riscos.

(b) CASO 2: da mesma forma, se uma medida de segurança pode controlar um perigo mas cria um conflito com outro perigo (medida D da Figura 6), não pode ser escolhida como "requisito de segurança". As outras medidas de segurança para o perigo considerado terão de ser usadas (medidas E e F Figura 6):

(1) Um exemplo típico do Sistema de Controlo e Comando é o uso da localização do comboio na linha quer para controlar a aplicação do freio, quer para autorizar a

(10) *Note-se que o guia não enumera todas as situações em que as medidas de segurança podem entrar em conflito com outros perigos identificados. São indicados apenas alguns exemplos ilustrativos.*

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

aceleração do comboio. O uso da parte frontal ou da cauda do comboio para determinar a localização do comboio , não é seguro em todas as situações:

(i) quando o sistema de controlo e comando ETCS tem de aplicar os freios de emergência como medida de segurança, recorre à PARTE FRONTAL COMO SEGURANÇA MÁXIMA, de modo a garantir que a frente do comboio pára mesmo antes de chegar ao Ponto de Perigo;

(ii) da mesma forma, quando o comboio recebe autorização para acelerar depois de uma limitação de velocidade, o sistema de controlo e comando ETCS usa a CAUDA COMO SEGURANÇA MÍNIMA;

(2) Outro exemplo é uma medida de segurança que pode ser válida para evitar, em praticamente todas as circunstâncias, que um comboio entre em modo de segurança (fail-safe), excepto se passar por um túnel ou ponte. Neste último caso, a medida D no CASO 2 do Figura 6 não será tomada.

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] Dependendo, por exemplo, de escolhas técnicas no design de um sistema, dos seus subsistemas e do equipamento, podem ser identificados novos perigos durante a fase de "demonstração da conformidade com os requisitos de segurança" (por exemplo, o uso de uma dada tinta pode provocar gases tóxicos em caso de incêndio). Estes perigos novos e os riscos associados devem de ser considerados como inputs novos num ciclo novo do processo iterativo de avaliação do risco. O apêndice A.4.3 da norma EN 50 129 contém outros exemplos em que novos perigos podem surgir e devem ser controlados.

2.2. Identificação dos perigos

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] Os perigos são expressos, na medida do possível, com o mesmo nível de pormenor. Pode acontecer que, durante as análises preliminares de perigo, sejam identificados perigos com vários níveis de pormenor (por exemplo, porque durante o – HAZOP – são reunidas pessoas com experiências diferentes).
O nível de pormenor depende também do princípio de aceitação do risco que é escolhido para controlar o(s) perigo(s) identificado(s). Por exemplo, se um perigo for controlado completamente por um código de práticas ou por um sistema de referência similar, não será necessário identificar o perigo com mais pormenor.

[G 2] Todos os perigos identificados durante o processo de avaliação do risco (incluindo os associados aos riscos genericamente aceitáveis), as medidas de segurança associadas e os riscos associados terão de ser inscritos no registo de perigos.

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

[G 3] Conforme a natureza do sistema a ser analisado, podem ser usados diferentes métodos para identificar os perigos:

(a) a identificação empírica de perigos pode ser usada recorrendo à experiência do passado (por exemplo, uso de listas de verificação ou listas genéricas de perigos);
(b) a identificação criativa de perigos pode ser usada em novas áreas que suscitam preocupação (previsão proactiva, por exemplo estudos “WHAT-IF” (o que aconteceria se…) estruturados tais como o FMEA ou HAZOP).

[G 4] Os métodos empírico e criativo de identificação de perigos podem ser usados em conjunto, complementando-se mutuamente, para garantir que a lista de potenciais perigos e as medidas de segurança, quando aplicáveis, são abrangentes.

[G 5] Como fase preliminar, a identificação do perigo pode começar com uma equipa de reflexão composta por peritos com competências diversas, abrangendo todos os aspectos relevantes da alteração significativa. Se o painel de peritos considerar necessário, poderão ser usados métodos empíricos para analisar uma função ou modo operacional específicos.

[G 6] Os métodos usados na identificação do perigo dependem da definição do sistema. O apêndice APÊNDICE B.

[G 7] Poderá encontrar mais informações sobre as técnicas de identificação de perigos no anexo A.2 e E do Guia da norma EN 50 126-2 0.

[G 8] A secção C.17 do apêndice C contém um exemplo de uma lista genérica de perigos.

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 accepQuadro 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] Para auxiliar o processo de avaliação do risco, os perigos significativos podem ser agrupados em diferentes categorias. Por exemplo, os perigos significativos podem ser classificados ou dispostos em função da gravidade esperada do risco e frequência da ocorrência. As orientações para esse exercício constam das normas do CENELEC: ver secção A.2. no Apêndice .

[G 2] A análise e a avaliação do risco descritas na secção 2.1.4 são aplicadas de forma prioritária, começando pelos perigos com classificação mais alta.

2.2.3. As a criterion, risks resulting from hazards may be classified as broadly accepQuadro 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 accepQuadro risks does not exceed a defined proportion of the overall risk.

[G 1] Por exemplo, um risco associado a um perigo pode ser considerado genericamente aceitável:

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

(a) caso o perigo seja inferior a uma dada percentagem (p. ex., x%) do Risco Máximo Tolerável para este tipo de perigo. O valor de x% pode basear-se nas melhores práticas e na experiência com várias abordagens de análise de risco, por exemplo, o rácio entre o risco genericamente aceitável e as classificações de risco intolerável nas curvas FN ou nas matrizes de risco. Isto pode ser representado conforme o Figura 7: Riscos Genericamente Aceitáveis;

(b) ou se a perda associada ao risco é tão pequena que não é razoável implementar contra medidas de segurança.

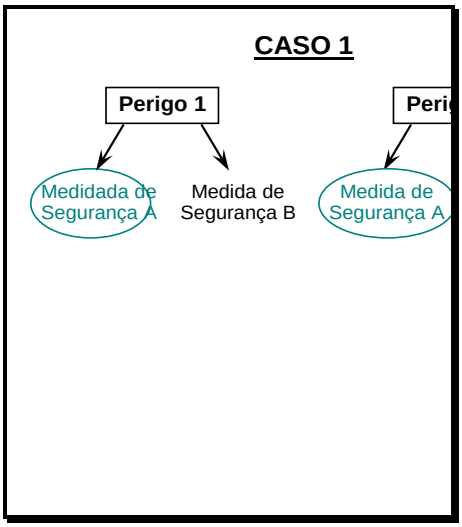

Figura 7: Riscos Genericamente Aceitáveis

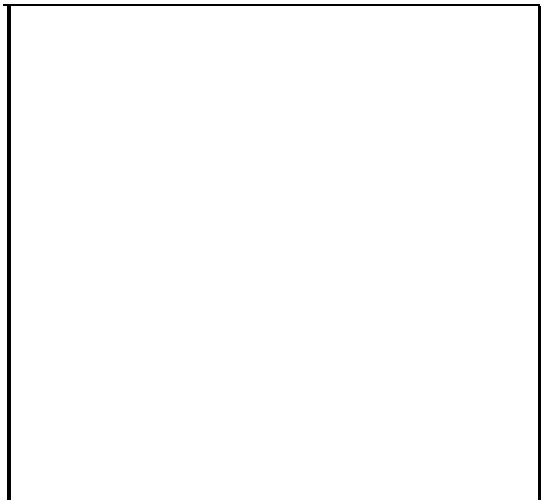

Figura 8: Filtração de perigos associados aos riscos genericamente aceitáveis.

[G 2] Além disso, se forem identificados perigos com diferentes níveis de pormenor (ou seja, por um lado, os perigos de nível alto, por outro, os sub-perigos pormenorizados), terão de ser tomadas precauções para evitar a classificação errada em perigos associados a riscos genericamente aceitáveis. A contribuição de todos os perigos associados ao(s) risco(s) genericamente aceitável (aceitáveis) não pode exceder um certo valor (p. ex., y%) do risco geral ao nível do sistema. Esta verificação é necessária para evitar que a lógica seja subvertida ao subdividir os perigos em muitos sub-perigos de nível baixo. Com efeito, se um perigo é expresso em vários sub-perigos "mais pequenos", cada um deles pode ser facilmente classificado como associado ao risco(s) genericamente aceitável, se avaliados de forma independente, mas associados a um risco significativo, se avaliados em conjunto (isto é, como um perigo de nível alto). O valor da proporção (p. ex., y%) depende dos critérios de aceitação de risco aplicáveis ao nível do sistema. Pode basear-se na experiência operacional, e calculado a partir da mesma, de sistemas de referência semelhantes.

[G 3] As duas verificações supra mencionadas (ou seja, de x% e y%) permitem que a avaliação de risco se concentre nos perigos mais importantes, garantindo, de igual forma, que os riscos significativos são controlados (ver Figura 8: Filtração de perigos associados aos riscos genericamente aceitáveis.).
Sem prejuízo dos requisitos legais de um Estado-membro, o proponente é responsável por definir, com base num parecer especializado, os valores de x% e y% e por fazer com que estes sejam avaliados de forma independente por um organismo de avaliação. Um exemplo de ordens de grandeza poderá ser x = 1% e y = 10%, caso seja considerado aceitável à luz do parecer dos especialistas.

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] A secção 2.2.2 exige que a classificação em "risco(s) genericamente aceitável" seja avaliada de forma independente por um organismo de avaliação.

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] O objectivo principal da actividade é a identificação de perigos que se relacionam com a alteração. Caso as medidas de segurança já tenham sido identificadas, terão de ser inscritas no registo de perigos. A natureza das medidas depende da alteração; poderão ser processuais, técnicas, operacionais ou organizacionais.

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] Mesmo se um risco é controlado num nível aceitável, o proponente poderá ainda decidir que são necessárias mais identificações de perigo pormenorizadas. Uma razão que poderá explicar isto é que poderão ser encontradas mais medidas de segurança de controlo de risco mais eficientes do ponto de vista dos custos, se forem realizadas mais identificações de perigo pormenorizadas.

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

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

[G 1] Não são consideradas necessárias explicações adicionais.

2.3. Uso de códigos de prática e avaliação de risco

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] Não são consideradas necessárias explicações adicionais.

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

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

(a) be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be accepQuadro 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] Não são consideradas necessárias explicações adicionais.

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] Não são consideradas necessárias explicações adicionais.

2.3.4. National rules notified in accordance with Artigo 8 of Directive 2004/49/EC and Artigo 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] Não são consideradas necessárias explicações adicionais.

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 accepQuadro. 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] Não são consideradas necessárias explicações adicionais.

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] Não são consideradas necessárias explicações adicionais.

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

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

[G 1] Não são consideradas necessárias explicações adicionais.

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 Artigo 6.*

Não são consideradas necessárias explicações adicionais.

2.4. Uso do sistema de referência e da avaliação de risco

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] A secção 8 do Guia da norma EN 50 126-2 0 contém mais informações sobre estes princípios.

2.4.2.	*A reference system shall satisfy at least the following requirements:* *(a) it has already been proven in-use to have an accepQuadro 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] Por exemplo, um antigo Sistema de Controlo e Comando cujo nível de segurança é considerado aceitável, sendo isso provado pelo uso, pode ser substituído por outro sistema com tecnologia mais recente e com um desempenho de segurança superior. É então pertinente verificar, de cada vez que se aplica um sistema de referência, se continua a reunir os critérios de aceitação.

[G 2] Por exemplo, dado que certos aspectos da segurança dos túneis ou da segurança do transporte de mercadorias perigosas podem ser específicos e podem depender de condições operacionais e ambientais, é necessário verificar em cada projecto que o sistema será usado nas mesmas condições.

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

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

(a) the risks associated with the hazards covered by the reference system shall be considered as accepQuadro;
(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] Não são consideradas necessárias explicações adicionais.

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 accepQuadro.

[G 1] A secção 8.1.3. do Guia da norma EN 50 126-2 0 contém mais informações sobre as análises das semelhanças.

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] Não são consideradas necessárias explicações adicionais.

2.5. Estimativa e determinação expressas dos riscos

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] Não são consideradas necessárias explicações adicionais.

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

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

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

[G 1] De modo a avaliar se os riscos do sistema em avaliação são aceitáveis ou não, são necessários critérios de aceitação de risco (ver caixas da "avaliação do risco" no Figura 1 : Quadro de gestão do risco no regulamento relativo ao MCS. N

[G 2]

Os critérios de aceitação de risco podem ser implícitos ou explícitos:

(a) Critérios de aceitação de risco implícitos: de acordo com as secções 2.3.5 e 2.4.3, os riscos abrangidos pela aplicação dos códigos de práticas e por comparação com referência a sistemas são considerados implicitamente aceitáveis, desde que (ver círculo tracejado da Figura)

(1) estejam reunidas as condições de aplicação dos códigos de práticas da secção 2.3.2;
(2) estejam reunidas as condições de uso de um sistema de referência na secção 2.4.2;

(b) Critérios de aceitação de risco explícitos: de modo a avaliar se o(s) risco(s) controlado(s) pela aplicação do cálculo de risco explícito é (são) aceitáveis ou não, são necessários critérios de aceitação de risco explícitos (ver círculo com linha normal no Figura 1 para o terceiro princípio). Estes podem ser definidos em níveis diferentes num sistema ferroviário. Poderão ser vistos como uma "pirâmide de critérios" (ver Figura 9) que começa pelos critérios de aceitação de risco de nível alto (expresso por exemplo, em risco social ou individual), até aos subsistemas e componentes (para abranger os sistemas técnicos), incluindo os operadores humanos durante a operação e as actividades de manutenção do sistema e subsistemas. Apesar de os critérios de aceitação de risco contribuírem para alcançar o desempenho de segurança do sistema, estando desta forma ligados aos objectivos comuns de segurança e aos valores de referência nacionais, é difícil criar um modelo matemático entre si. Ver 0 para mais pormenores.
O nível no qual são definidos os critérios de aceitação de risco explícitos terá de estar de acordo com a importância e complexidade da alteração significativa. Por exemplo, não é necessário avaliar o risco do sistema ferroviário global ao modificar um tipo de eixo no material circulante. A definição dos critérios de aceitação de risco pode centrar-se na segurança do material circulante. De igual forma, as grandes alterações ou adições ao sistema ferroviário existente não devem ser avaliadas somente com base no desempenho de segurança das funções individuais ou alterações que são acrescentadas. Deverá, também, ser verificado ao nível do sistema ferroviário que a alteração é, no geral, aceitável.

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

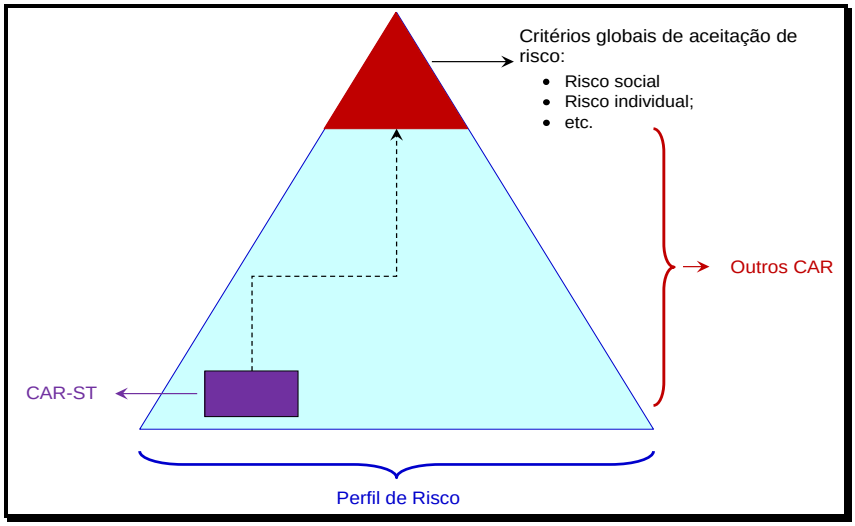

Figura 9: Pirâmide dos Critérios de Aceitação de Risco (CAR).

[G 3] Os critérios de aceitação de risco explícitos necessários para apoiar o reconhecimento mútuo serão harmonizados entre os Estados-membros pelo trabalho em curso da Agência no domínio dos critérios de aceitação de risco. Quando disponível, serão incluídas informações adicionais no presente documento.

[G 4] Entretanto, os riscos podem ser avaliados, por exemplo, através da matriz de risco que pode ser encontrada na secção 4.6 da norma da EN 50 126-1 0 Poderão também ser usados outros tipos de critérios adequados, desde que se considere que estes critérios proporcionam um nível de segurança aceitável no respectivo caso.

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

[G 1] Não são consideradas necessárias explicações adicionais.

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] Os pormenores suplementares sobre os CAR-ST, bem como os aspectos e funções do sistema técnico a que o critério se aplica, são fornecidos numa nota à parte da Agência associada ao presente documento: ver a secção A.3. do apêndice e o documento de referência 0.

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

2.5.5. Without prejudice to the procedure specified in Artigo 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 Artigos 23 and 25 of Directive 2008/57/EC shall apply.

[G 1] Não são consideradas necessárias explicações adicionais.

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 Artigo 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.

Não são consideradas necessárias explicações adicionais.

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.

Não são consideradas necessárias explicações adicionais.

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. DEMONSTRAÇÃO DO CUMPRIMENTO DOS REQUISITOS DE SEGURANÇA

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] Conforme explicado nos pontos [G 3] a [G 6] da secção 2.1.1, a "demonstração da conformidade do sistema com os requisitos de segurança" inclui as fases "6 a 10" do Ciclo em V CENELEC (ver CAIXA 3 do Figura 5). Ver ponto [G 3] da secção 2.1.1.

[G 2] Ver também o ponto 0 da secção 2.1.1 do presente documento.

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] Um exemplo de avaliações de segurança e de análises de segurança que podem ser realizadas ao nível do subsistema é a análise de causa: ver Figura 10. Porém, poderá ser usado qualquer outro método para demonstrar a conformidade do subsistema com os requisitos de segurança do input.

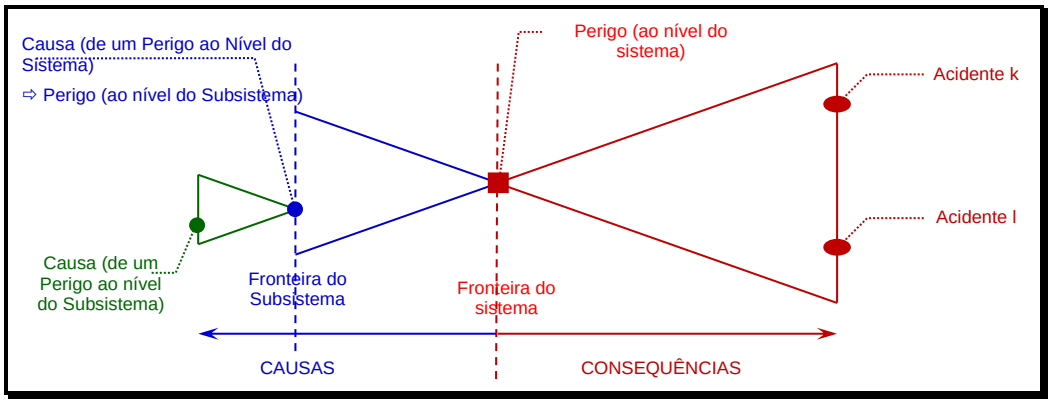

Figura 10: Figura A.4 da norma EN 50 129: Definição de perigos em relação à fronteira do sistema.

[G 2] A estruturação hierárquica dos perigos e das causas, relativamente aos sistemas e subsistemas, pode ser repetida para cada fase do nível inferior do Ciclo em V CENELEC da Figura 5. A identificação de perigos e as actividades relacionadas com as análises de causa (ou quaisquer métodos relevantes), bem como o uso de códigos de prática, sistemas de referência semelhantes e análises explícitas e avaliações, poderão ser repetidas em cada fase do ciclo de desenvolvimento do sistema de modo a inferir, a partir das medidas de segurança identificadas ao nível do subsistema, os requisitos de segurança a ser cumpridos na próxima fase. Este processo encontra-se ilustrado na Figura 11.

[G 3] Ver também o ponto 0 da secção 2.1.1 do presente documento.

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

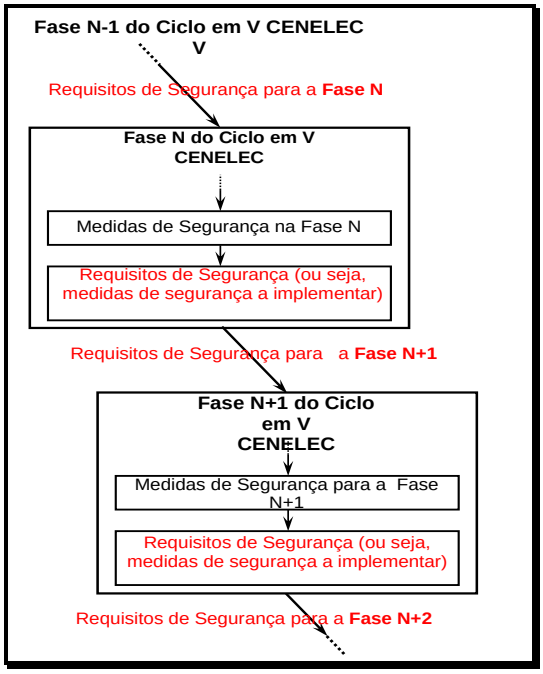

Figura 11: Derivação dos requisitos de segurança para as fases de nível inferior.

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] Todas as actividades representadas na CAIXA 3[(11)] do Ciclo V CENELEC na Figura 5 são por isso avaliadas de forma independente.

[G 2] O tipo e nível de pormenor da avaliação independente que é realizada pelos organismos de avaliação (ou seja, avaliação pormenorizada ou macroscópica) são abrangidos pelas explicações do Artigo 6.º.

