Agence ferroviaire européenne	
Exemples d'appréciation des risques et d'outils possibles pour faciliter l'application du règlement MSC	
Référence ERA:	ERA/GUI/02-2008/SAF
Version ERA:	1.1
Date:	06/01/2009

Document élaboré par	Agence ferroviaire européenne Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex France
Type de document:	Guide
Statut:	Public

	Nom	**Fonction**
Diffusion autorisée par	Marcel VERSLYPE	Directeur exécutif
Document révisé par	Anders LUNDSTRÖM Thierry BREYNE	Chef de l'unité Sécurité Chef du secteur Évaluation de sécurité
Écrit par (Auteur)	Dragan JOVICIC	Responsable projet Unité Sécurité

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

DESCRIPTION DU DOCUMENT

Historique des modifications

Tableau 1: État du document.

Version Date	Auteur(s)	Numéro de section	Description de la modification
Ancien titre et ancienne structure du document: *«Guide d'utilisation de la recommandation relative au 1er ensemble de MSC»*			
Guide Version 0.1 15/02/2007	Dragan JOVICIC	Toutes	Première version du «Guide d'utilisation» correspondant à la version 1.0 du «1er ensemble de recommandations MSC». C'est également la première version du document transmise au groupe de travail MSC pour une évaluation formelle.
Guide Version 0.2 07/06/2007	Dragan JOVICIC	Toutes	Réorganisation du document afin de correspondre à la structure de la version 4.0 de la recommandation MSC. Mise à jour suite au Processus formel d'évaluation du groupe de travail MSC sur la version 1.0 de la recommandation. Toutes
		Toutes	Mise à jour du document avec des informations additionnelles recueillies lors de réunions internes de l'ERA, ainsi qu'avec les demandes du groupe de travail MSC de développer de nouveaux points.
		Figure 1	Modification du diagramme illustrant le «Cadre de gestion des risques pour le premier ensemble de Méthodes Communes de Sécurité» conformément aux commentaires issus de l'évaluation et à la terminologie ISO.
Guide Version 0.3 20/07/2007	Dragan JOVICIC	Appendices	Réorganisation des appendices et création de nouveaux. Nouvel appendice rassemblant tous les diagrammes illustrant et facilitant la lecture et la compréhension du Guide.
		Toutes	Mise à jour du document visant à: • développer au maximum les sections existantes; • préciser la signification de la «démonstration du respect par le système des exigences de sécurité»; • créer un lien avec le cycle en V CENELEC (figure 8 et figure 10 de la norme EN 50 126); • préciser la nécessité d'une collaboration et d'une coordination entre les différents acteurs du secteur ferroviaire dont les activités peuvent avoir un impact sur la sécurité du système ferroviaire; • clarifier les preuves attendues (par ex. registre des risques et dossier de sécurité) pour démontrer aux organismes d'évaluation l'application correcte du processus d'appréciation des risques MSC; Document également mis à jour suite à la première évaluation interne au sein de l'Agence.
Guide Version 0.4 16/11/2007	Dragan JOVICIC	Toutes	Document mis à jour suite au processus formel d'évaluation conformément aux commentaires reçus sur la version 0.3 de la part des organisations et membres suivants du groupe de travail MSC et convenus avec eux au téléphone: • les ANS belge, espagnole, finlandaise, norvégienne, française et danoise; • SIEMENS (membre d'UNIFE); • le gestionnaire d'infrastructure norvégien (Jernbaneverket – membre de l'EIM)
Guide Version 0.5 27/02/2008	Dragan JOVICIC	Toutes	Document mis à jour conformément aux commentaires reçus sur la version 0.3 de la part des organisations et membres suivants du groupe de travail MSC et convenus avec eux au téléphone: • CER • ANS néerlandaise

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tableau 1: État du document.

Version Date	Auteur(s)	Numéro de section	Description de la modification
		Toutes	Document mis à jour conformément à la version signée de la recommandation MSC. Document mis à jour suite aux commentaires d'évaluation interne à l'Agence reçus de Christophe CASSIR et de Marcus ANDERSSON.
		Toutes Appendices	Renumérotation complète des paragraphes du document par rapport à la recommandation Inclusion d'exemples d'application de la recommandation MSC.
Nouveau titre et nouvelle structure du document: *«Exemples d'évaluations de risques et d'outils possibles pour faciliter l'application du règlement MSC»*			
Guide Version 0.1 23/05/2008	Dragan JOVICIC	Toutes	Première version du document suite à la division du «Guide d'utilisation» version 0.5 en deux documents complémentaires.
Guide Version 0.2 03/09/2008	Dragan JOVICIC	Toutes	Mise à jour du document conformément: • au Règlement MSC de la Commission européenne {Ref. 3}; • aux commentaires de l'atelier du 1er juillet 2008 avec les membres du Railway Interoperability and Safety Committee (RISC); • aux commentaires soumis par les membres du groupe de travail MSC (ANS norvégienne, ANS finlandaise, ANS britannique, ANS française, CER, EIM, Jens BRABAND [UNIFE] et Stéphane ROMEI [UNIFE]
Guide Version 1.0 10/12/2008	Dragan JOVICIC	Toutes	Mise à jour du document conformément au Règlement de la Commission européenne relatif à l'évaluation et à l'appréciation des risques {Ref. 3} adopté par le Railway Interoperability and Safety Committee (RISC) en sa séance plénière du 25 novembre 2008
Guide Version 1.1 06/01/2009	Dragan JOVICIC	Toutes	Mise à jour du document suite aux commentaires relatifs au Règlement MSC émis par les services juridiques et linguistiques de la Commission européenne.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Sommaire

DESCRIPTION DU DOCUMENT 2
Historique des modifications 2
Sommaire 4
Liste des illustrations 5
Liste des tableaux 6

0. INTRODUCTION 7
0.1. Champ d'application 7
0.2. Hors champ 8
0.3. Principe d'utilisation de ce document 8
0.4. Description du document 8
0.5. Documents de référence 10
0.6. Définitions, abréviations et terminologie normalisées 11
0.7. Définitions spécifiques 11
0.8. Termes et abréviations spécifiques 11

EXPLICATION DES ARTICLES DU RÈGLEMENT MSC 13
Article 1. Objet 13
Article 2. Champ d'application 13
Article 3. Définitions 15
Article 4. Changements significatifs 17
Article 4 (1) 17
Article 4 (2) 17
Article 5. Processus de gestion des risques 18
Article 6. Évaluation indépendante 19
Article 7. Rapports d'évaluation de la sécurité 20
Article 8. Gestion de la maîtrise des risques / audits internes et externes 21
Article 9. Retour d'information et progrès technique 22
Article 10. Entrée en vigueur 23

ANNEXE I – EXPLICATION DU PROCESSUS DANS LE RÈGLEMENT MSC 24

1. PRINCIPES GÉNÉRAUX APPLICABLES AU PROCESSUS DE GESTION DES RISQUES 24
1.1. Principes généraux et obligations 24
1.2. Gestion des interfaces 32

2. DESCRIPTION DU PROCESSUS D'APPRÉCIATION DES RISQUES 35
2.1. Description générale – correspondance entre le processus d'appréciation des risques MSC et le cycle en V CENELEC 35
2.2. Identification des dangers 42
2.3. Utilisation des codes de pratique et évaluation des risques 45
2.4. Utilisation du système de référence et évaluation des risques 46
2.5. Estimation et appréciation des risques explicites 48

3. DÉMONSTRATION DE LA CONFORMITÉ AUX EXIGENCES DE SÉCURITÉ 51

4. GESTION DES DANGERS 54
4.1. Processus de gestion des dangers 54

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

4.2. Échange d'informations 55

5. PREUVES D'APPLICATION DU PROCESSUS DE GESTION DES RISQUES 58

ANNEXE II DU RÈGLEMENT MSC 61

Critères à respecter par les organismes d'évaluation 61

APPENDICE A: CLARIFICATIONS SUPPLÉMENTAIRES 62

A.1. Introduction 62
A.2. Classification des dangers 62
A.3. Critère d'Acceptation des Risques pour les Systèmes Techniques (CAR-ST) 62
A.4. Preuve de l'évaluation de sécurité 73