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] Por exemplo, o método de extinção de um incêndio pode gerar um novo perigo (sufocação) que irá impor novos requisitos de segurança (por exemplo, um procedimento específico para

(11) *A correspondência de actividades entre o MCS e o Figura 5 (i.e. Figura 10 do ciclo em V CENELEC da norma 50 126) é descrita na secção 2.1.1. Em especial, o ponto [G 3] da secção 2.1.1 enumera as actividades do CENELEC que são incluidas na fase do MCS de "demonstração da conformidade do sistema com os requisitos de segurança".*

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

evacuar os passageiros). Um outro exemplo é o uso de vidro temperado para evitar que os vidros das janelas se quebrem durante os acidentes e que os passageiros sofram ferimentos provocados pelos vidros ou que sejam projectados. Deduz-se um novo perigo: a evacuação de emergência das carruagens através das janelas é mais difícil, o que poderá ter como resultado requisitos de segurança segundo os quais as janelas terão de ser especialmente concebidas para permitir a evacuação.

[G 2] Exemplo de uma alteração operacional: Exige-se que a passagem de todos os transportes de materiais perigosos seja interdita em linhas que atravessam zonas densamente povoadas. Ao invés, deverá então passar por uma rota alternativa com túneis, criando desta forma diferentes tipos de perigos.

[G 3] No apêndice A.4.3 da norma EN 50 129 poderão ser encontrados outros exemplos de novos perigos que podem ser identificados durante a demonstração da conformidade do sistema com os requisitos de segurança.

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. GESTÃO DOS PERIGOS

4.1. Processo de gestão dos perigos

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] O uso de um registo de perigos para registar, gerir e controlar as informações relevantes do ponto de vista da segurança é igualmente recomendado pelas normas CENELEC 50 126-1 0 e 50 129 0.

[G 2] Por exemplo, dependendo da complexidade do sistema, um actor pode ter um ou vários registos de perigos. Em ambos os casos, o(s) registo(s) de perigo(s) está/são sujeito(s) à avaliação independente do organismo(s) de avaliação. Por exemplo, uma solução poderá passar por:

(a) um "registo interno de perigos" para a gestão de todos os requisitos de segurança internos aplicáveis ao subsistema pelo qual o actor é responsável. O tamanho e a quantidade de trabalho de gestão dependem da sua estrutura e, obviamente, da complexidade do subsistema. Porém, dado que é usado para fins de gestão interna, o registo de perigos não tem de ser comunicado aos restantes actores. O registo interno de perigos contém todos os perigos identificados que são controlados, bem como as medidas de segurança associadas que são validadas;
(b) um "registo externo de perigos" para transferir aos restantes actores as medidas de segurança associadas (que o próprio actor não pode implementar completamente) de acordo com a secção 1.2.2. Normalmente, o segundo registo de perigos é mais pequeno e requer menos trabalho de gestão (ver o exemplo da secção C.16.4C.16.4 do Apêndice C.

[G 3] Se for complicado gerir vários registos de perigo, outra solução possível é gerir todos os perigos e as medidas de segurança associadas e abordadas nas alíneas a) e b) supra num único registo, mas com a possibilidade de dois relatórios de registo de perigos (ver exemplo na secção C.16.3. do Apêndice C):

(a) um relatório de registo interno de perigos que até poderá ser desnecessário se o registo de perigo está bem estruturado, de modo a permitir uma avaliação independente;
(b) Um relatório de registo externo de perigos para transferir perigos e as medidas de segurança associadas aos restantes actores.

[G 4] Conforme explicado na secção 4.2, no final do projecto quando o sistema é aceite:

(a) todos os perigos que são transferidos para os restantes actores são controlados pelo registo externo de perigos do actor que os transfere. Dado que são importados e geridos nos registos internos de perigos dos restantes actores, não têm de ser mais geridos pelo actor envolvido durante o ciclo de vida do subsistema;

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) contudo, todas as medidas de segurança associadas não devem ser validadas no registo de perigos pelas razões mencionadas no ponto (c)[G9] da secção 4.2. Com efeito, é útil que a organização que exporta as restrições de uso assinale de forma clara no seu registo de perigos que as medidas de segurança associadas não foram validadas.

[G 5] Reciprocamente, todos os registos internos de perigos são mantidos ao longo de todo o ciclo de vida do (sub)sistema. Isso permite acompanhar o progresso da monitorização dos riscos associados aos perigos identificados durante o funcionamento e manutenção do (sub)sistema, isto é, mesmo após a sua desactivação: ver CAIXA 4 do Ciclo em V CENELEC no Figura 5:

4.1.2. The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. In particulab, it shall contaif a cleab referejce to dhe obigin and to the selected risk acceptalce principles and sh!ll alear´y ideltify the aator(s) in charge of cmntrolling each hazard.

[G 1] A informação qobre os perigos e as medidas de segurança assoahadas rece`adas $oq 2estantes actores (ver secção 1.2.2) ijcduem todos os pressupostms(12(e restbições de uso(**Error! Bookmark not defined.**??) (também deqignadas condições da aplicação relacionadas com a segurança) aplicáveis aos vários subsistemas, aplicação genérica e casks de segurança de produtos genéricos que são produzidos pelos fabricantes, nos casos relefantes.

[G 2] A secção **Error! Reference source not found.** do Apêndice **Error! Reference source not found.** derapeve tm exemplo pnrsível de eqtrutura do registo de perigos.

4.2. Troca de informações

All hazardc and related safety reptiraments whhch cannot be bontrolled bx ole actor alone shall be communicated to anopher relevant actor in order to find jointly an adequate rolution. The hazards reci{4ered in the haz`rd recopd of the actor who transfers them shall only be "controlled" when the evaluation of t`e pisks associated with these hazards is lade by the other actor and the solution is agreed by all cnncerned.

[G 1] Por exemplo, no caso do subsistema de odometria do equipamento ETCS (sistema europeu de controlo dos comboios) a bordo, o fabricante pode validar no laboratório os algoritmos, simulando os sinais teóricos qua podem ser gerados pelos respectivos dispositivos sensíveis de odometria. Contudo, a validação completa do subsistema de odometria requer o auxílio das empresas ferroviárias e do gestor da infra-estrutura para se proceder à validação usando um comboio real e ema roda de comboio real em contacto com o carril.

(12) *Consulte o ponto [G 5] da secção 1.1.5 e as notas de rodapé 9 e 10 na página 31 deste documento para obter mais explicações sobre a terminologia dossiês de segurança "produto genérico e aplicação genérica e "pressupostos e restrições de utilização".*

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] Um outro exemplo poderá ser a tr`nsfepêjcaa do3 fabricantes para as emprerac &erroviápias das medidas de cegerança operacionais ou de manutanção relativas ao eatipamen`o técnico. Estaq me`ida1 de qeguranga tdbão de ser implemen4adas peda empbesa de caminhgs-$e-ferro.

[G 3] Para perlitir que estes perigos e ac medidas de segurajça associadas e os risaos sejam conjuntamente avaliados pelas organizaçõec envolvidas, sebá útil aue a crganizaçãg que gs identificou forleça tgdas as explicações necessárias p`ra que se compreenda alaramente o problema. Pode acnnteber pue a formulação ilicial dos perigos, das medidas de segurança e dms rircos tenha de ser alterada `a`a torna%los compreensmveis, sem que seja fecdssário discuti-los de novo em conjuntg. A rdavaliação conjenta dos perigos pode levar a que sejam identidicadas novas medidas de segurança.

[G 4] O actkr que recebe `s madidaa e responsável pela implementagão, vdrifi#ação e validação das ledidas de segurança novas ou rebebidas regista no seu próprio registo de pericgs todks os perigos relaaionadgs com ar medidas de seguralça associadas (quer as imporpadas, quer as annjuntalenpd identifacadas!.

[G 5] Se uma medida de segurança não for completamente validada, terá de ser elaborada uma restrição de (por exemplo, medidas de mitigação operacional) e registada no registo de perigos. Com efeito, é possível que as medidas de segurança tècnicas/de design

(a) não sejam correctamente implementadas, ou;
(b) não sejam implementadas na íntegra, ou;
(c) não sejam implemantadas, de forma deliberada, por exemplo, porque foram implementadas medidas de segurança diferentes das medidas registadas no registo de perigos (por exemplo, para fins de redução de custos). Dado que não foram validadas, essas medidas de segurança têm de ser claramente identificadas no registo de perigos. Terão de ser fornecidos dados concretos/justificações para explicar a razão por que as medidas implementadas [13] em alternativa são adequadas, bem como prova de que com as medidas de segurança substitutas o sistema cumpre os requisitos de segurança;
(d) etc.

Nestes casos, as medidas de segurança técnicas/ de design não podem ser verificadas nem validadas durante a gestão de perigos. O perigo(s) relacionado(s) e as medidas de segurança têm de ficar em aberto no registo de perigos, de modo a evitar o desvio das medidas de segurança para outros sistemas pela aplicação do princípio de aceitação de risco do "sistema de referência semelhante"

[G 6] Normalmente, as medidas de segurança “não correctamente ” e/ou “não completamente” implementadas” são detectadas ao início do ciclo de vida do sistema e corrigidas antes da aceitação do sistema. Contudo, se as medidas de segurança forem detectadas de forma tardia para serem implementadas de forma correcta e completa, a organização responsável pela implementação e gestão tem de identificar e registar no registo de perigos restrições de uso claras para o sistema que está a ser avaliado. Estas restrições de uso são frequentemente restrições de aplicação operacional do sistema em avaliação.

(13) *Se forem implementadas medidas de segurança diferentes das inicialmente especificadas, essas medidas terão igualmente de ser registadas no registo de perigos.*

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 7] Poderá também ser útil registar no registo de perigos se as medidas de segurança associadas serão correctamente implementadas numa fase tardia do ciclo de vida do sistema ou se o sistema vai continuar a ser usado com as restrições de uso identificadas. Também pode ser útil registar no registo de perigos a justificação da não implementação de forma correcta/completa das medidas de segurança técnicas associadas.

[G 8] O actor que recebe as restrições de uso:

(a) importa todas as restrições para o seu próprio registo de perigos;
(b) garante que as condições de uso do sistema em avaliação estão em conformidade com todas as restrições de uso recebidas;
(c) verifica e valida que o sistema em avaliação cumpre estas restrições de uso

[G 9] Dependendo das decisões acordadas pelas organizações envolvidas:

(a) ou as medidas técnicas de segurança são implementadas de forma correcta no design numa fase posterior.
A organização que exporta as restrições de uso continua a acompanhar a implementação técnica correcta das medidas de segurança associadas. Consequentemente, as medidas de segurança não podem ser validadas e os perigos a elas associados não podem ser controlados no registo de perigos desta organização, até que as medidas técnicas de segurança correspondentes não sejam completamente implementadas. Isto terá de ser garantido, mesmo que, entretanto, as restrições de uso exportadas sejam implementadas.

(b) ou as medidas técnicas de segurança não serão implementadas no design em fase posterior. O sistema continuará, portanto, a ser usado durante o seu ciclo de vida com as restrições de uso associadas. Neste caso, poderá ser feito o seguinte:

(1) a organização que exporta as restrições de uso não regista as medidas de segurança associadas como “validadas” no seu registo de perigos. Desta forma, ao usar o sistema como sistema de referência em outros projectos, as respectivas questões de segurança não serão negligenciadas. Por isso, mesmo que outro actor aceite gerir de forma diferente os riscos associados, é útil que a organização que exporta as restrições de uso identifique claramente nos seu registo de perigos que as medidas de segurança associadas não foram validadas, ou

(2) a descrição do sistema pode ser alterada de modo a incluir as restrições de uso no âmbito de aplicação do sistema (ou seja, nos pressupostos do sistema) e nos requisitos de segurança. Isto irá permitir que os perigos sejam controlados. Deste modo, ao usar-se o sistema como sistema de referência noutra aplicação:

(i) o sistema novo terá de ser usado nas mesmas condições (ou seja, terá de cumprir as restrições de uso associadas a esses pressupostos), ou;
(ii) a avaliação de risco adicional será realizada pelo proponente face aos desvios em relação a esses pressupostos.

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. EVIDÊNCIAS DA APLICAÇÃO DO PROCESSO DE GESTÃO DOS RISCOS

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.

O sistema de gestão de segurança do gestor da infra-estrutura e da empresa de caminhos-de-ferro já abrangem estes requisitos. Para os restantes actores do sector ferroviário que estão envolvidos na alteração significativa, embora o SMS não seja obrigatório, no geral, pelo menos ao nível do projecto, possuem um processo de gestão de qualidade (PGQ) e/ou um processo de gestão de segurança (PGS). Ambos os processos assentam numa hierarquia de documentação estruturada, quer dentro da empresa, quer, pelo menos, dentro do projecto. Dão igualmente resposta às necessidades de documentação da gestão da RAMS. Essa documentação estruturada pode ser basicamente composta pelo seguinte (ver também o Figura 12):

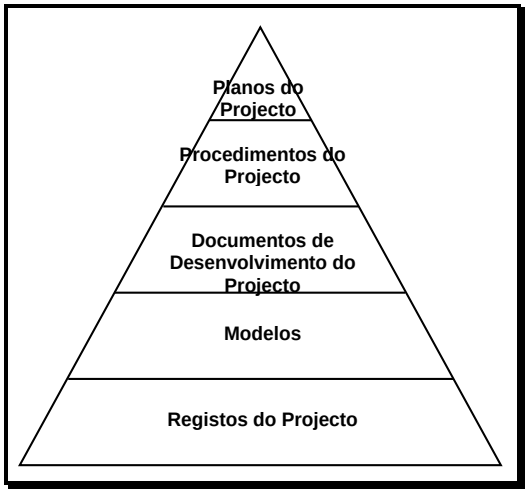

Figura 12: Hierarquia da documentação estruturada.

Planos do projecto elaborados para descrever a organização a ser criada para gerir uma actividade dentro do projecto

Procedimentos do projecto elaborados para descrever pormenorizadamente a forma de alcançar uma determinada tarefa . Normalmente, os procedimentos e instruções existem dentro da empresa e são usados como tal. Os procedimentos de projecto novos só são elaborados se houver necessidade de descrever uma tarefa específica dentro do projecto considerado.

Documentos de desenvolvimento do projecto elaborados durante o ciclo de vida do sistema representado no Figura 5.

Modelos da empresa ou pelo menos modelos de projecto existem para os diferentes tipos de documentos a apresentar.

Registos do projecto elaborados durante o projecto e necessários para demonstrar a conformidade com a gestão de qualidade da empresa e com os processos de gestão de segurança.

Esta é uma forma de satisfazer as necessidades de dados documentados. Poderá haver outras formas de o fazer, desde que os critérios do MCS sejam cumpridos.

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

As normas do CENELEC aconselham a demonstrar a conformidade do sistema com os requisitos funcionais e de segurança num documento de dossier de segurança (ou num relatório de segurança). Mesmo que não seja obrigatório, o uso de um dossier de segurança fornece num documento de justificação de segurança estruturada:

a prova da gestão de qualidade;
a prova da gestão de segurança;
a prova da segurança funcional e técnica;

Ao mesmo tempo, há a vantagem de apoiar e guiar o(s) organismo(os) de avaliação na avaliação independente da aplicação correcta do MCS.

O dossier de segurança descreve e resume a forma como os documentos do projecto resultantes da aplicação dos processos de gestão de qualidade e/ou segurança da empresa ou do projecto se relacionam entre si dentro do processo de desenvolvimento do sistema de modo a demonstrar a segurança do sistema. Normalmente, o dossier de segurança não inclui um grande volume de dados concretos e de documentação de apoio, mas dá referências precisas a esses documentos.

Dossier de segurança para sistemas técnicos: As normas do CENELEC podem ser usadas como guias para conceber e/ou estruturar os casos de segurança:

ver norma EN 50 129 {Ref. 7} relativa a "Aplicações Ferroviárias - Comunicação, Sinalização e Sistemas de Processamento - Sistemas Electrónicos de Segurança para a sinalização"; no apêndice H.2 do Guia EN 50 126-2 {Ref. 9} também se propõe uma estrutura para o dossier de segurança dos sistemas de sinalização;
ver apêndice H.1 do Guia EN 50 126-2 {Ref. 9} quanto à estrutura do dossier de segurança para o material circulante;
ver apêndice H.3 do Guia EN 50 126-2 {Ref. 9} quanto à estrutura do dossier de segurança para as infra-estruturas;

Como decorre destas referências, a estrutura do dossier de segurança para os sistemas técnicos, bem como o seu conteúdo, depende do sistema no qual terá de ser fornecida a demonstração de conformidade com a segurança.

O dossier de segurança identificado no apêndice H do Guia EN 50 126-2 {Ref. 9} fornece apenas exemplos e poderá não ser adequado a todos os sistemas de dada espécie. Por isso, terá de ser usado com o devido discernimento para se concluir sobre o que se adequa a cada aplicação específica.

Dossier de segurança para os aspectos organizacionais e operacionais dos sistemas ferroviários:

Presentemente, não há uma norma dedicada que indique a estrutura, o conteúdo e um guia para conceber o dossier de segurança para aspectos organizacionais e operacionais de um sistema ferroviário. Contudo, dado que o dossier de segurança visa demonstrar, de forma estruturada, a conformidade do sistema com os seus requisitos de segurança, o mesmo tipo de estrutura do dossier de segurança pode ser usado nos sistemas técnicos. Com efeito, as referências do ponto [G 4] da secção 0 fornecem conselhos e uma lista de verificação de itens aos quais terá de ser dada resposta, independentemente do tipo de sistema que está a ser avaliado. A gestão de alterações organizacionais e operacionais requerem o mesmo tipo de gestão de qualidade e de processos de gestão de segurança do que as alterações técnicas, com uma demonstração da conformidade do sistema com os requisitos de segurança especificados. Os requisitos das normas do CENELEC não aplicáveis aos aspectos organizacionais e operacionais são os meramente relacionados com as

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

instalações de design do sistema técnico, como por exemplo, os princípios "segurança inerente do hardware contra falhas", compatibilidade electromagnética (EMC), etc.

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

description of the organisation and the experts appointed to carry out the risk assessment process,

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 accepQuadro level.

[G 1] Dependendo da complexidade do sistema, estes elementos podem ser reunidos num ou vários casos de segurança. Ver respectivamente os pontos [G4] e [G5] da secção 0 quanto à estrutura do dossier de segurança dos sistemas técnicos e os aspectos operacionais e organizacionais.

[G 2] Ver também a secção A.4. do Apêndice A para possíveis exemplos de dados concretos.

[G 3] Calcula-se que a duração dos sistemas e subsistemas técnicos no sector ferroviário se situe, no geral, em cerca de 30 anos. Durante esse longo período de tempo é plausível esperar também um número de alterações significativas nesses sistemas. Poderão então ser realizadas mais avaliações de risco nestes sistemas e nas suas interfaces com a documentação de acompanhamento que terá de ser revista, completada e transferida entre os diferentes actores e organizações, usando os registos de perigos. Isto implica requisitos muito rigorosos no controlo da documentação e na gestão da configuração.

[G 4] É então útil que a empresa que arquiva toda a informação sobre a avaliação de risco e gestão de risco garanta que os resultados/informações sejam armazenados em suporte físico que possa ser lido/acedido durante todo o ciclo de vida do sistema (isto é, durante 30 anos).

[G 5] Os principais motivos deste requisito são, entre outros:

(a) garantir que todas as análises de segurança e registos de segurança do sistema em avaliação estão acessíveis durante toda a vida do sistema. Assim:

(1) em caso de mais alterações significativas no mesmo sistema, está disponível a documentação mais recente do sistema;

(2) em caso de problema durante a vida do sistema, é útil permitir retroceder nas análises de segurança associadas e nos registos de segurança;

(b) para garantir que as análises de segurança e os registos de segurança do sistema em avaliação estão acessíveis caso sejam usados noutra aplicação como sistema de referência semelhante.

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

ANEXO II AO REGULAMENTO RELATIVO AO MCS

Critérios a cumprir pelos Organismos de Avaliação

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 2] Não são consideradas necessárias explicações adicionais.

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

APÊNDICE A: ESCLARECIMENTOS ADICIONAIS

A.1. Introdução

A.1.1. Este apêndice tem como finalidade facilitar a leitura do presente documento. Em vez de se fornecerem grandes quantidades de informação no documento, os assuntos mais complexos têm uma explicação adicional no presente apêndice.

A.2. Classificação de perigos

A.2.1. É fornecido um guia na secção 4.6.3. da norma EN 50 126-1 {Ref. 8}, bem como no apêndice B.2 do Guia EN 50 126-2 0, para a classificação/posicionamento hierárquico de perigos.

A.3. Critério de aceitação dos riscos para sistemas técnicos (CAR-ST)

A.3.1. Limite superior ou Aceitabilidade do Risco de Sistemas Técnicos

A.3.1.1. O CAR-ST é descrito na secção 2.5.4. de 0.

A.3.1.2. A finalidade do CAR-ST é especificar um limite superior de aceitabilidade de risco para os sistemas técnicos para os quais os requisitos de segurança não podem ser obtidos pela aplicação de códigos de prática nem por comparação com sistemas de referência semelhantes. Consequentemente, define um ponto de referência, a partir do qual os métodos de análise de risco para os sistemas técnicos podem ser calibrados. Tal como se descreve na secção A.3.6. do apêndice A do presente documento, este ponto de referência ou limite superior de aceitabilidade de risco pode ser usado para determinar os critérios de aceitação de risco para outras falhas funcionais dos sistemas técnicos que não têm um potencial directo de consequências catastróficas credível (ou seja, com outra gravidade). Porém, o CAR-ST não é um método de análise de risco.

A.3.1.3. O CAR-ST é um critério semi-quantitativo. Aplica-se quer às falhas aleatórias do hardware, quer às falhas/erros sistemáticos do sistema técnico. As falhas/erros sistemáticos do sistema técnico que eventualmente resultam de erros humanos durante o processo de desenvolvimento do sistema técnico (ou seja, especificação, design, implementação e validação) são, desta foram, abrangidos. Contudo, os erros humanos durante a operação e manutenção dos sistemas técnicos não são abrangidos pelo CAR-ST.

A.3.1.4. De acordo com os apêndices A.3 e A.4 da norma CENELEC 50 129, as falhas/erros sistemáticos não são quantificáveis e assim sendo os objectivos quantitativos têm de ser demonstrados apenas em caso de falhas aleatórias de hardware, sendo que as falhas/erros

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

sistemáticos são tratados pelos métodos qualitativos [14]. *"Dado que não é possível avaliar a integridade de uma falha sistemática através de métodos quantitativos, os níveis de integridade de segurança são usados para agrupar métodos, ferramentas e técnicas que, se usados de forma eficiente, proporcionam um nível adequado de confiança na realização do sistema com o nível de integridade atribuído*

A.3.1.5. De igual forma, de acordo com as normas CENELEC, a integridade do software dos sistemas técnicos não é quantificável. A norma CENELEC 50 128 fornece um guia para o processo de desenvolvimento do software relacionado com a segurança, em função do nível de integridade de segurança exigido. Inclui-se o design, verificação, validação e os processos de garantia de qualidade do software.
De acordo com a norma CENELEC 50 128; no caso de um sistema de controlo electrónico programável, implementando funções de segurança, o nível de integridade de segurança mais alto possível para o processo de desenvolvimento de software é o SIL 4, que corresponde a uma taxa de perigo tolerável quantitativo de 10^{-9} h^{-1}.

A.3.1.6. Assim, dado que as falhas/erros sistemáticos não podem ser quantificados, têm de ser, ao invés, geridos de forma qualitativa pondo em prática um processo de qualidade e segurança compatível com o nível de integridade de segurança necessário para o sistema em avaliação.

a finalidade do processo de qualidade é "minimizar a incidência de erros humanos em cada fase do ciclo de vida, reduzindo assim o risco de falhas sistemáticas no sistema";
a finalidade do processo de segurança é "*reduzir a incidência dos erros humanos relacionados com a segurança ao longo do ciclo de vida, reduzindo assim o risco residual das falhas sistemáticas relacionadas com a segurança*".

A.3.1.7. As normas contêm orientações de gestão da incidência de falhas/erros sistemáticos, bem como orientações sobre as eventuais medidas de design de protecção contra falhas devidas a causas/modos comuns (CCF/CMF), para garantir também que o sistema técnico entra em modo de segurança caso surjam essas falhas/erros.

A norma CENELEC 50 126-1 {Ref. 8} e o seu Guia 50 126-2 {Ref. 9} enumeram as cláusulas da norma CENELEC 50 129 e indicam a sua aplicabilidade para as evidências documentadas de sistemas que não os de sinalização: ver Quadro 9.1 do Guia 50 126-2 {Ref. 9} . Esta enumeração dá orientações sobre como lidar com as falhas resultantes do próprio sistema e com o efeito no ambiente do sistema em avaliação;

Por exemplo, no *"Quadro E.5: Características de design (referida em 5.4)"* da norma CENELEC 50 129 {Ref. 7} são dadas técnicas/medidas para as características de design *"para evitar e controlar as falhas causadas por:*

"quaisquer falhas residuais de design";
"condições ambientais";

(14) *De acordo com as normas CENELEC 50 126, 50 128 e 50 129, o dado quantitativo que lida com as falhas aleatórias de hardware terá de estar sempre ligado a um nível de integridade de segurança para gerir as falhas/erros sistemáticos. Por isso, o dado 10^{-9} h^{-1} do CAR-ST requer, de igual forma, a criação de um processo adequado para também gerir as falhas/erros sistemáticos correctamente. Todavia, para facilitar a leitura da nota, refere-se frequentemente apenas as falhas de hardware aleatórias do sistema técnico.*

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

"utilização incorrecta ou erros de operação";
"quaisquer falhas residuais no software";
"factores humanos";

Os apêndices D e E da norma CENELEC 50 129 {Ref. 7} fornecem guias e medidas para evitar falhas sistemáticas e o controlo do hardware aleatório e das falhas/erros sistemáticos dos sistemas electrónicos relacionados com a segurança na sinalização. Muitas destas medidas podem ser alargadas a outros sistemas que não os de sinalização através de uma referência a estas orientações no Quadro 9.1 do Guia 50 126-2 {Ref. 9}.

a norma CENELEC 50 128 fornece orientações para o processo de desenvolvimento do software relacionado com a segurança em função do nível de integridade de segurança (SIL 0 a SIL 4) exigido para o software do sistema em avaliação.

A.3.1.8. O CAR-ST representa igualmente o nível de integridade mais alto que pode ser exigido de acordo com as normas CENELEC e IEC. Para facilidade de referência, são citados os requisitos da norma IEC 61508-1 e CENELEC 50 129:

IEC 61508-1: *"Esta norma fixa um limite inferior no objectivo das medidas de falha em modo perigoso de falha, que podem ser exigidas. Estas são especificadas como os limites inferiores do nível 4 de integridade de segurança. "Poderá ser possível realizar os designs dos sistemas relacionados com a segurança com valores mais baixos para os objectivos das medidas de falha, nos sistemas não complexos, mas considera-se que os valores do quadro representam o limite do que pode ser alcançado em sistemas relativamente complexos (por exemplo, sistemas electrónicos programáveis relacionados com a segurança)."*

EN 50129: *"Uma função com requisitos quantitativos mais exigentes do que 10^{-9} h^{-1} será tratada de uma das seguintes formas:*

se for possível dividir a função em sub-funções funcionalmente independentes, a THR pode ser dividida entre essas sub-funções e um nível de integridade do sistema (SIL) atribuído a cada sub-função:
se a função não puder ser dividida, as medidas e os métodos necessários para o SIL 4, deverão ser pelo menos, concretizados, e a função será usada em combinação com outras medidas técnicas e operacionais, de modo a alcançar a THR necessária."

A.3.1.9. Todos os sistemas técnicos precisam então de limitar o requisito de segurança quantitativo de acordo com esse número. Se houver necessidade de um nível maior de protecção, isso não poderá ser alcançado apenas com um sistema. A arquitectura do sistema tem de ser alterada, por exemplo, recorrendo a dois sistemas independentes em paralelo que se verificam mutuamente de modo a gerarem outputs seguros. Porém, desta forma, os custos do desenvolvimento do sistema técnico aumentam.

Observação: se existirem funções, por exemplo sistemas essencialmente mecânicos que, com base na experiência operacional alcançaram um nível de integridade superior, o nível de segurança poderá então ser descrito com um determinado código de prática ou os requisitos de segurança podem ser constituídos através de uma análise das semelhanças do sistema existente. No âmbito do MCS, o CAR-ST só poderá ser aplicado, caso não existam códigos de prática nem sistemas de referência.

A.3.1.10. Resumindo:

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

(a) de acordo com as normas CENELEC 50 126, 50 128 e 50 129 as falhas/erros sistemáticos no desenvolvimento não são quantificáveis;

a incidência das falhas/erros sistemáticos, bem como o seu risco residual, terá de ser controlada e gerida pela aplicação de processos de qualidade e de segurança adequados que sejam compatíveis com o nível de integridade de segurança requerido no sistema em avaliação;
o nível de integridade de segurança mais alto que se pode alcançar é o SIL4, quer nas falhas aleatórias de hardware, quer nas falhas/erros sistemáticos dos sistemas técnicos;
este limite do nível de integridade de segurança SIL 4 implica que a taxa de perigo máxima tolerável (THR), ou seja, a taxa de falha máxima, dos sistemas técnicos também tem de ser limitada a $10^{-9}\ h^{-1}$.

A.3.1.11. Uma taxa de perigo tolerável de $10^{-9}\ h^{-1}$ pode ser alcançada pelo sistema técnico como uma "arquitectura à prova de falhas" (que por definição cumpre tal desempenho de segurança) ou com uma "arquitectura redundante" (por exemplo, dois canais de processamento independentes que se verificam entre si).

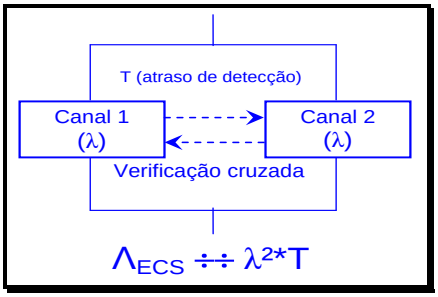

Figura 13: Arquitectura redundante de um sistema técnico.

No caso de uma arquitectura redundante, pode ser demonstrado que o erro crítico de segurança (Λ_{ECS}) (*wrong side failure*) do sistema técnico é proporcional a λ^2*T sendo que:

λ^2 representa o quadrado do erro crítico de segurança de um canal;

T representa o tempo necessário para que um canal detecte o erro(s) crítico de segurança do outro canal. Normalmente, é um múltiplo do tempo/ciclo de processamento de um canal. Regra geral, T é inferior a 1 segundo.

A.3.1.12. Com base nesta fórmula (λ^2*T), teoricamente é possível demonstrar (considerando apenas erros aleatórios no hardware do sistema técnico (consultar também o ponto A.3.1.13. do Apêndice que é possível atingir o requisito quantitativo de $10^{-9}\ h^{-1}$.para o CAR-ST. As falhas/erros sistemáticos deverão ser geridos por um processo: referido no ponto A.3.1.6. do Apêndice A. Por exemplo:

a) com um tempo médio entre falhas de 10 000 horas para o número de fiabilidade de um canal, e o pressuposto conservador que todas as falhas do canal não são seguras, o erro crítico de segurança do canal é 10-4 h-1;
b) mesmo com um tempo de 10 minutos (ou seja, $\approx 2*10^{-3}$ horas) para detector os erros críticos de segurança do outro canal, que é igualmente um pressuposto conservador;

O erro crítico de segurança geral é $\Lambda_{ECS} \approx 2 * 10^{-10}\ h^{-1}$

A.3.1.13. Na prática, no caso de uma arquitectura redundante, a avaliação quantitativa dos erros críticos de segurança do hardware globais tem de ser em consideração as medidas tomadas no design e de protecção contra CCF/CMF e para garantir que o sistema de

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

segurança entra em modo de segurança (*fail-safe*) em caso de falha/erro CCF/CMF. Esta avaliação do erro crítico de segurança (Λ_{ECS}) também terá de considerar:

os componentes comuns a todos os canais, por exemplo, inputs isolados ou comuns a todos os canais, fonte de alimentação, comparadores e votadores comuns, etc.;

b) o tempo para detectar as falhas pendentes ou latentes. Nos sistemas técnicos complexos, este tempo pode ser superior, em várias ordens de grandeza, a um segundo;

c) o impacto das falhas devidas a causas/modos comuns (CCF/CMF).

Poderão ser encontradas orientações nas normas aludidas no ponto A.3.1.7. do Apêndice A do presente documento.

A.3.2. Fluxograma do teste de aplicabilidade do CAR-ST

A.3.2.1 A forma de aplicar o CAR-ST aos perigos que decorrem das falhas dos sistemas técnicos pode ser representada tal como consta do Figura 14.

A.3.2.2 A descrição da aplicação desse fluxograma num exemplo encontra-se na secção C.15. do Apêndice C.

A.3.3. Definição de um Sistema Técnico do MCS

A.3.3.1. O CAR-ST aplica-se apenas aos sistemas técnicos. A definição que segue é a definição de "sistema técnico" que consta do Artigo 3.º (22)º do Regulamento relativo ao MCS:

entende-se por "sistema técnico" um produto ou uma montagem de produtos, incluindo o projecto, a implementação e a documentação de apoio. O desenvolvimento de um sistema técnico começa com a especificação dos seus requisitos e termina com a sua aceitação. Embora o projecto das interfaces relevantes com o comportamento humano seja tido em conta, os operadores humanos e as suas acções não fazem parte do sistema técnico. O processo de manutenção é descrito nos manuais de manutenção, mas, em si mesmo, não faz parte do sistema técnico.

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

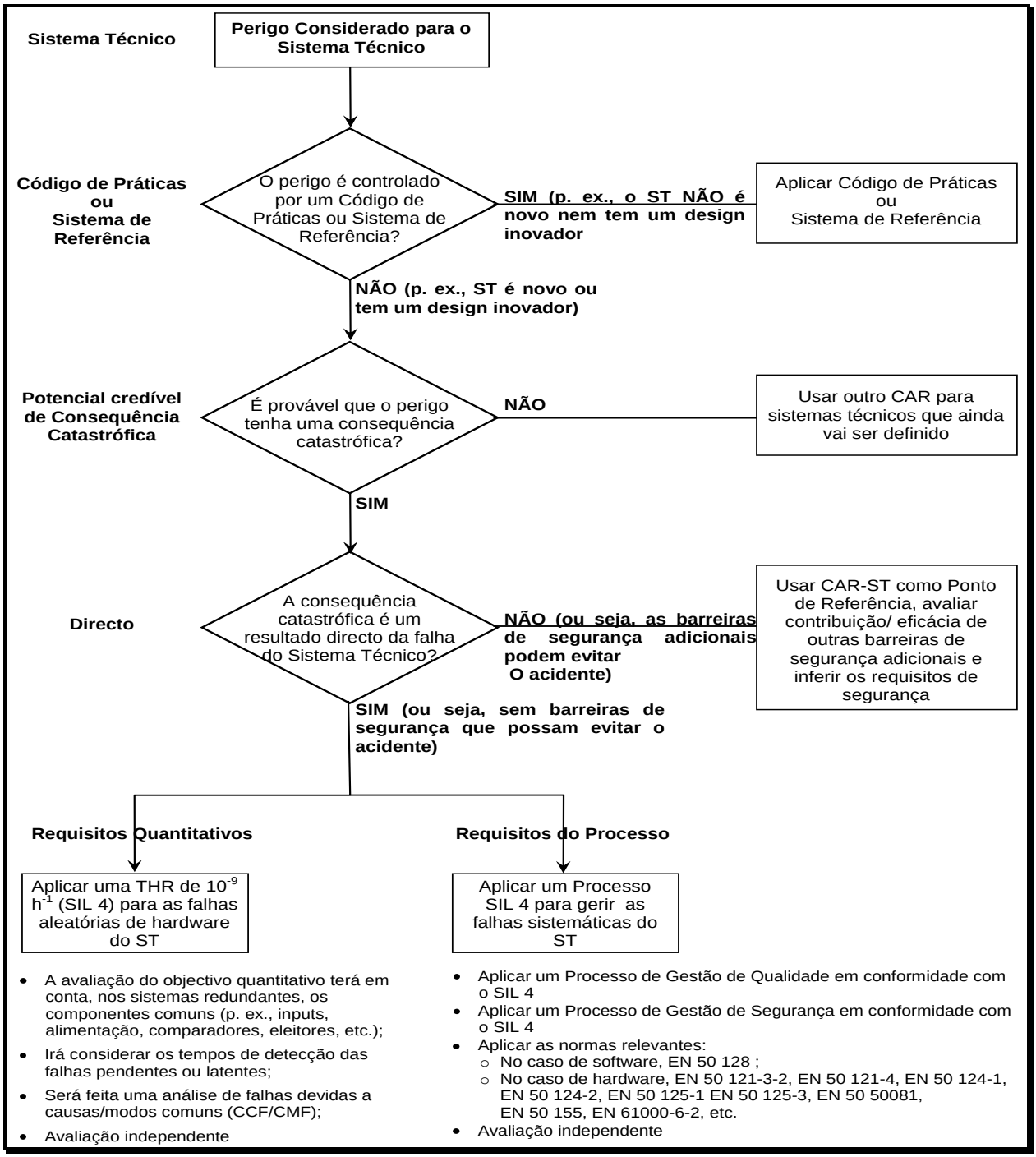

Figura 14: Fluxograma do teste de aplicabilidade do CAR-ST.

A.3.4. Explicação da definição de "sistema técnico"

A.3.4.1. Esta definição do sistema técnico descreve o âmbito do sistema técnico: *"por sistema técnico entende-se um produto ou uma montagem de produtos, incluindo o projecto, a implementação e a documentação de apoio."* Por conseguinte, inclui e consiste no seguinte:

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

(a) as partes físicas que constituem o sistema técnico;

(b) o software associado (caso exista);

(c) o design e a implementação do sistema técnico incluindo, se aplicável, a configuração ou parâmetros de um produto genérico para especificar os requisitos da aplicação específica;

(d) a documentação de apoio necessária para:

(1) O desenvolvimento do sistema técnico;
(2) a operação e manutenção do sistema técnico;

A.3.4.2. As notas associadas a esta definição aprofundam o âmbito do sistema técnico:

(a) "*O desenvolvimento de um sistema técnico começa com a especificação dos seus requisitos e termina com a sua aceitação*". Inclui as fases de 1 a 10 do Ciclo em V representadas na Figura 10 da norma CENELEC 50 126-1 {Ref. 8};

b) *"Embora o projecto das interfaces relevantes com o comportamento humano seja tido em conta, os operadores humanos e as suas acções não fazem parte do sistema técnico".* Apesar de os erros relacionados com o factor humano durante a operação e a manutenção do sistema técnico não fazerem parte do sistema técnico em si, o design das interfaces com os operadores humanos precisa de os considerar. O objectivo é minimizar a probabilidade dos erros humanos devido aos problemas de design das interfaces relevantes com os operadores humanos;

c) *"O processo de manutenção é descrito nos manuais de manutenção, mas, em si mesmo, não faz parte do sistema técnico."* Isto significa que o CAR-ST não tem de ser aplicado à operação e manutenção do sistema técnico; a operação e a manutenção dependem fortemente de processos e acções realizados por pessoas.
Todavia, para auxiliar a manutenção dos sistemas técnicos, a definição do sistema técnico terá de incluir os requisitos relevantes (por exemplo, manutenção periódica preventiva ou manutenção correctiva, em caso de falha) com um grau de pormenor suficiente. Porém, a forma como a manutenção tem de ser organizada e realizada no sistema técnico relevante, não faz parte da definição do sistema técnico, mas sim dos respectivos manuais de manutenção.

A.3.4.3. Ver também a secção A.3.1. no Apêndice A.

A.3.5. Funções dos Sistemas Técnicos aos quais se aplica o CAR-ST

A.3.5.1. De acordo com a definição do CAR-ST, este aplica-se aos erros críticos de segurança das funções a ser cumpridas pelo sistema técnico se existir um *"potencial credível e* ***directo*** *de consequência catastrófica"*: ver secção 2.5.4. de 0.

A.3.5.2. O CAR-ST também pode ser aplicado às funções que envolvem sistemas técnicos. mas cujas falhas não têm um "potencial directo de consequência catastrófica" Neste caso, o CAR-ST terá de ser aplicado como objectivo comum no conjunto de eventos que provocam a consequência catastrófica. Com base neste objectivo geral, a contribuição real de cada evento, e concomitantemente das falhas do sistema técnico envolvidas no cenário considerado terão de ser inferidas de acordo com a secção A.3.6. no Apêndice A.

Esse uso do CAR-ST ainda terá de ser discutido e acordado pelo grupo de trabalho do MCS.

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

A.3.5.3. O CAR-ST aplica-se a que funções do sistema técnico? De acordo com a norma IEC 61226:2005 :

neste contexto, uma função é definida como “uma finalidade ou objectivo específicos a serem alcançados e que podem ser especificados ou descritos sem referência aos meios físicos usados para alcançá-los.

uma função (considerada uma caixa negra) transfere os parâmetros de input (por exemplo, informações relativas a materiais ou energia) em parâmetros de output relacionados com os objectivos (por exemplo, informações relativas a materiais ou energia);

a análise da função é independente da sua efectivação técnica.

A.3.5.4. O CAR-ST aplica-se aos seguintes tipos de funções:

(a) Exemplos para o subsistema a bordo ETCS:

(1) “dar ao Maquinista as informações que o permitam conduzir o comboio em segurança e aplicar os freios em caso de velocidade excessiva.” Com base nas informações recebidas a partir da linha (velocidade permitida) e com o cálculo de velocidade do ECTS a bordo, o maquinista e o ECTS a bordo estão em condições de garantir que o comboio não excede o limite de velocidade permitido. O CAR-ST aplica-se à validação da velocidade do comboio através do sistema a bordo desde que:

(i) não haja uma barreira adicional (directa) pois a informação dada ao Maquinista também está sob avaliação;
(ii) o excesso de velocidade do comboio possa causar um descarrilamento, que é um acidente com um potencial de consequências catastróficas;

(2) “dar ao Maquinista as informações que permitam conduzir o comboio em segurança e aplicar os freios em caso de violação da autorização de movimento.”

b) exemplo de um circuito de via: “detectar a ocupação da secção da via”. O CAR-ST aplica-se nesses termos a esta função apenas se não existir uma função de “sequência de monitorização” implementada no sistema de encravamento;
c) exemplo de um ponto: “controlo da posição de ponto";

A.3.5.5. Algumas normas também definem as funções às quais o CAR-ST pode ser aplicado. Por exemplo:

(a) A norma prEN 0015380-4 0 (ModTrain Work) define na sua parte normativa os três níveis hierárquicos de função (alargada nos anexos informativos até cinco níveis). No total, a prEN 0015380-4 define várias centenas de funções relacionadas com os comboios;
b) No geral, recomenda-se a selecção das funções a partir dos três primeiros níveis da norma prEN 0015380-4 (mas não abaixo), tendo também em consideração a estrutura desagregada do produto;
c) para as funções fora do âmbito da norma prEN 0015380-4, os níveis funcionais adequados têm de ser decididos por comparação utilizando o parecer de peritos.

Estes exemplos de funções da norma prEN 0015380-4 ainda têm de ser trabalhados pela Agência no âmbito do trabalho relativo aos riscos genericamente aceitáveis e aos critérios de aceitação de risco.

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

A.3.5.6. O CAR-ST também é aplicável, por exemplo, à seguinte função da norma prEN 0015380-04 “controlo da pendulação” (código = CLB). A função pode ser usada ao nível do sistema nas seguintes formas:

(a) Primeiro caso: o comboio inclina-se nas curvas para o conforto dos passageiros e terá de monitorizar a conformidade com o gabarito da infra-estrutura.

(b) Segundo caso: o comboio inclina-se nas curvas para o conforto dos passageiros, mas não precisa de monitorizar a conformidade com o gabarito da infra-estrutura;

No primeiro caso, será aplicado o CAR-ST, mas não no segundo, pois a falha da função de pendulação não tem uma consequência catastrófica.

A.3.5.7. O exemplo (b) no ponto A.3.5.4. e os exemplos no ponto A.3.5.6. no Apêndice A mostram claramente que não será exequível produzir uma lista predefinida de funções à qual de aplica o CAR-ST em todos os casos. Isto dependerá sempre da forma como o sistema irá usar estas funções do subsistema.