APPENDICE B: EXEMPLES DE TECHNIQUES ET D'OUTILS D'AIDE AU PROCESSUS D'APPRÉCIATION DES RISQUES 76

APPENDICE C: EXEMPLES 77

C.1. Introduction 77
C.2. Exemples d'application des critères relatifs aux changements significatifs selon l'article 4, paragraphe 2 77
C.3. Exemples d'interfaces entre acteurs du secteur ferroviaire 78
C.4. Exemples de méthodes pour la définition des risques largement acceptables 79
C.5. Exemple d'appréciation des risques pour un changement organisationnel significatif 81
C.6. Exemple d'appréciation des risques pour un changement opérationnel significatif – modification des temps de conduite 83
C.7. Exemple d'appréciation des risques pour un changement technique significatif (SCC) 85
C.8. Exemple de la ligne directrice suédoise BVH 585.30 pour l'appréciation des risques des tunnels ferroviaires 88
C.9. Exemple d'appréciation des risques au niveau du système pour le métro de Copenhague 90
C.10. Exemple de fil conducteur OTIF pour le calcul de risques lors du transport ferroviaire de marchandises dangereuses 93
C.11. Exemple d'appréciation des risques de la demande d'approbation d'un nouveau type de matériel roulant 95
C.12. Exemple d'appréciation des risques pour un changement opérationnel significatif – opération par le conducteur seul 98
C.13. Exemple d'utilisation d'un système de référence pour la définition d'exigences de sécurité destinées à de nouveaux systèmes d'aiguillages électroniques en Allemagne 100
C.14. Exemple d'un critère d'acceptation de risque explicite pour l'exploitation de trains à base de radio FFB en Allemagne 102
C.15. Exemple de test d'applicabilité du CAR-ST 103
C.16. Exemples de structures possibles pour le registre des dangers 104
C.17. Exemple d'une liste générique de dangers pour l'exploitation d'un système ferroviaire 113

Liste des illustrations

Figure 1: Cadre de gestion des risques du règlement MSC {Ref. 3}. 27
Figure 2: MSC et SGS harmonisés. 28
Figure 3: Exemples de dépendances entre cas de sécurité (issu de la figure 9 de la norme EN 50 129). 30
Figure 4: Cycle en V simplifié de la figure 10 de la norme EN 50 126. 35
Figure 5: Figure 10 du cycle en V de la norme EN 50 126 (cycle de vie CENELEC du système) 36

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Figure 6: Sélection des mesures de sécurité adéquates pour maîtriser les risques.....41
Figure 7: Risques largement acceptables.....44
Figure 8: Filtrage des dangers associés à des risques largement acceptables. 44
Figure 9: Pyramide des critères d'acceptation des risques (CAR).....49
Figure 10: Figure A.4 de la norme EN 50 129: Définition des dangers par rapport aux limites du système. .51
Figure 11: Dérivation des exigences de sécurité pour les phases inférieures.....52
Figure 12: Hiérarchie de documentation structurée. 58
Figure 13: Architecture redondante d'un système technique.....65
Figure 14: Diagramme pour le test d'applicabilité du CAR-ST.....67
Figure 15: Exemple de changement non significatif Message téléphonique pour le contrôle d'un passage à niveau.....77
Figure 16: Remplacement d'une boucle de voie par un système radio. 86

Liste des tableaux

Tableau 1: État du document. 2
Tableau 2: Tableau des documents de référence.....10
Tableau 3: Tableau des termes spécifiques.....11
Tableau 4: Tableau des abréviations. 11
Tableau 5: Exemple typique d'une matrice de risques calibrée.....*71*
Tableau 6: Exemple de registre des dangers pour le changement organisationnel de la section C.5 de l'appendice C. *107*
Tableau 7: Exemple du registre des dangers d'un constructeur pour un sous-système embarqué de contrôle-commande. *108*
Tableau 8: Exemple d'un registre des dangers pour le transfert d'informations de sécurité vers d'autres acteurs.....*111*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0. INTRODUCTION

0.1. Champ d'application

0.1.1. L'objectif du présent document est d'apporter des clarifications supplémentaires sur le «Règlement de la Commission concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a), de la directive 2004/49/CE du Parlement européen et du Conseil» {Ref. 3}. Dans le cadre du présent document, ce règlement est désigné sous le nom de «règlement MSC».

0.1.2. Ce document n'est pas légalement contraignant et son contenu ne doit pas être interprété comme la seule façon de respecter les exigences de la MSC. Ce document a été conçu pour compléter le Guide d'application du règlement MSC {Ref. 4} expliquant la façon d'utiliser et d'appliquer le règlement MSC. Il fournit des informations pratiques supplémentaires sans imposer en aucune façon une procédure obligatoire à respecter et sans définir de pratique légalement contraignante. Ces informations peuvent servir à tous les acteurs[(1)] dont les activités sont susceptibles d'avoir un impact sur la sécurité des systèmes ferroviaires et qui sont tenus, directement ou indirectement, d'appliquer la MSC. Ce document fournit des exemples d'évaluations de risques et décrit quelques outils possibles pour faciliter l'application de la MSC. Ces exemples sont donnés uniquement à titre d'avis. Les acteurs sont libres d'utiliser des méthodes alternatives ou de continuer à utiliser leurs propres méthodes et outils existants pour se conformer à la MSC s'ils considèrent que ces outils et méthodes sont mieux adaptés.
En outre, les exemples et les informations complémentaires fournis dans ce document ne sont pas exhaustifs et ne couvrent pas toutes les situations possibles où des modifications significatives sont proposées. Ce document est donc fourni à titre purement informatif.

0.1.3. Ce document informatif doit être lu comme une aide supplémentaire à l'application du règlement MSC. Il sera lu idéalement en parallèle avec le règlement MSC {Ref. 3} et avec le guide associé {Ref. 4} afin de faciliter l'application de la MSC, mais il ne remplace pas le règlement MSC.

0.1.4. Ce document a été rédigé par l'Agence ferroviaire européenne (European Railway Agency, ERA) avec le soutien des associations ferroviaires et des experts des autorités nationales de sécurité membres du groupe de travail MSC. Il développe les idées et les informations rassemblées par l'Agence lors de réunions internes et de réunions avec le groupe de travail et les délégations MSC. L'ERA réexaminera ce document et le mettra à jour lorsque cela s'avèrera nécessaire pour refléter l'évolution des normes européennes, les modifications de la MSC relative à l'appréciation des risques et les expériences éventuelles relatives à l'utilisation du règlement MSC. Étant donné qu'il n'est pas possible de présenter un calendrier du processus de révision du guide au moment de sa rédaction, nous recommandons au lecteur de s'adresser à l'Agence ferroviaire européenne pour obtenir la dernière version disponible de ce document.

---

(1) *Les acteurs concernés sont les entités adjudicatrices telles qu'elles sont définies à l'article 2, point r), de la directive 2008/57/CE relative à l'interopérabilité du système ferroviaire au sein de la Communauté, ou encore les fabricants, désignés collectivement par le règlement sous l'appellation «proposant», ou leurs fournisseurs et prestataires de services.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0.2. Hors champ

0.2.1. Ce document ne fournit aucune information ni aucune recommandation sur la façon d'organiser, d'exploiter, de concevoir et de construire tout ou partie d'un système ferroviaire. Il ne définit pas non plus les accords et arrangements contractuels susceptibles d'exister entre certains acteurs pour l'application du processus de gestion des risques. Les arrangements contractuels spécifiques à chaque projet échappent au champ d'application du règlement MSC, du guide qui lui est associé et du présent document.

0.2.2. Bien qu'échappant au champ d'application du présent document, les dispositions convenues entre les acteurs concernés peuvent être portées aux différents contrats en début de projet sans préjudice des dispositions de la MSC. Ces dispositions contractuelles peuvent couvrir par exemple:

(a) les coûts inhérents à la gestion des risques liés à la sécurité aux interfaces entre les acteurs;
(b) les coûts inhérents aux transferts de dangers et des mesures de sécurité associées entre les acteurs qui ne sont pas encore connus en début de projet;
(c) la façon de gérer les conflits susceptibles d'apparaître au cours du projet;
(d) etc.

En cas de désaccord ou de conflit entre le proposant et ses sous-traitants pendant le développement du projet, il peut être fait référence aux contrats concernés pour résoudre les conflits.

0.3. Principe d'utilisation de ce document

0.3.1. Bien que ce document puisse être lu de façon isolée, il ne remplace pas le règlement MSC {Ref. 3}. Chaque article du règlement MSC est recopié dans ce document pour en faciliter la lecture. Si nécessaire, l'article concerné est expliqué au préalable dans le guide d'application du règlement MSC {Ref. 4}. Les paragraphes qui suivent fournissent des informations supplémentaires pour faciliter la compréhension du règlement MSC lorsque cela est jugé nécessaire.

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 {Ref. 4} is not copied in the present document.