A.3.5.8. Um exemplo da aplicação do CAR-SR é fornecido na secção C.15 do Apêndice C.

A.3.6. Exemplos de Aplicação do CAR-ST

A.3.6.1. Introdução

(a) este capítulo mostra exemplos sobre a forma de determinar a taxa de falha para as gravidades de perigo e sobre a forma de inferir os requisitos de segurança inferiores a $10^{-9}\,h^{-1}$. Este documento não prefere nem ordena um determinado método. Apenas indica informações sobre a forma de uso do CAR-ST para calibrar alguns métodos genericamente usados. Terá de ser desenvolvido pelos trabalhos da Agência no âmbito dos riscos genericamente aceitáveis e critérios de aceitação de risco.

(b) com efeito, o CAR-ST pode ser aplicado de forma directa apenas a um pequeno número de casos, dado que na prática não existem muitas falhas funcionais nos sistemas técnicos que originem acidentes de forma directa e com consequências potencialmente catastróficas. Por isso, de modo a aplicar o critério aos perigos com consequências, não catastróficas e para determinar a taxa de falha objectivo, é possível realizar ponderações (por exemplo, calibrando uma matriz de risco com este critério) entre os diferentes parâmetros, por exemplo, gravidade vs. frequência.

A.3.6.2. Exemplo 1: Cedência de risco de directo

(a) o CAR-ST pode ser facilmente aplicado a cenários em que variam alguns parâmetros independentes das condições de referência definidas no CAR-ST na secção 2.5.4 do Regulamento relativo ao MCS {Ref. 9};

(b) partamos do princípio que num determinado parâmetro p a relação com o risco é multiplicativa. Partamos do princípio que na condição de referência p* está presente enquanto que no cenário alternativ0 p’ é aplicável. Neste caso, apenas o parâmetro do rácio p*/p' é relevante e a taxa de ocorrência poderá ser reduzida. Este procedimento poderá ser sujeito a iterações se os parâmetros forem independentes.

(c) exemplo:

(1) Partamos do princípio que o potencial real da consequência catastrófica foi avaliado por parecer especializado em dez vezes inferior ao potencial sob as

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

condições de referência na secção 2.5.4 do Regulamento relativo ao MCS0 {Ref. 3} . Então, o requisito seria $10^{-8}\,h^{-1}$ e não $10^{-9}\,h^{-1}$

(2) Partamos do princípio que é identificada uma barreira de segurança adicional por outro sistema técnico (independentemente das consequências) e que é eficiente em 50% dos casos;

(3) Neste caso o requisito de segurança seria $5*10^{-7}\,h^{-1}$ (ou seja, $0.5*10^{-8}\,h^{-1}$) e não $10^{-9}\,h^{-1}$.

A.3.6.3. Exemplo 2: Calibração da Matriz de Risco

(a) Para usar devidamente o CAR-ST numa matriz de risco, a matriz tem de se relacionar com o nível de sistema correcto (comparável com o indicado na secção A.3.5. do Apêndice A).

(b) o CAR-ST define um campo da matriz de risco como tolerável que corresponde à coordenada (gravidade catastrófica; $10^{-9}\,h^{-1}$ frequência da ocorrência): ver campo vermelho do Quadro 5.. Todos os campos que se relacionam com uma frequência superior têm de ser classificados de "intoleráveis". Isto serve para notar que só em caso de um potencial directo credível de uma consequência catastrófica, a frequência de acidentes é igual à frequência de falha funcional.

(c) o resto da matriz poderá então ser preenchido, mas terão de ser tidos em consideração os efeitos tais como a aversão ao risco e o escalonamento das categorias. No caso mais simples de escalonamento linear de décadas (conforme identificado no Quadro 5: com a seta) o campo desta forma classificado como “aceitável” pelo CAR-ST é extrapolado de forma linear para o resto da matriz. Isto significa que todos os campos na mesma diagonal (ou abaixo da diagonal) também são classificados de “aceitáveis”. Os campos abaixo também podem ser classificados de “aceitáveis”.

Quadro 5: Exemplo Típico de uma Matriz de Risco calibrada.

Frequência da ocorrência de um acidente (causado por um perigo)	**Níveis de Risco**			
Frequente (10^{-4} por hora)	**Intolerável**	**Intolerável**	**Intolerável**	**Intolerável**
Provável (10^{-5} por hora)	**Intolerável**	**Intolerável**	**Intolerável**	**Intolerável**
Ocasional (10^{-6} por hora)	**Aceitável**	**Intolerável**	**Intolerável**	**Intolerável**
Remoto (10^{-7} por hora)	**Aceitável**	**Aceitável**	**Intolerável**	**Intolerável**
Improvável (10^{-8} por hora)	**Aceitável**	**Acceptable**	**Acceptable**	**Intolerável**
Incredível (10^{-9} por hora)	**Aceitável**	**Acceptable**	**Acceptable**	**Acceptable**
	Insignificante	Marginal	Crítico	Catastrófico
	Níveis de Gravidade da Consequência dos Perigos (ou seja, de acidente)			

Avaliação de Risco	**Redução/Controlo de Risco**
Intolerável	O risco será eliminado.
Aceitável	O risco é aceitável. É necessária Avaliação Independente.

d) uma vez preenchida a matriz, esta também pode ser aplicada aos perigos não catastróficos. Por exemplo, se outra falha funcional tiver uma gravidade classificada de "crítica", segundo a matriz de risco calibrada, a frequência de acidentes tolerável não deve ser superior a "improvável" (ou até menos).

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

e) deve notar-se que o uso da matriz de risco pode levar a resultados muito conservadores, quando se aplica às frequências de falha funcional (ou seja, em falhas funcionais que não provocam acidentes directamente).

A.3.6.4. Princípio de calibração de outros Métodos de Análise de Risco

Há outros métodos de análise de risco, por exemplo o esquema de número de prioridade de risco proposto ou o gráfico de risco da VDV 331 ou IEC 61508 que também podem ser calibrados através de um procedimento semelhante ao identificado na matriz de risco:

(a) primeiro passo: classificar o ponto de referência do CAR-ST como tolerável e os pontos com frequência mais alta ou gravidade mais alta como um CAR-ST intolerável.

(b) segundo passo: o uso de mecanismos de ponderação para o método particular para extrapolar a tolerância do risco para perigos não catastróficos (recorrendo à ponderação linear do risco como ponto de partida).

(c) Terceiro passo: quanto aos perigos não catastróficos, o CAR-ST pode então ser derivado do método de análise de risco calibrado, por comparação da coordenada (frequência; gravidade) com a curva FN obtida.

A.3.7. Conclusões do CAR-ST

A.3.7.1. No quadro geral de avaliação de risco proposto pelo MCS, os critérios de aceitação de risco são necessários para determinar quando o nível residual de risco(s) se torna aceitável e quando parar o cálculo de risco explícito.

A.3.7.2. O CAR-ST é um objectivo de design ($10^{-9}\,h^{-1}$) para sistemas técnicos.

A.3.7.3. Os principais objectivos do CAR-ST são:

(a) especificar um limite superior de aceitabilidade de risco e, consequentemente, um ponto de referência, a partir do qual os métodos de análise de risco dos sistemas técnicos podem ser calibrados

(b) permitir o reconhecimento mútuo dos sistemas técnicos, dado que o risco associado e as avaliações de segurança serão avaliados com o mesmo critério de aceitação de risco em todos os EM;

(c) poupar nos custos, dado que não são necessários requisitos de segurança quantitativos desnecessariamente altos;

(d) facilitar a concorrência entre fabricantes. O uso de diferentes critérios de aceitação de risco em função quer do proponente, quer do Estado-membro, levaria a indústria a realizar várias demonstrações diferentes dos mesmos sistemas técnicos. Por conseguinte, isso iria colocar em risco a competitividade dos fabricantes e tornar os produtos desnecessariamente caros.

A.3.7.4. O requisito semi-quantitativo presente no CAR-ST não terá de ser sempre demonstrado nos sistemas técnicos. Na verdade, no âmbito do MCS, o CAR-ST só tem de ser aplicado aos sistemas técnicos nos quais os perigos identificados não podem ser adequadamente controlados com o uso de códigos de prática nem através de comparação com os sistemas de referência. Isto permite definir requisitos de segurança mais baixos, desde que o nível de segurança global possa ser mantido

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

A.3.7.5. Apenas quando não existe nenhum código de prática nem um sistema de referência é necessário um critério harmonizado de aceitação de risco semi-quantitativo para os sistemas técnicos.

A.3.7.6. Dado que o nível de integridade de segurança para as falhas/erros sistemáticos é limitado ao SIL4, o nível de integridade de segurança para as falhas aleatórias de hardware dos sistemas técnicos terá igualmente de ser limitado a SIL4. Isto corresponde a uma taxa de perigo máximo tolerável de 10-9 h-1 (isto é, a taxa de falha máxima). De acordo com a norma CENELEC 50 129, se forem necessários requisitos de segurança mais exigentes, isso não poderá ser alcançado apenas com um sistema; a arquitectura do sistema tem de ser alterada, por exemplo, recorrendo a dois sistemas, o que inevitavelmente provoca um aumento drástico dos custos. Para mais pormenores, consulte a secção A.3.1. do Apêndice A.

A.3.7.7. Por fim, a secção A.3.6. do Apêndice A mostra como o CAR-ST pode ser usado como ponto de referência para calibrar os métodos de análise de risco em questão, se os sistemas técnicos tiverem um potencial de consequências menos graves do que catastróficas.

A.4. Evidências da avaliação de segurança

A.4.1. Esta secção fornece um guia de evidências, as quais são geralmente fornecidas a um organismo de avaliação, de modo a permitir a avaliação independente e realizar a aceitação de segurança, sem prejuízo dos requisitos nacionais do Estado-membro. Isto pode ser usado como uma “check-list" para verificar que todos os aspectos associados são abrangidos e documentados, quando relevante, durante a aplicação do MCS.

A.4.2. Plano de segurança: O CENELEC aconselha a apresentação de um plano de segurança no início do projecto, ou se tal não se revelar conveniente para o projecto, aconselha a que a descrição associada seja incluída em qualquer outro documento relevante. Se os organismos de avaliação forem nomeados ao início do projecto, o plano de segurança também pode ser submetido ao seu parecer. Em princípio, o plano de segurança descreve:

a organização criada e a competência das pessoas envolvidas no desenvolvimento e na avaliação de risco;
todas as actividades relacionadas com a segurança que são planeadas ao longo das várias fases do projecto, bem como os resultados esperados;

A.4.3. Dados necessários na fase de definição do sistema:

descrição do sistema:

(1) definição do âmbito/limites;
(2) descrição de funções;
(3) descrição da estrutura do sistema:
(4) descrição das condições operativas e ambientais;

descrição das interfaces externas;
descrição das interfaces internas;
descrição das fases do ciclo de vida;
descrição dos princípios de segurança;
descrição dos pressupostos que definem os limites da avaliação de risco;

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

A.4.4. Para garantir a realização da avaliação de risco, o contexto da alteração pretendida é tido em conta na definição do sistema:

(a) Se a alteração pretendida é uma modificação de um sistema existente, a definição do sistema descreve o sistema antes da alteração e também a alteração pretendida:
(b) Se a alteração pretendida é a construção de um novo sistema, a descrição está limitada à definição do sistema, dado que não há descrição de quaisquer sistemas existentes.

A.4.5. Dados necessários da fase de identificação do sistema:

Descrição e justificação (incluindo limitações) dos métodos e das ferramentas de identificação de perigos (método “top-down” , bottom-up, HAZOP, etc.);
resultados:

Listas de perigos:
Perigos do sistema (limites);
Perigos do subsistema;
Perigos da interface;
as medidas de segurança que podem ser identificadas durante esta fase;

A.4.6. Os seguintes dados <u>também são necessários na fase de análise de risco</u>:

demonstração que todos os requisitos em questão dos códigos de prática são cumpridos no sistema em avaliação, quando são usados códigos de prática para controlar perigos. Isto inclui a demonstração da correcta aplicação dos respectivos códigos de prática;

quando são usados sistemas de referência semelhantes para controlar perigos:

definição para o sistema em avaliação dos requisitos de segurança dos respectivos sistemas de referência;
demonstração que o sistema em avaliação está a ser usado em condições operacionais e ambientais semelhantes às do sistema de referência relevante. Se isto não puder ser feito, as demonstrações em como os desvios ao sistema de referência são correctamente avaliados
dados que comprovam que os requisitos de segurança dos sistemas de referência são correctamente implementados no sistema em avaliação;

se o cálculo do risco explícito for usado para controlar os perigos:

descrição e justificação (incluindo limitações) dos métodos e ferramentas de análise de risco (qualitativos, quantitativos, semi-quantitativos, análise não regressiva,...);
identificação das medidas de segurança existentes e factores de redução de risco para cada perigo (incluindo aspectos relacionados com os factores humanos);
avaliação e classificação do risco para cada perigo:

estimativa das consequências do perigo e justificação (com pressupostos e condições);
estimativa da frequência do perigo e justificação (com pressupostos e condições);
classificação de perigos de acordo com a sua gravidade e frequência de ocorrência;

identificação de medidas de segurança apropriadas adicionais que produzem riscos aceitáveis para cada perigo (processo repetido depois da fase de avaliação);

A.4.7. <u>Dados necessários na avaliação de risco:</u>

quando a estimativa de risco explícito é realizada:

definição e justificação dos critérios de avaliação de risco para cada perigo;

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

Demonstração/justificação de que as medidas de segurança e os requisitos de segurança cobrem cada perigo com um nível aceitável (de acordo com o critério de avaliação de risco supra);

Em virtude das secções 2.3.5 e 2.4.3 Regulamento relativo ao MCS, os riscos cobertos pela aplicação dos códigos de prática e por comparação com os sistemas de referência são considerados implicitamente aceitáveis, desde que, respectivamente, (ver círculo do Figura 1):

estejam reunidas as condições de aplicação dos códigos de prática da secção 2.3.2;
estejam reunidas as condições de uso de um sistema de referência na secção 2.4.2;

Os critérios de aceitação de risco são implícitos nestes dois princípios de aceitação de risco.

A.4.8. Evidências da gestão de perigos:

(a) registo de todos os perigos num registo de perigos, contendo os seguintes elementos:
perigo identificado;
medidas de segurança que previnem a ocorrência de perigos ou que mitigam as suas consequências;
requisitos de segurança relativos às medidas;
parte relevante do sistema;
actor responsável pelas medidas de segurança;
estado do perigo (por exemplo, em aberto, resolvido, transferido, controlado, etc.);
data de registo, revisão e controlo de cada perigo;

(b) descrição de como os perigos serão geridos de forma eficaz durante a totalidade do ciclo de vida;

(c) descrição da troca de informações entre as partes, dos perigos nas interfaces e atribuição de responsabilidades.

A.4.9. Evidências relacionadas com a qualidade da avaliação de risco e processo de avaliação:

(a) descrição das pessoas envolvidas no processo e da sua competência;

(b) nas estimativas de risco explícito, descrição de informações, dados e outras estatísticas usados no processo e justificação da adequação (por exemplo, estudos de sensibilidade relativos aos dados usados).

A.4.10. Evidências relativas à conformidade com os requisitos de segurança:

(a) lista de normas utilizadas;

(b) descrição do design e dos princípios operacionais;

(c) dados da aplicação de um sistema de boa qualidade e de gestão de segurança para o projecto: Ver alínea [G 3]da secção 1.1.2;

(d) resumo dos relatórios de análise de segurança (por exemplo, análise das causas do perigo) que demonstram o cumprimento dos requisitos de segurança;

(e) descrição e justificação dos métodos e ferramentas (FMECA, FTA,…) que são usados na análise das causas do perigo;

(f) resumo da verificação de segurança e testes de validação.

A.4.11. Dossier de segurança: O CENELEC aconselha a que todas os dados anteriormente mencionados sejam reagrupados e resumidos num documento que é apresentado ao organismo de avaliação: ver pontos [G 4] e [G5] da secção 0.

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

APÊNDICE B: EXEMPLOS DE TÉCNICAS E FERRAMENTAS QUE FACILITAM A APLICAÇÃO DO PROCESSO DE AVALIAÇÃO DO RISCO

B.1. Poderão ser encontradas técnicas e ferramentas para realizar as actividades de avaliação de risco abrangidas pelo MCS no anexo E do Guia EN 50126-2 {Ref. 9}. O quadro E.1 contém um resumo das técnicas e das ferramentas. Cada técnica é descrita e, quando necessário, é feita referência a outras normas, para mais informações.

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

APÊNDICE C: EXEMPLOS

C.1. Introdução

C.1.1. Este apêndice tem como finalidade facilitar a leitura do presente documento. Reúne exemplos com a finalidade de facilitar a aplicação do MCS.

C.1.2. Os exemplos de avaliações de risco ou de segurança mencionados neste apêndice, não resultam da aplicação do processo do MCS, dado que foram realizados antes existir o Regulamento relativo ao MCS. Os exemplos podem ser classificados em:

(a) Exemplos, com referência à sua origem, recebidos de peritos do grupo de trabalho do MCS.

(b) *Exemplos, deliberadamente sem referência à sua origem, também recebidos de peritos do grupo de trabalho do MCS.* Os peritos referidos solicitaram que a origem permanecesse confidencial;

(c) Exemplos, cuja origem não é mencionada, e que foram facultados pelos membros da equipa da Agência com base na sua anterior experiência profissional pessoal.

Para cada exemplo, é feita a comparação entre o entre o processo aplicado e o processo exigido pelo MCS, bem como os argumentos e o valor acrescentado da realização dos passos adicionais (se existirem) solicitados pelo MCS.

C.2. Exemplos da aplicação dos critérios de alteração significativa do Artigo 4.º (2)

C.2.1. A Agência está a trabalhar na definição daquilo que pode ser considerado uma “alteração significativa”. É indicado um exemplo desse trabalho nesta secção sobre como aplicar os critérios do Artigo 4.º (2).

C.2.2. A alteração consiste em modificar, numa passagem de nível operada manualmente, a forma como os controladores de circulação comunicam as informações sobre a direcção da aproximação de um comboio ao operador da passagem de nível. A alteração está representada na Figura 15:

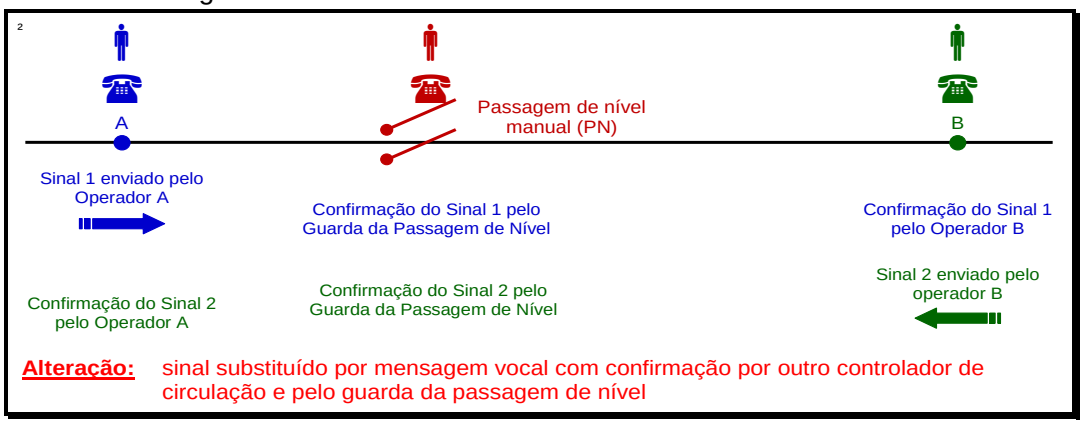

Figura 15: Exemplo de uma alteração não significativa Mensagem telefónica para controlar uma passagem de nível.

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

C.2.3. Sistema existente: antes de realizar a alteração pretendida, a informação sobre a direcção de chegada de um comboio era automaticamente indicada ao guarda da passagem de nível através do tom do sinal de chamada do telefone. O tom do sinal era diferente conforme a proveniência da chamada.

C.2.4. Alteração pretendida: dado que o sistema de telefones se tornou obsoleto e tem de ser substituído por um sistema digital, do ponto de vista técnico as respectivas informações já não podem ser incluídas no tom do sinal. O tom do sinal é exactamente o mesmo independentemente do controlador de circulação que o origina. Decide-se, então, alcançar a mesma função através de um procedimento operacional:

(a) aquando da partida do comboio, o controlador de circulação informa verbalmente o guarda da passagem de nível sobre a direcção de chegada do comboio;

(b) é verificada a conformidade da informação com o horário e reconhecida por ambos, quer pelo guarda da passagem de nível, quer pelo outro controlador de circulação, de modo a evitar mal-entendidos da parte do guarda da PN.

A alteração pretendida e o procedimento operacional associado são ilustrados no Figura 15::

C.2.5. Apesar de a alteração parecer ter um impacto potencial na segurança (o risco de a guarda da passagem de nível não fechar a tempo), há outros critérios *do* Artigo 4.º (2) tais como:

(a) Baixa complexidade;
(b) Falta de inovação, e;
(c) Fácil monitorização;

que podem sugerir que a alteração pretendida não é significativa.

C.2.6. Neste exemplo, é no entanto necessária alguma análise de segurança ou argumento para mostrar que, nesta tarefa crítica de segurança, a substituição de um sistema técnico antigo por um procedimento operacional (com pessoal a verificar-se entre si) iria levar a um nível de segurança semelhante. A questão é saber se isso exigiria a aplicação de todo o processo do MCS, com registo de perigos, avaliação independente por um organismo de avaliação, etc. Neste caso, é questionável se isto iria trazer algum valor acrescentado, significando que tal alteração não poderia então ser considerada significativa.

C.3. Exemplos de interfaces entre os actores do sector ferroviário

C.3.1. Eis alguns exemplos de interfaces e motivos para a cooperação entre os actores do sector ferroviário:

GI - GI Por exemplo, ambas as infra-estruturas terão de contemplar medidas de segurança para garantir uma transição segura dos comboios de uma infra-estrutura para a outra;

GI – EF: Por exemplo, pode haver regras operacionais específicas, dependendo da infra-estrutura, que terão de ser observadas pelo maquinista;

GI – Fabricante: Por exemplo, os subsistemas do fabricante podem ter restrições de uso que têm de ser cumpridas pelo GI;

GI – Fornecedor de Serviços: por exemplo, pode haver restrições específicas para a manutenção da infra-estrutura que têm de ser cumpridas pelo subcontratante das actividades de manutenção;

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

EF – Fabricante: Por exemplo, os subsistemas do fabricante podem ter restrições de uso que têm de ser cumpridas pela EF;

EF - Fornecedor de Serviços: por exemplo, pode haver restrições específicas para manutenção da infra-estrutura que têm de ser cumpridas pelo subcontratante das actividades de manutenção;

EF – Detentores: por exemplo, podem existir restrições de uso específicas dos veículos que têm de ser cumpridas pela empresa ferroviária que os opera;

Fabricante – Fabricante: Por exemplo, a gestão das interfaces técnicas relacionadas com a segurança entre os subsistemas de dois fabricantes diferentes;

Fabricante - Fornecedor de Serviços: Por exemplo, a gestão pelo fabricante do registo de perigos quando subcontrata os trabalhos de uma empresa cujo tamanho é demasiado pequeno para ter uma organização de segurança no projecto considerado;

Fornecedor de Serviços – Fornecedor de Serviços: exemplo semelhante ao da alínea i) supra;

C.3.2. Os fornecedores de serviços abrangem todas as actividades subcontratadas quer pelo GI ou pelo EF ou pelo fabricante, tais como a manutenção, emissão de bilhetes, serviços de engenharia etc.

C.3.3. De modo a ilustrar a gestão de interface e a identificação de perigos associados, é dado o seguinte exemplo. Considera-se a interface entre o fabricante de um comboio e um proponente (EF). Em seguida, é descrita a forma como os critérios exigidos no ponto .[G 3] da secção 1.2.1 podem ser cumpridos:

(a) Direcção: o proponente (EF);

(b) Inputs:

(1) lista(s) dos perigos relevantes que advêm de projectos semelhantes;
(2) descrição de todos os inputs e outputs (I/O) da interface, incluindo as características do desempenho;

(c) Métodos Ver apêndice A.2 do guia EN 50 126-2 Guia {Ref. 9};

(d) Participantes necessários:

Gestor de garantia de segurança do proponente (EF);

(2) Gestor de garantia de segurança do fabricante do comboio;

Responsável de design do proponente do comboio;
Responsável de design do fabricante do comboio;
Equipa de manutenção do proponente do comboio (dependendo em parte do I/O analisado);
Maquinistas (dependendo em parte do I/O analisado);

(e) Outputs:

Relatório de identificação de perigos conjuntamente acordados;
Medidas de segurança para o registo de perigos com uma descrição clara da responsabilidade.

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

C.4. Exemplos de métodos para determinar os riscos genericamente aceitáveis

C.4.1. Introdução

C.4.1.1. Os riscos genericamente aceitáveis são definidos no Regulamento relativo ao MCS como riscos “tão pequenos que não é razoável implementar medidas de segurança adicionais (para reduzir ainda mais o risco)". Na identificação de perigos, ao classificar alguns perigos como associados a riscos genericamente aceitáveis não permite que esses perigos sejam analisados posteriormente no processo de avaliação de riscos. A definição de riscos genericamente aceitáveis supracitada dá alguma margem de interpretação. É por isso que se indica no regulamento que a decisão de classificar perigos associados a riscos genericamente aceitáveis é deixada ao parecer de especialistas.

C.4.1.2. Na verdade, é difícil definir um critério comum de perigos genericamente aceitáveis mais explícito, que seja aplicável a todos os diferentes possíveis níveis do sistema em que tais perigos possam ser identificados e que também sejam responsáveis pelos diferentes factores de aversão ao risco que possam prevalecer em diferentes aplicações. Contudo, dado ser importante garantir que o parecer dos peritos seja facilmente compreendido e rastreável, é útil ter alguma orientação quanto à forma de definir os riscos como genericamente aceitáveis. Os critérios para a definição dos riscos genericamente aceitáveis podem ser quantitativos, qualitativos ou semi-qualitativos. A seguir, são apresentados alguns exemplos sobre como derivar os critérios que permitem a avaliação de forma quantitativa ou semi-quantitativa dos riscos genericamente aceitáveis.

C.4.1.3. Os exemplos que se seguem ilustram esse princípio. Foram retirados de: *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Derivação de um critério quantitativo

C.4.2.1. Podemos definir os riscos genericamente aceitáveis como riscos mais pequenos do que o risco aceitável para uma dada classe de perigos. Recorrendo a dados estatísticos, poderá ser possível calcular qual é o actual nível de risco dos sistemas ferroviários e desta forma declarar esse nível calculado como aceitável. Dividindo esse nível de risco pelo número (N) de perigos (por exemplo, podemos partir, de forma arbitrária, do princípio que existem cerca de N = 100 categorias principais de perigos num sistema ferroviário), obtém-se um nível aceitável de risco por categoria de perigo. Podemos então afirmar que um perigo com um risco inferior em duas ordens de grandeza ao nível de risco aceitável por perigo (este é o parâmetro x % do ponto [G 1] da secção 2.2.3) seria considerado como um risco genericamente aceitável.

C.4.2.2. Contudo, terá de ser verificado se a contribuição de todos os perigos associados ao(s) risco(s) genericamente aceitável não excede um certo valor (p. ex., y%) do risco geral ao nível do sistema. Ver secção 2.2.3 e a explicação do ponto [G 2] da secção 2.2.3.

C.4.3. Avaliação dos riscos genericamente aceitáveis

C.4.3.1. Os valores limite dos riscos genericamente aceitáveis, conforme inferidos a partir dos exemplos supra, poderão então ser utilizados para calibrar as ferramentas qualitativas,

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

como por exemplo uma matriz de risco, um gráfico de risco, valores de prioridade de risco, de modo a auxiliar o perito a tomar a decisão de classificar o risco como genericamente aceitável. É importante sublinhar que o facto de se possuir critérios de avaliação quantitativos como critérios para os riscos genericamente aceitáveis não significa que é necessário realizar uma estimativa ou análise de risco exactas, de modo a decidir sobre a aceitabilidade geral do risco. É nesta fase que se aplica o parecer do perito para dar uma estimativa por alto na fase de identificação de perigos

C.4.3.2. Também é importante verificar que a contribuição de todos os perigos associados ao(s) risco(s) genericamente aceitável não excede um certo valor (p. ex., y%) do risco geral ao nível do sistema. Ver secção 2.2.3 e a explicação do ponto [G 2] da secção 2.2.3.

C.5. Exemplo de avaliação de risco de uma alteração organizativa significativa

C.5.1. **Observação:** Este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

b) realizar a comparação entre o processo existente e o processo exigido pelo MCS;

c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.5.2. O exemplo está relacionado com uma alteração organizacional. Foi considerada significativa pelo respectivo proponente. Foi utilizada uma abordagem baseada na avaliação e risco para avaliar a alteração.

C.5.3. Uma divisão da organização do gestor da infra-estrutura que, até à data da alteração, realizava actividades de manutenção (excepto sinalização e telemática), teve de entrar em concorrência com outras empresas que trabalhavam na mesma área. O impacto directo foi uma necessidade de redução de efectivos e uma redistribuição da equipa e das tarefas dentro da divisão da organização do GI acima referida.

C.5.4. Preocupações do gestor da infra-estrutura afectado:

(a) A equipa do GI afectada pela alteração era responsável pela manutenção de emergência e pelas reparações necessárias provocadas por falhas súbitas na infra-estrutura. A equipa também estava a realizar algumas actividades de manutenção planeadas ou projectadas tais como o enchimento das linhas, limpeza do balastro, controlo da vegetação;

(b) estas tarefas foram consideradas críticas para a segurança e pontualidade da operação. Estas tarefas tiveram então de ser analisadas, de modo a encontrar as medidas correctas para garantir que situação não se deteriora, devido ao facto de os responsáveis pelas medidas de segurança estarem a deixar a organização do GI.

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) o mesmo nível de segurança e pontualidade dos comboios têm de ser mantidos durante e após a alteração da organização.

C.5.5. Em comparação com o processo do MCS, foram aplicados os seguintes passos (ver também Figura 1

(a) descrição do sistema [secção 2.1.2]:

(1) descrição das tarefas realizadas pela organização existente (ou seja, pela organização do GI antes da alteração);
(2) descrição das alterações planeadas na organização do GI.
(3) as interfaces da "divisão a destacar" com outras organizações envolvidas ou com o ambiente físico apenas podem ser brevemente descritas. Os limites podem não estar 100% claramente presentes;

(b) identificação do perigo [secção 2.2]:

(1) "brainstorming" do grupo de peritos:

(i) para encontrar todos os perigos que tenham uma influência relevante no risco causado pela alteração organizacional pretendida;
(ii) identificar as possíveis acções para controlar o risco;

(2) classificação de perigos:

(i) em função da gravidade do risco associado: Risco alto, médio, baixo;
(ii) em função do impacto da alteração: Risco aumentado, não alterado, diminuído;

(c) uso de um sistema de referência [secção 2.4]:

Considerava-se que o sistema antes da alteração tinha um nível aceitável de segurança. Era então usado como "sistema de referência" para inferir os critérios de aceitação de risco (CAR) para a alteração da organização;

(d) estimativa e cálculo de risco explícito [secção 2.5]

Para cada perigo com risco aumentado devido à alteração da organização, são identificadas medidas de redução de riscos. O risco residual é comparado com o CAR a partir do sistema de referência para verificar se há necessidade de identificar medidas adicionais;

(e) Demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

(1) a análise de risco e o registo de perigos mostram que os perigos não podem ser controlados até serem verificados e até se provar que os requisitos de segurança (ou seja, as medidas de segurança seleccionadas) foram implementados;
(2) a análise de risco e o registo de perigos eram documentos em progresso. A eficácia das acções decididas foi monitorizada em intervalos regulares, de modo a verificar se as condições foram alteradas e se a análise de risco e a avaliação de risco necessitam de ser actualizadas;
(3) se as medidas implementadas não fossem suficientemente eficazes, a análise de risco, a avaliação de risco e o registo de perigos seriam actualizados e monitorizados novamente

(f) gestão do perigo [secção 4.1]:

Os perigos identificados e as medidas de segurança foram registados e geridos num registo de perigos. Uma das conclusões do exemplo foi actualizar continuamente a

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

análise de risco e o registo de perigos dado que as decisões e as acções foram tomadas durante a alteração da organização. O risco nas interfaces com, por exemplo, os subcontratantes e os empresários foi igualmente abrangido pela análise de risco.

A estrutura e os campos usados no registo de perigos, bem como no extracto de algumas linhas são incluídos na secção C.16.2. do apêndice C.

(g) avaliação independente [Artigo 6.º]:

Foi também realizada uma avaliação independente por terceiros para:

verificar que a gestão de risco e a avaliação de risco foram realizadas correctamente;
verificar que a alteração organizacional é adequada e irá permitir manter o mesmo nível de segurança existente antes da alteração.

C.5.6. O exemplo mostra que os princípios exigidos pelo método comum de segurança são métodos existentes no sector ferroviário já aplicados na avaliação de riscos de alterações organizacionais. A avaliação de risco do exemplo cumpre todos os requisitos do MCS. Usa dois de três princípios de aceitação de risco permitidos pela abordagem harmonizada do MCS:

(a) é aplicado um "sistema de referência" para determinar os critérios de aceitação de risco necessários para avaliar a aceitação de risco da alteração organizacional;

(b) “estimativa do risco explícito e avaliação”:

analisar os desvios da alteração do sistema de referência;
Identificar medidas de redução de risco para os riscos acrescidos que decorrem da alteração;
avaliar se um nível aceitável de risco é alcançado.

C.6. Exemplo de avaliação de risco de uma alteração operacional significativa – alteração das horas de condução

C.6.1. **Observação:** Este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

realizar a comparação entre o processo existente e o processo exigido pelo MCS;

justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.6.2. O exemplo é uma alteração operacional em que a empresa ferroviária pretendia atribuir novas itinerários e, potencialmente, novos horários de trabalho (incluindo rotações e escalas) aos maquinistas.

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

C.6.3. Em comparação com o processo do MCS, foram aplicados os seguintes passos (ver também no Figura 1):

(a) Carácter significativo da alteração [Artigo 4.º]:

A empresa ferroviária realizou uma avaliação de risco preliminar em que se concluiu que a alteração operacional foi significativa. Dado que os maquinistas tinham de percorrer novos itinerários, e possivelmente fora do horário normal de trabalho, o potencial de ultrapassar sinais fechados, de exceder os limites de velocidade e de ignorar os limites de velocidade temporários não podia ser negligenciado.

Ao compararmos esta avaliação preliminar de risco com os critérios do Artigo 4.º (2) do Regulamento relativo ao MCS

relevância de segurança: a alteração está relacionada com a segurança porque o impacto da modificação do modo de trabalhar dos maquinistas pode ser catastrófica;
consequência da falha: os erros dos maquinistas supramencionados têm o potencial de gerar consequências catastróficas;
novidade: eventualmente a EF pode introduzir novas formas de trabalho dos maquinistas;
consequências da alteração: poderia ser complicado modificar as horas de condução, dado que isso iria exigir uma avaliação completa e modificações das condições de trabalho existentes;

definição do sistema [secção 2.1.2]:

A definição do sistema descrevia inicialmente:

as condições de trabalho existentes: horário de trabalho, escalas, etc.;
alterações das horas de trabalho;
os problemas da interface (por exemplo, com o gestor da infra-estrutura)

Durante as várias iterações, a definição do sistema foi actualizada com os requisitos de segurança resultantes do processo de avaliação de risco. Os representantes chave do pessoal estiveram envolvidos neste processo iterativo de identificação de perigos e da actualização da definição do sistema.

identificação do perigo [secção 2.2]:

Os perigos e as medidas de segurança possíveis para as novas itinerários e escalas foram identificados por reflexão de um grupo de peritos, incluindo os representantes dos maquinistas. As tarefas dos maquinistas nas novas condições foram consideradas de modo a avaliar se estavam a afectar os maquinistas, a sua carga de trabalho, o âmbito geográfico e o tempo de trabalho do sistema de escalas .
A EF também consultou os sindicatos dos trabalhadores para averiguar se podiam facultar informações adicionais e rever o risco dos níveis de fadiga e doença que poderiam ser causados devido ao aumento das horas extra provocado pelas viagens alargadas em itinerários desconhecidos.
A cada um dos perigos foi atribuído um nível de gravidade de risco e consequências (alto, médio, baixo) e o impacto da alteração proposta foi revisto tendo em conta esse nível de risco (acrescido, inalterado, diminuído).

uso de códigos de práticas [secção 2.3]:

Os códigos de prática relacionados com as horas de trabalho e com os riscos de fadiga humana foram usados para rever as condições de trabalho existentes e para determinar os novos requisitos de segurança. As regras operacionais necessárias foram

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

concebidas de acordo com os códigos de prática do novo sistema de escalas. As partes interessadas foram envolvidas na revisão dos procedimentos operacionais revistos e no acordo para proceder à alteração.

demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

Os procedimentos operacionais revistos foram introduzidos no sistema de gestão de segurança da EF. Foram monitorizados e foi posto em prática um processo de revisão para garantir que os perigos identificados continuam a ser correctamente controlados durante a operação do sistema ferroviário.

gestão do perigo [secção 4.1]:

Ver ponto supra dado que no caso das empresas ferroviárias, o processo de gestão de perigos pode fazer parte do seu sistema de segurança para registar e gerir os riscos. Os perigos identificados foram registados num registo de perigos com os requisitos de segurança (ou seja, com referência aos procedimentos operacionais revistos) que controlam o risco associado.
Os procedimentos foram monitorizados, e revistos quando necessário, para garantir que os perigos identificados continuem a ser correctamente controlados durante a operação do sistema ferroviário.

avaliação independente [Artigo 6.º]:

O processo de avaliação de risco e de gestão de risco foi avaliado por uma pessoa competente da EF e independente do processo de avaliação. A pessoa competente avaliou quer o processo, quer os resultados, ou seja, os requisitos de segurança identificados.

A EF baseou a sua decisão de implementar o sistema, no relatório de avaliação independente realizado pela pessoa competente.

C.6.4. O exemplo mostra que os princípios e o processo usados pela empresa ferroviária estão em conformidade como o método comum de segurança. O processo de gestão de risco e de avaliação de risco cumpriu todos os requisitos do MCS.

C.7. Exemplo de avaliação de risco de uma alteração técnica significativa (CCS)

C.7.1. **Observação:** Este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

realizar a comparação entre o processo existente e o processo exigido pelo MCS; justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração

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

significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.7.2. O exemplo está relacionado com a alteração técnica do sistema de controlo-comando. Foi considerada significativa pelo respectivo fabricante. Foi utilizada uma abordagem baseada na avaliação do risco para avaliar a alteração.

C.7.3. Descrição da alteração: a alteração consiste na substituição de um *loop* na via situado antes de um sinal, por um subsistema "rádio infill + GSM" (ver Figura 16).

C.7.4. Preocupação: manter o nível de segurança do sistema depois de realizada a alteração.

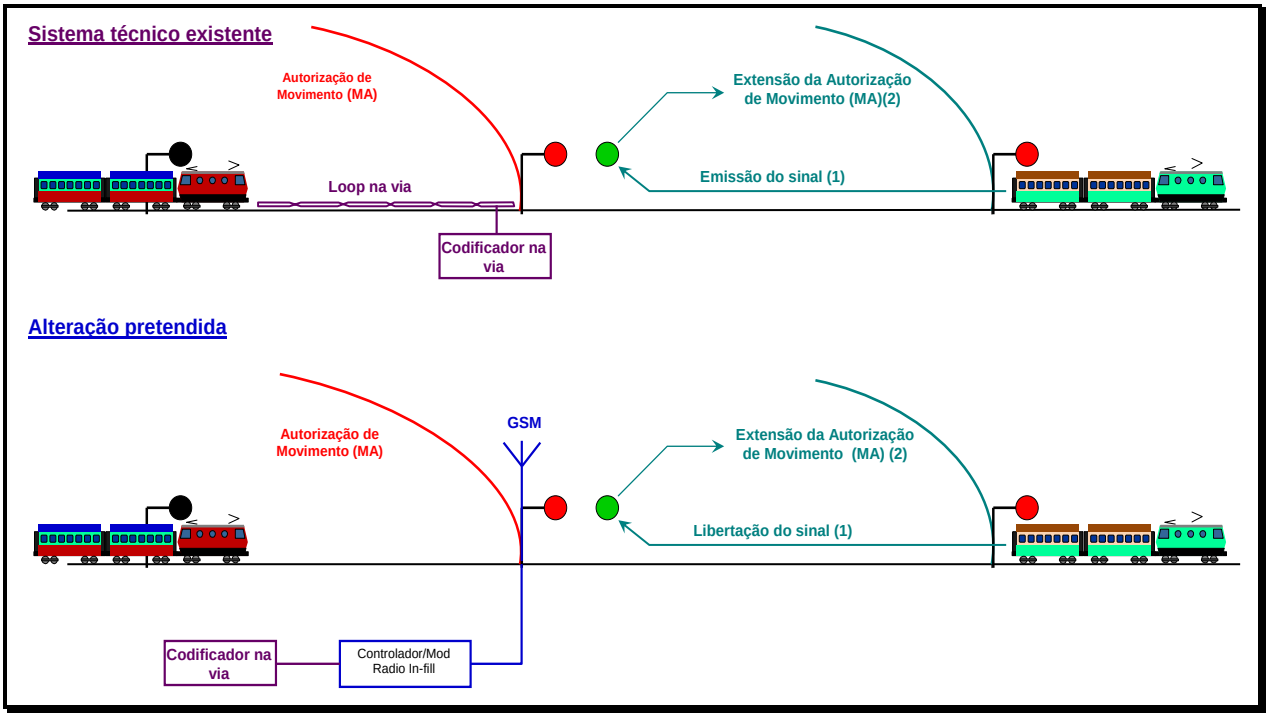

Figura 16: Alteração de um loop na via por um subsistema radio in-fill.

C.7.5. Em comparação com o processo do MCS, são aplicados os seguintes passos (ver também Figura 1):

(a) avaliação do carácter significativo da alteração [Artigo 4.º]

Os critérios do Artigo 4.º (2) são usados para avaliar o carácter significativo de uma alteração. Essencialmente, foram usadas a complexidade e novidade para decidir se essa alteração é significativa.

(b) descrição do sistema [secção 2.1.2]:

(1) análise do sistema existente: *loop* e as suas funções no sistema de controlo-comando;
(2) Descrição da alteração planeada pelo proponente e pelo fabricante;
(3) descrição das interfaces funcionais e físicas do *loop* com o resto do sistema;

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

A função do "*loop* + codificador" no sistema existente é de emitir um sinal mediante a aproximação de um comboio quando a secção que antecede o sinal (ou seja, à frente do comboio que se aproxima) fica desocupada: ver Figura 16.

(c) identificação do perigo [secção 2.2]:

O processo iterativo de avaliação de risco e a identificação de perigo (ver secção 2.1.1) são aplicados com base na reflexão de um grupo de peritos de modo a:

Identificar os perigos com uma influência relevante no risco causado pela alteração pretendida;
identificar as acções possíveis para controlar o risco;

Quando o *loop*, e concomitantemente o "rádio infill", emite o sinal, há o risco de se dar uma autorização de circulação não segura ao comboio que se aproxima, enquanto o comboio anterior ainda ocupa uma secção à frente do sinal. O risco terá de ser controlado num nível aceitável.

(d) uso de um sistema de referência [secção 2.4]:

Considerava-se que o sistema antes da alteração (*loop*) tinha um nível aceitável de segurança. É então usado como "sistema de referência" para que se possam inferir os requisitos de segurança para o subsistema de "rádio infill".