0.3.3. Afin de faciliter la lecture, la structure du présent document est calquée sur celle du règlement MSC et de son guide d'application.

0.4. Description du document

0.4.1. Ce document comporte les parties suivantes:

(a) Chapitre 0 définissant le champ d'application du document et fournissant une liste de documents de référence;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) Annexes I et II fournissant des informations supplémentaires sur les sections correspondantes du règlement MSC {Ref. 3} et du guide associé {Ref. 4};
(c) Nouveaux appendices développant plus avant certains aspects spécifiques et fournissant des exemples.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0.5. Documents de référence

Tableau 2: Tableau des documents de référence

{Ref. N°}	Titre	Référence	Version
{Ref. 1}	Directive 2004/49/CE du Parlement européen et du Conseil du 29 avril 2004 concernant la sécurité des chemins de fer communautaires et modifiant la directive 95/18/CE du Conseil concernant les licences des entreprises ferroviaires, ainsi que la directive 2001/14/CE concernant la répartition des capacités d'infrastructure ferroviaire, la tarification de l'infrastructure ferroviaire et la certification en matière de sécurité (directive sur la sécurité ferroviaire)	2004/*49/CE* JO L 164, 30.4.2004, p. 44, rectifiée par JO L 220, 21.6.2004, p. 16.	-
{Ref. 2}	Directive 2008/57/CE du Parlement européen et du Conseil du 17 juin 2008 relative à l'interopérabilité du système ferroviaire au sein de la Communauté	2008/57/CE JO L 191 du 18.07.08, p. 1.	-
{Ref. 3}	Règlement de la Commission (CE) n°.../... du [...] concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a), de la directive 2004/49/CE du Parlement européen et du Conseil	xxxx/aa/CE	adopté par le comité RISC le 25/11/2008
{Ref. 4}	Guide d'application du règlement de la Commission concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a) de la directive sur la sécurité ferroviaire	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Directive 2008/57/CE du Parlement européen et du Conseil du 17 juin 2008 relative à l'interopérabilité du système ferroviaire au sein de la Communauté	2008/57/CE JO L 191 du 18.07.08, p. 1.	-
{Ref. 6}	Système de Gestion de la Sécurité -- Critères d'évaluation pour les entreprises ferroviaires et les gestionnaires d'infrastructure	Critères d'évaluation SGS Partie A – Certifications de sécurité et autorisations	31/05/2007
{Ref. 7}	Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Systèmes électroniques de signalement en matière de sécurité	EN 50129	Février 2003
{Ref. 8}	Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) – Partie 1: la norme	EN 50126-1	Septembre 2006
{Ref. 9}	Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) -- Partie 2: guide d'application de la norme EN 50126-1 en matière de sécurité	EN 50126-2 (Ligne directrice)	Projet final (août 2006)
{Ref. 10}	Fil conducteur général pour le calcul de risques lors du transport ferroviaire de marchandises dangereuses	Fil conducteur OTIF approuvé par le comité d'experts RID	24 novembre 2005
{Ref. 11}	Critère d'Acceptation des Risques pour les Systèmes Techniques	Note 01/08	1.1 (25/01/2008)
{Ref. 12}	Unité Sécurité de l'ERA: Étude de faisabilité – « Attribution d'objectifs de sécurité (à des sous-systèmes STI) et consolidation des STI du point de vue de la sécurité » WP1.1: Évaluation de la faisabilité d'attribuer des objectifs de sécurité communs	WP1.1	1.0
{Ref. 13}	«Applications ferroviaires – Système de classification pour les véhicules ferroviaires – Partie 4: EN 0015380 Partie 4: Groupes fonctionnels ».	EN 0015380 Partie 4	

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

0.6. Définitions, abréviations et terminologie normalisées

0.6.1. Les définitions, abréviations et termes génériques utilisés dans ce document peuvent être consultés dans un dictionnaire standard.

0.6.2. Les sections ci-dessous définissent les abréviations, définitions et termes nouveaux utilisés dans ce guide.

0.7. Définitions spécifiques

0.7.1. Voir Article 3

0.8. Termes et abréviations spécifiques

0.8.1. Cette section définit les abréviations et termes nouveaux et spécifiques utilisés fréquemment dans ce document.

Tableau 3: Tableau des termes spécifiques.

Terme	Définition
Agence	l'Agence ferroviaire européenne (ERA)
Guide	le «Guide d'application du règlement de la Commission (CE) n° .../... du [...] concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a), de la directive 2004/49/CE du Parlement européen et du Conseil».
Règlement MSC	le «Règlement de la Commission (CE) n° .../... du [...] concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3, point a), de la directive 2004/49/CE du Parlement européen et du Conseil.» {Ref. 3}

Tableau 4: Tableau des abréviations.

Abréviation	Signification
CCS	Contrôle-commande et signalement
MSC	Méthode de sécurité commune
OSC	Objectifs de sécurité communs
CE	Commission européenne
ERA	Agence ferroviaire européenne
GI	Gestionnaire d'infrastructure
ISA	Vérificateur indépendant de sécurité (Independent Safety Assessor)
OTIF	Organisation intergouvernementale pour les transports internationaux ferroviaires
EM	État membre
ONO	Organisme notifié
ANS	Autorité nationale de sécurité
PGQ	Processus de gestion de la qualité
SGQ	Système de gestion de la qualité
RISC	Railway Interoperability and Safety Committee (Comité sur l'interopérabilité et la sécurité ferroviaire)
EF	Entreprise ferroviaire
SMP	Processus de gestion de la sécurité
SGS	Système de gestion de la sécurité
STF	Sécurité dans les tunnels ferroviaires

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Tableau 4: Tableau des abréviations.

Abréviation	Signification
TBC	À compléter (to be completed)
STI	Spécifications techniques d'interopérabilité

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

EXPLICATION DES ARTICLES DU RÈGLEMENT MSC

Article 1. Objet

Article 1 (1)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 1 (2)

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 2. Champ d'application

Article 2 (1)

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

[G 1] La MSC s'applique à l'ensemble du système ferroviaire et couvre l'évaluation des modifications suivantes apportées aux systèmes ferroviaires si ces modifications sont considérées comme significatives au sens de l'Article 4:

(a) construction de nouvelles lignes ou modification de lignes existantes;
(b) introduction de nouveaux systèmes techniques ou de systèmes techniques modifiés;
(c) modifications opérationnelles (par ex. nouvelles règles ou règles modifiées en matière d'exploitation et de maintenance);
(d) modifications au sein de l'organisation des EF/GI.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Dans le contexte de la MSC, le terme «système» fait référence à tous les aspects d'un système, y compris son développement, son exploitation, sa maintenance etc. jusqu'à sa mise hors service ou son élimination.

[G 2] La MSC couvre les changements significatifs apportés soit:

(a) à des systèmes «petits et simples» composés éventuellement de quelques éléments ou sous-systèmes techniques;
(b) à des systèmes «vastes et plus complexes» (comprenant par exemple des gares et des tunnels).

Article 2 (2)

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

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

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

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

[G 1] Par exemple, conformément à la directive sur la sécurité ferroviaire {Ref. 1} et à la directive sur l'interopérabilité des systèmes ferroviaires {Ref. 2}, un nouveau type de matériel roulant destiné à une ligne à grande vitesse doit respecter la STI relative au matériel roulant à grande vitesse. Bien que la plus grande partie du système évalué soit couverte par la STI, la question essentielle des facteurs humains liés au poste de pilotage n'est pas couverte par la STI. Par conséquent, pour assurer l'identification et la maîtrise correcte de tous les dangers raisonnablement prévisibles liés au facteur humain (c'est-à-dire aux interfaces entre le conducteur, le matériel roulant et le reste du système ferroviaire), il convient d'utiliser le processus MSC.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Article 2 (3)

This Regulation shall not apply to:

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 2 (4)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 3. Définitions

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

The following definitions shall also apply:

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

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

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

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

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

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

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

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

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

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

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

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

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

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

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

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

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

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

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

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

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

(22) 'technical system' means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;

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

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

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

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

---

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

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

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 4. Changements significatifs

Article 4 (1)

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

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

[G 1] En l'absence d'une règle nationale notifiée, la décision revient au proposant. L'évaluation de l'importance de la modification repose sur un avis d'expert. Par exemple, si la modification prévue d'un système existant est complexe, elle peut être considérée comme significative si le risque d'impact sur les fonctions existantes[6] du système est élevé, même si la modification elle-même n'est pas étroitement liée à la sécurité.