(e) estimativa e cálculo de risco explícito [secção 2.5]

(1) As diferenças entre os subsistemas "loop" e "rádio infill+GSM" são analisadas através da avaliação e estimativa de risco explícito. São identificados os seguintes perigos novos para o subsistema "rádio infill + GSM":

(i) Transmissão de informações não seguras no ar por piratas informáticos, dado que o subsistema "rádio infill + GSM" é de transmissão aberta;
(ii) transmissão atrasada ou transmissão de pacotes de dados memorizados, pelo ar;

(2) Estimativa de risco explícito e o uso dos CAR-ST na parte do Controlador do Rádio Infill;

(f) uso de códigos de prática [secção 2.3]:

(1) a norma EN 50159-2 ("*Aplicações Ferroviárias: Parte 2: Comunicação de segurança em sistemas de transmissão abertos*") fornece os requisitos de segurança para controlar os novos perigos a um nível aceitável, por exemplo**:**

(i) encriptação e protecção de dados;
(ii) sequenciação de mensagens e marcação do tempo;

(2) por exemplo, o uso da norma EN 50 128 para o desenvolvimento do Controlador de Rádio Infill;

(g) Demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

(1) acompanhamento da implementação dos requisitos de segurança através do processo de desenvolvimento do subsistema "rádio infill + GSM";
(2) verificação que o sistema, conforme concebido e instalado, está em conformidade com os requisitos de segurança

(h) gestão do perigo [secção 4.1]:

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

Os perigos identificados, as medidas de segurança e os requisitos de segurança resultantes emitidos a partir da avaliação de risco e a aplicação dos três princípios de aceitação de risco são registados e geridos num registo de perigos.

(i) avaliação independente [Artigo 6.º]:

É também realizada uma avaliação independente por terceiros para:

(3) verificar que a gestão de risco e a avaliação de risco são realizadas correctamente;
(4) verificar que a alteração técnica é adequada e irá permitir manter o mesmo nível de segurança existente antes da alteração.

C.7.6. O exemplo mostra que os três princípios de aceitação de risco exigidos pelo método comum de segurança são usados de forma complementar, de modo a definir os requisitos de segurança do sistema em avaliação. A avaliação de risco do exemplo cumpre todos os requisitos do MCS resumidos no Figura 1, incluindo a gestão de registo de perigos e a avaliação de segurança independente realizada por terceiros.

C.8. Exemplo do guia sueco BVH 585.3 para a avaliação de risco dos túneis ferroviários

C.8.1. **Observação:** Este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;
realizar a comparaçãorealizar a comparação entre o processo existente e o processo exigido pelo MCS;
justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.8.2. O objectivo do exemplo é comparar o processo do MCS com o guia BVH 585.30 usado pelo gestor da infra-estrutura sueco, Banverket, no design e na verificação da obtenção de um nível de segurança satisfatório no planeamento e construção dos novos túneis ferroviários. Os pontos em comum e as diferenças no âmbito do MCS são enumerados adiante; os requisitos de avaliação de risco pormenorizada podem ser encontrados no guia BVH 585.30.

C.8.3. Em comparação com o processo do MCS da Figura :

(a) O guia BVH 585.30 tem os seguintes pontos em comum:

descrição do sistema [secção 2.1.2]:

O guia exige uma descrição de sistema pormenorizada contendo:

a descrição do túnel;
a descrição da via;

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

a descrição do tipo de material circulante (incluindo o pessoal a bordo);
a descrição do tráfego e das operações pretendidas;
a descrição da assistência externa (incluindo os serviços de socorro);

Identificação do perigo [secção 2.2]:

O guia não exige explicitamente a identificação de perigos. Exige a identificação de riscos e um "catálogo de acidentes" que contém os tipos de potenciais acidentes identificados que se considere terem um impacto significativo ao nível do risco no túnel e que terão de ser cobertos pela avaliação subsequente. Exemplos de acidentes:

"descarrilamento de um comboio de passageiros";
"descarrilamento de um comboio de mercadorias";
"acidente que envolve mercadorias perigosas";
"incêndio na carruagem";
"colisão de um comboio de passageiros com um objecto leve/pesado";
etc.

não está prevista a aplicação de códigos de prática ou de sistemas de referência semelhantes. Considera-se que as análises de risco devem ser realizadas em todo o caso;

estimativa e cálculo de risco explícito [secção 2.5]:

regra geral, o guia recomenda que, para cada tipo de acidente, se realize uma Árvore de Acontecimentos com base na análise de risco quantitativo. Todavia, dado que a análise de risco tem por objectivo analisar o nível de segurança global do túnel e não analisar a segurança de forma individual em níveis mais pormenorizados, as consequências de todos os cenários são reunidas para se obter o nível de risco global do túnel;

a aceitabilidade deste nível de risco global do túnel terá de ser comparada com o critério de aceitação de risco quantitativo explícito que se segue. "*o tráfego ferroviário por quilómetro nos túneis será tão seguro como o tráfego ferroviário por quilómetro em via a céu aberto, excluindo as passagens de nível*". O critério é transformado numa curva F-N baseada nos dados históricos dos acidentes ferroviários da Suécia e é extrapolada para abranger de igual forma as consequências não presentes nas estatísticas;

Para além do critério do nível de risco global do túnel, também há requisitos adicionais a cumprir especificamente em caso de evacuação dos túneis e das possibilidades de operação dos serviços de socorro:

Verificar que o socorro individual próprio é possível em caso de incêndio num comboio num "pior caso credível" (os critérios para esta avaliação também são fornecidos);

o túnel deve ser planeado de modo a permitir que as operações de socorro sejam possíveis num dado conjunto de cenários;

output da avaliação de risco [secção 2.1.6]:

Os outputs da avaliação de risco são:

uma lista de medidas de segurança do padrão mínimo baseado em TSI-SRT e nas normas nacionais a usar no design do túnel e;

todas as medidas de segurança adicionais identificadas como necessárias pela análise de risco, indicando a sua finalidade. Declara-se que as medidas deverão ser determinadas de acordo com a seguinte ordem de prioridade:

prevenir acidentes;
reduzir as consequências dos acidentes;
facilitar a evacuação;
facilitar as manobras de socorro;

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

gestão do perigo [secção 4.1]:

O guia não exige explicitamente que se mantenha um registo de perigos. Isto relaciona-se com o facto de que o nível da avaliação é global e, por essa razão, os perigos não são avaliados nem controlados individualmente. A aceitabilidade do risco global do túnel é avaliada, sem repartição do critério de aceitação de risco pelos diferentes tipos de acidentes ou perigos subjacentes.

Existe, contudo, uma lista de todas as medidas de segurança, quer as resultantes do "padrão mínimo", quer as identificadas como necessárias pela análise de risco: Ver alínea (a)(5)(ii) supra. Deve indicar-se na lista de medidas de segurança se as medidas dizem respeito à infra-estrutura do túnel, à via, às operações ou ao material circulante e também que o seu efeito pretendido está de acordo com a lista da alínea (a)(5)(ii). Mas o guia não exige explicitamente que se mencione quais os perigos controlados pelas medidas de segurança e quem é responsável pelas medidas.

avaliação independente [Artigo 6.º]:

É obrigatória uma avaliação independente realizada por terceiros para:

verificar que o processo de avaliação de risco recomendado pelo guia BVH 585.30 é feito de forma correcta;
para considerar a análise de risco aceitável;
para verificar que se indica de forma clara como a futura gestão de segurança deve ser realizada no projecto;

O documento de análise de risco final é assinado pelo avaliador independente e também pelo coordenador de segurança do projecto.

O guia BVH 585.30 difere nos seguintes aspectos:

Demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

O guia BVH 585.30 não exige nem o rastreio da forma como os requisitos de segurança identificados são implementados nem a verificação em como o design final do túnel cumpre os requisitos de segurança mencionados. Apenas descreve a forma como estes requisitos devem ser transferidos, de modo a garantir que são implementados durante a fase de construção.

O guia determina os requisitos de segurança a serem usados, para verificar que a análise de risco foi realizada de forma adequada e transparente e que pode ser aceite pelo projecto.

C.8.4. Concluindo, a comparação com o MCS mostra que:

(a) o guia BVH 585.30 cumpre as partes relevantes do MCS, não obstante o seu âmbito e finalidade não serem exactamente os mesmos;
b) o guia BVH 585.30 avalia o nível de risco geral do túnel ferroviário;
c) os perigos não são controlados individualmente e, por essa razão, há uma menor incidência na gestão de perigo;
d) a demonstração da conformidade e verificação da implementação correcta de todas as medidas de segurança não se encontra explicitamente mencionada. O guia menciona, contudo, que o papel do coordenador de segurança no projecto (papel e competência exigidos pelo BVH 585.30) é verificar que as conclusões da análise de risco são implementadas nos documentos e desenhos do projecto e também controlar que são correctamente implementadas durante a fase de construção;

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

C.8.5. O MCS é mais geral do que o guia BVH 585.30 no sentido em que oferece a aplicação de três princípios de aceitação de risco diferentes. Contudo, não há problema em aplicar o guia BVH 585.30 no quadro do MCS, pois é compatível com o uso do terceiro princípio da estimativa de risco explícito.

C.9. Exemplo da avaliação de risco ao nível do sistema no Metro de Copenhaga

C.9.1. **Observação:** Este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

realizar a comparação entre o processo existente e o processo exigido pelo MCS;

justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.9.2. O exemplo relaciona-se com um sistema de metro completo, complexo e sem condutor, incluindo os subsistemas técnicos subjacentes (por exemplo, protecção automática dos comboios e material circulante) bem como a operação e manutenção do sistema. Uma abordagem baseada na avaliação de risco foi aplicada para avaliar o sistema e os subsistemas subjacentes. O projecto também abrangeu a certificação do SGS da empresa que tinha de operar o sistema. Isto está relacionado com a capacidade da EF e do GI manterem a segurança geral do sistema ao longo do ciclo de vida do sistema.

C.9.3. Em comparação com o processo do MCS, foram aplicados os seguintes passos (ver também Figura 1):

(a) descrição do sistema [secção 2.1.2]:

(1) descrição dos requisitos de desempenho do sistema;
(2) descrição das normas operacionais;
(3) descrição clara das interfaces e responsabilidades entre os diferentes actores, em especial entre os subsistemas técnicos;
(4) definição dos requisitos de alto nível do sistema (em termos de frequência aceitável de acidentes e definição de uma zona ALARP);

b) Identificação do perigo [secção 2.2]:

análise de perigo preliminar ao nível do sistema;
análise funcional ao nível do sistema salientando todos os subsistemas e não apenas aqueles críticos do ponto de vista da segurança (por exemplo, protecção automática dos

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

comboios e material circulante) que participam nas funções de segurança e têm um papel activo na garantia da segurança dos passageiros e dos trabalhadores;

Intensa coordenação entre os actores (adjudicatário, fornecedores do subsistema dos subsistemas técnicos e dos trabalhos de engenharia civil) para:

Identificar de forma sistemática todos os perigos razoavelmente previsíveis;

identificar acções possíveis para controlar todos os riscos associados aos perigos identificados a um nível aceitável;

c) uso de códigos de prática [secção 2.3]:

diferentes Códigos de prática, normas e regulamentos, foram usados, por exemplo:

(1) Regulamento BOStrab relativo à construção e operação de carros eléctricos (regulamento alemão aplicável aos sistemas ferroviários urbanos) e à operação sem condutor;
(2) Documentos VDV (códigos de prática alemães) relacionados com os requisitos de equipamento para garantir a segurança dos passageiros em estações com operação sem condutor;
(3) Normas CENELEC relativas aos sistemas ferroviários (EN 50 126, 50 128 e 50 129). Estas normas debruçam-se, em especial, sobre os sistemas técnicos ferroviários. Porém, dado que contêm uma abordagem metodológica com validade geral, foram genericamente adoptados pelo metro de Copenhaga:

(i) A EN 50 126 foi usada para as actividades de gestão de risco e de avaliação de risco do sistema ferroviário completo
(ii) A EN 50 129 foi usada em todo o sistema de sinalização;
(iii) A EN 50 128 foi usada no desenvolvimento de software (incluindo a sua verificação e validação) dos subsistemas técnicos;

(4) normas relativas à protecção contra incêndios (NEPA 130);
(5) normas relativas à engenharia civil e às obras de construção (Códigos Europeus);

d) uso de um sistema de referência [secção 2.4]:

O metro teve de atingir o nível de segurança correspondente às instalações modernas da Alemanha, França ou Grã-Bretanha. Estes sistemas existentes foram usados como sistemas de referência semelhante para se inferir os critérios de aceitação de risco em termos das frequências aceitáveis de acidentes no metro de Copenhaga;

e) estimativa e cálculo de risco explícito [secção 2.5]:

(1) para a estimativa dos riscos relacionados com os perigos específicos;
(2) Para o controlo da ventilação nos túneis de emergência (incluindo os factores humanos que envolvem os bombeiros);
(3) Para identificar as medidas de redução do risco;
(4) Para avaliar se um nível aceitável de risco é alcançado em todo o sistema;

f) Demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

(1) esforços técnicos e de gestão em conformidade com a complexidade do sistema para demonstrar a segurança do sistema;
(2) repartição dos requisitos de segurança do sistema em subsistemas técnicos e obras de construção civil, bem como em todas as funções do metro relacionadas com a segurança;
(3) demonstração que cada subsistema cumpre, tal como foi construído, todos os seus requisitos de segurança;

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) no caso das funções realizadas por mais do que um subsistema, a demonstração de conformidade com os requisitos de segurança não foi feita ao nível do subsistema. Foi realizada ao nível do sistema, integrando os diferentes subsistemas, ferramentas e procedimentos;
(5) demonstração que o sistema global cumpre os requisitos de segurança de alto nível;

g) gestão do perigo [secção 4.1]:

Os perigos identificados, as medidas de segurança associadas e os requisitos de segurança resultantes foram registados e geridos num registo central de perigos. O gestor de segurança global do projecto foi responsável por este registo de perigos. Os perigos operacionais identificados durante o design e a instalação, bem como os perigos relacionados com a operação e manutenção foram incluídos no registo de perigos;

h) evidências da gestão de risco e da avaliação de risco [secção 5]:

Os resultados da avaliação de risco foram documentados formalmente e apoiados por um dossier de segurança em conformidade com os requisitos das normas CENELEC:

(1) dossier de segurança do sistema geral;
(2) dossier de segurança para cada subsistema técnico (incluindo os subsistemas de sinalização e obras de construção civil);
(3) Dossier de segurança para as obras de construção civil (estações, túneis, viadutos, taludes);
(4) Dossier de segurança de instalação;
(5) Dossier de segurança de veículos;
(6) Dossier de segurança de operador (em apoio da certificação da EF e o SGS do GI, ou seja, demonstração da capacidade do proponente em operar e manter a segurança do sistema);

i) avaliação independente [Artigo 6.º]:

O processo geral foi acompanhado e avaliado por um avaliador de segurança independente, agindo com uma delegação da Autoridade de Supervisão Técnica (ou seja, do Ministério dos Transportes da Dinamarca). Os papéis do avaliador de segurança independente são identificados no respectivo código de prática. Isto inclui:

(1) a verificação da correcta gestão e avaliação de risco;
(2) a verificação que o sistema se adequa à finalidade e que será operado e mantido em segurança durante todo o ciclo de vida;
(3) recomendação de aprovação à Autoridade de Supervisão Técnica.

C.9.4. O projecto completo foi apoiado por um processo adequado de gestão de qualidade.

C.9.5. No projecto, as evidências dos fornecedores (ou seja, os casos de segurança e a documentação de apoio pormenorizada para os subsistemas técnicos e obras de construção civil) foram comunicados ao gestor de segurança do proponente. Estes dados foram então revistos pela organização do gestor de segurança, bem como pelo avaliador de segurança independente, cujas conclusões foram mencionadas num relatório de avaliação.
O relatório de avaliação de segurança independente foi revisto pela gestão de segurança do proponente e entregue ao proponente que remeteu todos os ficheiros à Autoridade de Supervisão Técnica (ou seja, o Ministério dos Transportes da Dinamarca) para aprovação final.

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

C.9.6. O exemplo mostra que os princípios exigidos pelo método comum de segurança são métodos existentes no sector ferroviário. A avaliação de risco do exemplo cumpre todos os requisitos do MCS. Em especial, recorre aos três princípios de aceitação de risco permitidos pela abordagem harmonizada do MCS.

C.10. Exemplo da guia da OTIF para o cálculo do risco resultante do transporte ferroviário de mercadorias perigosas

C.10.1. **Observação**: este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;
b) realizar a comparação entre o processo existente e o processo exigido pelo MCS;
c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.10.2. A filosofia geral do guia OTIF está em conformidade com a finalidade do MCS, mas a guia têm um âmbito limitado. O objectivo do guia OTIF é “conseguir uma abordagem mais uniforme na avaliação de risco do transporte de mercadorias perigosas nos Estados-membros da Convenção relativa aos transportes internacionais ferroviários (COTIF) e, consequentemente, fazer com que as avaliações de risco individuais sejam comparáveis”. Apoia, desta forma, a aceitação cruzada, entre os Estados membros da COTIF, das avaliações de risco do transporte de mercadorias perigosas por via ferroviária.

C.10.3. Comparação com o MCS e o fluxograma do Figura 1:

(a) o guia OTIF tem os seguintes pontos em comum:

(1) é uma abordagem comum na avaliação de risco, no entanto baseada no cálculo do risco explícito (isto é, o terceiro princípio de aceitação de risco do MCS);

(2) a avaliação de risco OTIF é composta por:

uma fase de análise de risco que inclui:

uma fase de identificação de perigos;

uma fase de estimativa de risco;

uma fase de avaliação de risco baseada nos critérios de (aceitação de) risco ainda por harmonizar. Com efeito, há várias especificidades nacionais que podem influenciar estes critérios;

(b) O guia OTIF difere nos seguintes aspectos:

1) o âmbito de aplicação é diferente. Ao passo que o MCS tem de ser aplicado apenas nas alterações significativas ao sistema ferroviário, o guia OTIF deve ser aplicado à

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

avaliação dos riscos do transporte ferroviário de mercadorias perigosas, quer isso constitua uma alteração significativa ou não no sistema ferroviário;

2) não há possibilidade de escolha entre os três princípios de aceitação de risco para controlar o(s) risco(s). O terceiro princípio, isto é, o cálculo de risco explícito, é o único princípio aceite. Além disso, terá de ser baseado exclusivamente num cálculo quantitativo e não qualitativo. A análise de risco qualitativa poderá adequar-se apenas á comparação de opções de medidas (de segurança) para a redução de risco;
3) a aplicação do princípio ALARP é requerida, de modo a determinar se as medidas de segurança adicionais podem continuar a reduzir o risco avaliado a um preço razoável;
4) não há um conceito de “perigos associados a genericamente aceitáveis” permitindo concentrar o esforço da avaliação de risco nos perigos mais importantes. No entanto, recomenda-se a redução do número de cenários de acidentes potenciais para um número razoável de cenários básicos (ver secção 3.2 em {Ref. 10});
5) o processo concentra-se na avaliação de risco, mas não inclui:

o processo de selecção e implementação das medidas (de segurança) para modificar o risco;

o processo de aceitação de risco;

o processo de demonstração da conformidade do sistema com os requisitos de segurança

6) o processo de comunicação do risco aos restantes actores envolvidos (ver ponto seguinte);não dá orientações sobre os dados que o processo de avaliação de risco tem de indicar;
7) não se exige a gestão de perigos;
8) não se exige a avaliação independente realizada por terceiros da aplicação correcta da abordagem comum.

C.10.4. A comparação entre o guia da OTIF e o MCS mostra que ambos são compatíveis, não obstante o âmbito e a finalidade não serem exactamente iguais. O MCS é mais geral do que o guia da OTIF, sendo neste sentido mais flexível. Por outro lado o MCS abrange também mais actividades de gestão de risco:

a) permite usar três princípios de aceitação de risco que se baseiam nas práticas existentes nas ferrovias: consulte a secção 2.1.4;
b) a sua aplicação exige-se apenas em caso de alterações significativas e é necessária uma posterior análise de risco apenas para os perigos que não estão associados a um risco genericamente aceitável;
c) inclui a selecção e execução das medidas de segurança que vão controlar os perigos identificados e os riscos associados;
d) harmoniza o processo de gestão de risco, incluindo:
   (1) a harmonização dos critérios de aceitação de risco que é feita no âmbito do trabalho da Agência relativo ao riscos genericamente aceitáveis e aos critérios de aceitação de risco,
   (2) demonstração da conformidade do sistema com os requisitos de segurança;
   (3) os resultados e as evidências resultantes do processo de avaliação de risco;
   (4) a troca de informações relacionadas com segurança entre os actores envolvidos nas interfaces;
   (5) a gestão num registo de perigos de todos os perigos identificados e das medidas de segurança associadas;
   (6) a avaliação independente, realizada por terceiros, da aplicação correcta do MCS.

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.10.5. A aplicação do guia do OTIF no âmbito do MCS (no caso do transporte de mercadorias perigosas constituir uma alteração significativa para um GI ou EF) não coloca, todavia, quaisquer problemas, dado que é compatível com o uso do terceiro princípio do cálculo de risco explícito.

C.11. Exemplo de avaliação de risco de uma aplicação de aprovação de um novo tipo de material circulante

C.11.1. **Observação**: este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;
b) realizar a comparação entre o processo existente e o processo exigido pelo MCS;
c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.11.2. O exemplo de avaliação de risco está relacionado com um pedido de aprovação de um novo tipo de material circulante. Foi realizada uma análise de risco para avaliar os riscos relacionados com a introdução de um novo vagão de mercadorias.

C.11.3. A finalidade da alteração foi aumentar a eficácia, capacidade, desempenho e fiabilidade do transporte de produtos a granel numa dada linha de mercadorias. Dado que os vagões se destinavam ao trânsito transfronteiriço, era necessária a autorização de duas ANS. O proponente era o operador das mercadorias que por sua vez era detido pela empresa que produz os bens a transportar.

C.11.4. O desenvolvimento do projecto abrangeu a construção, produção, montagem, colocação em serviço e verificação do novo material circulante. A análise de risco foi realizada para verificar que o novo design cumpria os requisitos de segurança em cada um dos subsistemas, bem como na totalidade do sistema.

C.11.5. Na análise de risco, é feita referência aos procedimentos e definições da CENELEC EN 50126 e a avaliação de risco é realizada de acordo com esta norma.