Article 4 (2)

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

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

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

(c) complexity of the change;

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

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

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

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Exemple de modifications mineures**: après la mise en service du système, le fait d'augmenter de 5 km/h la vitesse maximale sur une ligne peut ne pas être significatif. Mais si la vitesse maximale de ligne continue à être augmentée par tranches de 5 km/h, la somme des modifications successives (considérées individuellement comme non significatives) pourrait devenir un changement significatif par rapport aux exigences de sécurité initiales du système.

(6) *Étant donné que les fonctions d'un système ne sont pas toujours indépendantes, la modification de certaines fonctions peut également avoir un impact sur d'autres fonctions du système même si celles-ci ne paraissent pas directement concernées par ces changements.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Afin d'évaluer si une série de modifications successives (non significatives) devient significative dans son ensemble, il convient d'évaluer tous les dangers et les risques associés liés aux modifications. L'ensemble des modifications envisagées peut être considéré comme non significatif si le risque qui en découle est largement acceptable.

[G 3] Le travail réalisé par l'Agence en matière de modifications significatives a permis d'aboutir aux conclusions suivantes:

(a) il n'est pas possible d'identifier des seuils ou des règles harmonisés permettant, pour une modification donnée, de déterminer l'importance de cette modification;
(b) il n'est pas possible de définir une liste exhaustive de modifications significatives;
(c) la décision ne peut pas être valide pour tous les proposants et toutes les conditions techniques, opérationnelles, organisationnelles et environnementales.

Il est donc essentiel de laisser aux proposants la responsabilité de cette décision. Selon l'article 4, paragraphe 3, de la directive sur la sécurité ferroviaire {Ref. 1}, ceux-ci sont en effet responsables de l'exploitation en toute sécurité et de la maîtrise des risques associés à leur partie du système.

[G 4] Afin d'aider le proposant, la section C.2 de l'appendice C fournit un exemple d'«évaluation et utilisation des critères».

[G 5] La MSC ne doit pas être appliquée si la modification en matière de sécurité n'est pas considérée comme significative. Mais cela ne signifie pas qu'il n'y a rien à faire. Le proposant effectue des analyses de risques (préliminaires) afin de décider si la modification est significative. Ces analyses de risques ainsi que les justifications et arguments doivent être documentés afin de permettre aux ANS d'effectuer des audits. L'évaluation de l'importance d'une modification, et la décision de considérer une modification comme non significative, ne doit pas être évaluée indépendamment par un organisme d'évaluation.

Article 5. Processus de gestion des risques

Article 5 (1)

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 5 (2)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Article 5 (3)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 6. Évaluation indépendante

Article 6 (1)

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

[G 1] Le degré d'indépendance requis pour l'organisme d'évaluation dépend du niveau de sécurité requis pour le système faisant l'objet d'une évaluation. En attendant l'harmonisation de ce sujet, la meilleure pratique dans ce domaine à la clause 8 d'IEC61508-1:2001 ou au § 5.3.9. de la norme EN 50 129 {Ref. 7}. Le degré d'indépendance dépend à la fois de la gravité des conséquences du danger associé à l'équipement et du degré d'innovation. La section § 9.7.2 de la norme EN 50 126-2 et EN 50129 définit le degré d'indépendance pour les systèmes de signalisation. Le même degré peut en principe s'appliquer à d'autres systèmes.

[G 2] L'Agence travaille encore à la définition des rôles et responsabilités des différents organismes d'évaluation (ANS, ONO et ISA) ainsi que des interfaces requises entre ces organes. Cette définition précisera lequel (si possible) de ces organismes d'évaluation interviendra, sur quoi et selon quelles modalités. Elle permettra au final de déterminer comment:

(a) vérifier, sur la base des preuves disponibles, que les processus de gestion et d'appréciation des risques couverts par la MSC sont appliqués correctement, et:
(b) d'aider le proposant dans sa décision d'accepter la modification significative dans le système en cours d'évaluation.

Article 6 (2)

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

[G 1] Le travail de l'Agence relatif aux rôles et responsabilités des organismes d'évaluation fournira des informations complémentaires.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Article 6 (3)

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

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

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

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

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

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 6 (4)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 7. Rapports d'évaluation de la sécurité

Article 7 (1)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 7 (2)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Article 7 (3)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 7 (4)

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

[G 1] Ce principe de reconnaissance mutuelle est déjà accepté par les normes CENELEC: voir la section § 5.5.2 d'EN 50 129 et la section § 5.9 d'EN 50 126-2. Dans CENELEC, le principe d'acceptation croisée ou de reconnaissance mutuelle est appliqué par les proposants ou les évaluateurs indépendants de sécurité aux produits et aux applications génériques[7] pour autant que les évaluations et démonstrations de sécurité soient effectués conformément aux exigences des normes CENELEC.

[G 2] La reconnaissance mutuelle doit être appliquée également pour la réception de systèmes nouveaux ou modifiés si leur évaluation de risques et la démonstration de la conformité du système avec les exigences de sécurité sont effectuées conformément aux dispositions du règlement MSC {Ref. 3}.

Article 8. Gestion de la maîtrise des risques / audits internes et externes

Article 8 (1)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

---

(7) *Voir le point [G 5] de la section 1.1.5 et les notes de bas de page [9] et [10] en page 31 ainsi que la Figure 3 de ce document pour une explication plus détaillée de la terminologie «produit générique et application générique» et des principes inhérents.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Article 8 (2)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 9. Retour d'information et progrès technique

Article 9 (1)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 9 (2)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 9 (3)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 9 (4)

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

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

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 10. Entrée en vigueur

Article 10 (1)

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Article 10 (2)

This Regulation shall apply from 1 July 2012.

However, it shall apply from 19 July 2010:

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

ANNEXE I – EXPLICATION DU PROCESSUS DANS LE RÈGLEMENT MSC

1. PRINCIPES GÉNÉRAUX APPLICABLES AU PROCESSUS DE GESTION DES RISQUES

1.1. Principes généraux et obligations

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

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

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

[G 1] La Figure 1 illustre le cadre de gestion des risques de la MSC et le processus de gestion des risques correspondant. Chaque fois que cela est jugé nécessaire, les différents cadres/activités de ce diagramme font l'objet d'une description plus poussée dans une section spécifique de ce document.

[G 2] CENELEC recommande de décrire les processus de gestion et d'appréciation des risques dans un plan de sécurité. Mais si le projet ne se prête pas à une telle approche, la description concernée peut être intégrée à n'importe quel autre document pertinent. Voir la section 1.1.6.

[G 3] Le processus d'appréciation des risques part d'une définition préliminaire du système. Pendant la réalisation du projet, la définition préliminaire du système est progressivement mise à jour et remplacée par la définition du système. S'il n'existe aucune définition préliminaire du système, la définition formelle du système est utilisée pour l'appréciation des risques. Il est toutefois utile que tous les acteurs concernés par le changement significatif se réunissent en début de projet afin:

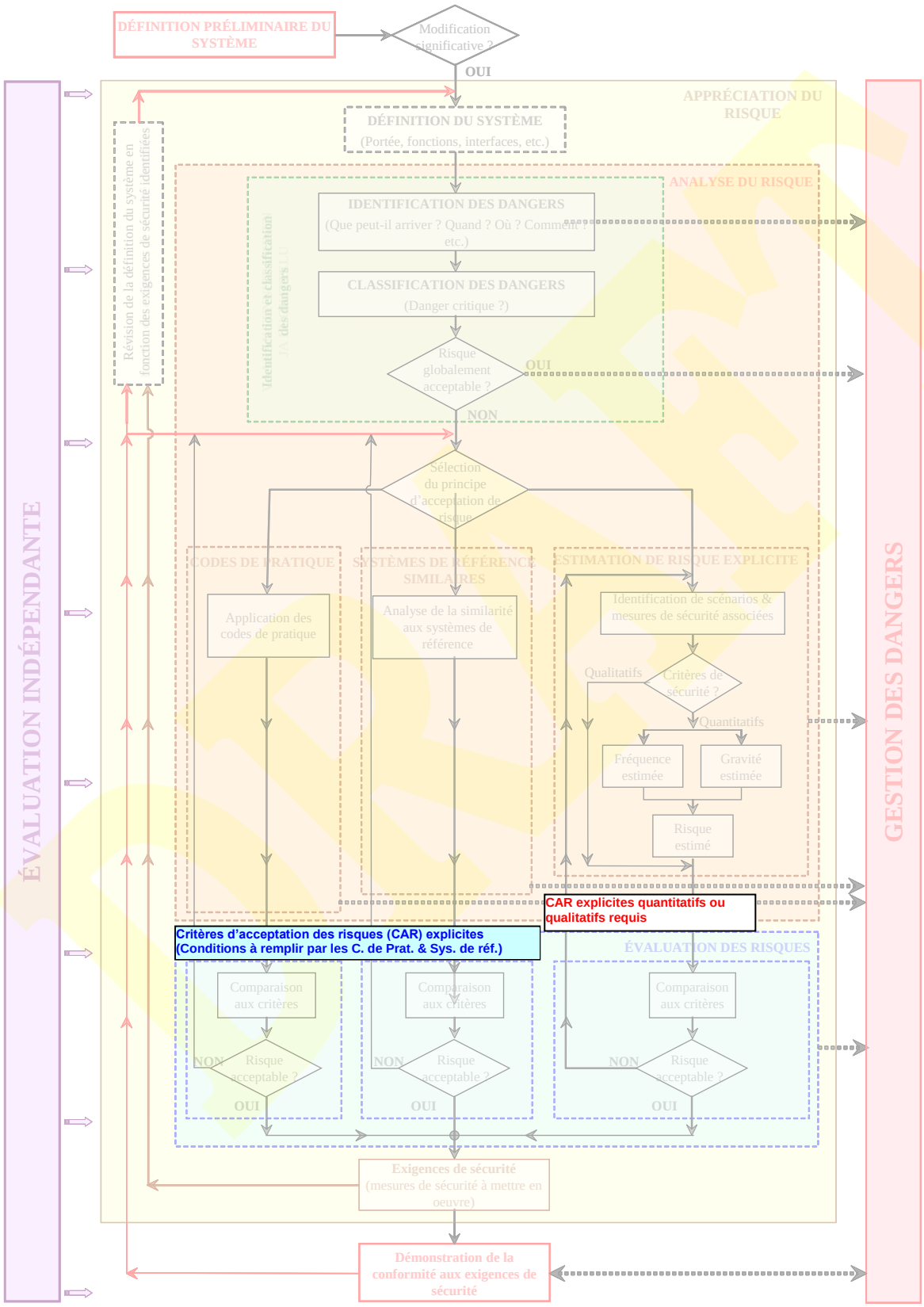
(a) de convenir des principes généraux du système, des fonctionnalités du système, etc. En principe, ceci pourrait être décrit dans une définition préliminaire du système;
(b) de définir l'organisation du projet;
(c) de se mettre d'accord sur le partage des rôles et des responsabilités entre les différents acteurs déjà impliqués, y compris l'ANS, l'ONE et l'ISA dans les cas où cela est pertinent.

Une telle coordination, par exemple pendant la définition préliminaire du système, donne l'opportunité au proposant, aux sous-traitants, à l'ANS, à l'ONO et à l'ISA, si nécessaire, de

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

convenir à un stade précoce des codes de pratique ou des systèmes de référence dont l'utilisation est acceptable dans le cadre du projet.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu



Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Figure 1: Cadre de gestion des risques du règlement MSC {Ref. 3}.

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] Le système de gestion de la sécurité (SGS) de l'entreprise ferroviaire ou du gestionnaire d'infrastructure définit le processus et les procédures qui:

(a) vérifient que le système reste sûr pendant toute sa durée de vie (c'est-à-dire en phase d'exploitation et de maintenance);
(b) garantissent la sécurité du démantèlement ou du remplacement du système concerné.

Ce processus n'est pas couvert par la MSC relative à l'appréciation des risques.

[G 2] Pour mettre en œuvre la MSC, il est nécessaire que toutes les parties impliquées soient compétentes (c'est-à-dire qu'elles possèdent les compétences, les connaissances et l'expérience adéquates). Les acteurs du secteur ferroviaire ont un besoin constant de gestion des compétences:

(a) pour les entreprises ferroviaires et les gestionnaires d'infrastructure, ce point est couvert par leur système de gestion de la sécurité (SGS) selon l'annexe III, point 2, sous e), de la directive sur la sécurité ferroviaire {Ref. 1};
(b) pour les autres acteurs dont les activités sont susceptibles d'avoir un impact sur la sécurité du système ferroviaire, bien que le SGS ne soit pas obligatoire, ils possèdent au moins au niveau du projet (voir le point 5.1 de la section 5.1) un système de gestion de la qualité (SGQ) et/ou un processus de gestion de la sécurité (PGS) couvrant cette exigence.

[G 3] Les sections suivantes de la norme CENELEC EN 50 126-1 {Ref. 8} donnent des indications en matière de compétences:

(a) section § 5.3.5.(b): «*tout le personnel possédant des responsabilités dans le cadre du processus de gestion*» des risques doit être «*compétent pour assumer ses responsabilités*»;
(b) § 5.3.5.(d): les exigences de la gestion et de l'appréciation des risques doivent être «*mises en œuvre dans le cadre de processus métier soutenus par un système de gestion de la qualité (SGQ) conforme aux exigences EN ISO 9001, EN ISO 9002 ou EN ISO 9003 appropriées pour le système» évalué.* La section § 5.2 de la norme EN 50 129 {Ref. 7} donne un exemple des aspects contrôlés par le système de gestion de la qualité.

Ces compétences concernent les activités d'assurance qualité ainsi que les compétences et la formation des personnes / du personnel nécessaires pour prendre en charge le processus couvert par la MSC.

[G 4] Très souvent, le processus d'appréciation des risques est suivi par un organisme d'évaluation dès le début du projet. Toutefois, bien qu'elle soit recommandée, cette implication précoce de l'organisme d'évaluation n'est pas obligatoire sauf si la législation nationale d'un État membre l'exige. L'opinion de l'organisme d'évaluation indépendant peut être utile avant de passer d'une phase à l'autre dans l'appréciation des risques. Voir l'Article 6 pour de plus amples détails concernant l'évaluation indépendante.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● 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] Aucune explication supplémentaire n'est considérée nécessaire.

1.1.4.	*The actors who already have in place methods or tools for risk assessment may continue to apply them as far as they are compatible with the provisions of this Regulation and subject to the following conditions:* *(a) the risk assessment methods or tools are described in a safety management system which has been accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC, or;* *(b) the risk assessment methods or tools are required by a TSI or comply with publicly available recognised standards specified in notified national rules.*

[G 1] La Figure 2 illustre la relation entre la MSC et les «systèmes de gestion de la sécurité et processus d'appréciation des risques».

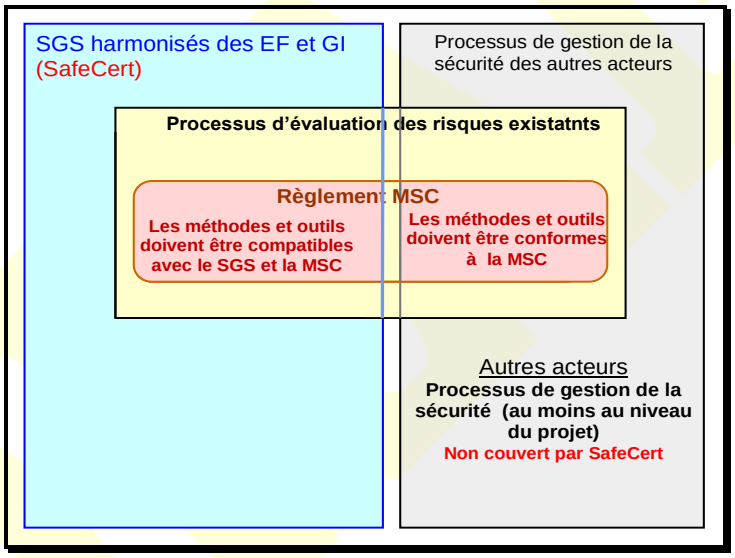


Figure 2: MSC et SGS harmonisés.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

[G 1] Si le proposant est un gestionnaire d'infrastructure ou une entreprise ferroviaire, il peut parfois être nécessaire d'impliquer d'autres acteurs dans le processus[8] (voir section 1.2.1).

Dans certains cas, le gestionnaire d'infrastructure ou l'entreprise ferroviaire peut sous-traiter partiellement ou entièrement les activités d'appréciation des risques. Les rôles et responsabilités de chaque acteur sont habituellement convenus entre les acteurs concernés à un stade précoce du projet.

[G 2] Il est important de noter que le proposant reste toujours responsable de l'application de la MSC pour l'acceptation du risque et donc pour la sécurité du système. Ceci inclut de veiller:

(a) à ce qu'il y ait une pleine coopération entre les acteurs impliqués afin de fournir toutes les informations nécessaires, et
(b) à déterminer clairement qui doit mettre en œuvre une exigence MSC particulière (par exemple la réalisation de l'analyse des risques ou la gestion du registre des dangers).