C.11.6. Em comparação com o processo do MCS, foram aplicados os seguintes passos:

(a) descrição do sistema [secção 2.1.2]:

Em cada fase do projecto, existiam requisitos relativos à documentação da verificação da segurança e descrição do design do sistema:

(1) fase conceptual: Descrição preliminar das exigências operacionais do operador;
(2) fase de especificação: Especificação funcional, normas técnicas aplicáveis, plano de testes e verificações. Foram também incluídos requisitos do operador relativos ao uso e à manutenção do vagão;

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) fase de produção: Documentação técnica do fabricante, incluindo desenhos, normas, cálculos, análises, etc. Análise de risco aprofundada em designs novos ou inovadores ou em novas áreas de uso;

(4) fase de verificação:

A verificação do comportamento técnico do vagão (relatórios de teste, cálculos, verificações em conformidade com as normas e requisitos funcionais);
Documentação das medidas de redução de risco e relatórios de teste para provar a compatibilidade dos vagões com a infra-estrutura ferroviária;
Documentos de manutenção e formação, manuais do utilizador, etc.

(5) Fase de aceitação:

(i) Declaração de segurança do fabricante e evidências de segurança (dossier de segurança);

(ii) A aceitação por parte do operador do vagão de mercadorias e da sua documentação;

Identificação do perigo [secção 2.2]:

Foi realizada de forma contínua em todas as fases de design. Em primeiro lugar foi utilizada uma abordagem “bottom-up” em que os vários fabricantes avaliaram as sequências de risco resultantes da falha dos componentes do seu subsistema. A divisão em subsistemas foi a seguinte:

chassis;
sistema de frenagem;
Engate central;
etc.

Foi então aplicada uma abordagem “top down” , de modo a identificar falhas ou informações em falta. Os riscos que não puderam ser imediatamente aceites foram transferidos para o registo de perigos para serem posteriormente tratados e classificados.

uso de princípios de aceitação de risco [secção 2.1.4]:

O cálculo de risco explícito foi realizado na totalidade do sistema. Porém, puderam ser usados códigos de prática ou sistemas de referência semelhantes para avaliar os perigos individuais. Por princípio, os subsistemas novos devem ser, no mínimo, tão seguros como o subsistema que substituem, gerando desta forma um subsistema novo e completo com um nível se segurança superior ao anterior. A matriz de risco da EN50126 foi usada para marcar os perigos identificados. Foram igualmente aplicados critérios de aceitação de risco adicionais, entre outros:

1) uma falha isolada não deve gerar uma situação em que as pessoas, o material ou o ambiente possam ser gravemente afectados;
2) se isto não puder ser evitado por meios de construção técnicos, deverá ser evitado por normas operacionais ou requisitos de manutenção. Isto apenas se aplicava aos perigos em que era possível identificar a falha ocorrida antes de criar uma situação perigosa;
3) no caso de componentes com alta probabilidade de falha, ou se as falhas não puderem ser detectadas antecipadamente ou evitadas através da manutenção ou regras operacionais, deverão ser consideradas funções e barreiras de segurança adicionais;

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) os sistemas redundantes com componentes que possam desenvolver falhas não detectáveis durante a operação devem ser protegidos por medidas de manutenção, de modo a evitar a redução da redundância ;
5) o nível final de segurança resultante foi uma decisão da gestão, baseada na análise de risco quantitativa e qualitativa;

Demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

Foram registados todos os riscos e perigos identificados e a lista foi consultada e actualizada de forma contínua. Os perigos restantes foram registados no registo de perigos juntamente com lista de medidas de redução de risco correspondente a ter em conta na construção, operação e manutenção. Com base nisto, foi concebido um relatório final de segurança com a verificação de que os requisitos de segurança foram implementados;

gestão do perigo [secção 4.1]:

Conforme anteriormente mencionado, os perigos e as medidas de segurança associadas foram registados num registo de perigo em que se acompanha todos os perigos e medidas de segurança identificados. Os perigos relacionados com os riscos que eram aceitáveis sem as medidas não foram, todavia, incluídos no registo de perigos;

avaliação independente [Artigo 6.º]:

Não foi feita menção a uma avaliação independente nos documentos recebidos e relacionados com a alteração significativa.

C.11.7. O exemplo de avaliação de risco baseia-se na norma CENELEC EN 50126, enquadrando-se perfeitamente no processo do MCS. O exemplo de avaliação de risco cumpre todos os requisitos do MCS, excepto o requisito de uma avaliação independente que não foi clarificado de forma explícita nos documentos recebidos. Os critérios de aceitação de risco explícito foram usados e claramente indicados.

C.12. Exemplo de avaliação de risco de uma alteração operacional significativa – Operação em regime de agente único no comboio

C.12.1. **Observação**: este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;
b) realizar a comparação entre o processo existente e o processo exigido pelo MCS;
c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.12.2. O exemplo é uma alteração operacional e quem a empresa ferroviária decidiu que o comboio tinha de ser operado apenas pelo maquinista (Driver Only Operation – DOO) num

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

trajecto em que anteriormente existia um revisor a bordo para auxiliar o maquinista no serviço do comboio.

C.12.3. Em comparação como o processo do MCS, foram aplicados os seguintes passos (ver também Figura 1 :

a) Carácter significativo da alteração [Artigo 4.º]:

A empresa ferroviária realizou uma avaliação de risco preliminar em que se concluiu que a alteração operacional foi significativa. Dado que o maquinista tinha de operar sozinho, sem apoio, o potencial de que os passageiros pudessem ser entalados pelas portas ou cair para a via (por exemplo, se as portas abrirem do lado errado) não podia ser negligenciado.

Ao compararmos esta avaliação preliminar de risco com os critérios do Artigo 4.º do Regulamento relativo ao MCS

1) relevância de segurança: a alteração está relacionada com a segurança, dado que as consequências da exigência de gerir de forma completamente diferente a operação do comboio podem ser catastróficas;
2) consequência da falha: o efeito potencial do comportamento do maquinista pode levar a consequências catastróficas, se a operação não for efectivamente controlada;
3) novidade: a operação exclusiva do maquinista pode exigir formas inovadoras de operar comboios cujo risco terá de ser avaliado;

b) definição do sistema [secção 2.1.2]:

A definição do sistema descrevia:
1) O sistema existente, explicando de forma clara quais as tarefas realizadas pelo maquinista e quais eram as outras realizadas pelos operadores comerciais a bordo (ou revisor) para ajudar o maquinista;
2) a alteração das responsabilidades do maquinista, em virtude da retirada do revisor;
3) Os requisitos técnicos do sistema para cobrir as alterações na operação;
4) as interfaces existentes entre a os operadores comerciais a bordo , o maquinista e o pessoal do gestor da infra-estrutura;

Durante as várias iterações, a definição do sistema foi actualizada com os requisitos de segurança resultantes do processo de avaliação de risco. As pessoas chave do pessoal (incluindo maquinistas, representantes das equipas e o gestor da infra-estrutura) estiveram envolvidas neste processo iterativo de identificação de perigos e da actualização da definição do sistema.

c) Identificação do perigo [secção 2.2]:

Os perigos e as medidas de segurança possíveis foram identificados em “brainstorming” por um grupo de peritos, incluindo, entre outros:
1) representantes dos maquinistas e dos outros trabalhadores pela sua experiência operacional;
2) Representantes dos GI, dado que a infra-estrutura também pode ser afectada pela alteração, implicando, por exemplo, alterações nas estações (por exemplo, a instalação de espelhos, circuitos internos de televisão [CCTV] nas plataformas);

As tarefas adicionais a serem realizadas pelos maquinistas foram submetidas a um escrutínio, de modo a identificar todos os perigos previsíveis que possam ocorrer como consequência da retirada do revisor. Em especial, a identificação de perigos focou o

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

que poderiam ser perigos operacionais nas estações, nos trajectos existentes em que existia apoio do revisor ou do pessoal do gestor infra-estrutura , incluindo a segurança da ordem de partida dos comboios, questões específicas relacionadas com o maquinista, material circulante (por exemplo, abertura das portas/verificação do fecho), requisitos de manutenção, etc.

A cada um dos perigos identificado foi atribuído um nível de gravidade de risco e consequências (alto, médio, baixo) e as consequências da alteração proposta foram revistas tendo em conta esse nível de risco (acrescido, inalterado,diminuido).

d) uso de códigos de prática [secção 2.3] e o uso de sistemas de referência semelhantes [secção 2.4]:

Ambos os códigos de prática (ou seja, um conjunto de normas para a operação apenas pelo maquinista) e os sistemas de referência semelhantes foram usados para definir os requisitos de segurança para os perigos identificados. Estes requisitos de segurança incluíram:

1) os procedimentos operacionais revistos para o maquinista que são necessários para operar de forma segura os comboios sem apoio a bordo;
2) quaisquer equipamentos necessários a bordo ou na via, de modo a garantir de forma segura e fiável a partida dos comboios;
3) uma lista de verificação para garantir que a cabina de condução é adequada, tendo em conta a interface entre o sistema ferroviário (quer a bordo, quer na via) e o maquinista;

As normas operacionais necessárias foram revistas de acordo com os requisitos a partir dos códigos de prática aplicáveis e dos sistemas de referência relevantes. As partes interessadas foram envolvidas nos procedimentos operacionais revistos e no acordo em proceder à alteração.

e) demonstração da conformidade do sistema com os requisitos de segurança [secção 3]:

O sistema foi implementado de acordo com os requisitos de segurança identificados (equipamentos adicionais e procedimentos revistos). Estes foram verificados como sendo meios apropriados para garantir um nível de segurança suficiente para o sistema em avaliação.

Os procedimentos operacionais revistos foram introduzidos no sistema de gestão de segurança da EF. Os procedimentos foram monitorizados, e revistos quando necessário, para garantir que os perigos identificados continuam a ser correctamente controlados durante a operação do sistema ferroviário.

f) gestão do perigo [secção 4.1]:

Ver ponto supra dado que no caso das empresas ferroviárias, o processo de gestão de perigos pode fazer parte do seu sistema de segurança para registar e gerir os riscos. Os perigos identificados foram registados num registo de perigos com os requisitos de segurança a controlar o risco associado, ou seja, a referência ao equipamento adicional a bordo e na via, bem como aos procedimentos operacionais revistos.
Os procedimentos foram monitorizados, e revistos quando necessário, para garantir que os perigos identificados continuam a ser correctamente controlados durante a operação do sistema ferroviário.

g) avaliação independente [Artigo 6.º]:

O processo de avaliação de risco e de gestão de risco foi avaliado por uma pessoa competente da EF e independente do processo de avaliação. A pessoa competente

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

avaliou quer o processo, quer os resultados, ou seja, os requisitos de segurança identificados.

A EF baseou a sua decisão de activar o sistema no relatório de avaliação independente realizado pela pessoa competente.

C.12.4. O exemplo mostra que os princípios e o processo usados pela empresa ferroviária estão em conformidade como o método comum de segurança. O processo de gestão de risco e de avaliação de risco cumpriu todos os requisitos do MCS.

C.13. Exemplo do uso de um sistema de referência para derivar os requisitos de segurança dos novos sistemas electrónicos de encravamento na Alemanha

C.13.1. **Observação**: este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

b) realizar a comparação -entre o processo existente e o processo exigido pelo MCS;

c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.13.2. De modo a derivar requisitos de segurança padrão para os futuros sistemas electrónicos de encravamento, a Deutsche Bahn realizou uma análise de risco num sistema electrónico já aprovado. Este último sistema já tinha sido aprovado de acordo com os códigos de prática alemães (Mü 8004).

C.13.3. A análise de risco foi feita de acordo com as normas CENELEC (EN 50126 e EN 50129) e incluiu os seguintes passos:

a) Definição do sistema;
b) Identificação de perigos;
c) Análise e quantificação de perigos.

C.13.4. Quanto à definição do sistema, foi tida em conta a definição das fronteiras do sistema, as suas funções e interfaces. O principal desafio foi definir o sistema de modo a ser independente da arquitectura interna de um sistema de bloqueio, continuando a ser compatível com os sistemas de encravamento existentes. Foi então dada particular atenção à definição, de forma clara, das interfaces com os sistemas externos que interagem com o encravamento, sem detalhar as funções internas do encravamento.

C.13.5. Os perigos foram então identificados apenas nas interfaces, de modo a permanecerem genéricos (ou seja, para evitar quaisquer dependências com as arquitecturas específicas).

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

Apenas os perigos resultantes das falhas técnicas foram considerados. Foram então identificados dois perigos genéricos para cada interface:

a) output errado do encravamento transmitido à interface

b) o input (correcto) é corrompido na interface

C.13.6. Foram então dadas mais características específicas a esses perigos genéricos de cada interface.

C.13.7. Na fase seguinte, as contribuições dos componentes existentes do sistema para os perigos identificados foram analisadas e apresentadas numa árvore de falhas. Isto permitiu, com base nas taxas de falha calculadas dos componentes, calcular uma taxa de ocorrência para cada perigo e usar essas taxas como taxas de perigo tolerável (THR) nas gerações futuras dos sistemas electrónicos de bloqueio.

C.13.8. A análise de risco foi acompanhada e avaliada pela autoridade nacional de segurança (EBA).

C.13.9. No âmbito da análise de risco, foi também realizada uma análise das funções de controlo e de visualização do sistema electrónico. Mais uma vez, usou-se como referência um sistema electrónico de bloqueio existente e aprovado, de modo a inferir os requisitos de segurança das funções do interface homem-máquina (MMI) para controlar quer as falhas e perturbações aleatórias, quer as falhas sistemáticas. Por conseguinte, foram determinados os níveis de integridade de segurança (SILs) das diferentes funções: para as funções MMI em operação normal, para as funções MMI em operação Comando-Libertação (modo degradado) e para a funcionalidade da visualização.

C.13.10. A análise de risco foi também acompanhada e avaliada pela autoridade nacional de segurança (EBA).

C.13.11. Estes exemplos de avaliação de risco ilustram a forma como a segunda aceitação de risco (sistema de referência) do MCS pode ser usada para inferir os requisitos de segurança dos novos sistemas. Além disso, foram baseados nas normas CENELEC, estando desta forma de acordo com o processo do MCS. A avaliação de risco dos exemplos cumpre os requisitos do MCS relacionados com as fases abrangidas. Mas dado que não se inclui nenhuma actividade de design, não há uma referência à gestão do registo de perigos nem à demonstração da conformidade do sistema em avaliação com os requisitos de segurança identificados.

C.13.12. Poderão ser encontradas mais informações sobre estas análises de risco em:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15, e;

(b) Bock, H., Braband, J., and Harborth, M.: *"SAFEty Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

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.14. Exemplo de um critério de aceitação de risco explícito na operação de comboios na Alemanha assente em radiocomunicações FFB

C.14.1. **Observação**: este exemplo de avaliação de risco não foi feito em resultado da aplicação do processo do MCS; foi realizado antes da existência do MCS. O exemplo tem por objectivo:

a) identificar as semelhanças existentes entre os métodos de avaliação do risco existentes e o processo do MCS;

b) realizar a comparação entre o processo existente e o processo exigido pelo MCS;

c) justificar o valor acrescentado da realização de passos adicionais (se existirem) exigidos pelo MCS.

Deve ser salientado que este exemplo é fornecido a título meramente informativo. Tem por finalidade auxiliar o leitor a compreender os processos do MCS. Porém, o exemplo em si não poderá ser transposto nem usado como um sistema de referência noutra alteração significativa. A avaliação de risco será feita para cada alteração significativa, em conformidade com o Regulamento relativo ao MCS.

C.14.2. Foi realizada uma análise de risco de acordo com as normas CENELEC no procedimento operacional totalmente novo que foi projectado (mas nunca introduzido) na Alemanha para as linhas ferroviárias convencionais. O conceito consistia em operar os comboios de forma segura apenas através do controlo assente em radiocomunicações (do trajecto e do comboio). Dado que não existiam códigos de prática (normas de engenharia reconhecidas) e sistemas de referência para este sistema novo, foi realizado um cálculo de risco explícito, de modo a demonstrar a segurança do novo procedimento. Foi necessário mostrar que o nível de risco para o passageiro em virtude de um novo sistema não excederia um valor de risco aceitável (critério de aceitação de risco explícito).

C.14.3. Este critério de aceitação de risco explícito foi calculado com base nas estatísticas de acidentes ocorridos na Alemanha e cuja causa se atribuiu à sinalização e aos sistemas de controlo e a sua plausibilidade foi também confirmada com o critério MEM. Essa demonstração de segurança está de acordo com o requisito alemão EBO de ter “o mesmo nível de segurança” em caso de desvios das regras de engenharia. A análise de risco foi também acompanhada e avaliada pela autoridade nacional de segurança (EBA).

C.14.4. Este exemplo de avaliação de risco mostra como um critério explícito global (para o terceiro princípio de aceitação de risco dos MCS) pode ser inferido para os novos sistemas sem códigos de prática aplicáveis nem sistemas de referência. A análise de risco que foi subsequentemente realizada no novo sistema baseia-se nas normas CENELEC, estando desta forma de acordo com o processo do MCS. A avaliação de risco do exemplo cumpre os requisitos dos MCS, mas não há referência à gestão de registo de perigos, nem à demonstração da conformidade do sistema em avaliação como os requisitos de segurança identificados.

C.14.5. Poderão ser encontradas mais informações sobre estas análises de risco em: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, 10-15

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

C.15. Exemplo do teste de aplicabilidade dos CAR-ST

C.15.1. A finalidade deste apêndice é mostrar como num exemplo da função do subsistema a bordo ETCS como usar o critério da secção 2.5.4 e como determinar se os CAR-ST são aplicáveis.

C.15.2. O subsistema a bordo ETCS é um sistema técnico. É considerada a seguinte função: "*dar ao Maquinista as informações que o permitam conduzir o comboio em segurança e aplicar os freios em caso de velocidade excessiva*."

Descrição da função: com base nas informações recolhidas na via (velocidade autorizada) e na velocidade do comboio calculada pelo subsistema ETCS a bordo:

a) o maquinista conduz o comboio e garante que a velocidade do comboio não excede a velocidade autorizada;
b) igualmente, o subsistema ETCS verifica que o comboio nunca excede o limite de velocidade autorizada. Em caso de excesso de velocidade, o sistema aplica automaticamente os freios.

Quer o maquinista, quer o subsistema ETCS estão a usar a avaliação da velocidade do comboio que é calculada pelo subsistema ETCS .

C.15.3. Pergunta: "O CAR-ST aplica-se à avaliação da velocidade do comboio através do subsistema a bordo?":

C.15.4. Aplicação do fluxograma do Figura 14 e respostas às diferentes perguntas:

a) Perigo considerado para o sistema técnico:

"*Ultrapassagem da velocidade de segurança tal como recomendado pelo ETCS*" (ver UNISIG SUBSET 091).

b) O perigo pode ser controlado por um código de prática ou por um sistema de referência?

NÃO. Parte-se do princípio que o sistema ETCS constitui um design novo e inovador. Por isso, não existem códigos de prática nem sistemas de referência que possam controlar o perigo a um nível de risco aceitável.

c) É provável que o perigo possa ter consequências catastróficas?

SIM, dado que a "*ultrapassagem da velocidade de segurança tal como recomendado pelo ETCS*" pode resultar potencialmente em "*mortes e ou múltiplas lesões graves e/ou danos graves no ambiente*".

d) A consequência catastrófica é uma consequência directa da falha do Sistema Técnico?

SIM, se não existirem barreiras de segurança adicionais. A mesma avaliação da velocidade do comboio que é calculada pelo subsistema ETCS é indicada ao Maquinista e à função de controlo dos freios do subsistema ETCS. Por isso, partindo do princípio que o maquinista está a conduzir o comboio (por questões de comportamento) à velocidade máxima autorizada pela via, nem o maquinista nem o subsistema ETCS vão detectar que o comboio está em excesso de velocidade em caso de subvalorização da velocidade do comboio. Isso poderá provocar um descarrilamento com consequências catastróficas.

e) Conclusões:

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) nos requisitos quantitativos: aplicar uma THR de 10^{-9} h^{-1} para as falhas de hardware aleatórias do subsistema ETCS a bordo, garantindo que:

i. a avaliação deste objectivo quantitativo tem em consideração, em sistemas redundantes, os componentes comuns (por exemplo, inputs isolados ou comuns a todos os canais, fonte de alimentação comum, comparadores, votadores, etc.);
ii. são abrangidos os tempos de detecção de falhas pendentes ou latentes;
iii. é realizada uma análise das falhas devidas a causas/modos comuns (CCF/CMF);
iv. é realizada uma Avaliação Independente;

(2) nos requisitos do processo: aplicar o processo SIL 4 na gestão das falhas/erros sistemáticos do subsistema ETCS a bordo. Isto exige a aplicação:

i. de um processo de gestão de qualidade em conformidade com o SIL 4;
ii. de um processo de gestão de segurança em conformidade com o SIL 4;
iii. das normas relevantes, por exemplo:
- no desenvolvimento do software, usar a norma EN 50 128 ;
- no desenvolvimento do hardware, usar as normas EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2, etc;

(3) de uma Avaliação Independente do(s) processo(s).

C.16. Exemplos das estruturas possíveis do registo de perigos

C.16.1. Introdução

C.16.1.1. Os requisitos mínimos a registar no registo de perigos estão identificados na secção 4.1.2 do Regulamento relativo ao MCS. Estes são indicados em fundo sombreado nos exemplos de registos de perigos que se seguem.

C.16.1.2. Poderá haver várias formas de estruturar um registo de perigos, bem como informações adicionais que podem caracterizar os perigos e as medidas de segurança associadas. Por exemplo, os perigos e as medidas de segurança associadas podem ser dotados de um campo por cada elemento de informação. Contudo, independentemente da estrutura que é usada, é importante que o registo de perigos forneça ligações claras entre os perigos e as medidas de segurança associadas. Uma solução possível é que o registo de perigos contenha, para cada perigo e para cada medida de segurança associada, pelo menos um campo com:

(a) uma descrição clara incluído referências da sua origem e dos princípios de aceitação de risco seleccionados para controlar o perigo associado. Este campo permite compreender o perigo e as medidas de segurança associadas, bem como saber em que análises de segurança são identificados.