En cas de désaccord entre les acteurs concernant les exigences de sécurité à respecter, il est possible de demander l'avis de l'ANS. Mais le proposant reste responsable de trouver une solution, et ne peut transférer cette responsabilité à l'ANS: voir également la section 0.2.2.

[G 3] Si la tâche est sous-traitée, le sous-traitant n'est pas tenu de posséder sa propre organisation de sécurité s'il n'est pas un gestionnaire d'infrastructure ou une entreprise ferroviaire, ou surtout si la structure/taille du sous-traitant est réduite ou si sa contribution au système global est limitée. L'organisation de plus haut niveau (le client du sous-traitant) peut rester responsable de la responsabilité de la gestion des risques, y compris les activités d'appréciation des risques et de gestion des dangers. Cependant, le sous-traitant est toujours tenu de fournir les informations correctes concernant ses activités dont l'organisation de plus haut niveau a besoin pour élaborer sa documentation de gestion des risques.
Les organisations collaboratrices peuvent également décider de créer une organisation de sécurité commune, par exemple afin d'optimaliser les coûts. Dans un tel cas, une seule organisation gèrera les activités de sécurité de toutes les organisations impliquées. L'exactitude des informations (dangers, risques et mesures de sécurité) et la mise en œuvre des mesures de sécurité restent sous la responsabilité de l'organisation chargée de contrôler les dangers auxquels sont associées ces mesures de sécurité.

[G 4] Le proposant définit normalement les «niveaux de sécurité» et les «exigences de sécurité» attribués aux acteurs impliqués dans le projet et aux différents sous-systèmes et équipements de ces acteurs:

(a) dans les contrats passés entre le proposant et les acteurs concernés (sous-traitants);

(8) *Ceci est conforme à l'appendice A.4 de la norme CENELEC 50 129 {Ref. 7}.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) dans un plan de sécurité ou tout autre document pertinent répondant au même objectif, avec la description de l'organisation globale du projet et des responsabilités de chaque acteur, y compris celles du proposant: voir la section 1.1.6;
(c) dans le(s) registre(s) des dangers du proposant: voir la section 4.1.1.

Cette attribution de «niveaux de sécurité» et d'«exigences de sécurité» aux sous-systèmes et aux équipements sous-jacents, et donc aux acteurs concernés y compris le proposant lui-même, peut être mise au point / étendue durant la «phase de démonstration de la conformité du système aux exigences de sécurité»: voir la Figure 1. Par comparaison au cycle en V CENELEC (voir section 2.1.1 et Figure 5 en page 36), cette activité correspond à la phase 5 relative à la «définition des exigences systèmes» jusqu'aux différents sous-systèmes et composants.

[G 5] L'Article 5 (2) permet à d'autres acteurs que l'EF et le GI d'assumer la responsabilité globale de la conformité avec la MSC selon leurs besoins respectifs. Pour des produits ou des applications génériques[9] par exemple, le fabricant peut effectuer l'appréciation des risques sur la base d'une «définition générique du système» afin de préciser les niveaux de sécurité et les exigences de sécurité à respecter par les produits et les applications génériques.

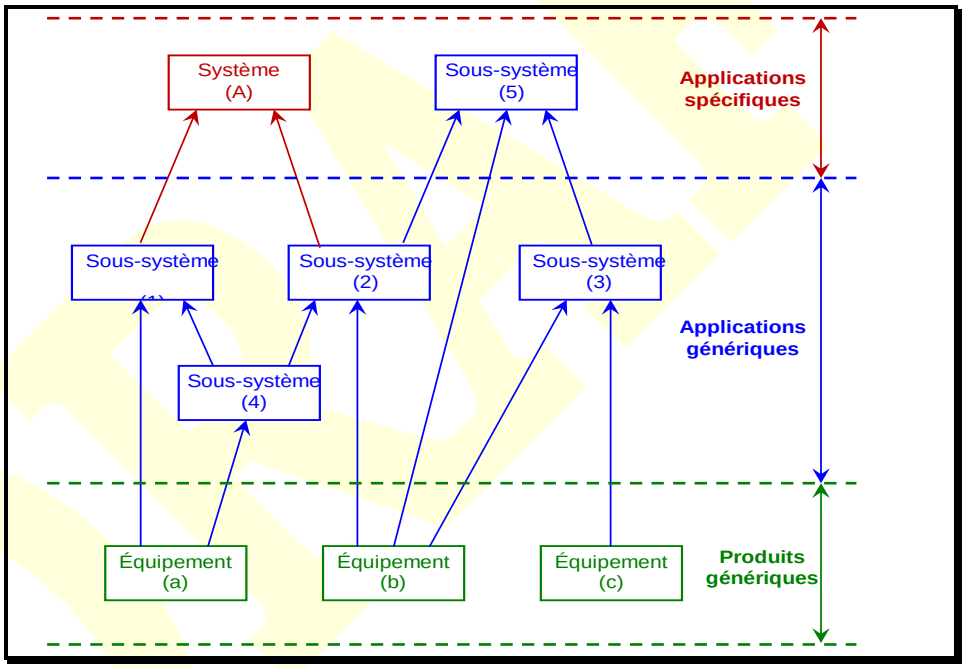


Figure 3: Exemples de dépendances entre cas de sécurité (issu de la figure 9 de la norme EN 50 129).

[G 6] CENELEC recommande que le fabricant fournisse une preuve documentaire de l'appréciation des risques des cas de sécurité des produits génériques (ou applications

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

génériques[9]) et des registres de dangers. Ces cas de sécurité et registres de dangers contiennent toutes les hypothèses[10] et les «restrictions d'utilisation» identifiées (c'est-à-dire les conditions d'application liées à la sécurité) applicables aux produits ou applications génériques concernés. Par conséquent, lorsqu'un produit générique et une application générique sont utilisés en opération dans une application spécifique, il convient de démontrer la conformité à toutes ces hypothèses[9] et «restrictions d'utilisation» (ou conditions d'application liées à la sécurité) dans chaque application spécifique.

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] Très souvent, sauf en cas d'accord contractuel contraire en début de projet, chaque projet possède un document décrivant les activités de gestion des risques. Le document pertinent

---

(9) *La terminologie «application générique» et «dossiers de sécurité des produits génériques» est reprise de CENELEC, où trois catégories différentes de dossiers de sécurité peuvent être envisagés (voir Figure 3: Exemples de dépendances entre cas de sécurité (issu de la figure 9 de la norme EN 50 129).:*

(a) ***Dossier de sécurité de produit générique*** *(indépendant de l'application). Un produit générique peut être utilisé pour différentes applications indépendantes;*

(b) ***Dossier de sécurité d'application générique*** *(pour une classe d'applications). Une application générique peut être réutilisée pour une classe / un type d'application présentant des fonctions communes;*

(c) ***Dossier de sécurité d'application spécifique*** *(pour une application spécifique). Une application spécifique est utilisée uniquement pour une installation particulière.*

Pour plus d'informations sur leur interdépendance, voir la section § 9.4 et la figure 9.1 de la ligne directrice CENELEC 50 126-2 {Ref. 9}

(10) *Ces hypothèses et restrictions d'utilisation déterminent les limites et la validité des «évaluations de sécurité» et des «analyses de sécurité» associées aux dossiers de sécurité de produits et d'applications génériques associés. Si l'application spécifique envisagée ne les respecte pas, il est nécessaire de mettre à jour ou de remplacer les «évaluations de sécurité» et les «analyses de sécurité» correspondantes (par ex. les analyses causales) par de nouvelles.*

> *Ceci est conforme au principe de sécurité général suivant: «Lorsque la conception d'un (sous-)système spécifique se base sur des applications génériques et des produits génériques, il convient de démontrer que le (sous-)système spécifique respecte toutes les hypothèses et les restrictions d'utilisation (appelées conditions d'applications liées à la sécurité dans CENELEC) exportées vers les dossiers de sécurité d'application et de produit génériques correspondants (voir Figure 3: Exemples de dépendances entre cas de sécurité (issu de la figure 9 de la norme EN 50 129).)»*

Si, pour une application spécifique, la conformité avec certaines hypothèses et restrictions d'utilisation ne peut être atteinte au niveau du sous-système (par ex. dans le cas d'exigences de sécurité opérationnelles), les hypothèses et restrictions d'utilisation correspondantes peuvent être transférées à un niveau supérieur (c'est-à-dire généralement au niveau du système). Ces hypothèses et restrictions d'utilisation sont alors clairement identifiées dans le «dossier de sécurité d'application spécifique» du sous-système concerné. Ceci est essentiel pour garantir, dans ces cas de dépendance, que les conditions d'application liées à la sécurité de chaque dossier de sécurité sont respectées dans le dossier de sécurité de niveau supérieur, ou qu'elles sont transférées aux conditions d'application liées à la sécurité du dossier de sécurité de plus haut niveau (dossier de sécurité système).

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

est tenu à jour et révisé chaque fois que des changements significatifs sont apportés au système original.

[G 2] Un tel document décrit la structure organisationnelle, les responsabilités du personnel, les processus, procédures et activités qui, ensemble, garantissent que le système évalué respecte les exigences de sécurité et les niveaux de sécurité spécifiés. Ce document doit être conforme à la MSC dans la mesure où il aide et guide le travail de l'organisme d'évaluation. Les normes CENELEC recommandent d'inclure ces informations dans un plan de sécurité ou dans un document dédié en partie à ces sujets.

[G 3] Le plan de sécurité du proposant en particulier, ou tout autre document pertinent, présente l'organisation globale du projet. Il décrit le partage des rôles et responsabilités entre les différents acteurs impliqués. Pour des informations détaillées, on peut se référer aux plans de sécurité ou aux organisations de sécurité des différents acteurs impliqués. Généralement, le partage des responsabilités entre les différents acteurs est abordé et convenu pendant la phase de définition préliminaire du système (c'est-à-dire en début de projet), s'il y en a une.

[G 4] Le plan de sécurité est un document vivant mis à jour chaque fois que nécessaire pendant la durée de vie du projet.

[G 5] On trouvera plus de détails concernant le contrôle du plan de sécurité dans la norme EN 50 126-1 {Ref. 8} et sa ligne directrice correspondante 50 126-2 {Ref. 9}.

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] Aucune explication supplémentaire n'est considérée nécessaire.

1.2. Gestion des 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] Par exemple si, pour des raisons opérationnelles, une entreprise ferroviaire a besoin qu'un gestionnaire d'infrastructure apporte des changement bien définis à l'infrastructure, en vertu des exigences de l'annexe III, point 2, sous g, de la directive sur la sécurité ferroviaire {Ref. 1}, l'EF contrôle également l'ensemble du travail afin de garantir la réalisation correcte des changements attendus. Cependant, la direction de l'EF n'enlève pas au GI sa responsabilité d'informer les autres entreprises ferroviaires si celles-ci sont également concernées par la modification prévue de l'infrastructure. Le GI peut même avoir à effectuer une appréciation des risques conformément à la MSC si le changement est significatif de son point de vue

[G 2] Des transferts de responsabilités entre les différents acteurs sont possibles et même, dans certaines circonstances, nécessaires. Cependant, lorsque plusieurs acteurs sont impliqués dans un système, l'un d'entre eux est souvent désigné comme le responsable de l'ensemble du système. Il existe toujours des dépendances entre les sous-systèmes et les opérations qui nécessitent des efforts d'identification particuliers. Il est donc nécessaire que quelqu'un

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

assume la responsabilité globale des analyses de sécurité et bénéficie d'un accès complet à toute la documentation pertinente. Bien entendu, le proposant qui souhaite introduire le changement significatif est généralement responsable de veiller à ce que l'appréciation des risques soit systématique et complète.

[G 3] Les principaux critères à définir pour la gestion d'une interface entre les acteurs concernés sont:

(a) la direction, généralement assurée par le proposant qui souhaite introduire le changement significatif;
(b) les données d'entrée nécessaires;
(c) les méthodes d'identification des dangers et d'appréciation des risques;
(d) les participants requis avec les compétences nécessaires (combinaison de connaissances, de techniques et d'expérience pratique – voir également la définition de la «compétence du personnel» au point [G2](b) de l'article 3 du document {Ref. 4});
(e) les sorties attendues.

Ces critères sont décrits dans les plans de sécurité (ou d'autres documents pertinents) des sociétés impliquées dans les interfaces concernées.

[G 4] La section C.3 de l'appendice C donne des exemples d'interfaces ainsi qu'un exemple de l'application de ces principaux critères pour la gestion de l'interface entre un fabricant de trains et un gestionnaire d'infrastructure ou une entreprise ferroviaire

[G 5] La gestion des interfaces doit également tenir compte, pour la conception de ces interfaces, des risques qui peuvent se présenter aux interfaces avec des opérateurs humains (utilisés durant l'exploitation et la maintenance).

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] Le processus de transfert des dangers et des mesures de sécurité correspondantes entre les différents acteurs est également applicable aux niveaux inférieurs du cycle en V CENELEC illustré à la Figure 5 de la page 36. Il peut être appliqué, par exemple, chaque fois qu'il est nécessaire d'échanger de telles informations entre un acteur et ses sous-traitants. La différence par rapport à ce même processus au niveau du système est que le proposant n'est pas tenu d'être informé de tous les transferts de dangers et de mesures de sécurité associées au niveau des sous-systèmes. Le proposant est informé uniquement lorsque les dangers et les mesures de sécurité associées transférées sont liés aux interfaces de haut niveau (c'est-à-dire lorsqu'il y a un impact sur une interface avec le proposant).

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] Le système de gestion de la sécurité (SGS) de l'EF et du GI couvre les dispositions et procédures destinées à assurer une gestion correcte des non-conformités ou des inadéquations des mesures de sécurité. Ces dispositions et procédures ne font donc pas partie de la MSC.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] De même, les dispositions et procédures(11) devant être mises en place par d'autres acteurs(12) afin d'assurer une gestion correcte des non-conformités ou des inadéquations des mesures de sécurité et, si nécessaire, le transfert des mesures de sécurité vers tous les acteurs concernés, sont convenues entre les acteurs concernés au début du projet et décrites en détail dans leur plan de sécurité: voir la section 0.2.

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

[G 1] Ceci permettra donc de gérer la non-conformité ou l'inadéquation de la mesure de sécurité au sein du système évalué ou d'autres systèmes semblables utilisant la même mesure.

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] Aucune explication supplémentaire n'est considérée nécessaire.

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] Aucune explication supplémentaire n'est considérée nécessaire.

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] Aucune explication supplémentaire n'est considérée nécessaire.

(11) *En principe, ces dispositions et procédures sont couvertes par le processus de gestion de la qualité et/ou de la sécurité de ces acteurs tels qu'ils sont définis au moins au niveau du projet (voir également la Figure 2: MSC et SGS harmonisés.).*

(12) *Le terme «autres acteurs» désigne tous les acteurs concernés autres que les EF et GI.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2. DESCRIPTION DU PROCESSUS D'APPRÉCIATION DES RISQUES

2.1. Description générale – correspondance entre le processus d'appréciation des risques MSC et le cycle en 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.

[G 1] Le processus de gestion des risques couvert par la MSC peut être représenté sous la forme d'un cycle en V commençant par la définition (préliminaire) du système et se terminant par la réception du système: voir Figure 4. Ce cycle en V simplifié peut être mis en relation avec le cycle en V classique de la figure 10 de la norme EN 50 126-1 {Ref. 8}. Afin de montrer la correspondance avec le processus de gestion des risques MSC à la Figure 1, le cycle en V CENELEC de la figure 10 est reproduit à la Figure 5:

(a) la «définition préliminaire du système» de la MSC à la Figure 1 correspond à la phase 1 du cycle en V CENELEC, c'est-à-dire à la définition du « concept » du système (voir CADRE 1 à la Figure 5);
(b) l'«appréciation des risques» de la MSC à la Figure 1 inclut les phases suivantes du cycle en V CENELEC (voir CADRE 2 à la Figure 5):
    (1) Phase 2 de la Figure 5: «définition du système et conditions d'application»;
    (2) Phase 3 de la Figure 5: «analyse des risques»;
    (3) Phase 4 de la Figure 5: «exigences système»;
    (4) Phase 5 de la Figure 5: «attribution des exigences système» jusqu'aux différents sous-systèmes et composants.