Dado que o registo de perigos é usado e mantido durante todo o ciclo de vida do sistema (ou seja, durante a operação e manutenção do sistema), é útil uma rastreabilidade clara, ou ligação, entre cada perigo e:

(1) o risco associado;
(2) as causas de perigo, se já identificadas;
(3) as medidas de segurança associadas, bem como os pressupostos que definem os limites do sistema em avaliação;

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) as análises de segurança associadas quando o perigo é identificado;

Além disso, a formulação das medidas de segurança (em especial as relacionadas com a transferência para outros actores tais como o proponente) e a formulação dos perigos e riscos associados tem de ser clara e suficiente. “Clara e suficiente” significa que podem ser compreendidos os riscos que as medidas de segurança e os perigos associados vão controlar, sem que haja necessidade de se reportar às análises de segurança relacionadas.

(b) o princípio de aceitação de risco usado para controlar o perigo de modo a apoiar o reconhecimento mútuo e auxiliar o organismo de avaliação a avaliar a aplicação correcta do MCS;

(c) uma informação clara sobre o seu estado: este campo indica se o perigo relacionado/medida de segurança ainda está aberto ou controlado/validado.

(1) um perigo aberto/medida de segurança é registado até ser controlado/validado;
(2) reciprocamente, os perigos/medidas de segurança controlados/validados não são mais registados a não ser que ocorram alterações significativas na operação ou manutenção do sistema: ver ponto [G 6](b) na secção 2.1.1. Se isso acontecer:

(i) o MCS é aplicado de novo nas alterações solicitadas de acordo com o Artigo 2.º. Ver também ponto [G 6](b)(1) da secção 2.1.1;
(ii) todos os perigos controlados e as medidas de segurança são reconsiderados de modo a verificar que não são afectados pelas alterações. Se afectados, os perigos relacionados e as medidas de segurança associados são reabertos e geridos de novo no registo de perigos;

Poderão ser implementadas medidas de segurança diferentes das medidas registadas no registo de perigos (por exemplo, para fins de redução de custos). As medidas de segurança implementadas são então registadas no registo de perigos com as evidências/justificação em como são adequadas e a demonstração que com estas medidas o sistema está em conformidade com os requisitos de segurança.

(d) a referência aos dados associados que controlam um perigo ou que validam uma medida de segurança. Este campo permite que mais tarde se encontrem os dados que permitiram o controlo do perigo e validar a(s) medida(s) de segurança associada(s);

Um perigo pode ser controlado no registo de perigos apenas se todas as medidas de segurança associadas, relacionadas com o perigo, forem validadas antecipadamente;

(e) a(s) organização(ões) ou entidade(s) responsáveis pela sua gestão.

C.16.1.3. O Apêndice A.3. da EN 50126-2 guia {Ref. 9} contém outro exemplo dos conteúdos de um registo de perigo.

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

C.16.2. Exemplo do registo de perigos para a alteração organizacional da secção C.5. do apêndice Apêndice C

Quadro 6: Exemplo do Registo de Perigos para a alteração organizacional da secção C.5. do C

Descrição do Perigo	**Medidas de Segurança**	**Prioridade/ Segurança Pontualidade**	**Imple-mentação(15)**	**Observações**	**Responsabilidade(19)**	**Origem**	**Princípio de aceitação de risco usado**	**Responsabilidade pela verificação**	**Forma de verificação**	**Estado xx.xx.xx**
Motivação reduzida entre os trabalhadores que continuam na Empresa o que leva à contínua saída dos trabalhadores Gestores desmotivados / esgotados	Nova ronda de trabalho de motivação para os trabalhadores, a ser realizado em grupos mais pequenos Redistribuição de fundos, de modo a que a Empresa obtenha tarefas significativas para realizar Inspecções mais frequentes por parte do gestor da via Atribuir fundos para garantir que o pessoal chave permaneça durante o processo. Dar especial atenção para garantir que as informações e os conhecimentos são transferidos no período que medeia entre a saída dos trabalhadores e os que assumem as tarefas. etc.	Alta/Alta	Coordenação por XYZ As regiões terão de procurar medidas para aumentar o controlo das linhas sobreposição de trabalhadores e seguimento pelo gestor da linha	O reforço das inspecções tem de ser incluído nos contratos. etc.	Gestor da empresa	”Brainstorming” Relatório HAZID R_X	N/D			A alteração das condições das circunstâncias reduziu significativamente este risco Realizada análise do ambiente de trabalho e alguma formação do pessoal.
Subcontratantes dos empresários, com falta de competência e controlo de qualidade	Reforço da procura de competências documentadas. Controlo sistemático das tarefas realizadas	Alta / Média	O GI tem de coordenar. As regiões terão de implementar medidas que exijam competências e controlo do trabalho	Implementado pelo acompanhamento do contratol. Input para o planeamento da revisão.	Gestor da infra-estrutura	”Brainstorming” Relatório HAZID R_X	N/D	Gestor de segurança		Reforço da incidência nas rotinas de controlo (2 controlos operativos por mês e área operativa)
Incerteza quanto	Definir papéis e responsabilidades.	Média/Média	Em cada região	Implementado pelo	Directores	reflexã	N/D	Gestor de		As regiões

(15) *Estas duas colunas relacionam-se com a informação/campo relativo aos actores responsáveis pelo controlo dos perigos identificados.*

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

Quadro 6: Exemplo do Registo de Perigos para a alteração organizacional da secção C.5. do C

Descrição do Perigo	**Medidas de Segurança**	**Prioridade/ Segurança Pontualidade**	**Imple-mentação**[15]	**Observações**	**Responsabilidade**[19]	**Origem**	**Princípio de aceitação de risco usado**	**Responsabilidade pela verificação**	**Forma de verificação**	**Estado xx.xx.xx**
aos papéis e responsabilidades na interface entre a Empresa e GI (gestor da linha).	Identificar todas as interfaces e definir quem é responsável pelas interfaces.		separadamente	contrato de manutenção e pelo plano estratégico de reorganização	regionais	o Relatório HAZID R_X		segurança		apresentaram a sua estratégia.

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

C.16.3. Exemplo de um registo de perigos completo para um subsistema de controlo/comando a bordo

C.16.3.1. Esta secção dá um registo de perigos isolado como exemplo (ver ponto [G 3] da secção 4.1.1) para gerir:
(a) Todos os requisitos de segurança internos aplicáveis ao subsistema pelo qual o actor é responsável; e
(b) todos os perigos identificados e medidas de segurança associadas que o actor pode implementar e que terão de ser transferidos para outros actores

Quadro 7 : Exemplo de um registo de perigos do fabricante para um subsistema de controlo/comando a bordo

N.º Perigo	Origem	Descrição do Perigo	Informações adicionais	Actor responsável	Medida de Segurança	Princípio de aceitação de risco usado	Exportado	Estado
1	Relatório HAZOP R_X	Velocidade máxima do comboio fixada com valor muito alto (Vmax)	Errada configuração específica do subsistema a bordo (equipa de manutenção) Introdução de Dados Errados a bordo (maquinista)	Empresa ferroviária	• Definir um procedimento para a aprovação dos dados de configuração do subsistema a bordo; • Definir um procedimento operacional para o Processo de Introdução de Dados pelo maquinista;	Cálculo do risco explícito	Sim	Controlado (exportado para a EF) Consultar também a secção C.16.4.2. do Apêndice C..
2	Relatório HAZOP R_X	Curvas de frenagem (ou seja, Autorização de Movimento) na configuração do subsistema a bordo com dados muito permissivos	O procedimento para configuração específica do subsistema a bordo depende: • das margens de segurança assumidas pelo sistema de frenagem do comboio, • do tempo de reacção do sistema de frenagem do comboio (directamente dependente do comprimento do comboio, em especial quando se trata de comboios de mercadorias)	Empresa ferroviária	• Especificar correctamente os requisitos do sistema na Definição do Sistema; • Assumir margens de segurança suficientes no sistema de travagem do comboio em questão;	Cálculo do risco explícito	Sim	Controlado (exportado para a EF) Consultar também a secção C. 16.4.2. do Apêndice C
3	Relatório HAZOP R_X	• Velocidade máxima do comboio comboio fixada com valor muito alto (Vmax) • Curvas de frenagem (ou seja, Autoridade de Circulação) na configuração do	Falha na actualização do diâmetro da roda do comboio na configuração específica do sub-sistema a bordo (pessoal de manutenção).	Empresa ferroviária	• Definir um procedimento para medir o diâmetro da roda do comboio pelo pessoal da manutenção; • Definir um procedimento para a actualização regular do diâmetro da roda do comboio no subsistema a bordo;	Cálculo do risco explícito	Sim	Controlado (exportado para a EF) Consultar também a secção C. 16.4.2. do Apêndice C

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

Quadro 7 : Exemplo de um registo de perigos do fabricante para um subsistema de controlo/comando a bordo

N.º Perigo	Origem	Descrição do Perigo	Informações adicionais	Actor responsável	Medida de Segurança	Princípio de aceitação de risco usado	Exportado	Estado
		subsistema a bordo com dados muito permissivos						
			Falha no procedimento do fabricante na preparação e no carregamento dos dados de configuração no subsistema a bordo	Fabricante:	Definir um procedimento para actualizar o diâmetro da roda do comboio nos dados de configuração a bordo	Cálculo do risco explícito	Sim	Controlado pelo Procedimento P_X
4	Relatório HAZOP R_X	Entrada de um comboio a alta velocidade (160 km/h se não existir sinal na linha) na linha sem o subsistema a bordo activo e sem sinalização na linha	Apenas controlável pela vigilância do maquinista. A entrada numa área da via com ATP depende do procedimento de reconhecimento por parte do maquinista antes do local de transição Em caso de ausência de reconhecimento, o subsistema de controlo-comando a bordo aplica automaticamente os freios.	Gestor da infra-estrutura	Gestor da infra-estrutura deverá garantir que os comboios que não possuem um subsistema activo de controlo-comando a bordo não entram na via respectiva. Definir um procedimento para a gestão de tráfego.	Cálculo do risco explícito	Sim	Consultar também a secção C. 16.4.2. do Apêndice C
				Empresa ferroviária	Garantir a formação do maquinista para entrar numa área da via equipada com ATP	Cálculo do risco explícito	Sim	Controlado (exportado para o GI) Consultar também a secção C. 16.4.2. do Apêndice C
5	Relatório HAZOP R_X	Excessiva velocidade máxima do comboio apresentada ao maquinista (Vmax)	A informação mostrada na interface do maquinista é monitorizada pelo subsistema de controlo-comando a bordo SIL 4 que aplica os freios de emergência em caso de discrepância entre o mostrador e o valor esperado. Em caso de não conformidade com a autorização de de movimento o subsistema de controlo-comando a bordo aplica os freios de emergência	Fabricante:	Desenvolver um subsistema de controlo-comando embarcado tipo SIL 4	Cálculo do risco explícito	Sim	Dossier de segurança demonstrando que o subsistema SIL 4, avaliado por um Avaliador de Segurança Independente
6	Relatório HAZOP R_X	Comboio parte sem a interface homem-máquina	Perda da redundância do subsistema embarcado	Fabricante:	Desenvolver um subsistema de controlo-comando embarcado tipo SIL 4	Cálculo do risco explícito	Sim	Dossier de segurança demonstrando que o um subsistema é tipo SIL 4, avaliado por um Avaliador de Segurança Independente
etc.								

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

C.16.4. Exemplo de um registo de perigos para transferência de informações a outros actores

C.16.4.1 Esta secção dá como exemplo um registo de perigos para transferir a outros actores os perigos identificados e as medidas de segurança associadas que um dado actor não consegue implementar. Ver ponto [G 1] da secção 4.1.1.
Este exemplo é igual ao exemplo da secção C.16.3. do APÊNDICE C. A única diferença é que são retirados os perigos internos e as medidas de segurança que podem ser controladas pelos respectivos actores.

C.16.4.2. A última coluna do Quadro 8: é usada para cumprir o requisito da secção 4.2 do Regulamento relativo ao MCS. Há diferentes maneiras de cumprr esse requisito. Uma forma poderá ser fazer referência às evidências usados pelo actor que recebe a informação de segurança exportada. Uma outra forma pode ser fazer uma reunião entre os dois actores de modo a encontrarem em conjunto uma solução adequada para controlar o(s) risco(s) associado(s). Os resultados dessa reunião podem constar de um documento acordado (por exemplo, na acta da reunião), a que o actor que exporta as informações relativas à segurança pode fazer referência para fechar os respectivos perigos no seu registo de perigos.

Quadro 8: Exemplo de um registo de perigos para transferir informações relacionadas com a segurança a outros actores.

N.º Perigo	Origem do Perigo		Descrição do Perigo	Informações adicionais	Actor responsável	Medida de Segurança	Comentários do receptor
	N.° no Quadro 7 :	Outro					
1	N.º1	Relatório HAZOP R_X	Velocidade máxima do comboio comboio fixada com valor muito alto (Vmax)	Configuração específica errada do subsistema a bordo (equipa de manutenção) Introdução de Dados Errados a bordo (maquinista)	Empresa ferroviária	• Definir um procedimento para a aprovação dos dados de configuração do subsistema a bordo; • Definir um procedimento operacional para o Processo de Introdução de Dados pelo maquinista;	• Os dados de configuração do subsistema de controlo-comando a bordo dependem das características físicas do material circulante. • São então aplicadas margens de segurança nestes dados em coordenação entre o Gestor da infra-estrutura e a Empresa Ferroviária. • Os dados são carregados no subsistema a bordo de acordo com os procedimentos adequados do fabricante durante a instalação, integração no material circulante e aceitação do subsistema de controlo-comando. • Os maquinistas são treinados e avaliados face ao procedimento D_P. • Os maquinistas são também avaliados pelo GI face às normas aplicáveis à infra-estrutura do GI.
2	N.2	Relatório HAZOP R_X	Curvas de frenagem (ou seja, Autorização de Movimento) na configuração do subsistema a bordo com dados muito	O procedimento da configuração específica do subsistema a bordo depende: • das margens de segurança assumidas pelo sistema de frenagem do comboio,	Empresa ferroviária	• Especificar correctamente os requisitos do sistema na Definição do Sistema; • Assumir margens de segurança suficientes no sistema de travagem do	Ver comentário da linha 1 supra.

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

Quadro 8: Exemplo de um registo de perigos para transferir informações relacionadas com a segurança a outros actores.

N.º Perigo	Origem do Perigo		Descrição do Perigo	Informações adicionais	Actor responsável	Medida de Segurança	Comentários do receptor
	N.° no Quadro 7 :	Outro					
			permissivos	• do tempo de reacção do sistema de frenagem do comboio (directamente dependente do comprimento do comboio, em especial quando se trata de comboios de mercadorias)		comboio em questão;	
3	N.3	Relatório HAZOP R_X	• Velocidade máxima do comboio excessiva(Vmax) • Curvas de frenagem (ou seja, Autorização de Movimento) na configuração do subsistema a bordo com dados muito permissivos	Falha na actualização do diâmetro da roda do comboio na configuração específica do sub-sisitema a bordo (pessoal de manutenção).	Empresa ferroviária	• Definir um procedimento para medir o diâmetro da roda do comboio pelo pessoal da manutenção; • Definir um procedimento para a actualização regular do diâmetro da roda do comboio no subsistema a bordo;	• A manutenção do subsistema de controlo-comando a bordo é feita de acordo com o "Procedimento de Manutenção PM_Z" • O diâmetro da roda do comboio é actualizado em intervalos definidos de acordo com o procedimento $P_{W.}$ • No Processo de Introdução de Dados, os maquinistas são treinados e avaliados face ao "Procedimento P_{DE}"
4	N. 4	Relatório HAZOP R_X	Entrada de um comboio a alta velocidade (160 km/h se não existir sinal na linha) na linha sem o subsistema a bordo activo e sem sinalização na linha	Apenas controlável pela vigilância do maquinista. A entrada numa área da via com ATP depende do procedimento de reconhecimento por parte do maquinista antes do local de transição Em caso de ausência de reconhecimento, o subsistema de controlo-comando a bordo aplica automaticamente os freios.	Gestor da infra-estrutura	Gestor da infra-estrutura deverá garantir que os comboios que não possuem um subsistema activo de controlo-comando a bordo não entram na via respectiva. Definir um procedimento para a gestão de tráfego.	A gestão do tráfego na infra-estrutura do GI é regida pelo conjunto de normas R_{TM}
					Empresa ferroviária	Garantir a formação do maquinista para entrar numa área da linha equipada com ATP	• Os maquinistas são treinados em intervalos regulares face ao procedimento P_{GI_PM} do GI. • Os maquinistas são também avaliados pelo GI face ao conjunto de normas (S_R) aplicáveis à infra-estrutura do GI.
etc.							

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

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

C.17. Exemplo de uma lista de perigos genérica para operação ferroviária

C.17.1. A Análise de Segurança Ferroviária Optimizada (ROSA), um projecto no quadro da cooperação franco-alemã (DEUFRAKO), tentou estabelecer uma lista de perigos genérica e abrangente que cobre a operação ferroviária padrão. O objectivo e o desafio era definir estes perigos com o máximo pormenor possível, mas sem reflectir as especificidades da ferrovia francesa e alemã. A lista foi estabelecida usando as listas de perigos actuais de ambos os países (SNCF e DB) e foi igualmente realizada uma verificação cruzada com as listas de perigos de outros países. Não obstante o objectivo declarado ser abrangente e genérico, a lista é aqui apresentada apenas como um exemplo indicativo que poderá ser útil aos actores quando tiverem de identificar perigos num determinado projecto. Em princípio, os perigos apresentados nesta lista teriam ainda de ser especificados ou completados, de modo a reflectir as eventuais especificidades do projecto.

C.17.2. Os perigos do "projecto de lista" que se segue são designados "ponto de partida dos perigos " (PPP) e significam os perigos a partir dos quais a análise de consequências e a análise de causas podem ser realizadas para determinar as medidas/barreiras de segurança e os requisitos de segurança para controlar esses perigos.

C.17.3. Lista de perigos do projecto ROSA:

SPH 01	Determinação inicial errada da velocidade limite (relacionada com a infra-estrutura)
SPH 02	Determinação errada do limite de velocidade (relacionada com o comboio)
SPH 03	Distância de frenagem mal determinada/perfil de velocidade errado/curvas de frenagem erradas
SPH 04	Desaceleração insuficiente (causas físicas)
SPH 05	Comando de velocidade/frenagem, errado/inapropriado
SPH 06	Velocidade errada registada (velocidade do comboio errada)
SPH 07	Falha na comunicação do limite de velocidade
SPH 08	Fuga do comboio
SPH 09	Sentido de marcha errado/retroceder intencional – (combinação do SPH 08 e SPH 14)
SPH 10	Registada posição absoluta/relativa errada
SPH 11	Falha na detecção do comboio
SPH 12	Perda da integridade do comboio
SPH 13	Itinerário do comboio possivelmente errado
SPH 14	Falha na transmissão/comunicação do horário/AC (autoridade de circulação)
SPH 15	Falha estrutural do guiamento
SPH 16	Componente da agulha avariado
SPH 17	Comando errado da agulha
SPH 18	Comprovação errada da agulha
SPH 19	Objecto do sistema na via / dentro do gabarito (excl. balastro)
SPH 20	Objecto estranho na via / dentro do gabarito
SPH 21	Utilizador rodoviário em Passagem de Nível (PN)
SPH 22	Efeitos de sopro no balastro
SPH 23	Impacto das forças aerodinâmicas no comboio
SPH 24	Equipamento/elemento/carregamento do comboio ultrapassa o gabarito do comboio
SPH 25	Dimensão inadequada do gabarito da via para o comboio
SPH 26	Distribuição errada da carga

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

SPH 27	Roda partida, eixo partido
SPH 28	Eixo/roda/rolamento quentes
SPH 29	Falha do bogie/suspensão, amortecimento
SPH 30	Falha do estrutura/caixa do veículo
SPH 31	Intrusão (aspecto de segurança)
SPH 32	Pessoa autorizada atravessa a via
SPH 33	Pessoal a trabalhar na via
SPH 34	Pessoas não autorizadas invadem a via (negligência)
SPH 35	Pessoa cai do bordo da plataforma para a via
SPH 36	Efeito de sopro / pessoa muito próxima do bordo da plataforma
SPH 37	Pessoal a trabalhar perto da via, por exemplo, na via adjacente
SPH 38	Pessoa sai do comboio intencionalmente (excl. embarque/desembarque de passageiros)
SPH 39	Pessoa cai da porta (lateral)
SPH 40	Pessoa cai da porta (frente/cauda)
SPH 41	Comboio parte/avança com as portas abertas (gabarito não ultrapassado)
SPH 42	Pessoa cai na zona de ligação entre duas carruagens
SPH 43	Passageiro inclina-se para fora da porta
SPH 44	Passageiro inclina-se para fora da janela
SPH 45	Pessoal/revisor inclina-se para fora da porta
SPH 46	Pessoal/revisor inclina-se para fora da janela
SPH 47	Pessoal envolvido nas manobras inclina-se para fora do degrau
SPH 48	Pessoa cai/sobe da plataforma para o espaço entre o veículo e a plataforma
SPH 49	Pessoa cai/sai do comboio sem a presença da plataforma
SPH 50	Pessoa cai na zona da porta aquando do embarque/desembarque de passageiros.
SPH 51	Portas do comboio fecham com pessoa na zona das portas
SPH 52	Comboio avança durante o embarque/desembarque de passageiros
SPH 53	Possibilidade de pessoa ferida no comboio
SPH 54	Perigo de incêndio/explosão (no/perto do comboio) – categoria do acidente, consequência de SPH 55, SPH 56)
SPH 55	Temperatura inadequada (no comboio)
SPH 56	Intoxicação/asfixia (no/perto do comboio)
SPH 57	Electrocussão (no/perto do comboio)
SPH 58	Pessoa cai da plataforma (excluindo embarque/desembarque)
SPH 59	Temperatura inadequada (na plataforma)
SPH 60	Intoxicação/asfixia (na plataforma)
SPH 61	Electrocussão (na plataforma)

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