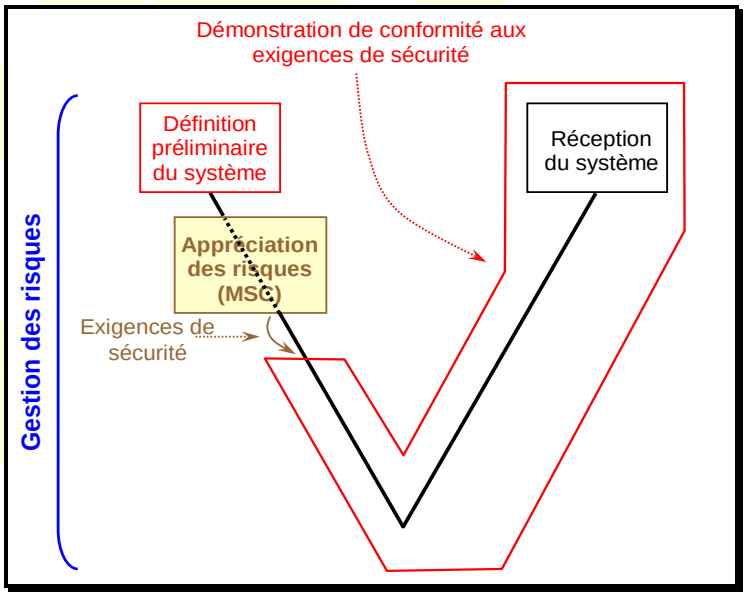


Figure 4: Cycle en V simplifié de la figure 10 de la norme EN 50 126.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

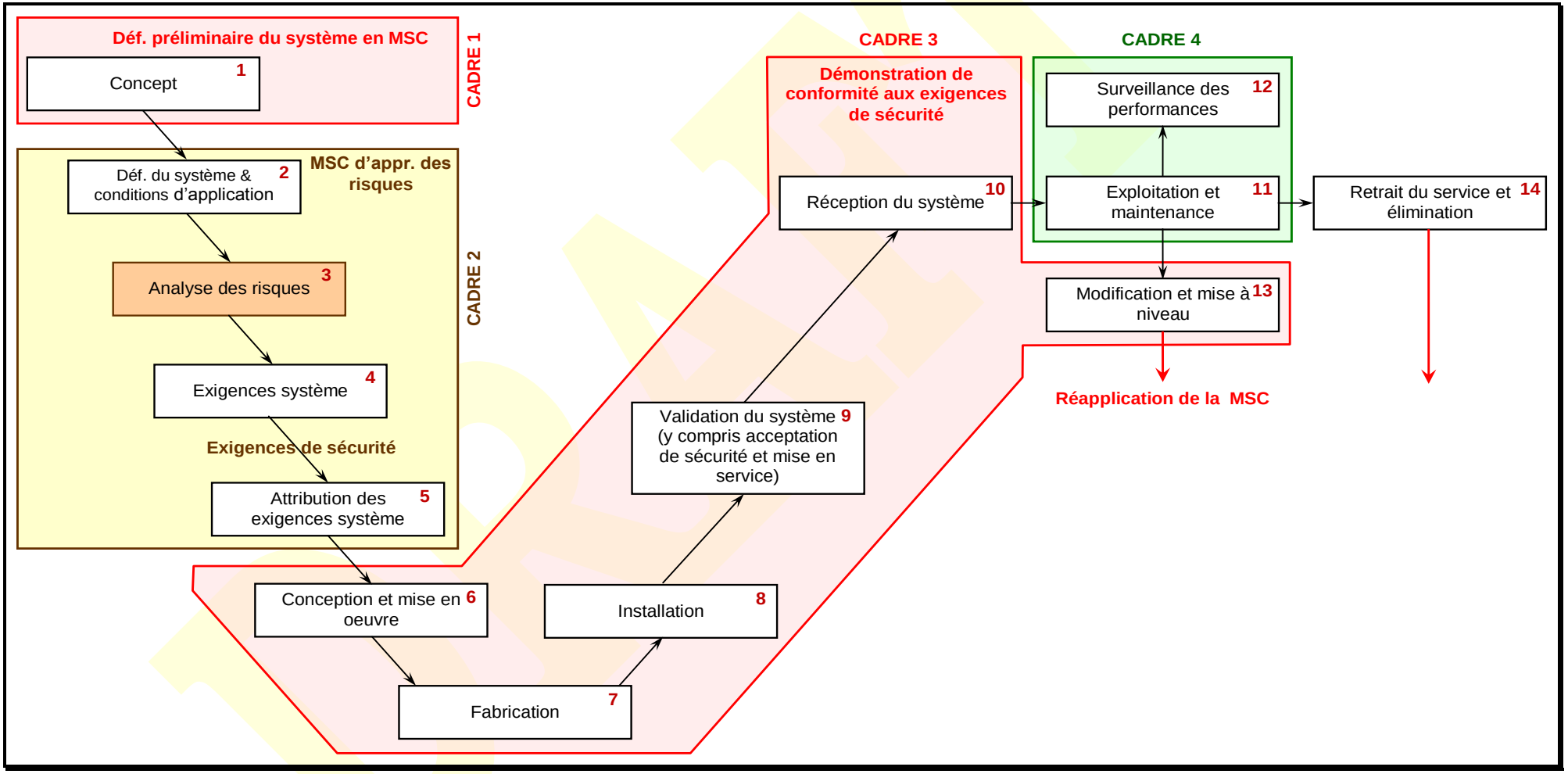


Figure 5: Figure 10 du cycle en V de la norme EN 50 126 (cycle de vie CENELEC du système)

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 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] Les sorties du processus d'appréciation des risques dans la MSC sont les suivantes (après itérations – voir Figure 1):

(a) la «définition du système» mise à jour via les «exigences de sécurité» issues des activités d'«analyse des risques» et d'«évaluation des risques» (voir section 2.1.6);
(b) l'«attribution des exigences système» jusqu'aux différents sous-systèmes et composants (phase 5 de la Figure 5);
(c) le «registre des dangers», qui documente:

(1) tous les dangers identifiés et les mesures de sécurité associées;
(2) les exigences de sécurité qui en découlent;
(3) les hypothèses prises en compte pour le système évalué qui déterminent les limites et la validité de l'appréciation des risques (voir le point (g) de la section 2.1.2);

(d) et de façon générale, toutes les preuves issues de l'application de la MSC: voir la section 5;

Les sorties de l'appréciation des risques de la MSC correspondent aux sorties liées à la sécurité de la phase 4 du cycle en V CENELEC, c'est-à-dire à la spécification des exigences système à la Figure 5.

[G 3] La définition du système mise à jour sur la base des résultats de l'appréciation des risques ainsi que le registre des dangers constituent les entrées sur la base desquelles le système est conçu et réceptionné. La «démonstration de la conformité du système aux exigences de sécurité» de la MSC correspond aux phases suivantes du cycle en V CENELEC (voir CADRE 3 de la Figure 5):

(a) Phase 6 de la Figure 5: «conception et mise en œuvre»;
(b) Phase 7 de la Figure 5: «fabrication»;
(c) Phase 8 de la Figure 5: «installation»;
(d) Phase 9 de la Figure 5: «validation du système (y compris l'acceptation de sécurité et la mise en service)»;
(e) Phase 10 de la Figure 5: «réception du système».

[G 4] La démonstration de la conformité du système aux exigences de sécurité dépend de la nature technique, opérationnelle ou organisationnelle du changement significatif. Par conséquent, les différentes étapes du cycle en V CENELEC illustré à la Figure 5 ne s'appliquent pas nécessairement à tous les types de changements significatifs. Le cycle en V de la Figure 5 doit être considéré en conséquence et utilisé en tenant compte de ce qui correspond à chaque application spécifique (par exemple, pas de phase de fabrication pour les changements opérationnels et organisationnels).

[G 5] Cela signifie que la «démonstration de la conformité du système aux exigences de sécurité» de la MSC ne comprend pas uniquement les activités de «vérification et de validation» au moyen de tests et de simulations. En pratique, elle couvre l'ensemble des phases «6 à 10» (voir la liste ci-dessus et la Figure 5) du cycle en V CENELEC. Ces phases couvrent les activités de conception, de fabrication, d'installation, de vérification et de validation ainsi que les activités RAMS associées et la réception du système.

[G 6] Durant la «démonstration de la conformité du système aux exigences de sécurité», le principe général est de focaliser l'appréciation des risques uniquement sur les fonctions et interfaces du système ayant une incidence sur la sécurité. Cela signifie que lorsque l'une des phases du cycle en V CENELEC de la Figure 5 nécessite des activités d'appréciation des risques et de la sécurité, celles-ci se focalisent sur:

(a) les fonctions et interfaces ayant une incidence sur la sécurité;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) les sous-systèmes et/ou composants impliqués dans la réalisation des fonctions et/ou interfaces liées à la sécurité pendant les activités d'appréciation des risques de plus haut niveau.

[G 7] Il résulte donc de la comparaison avec le cycle en V CENELEC classique de la Figure 5 que:

(a) la MSC couvre les phases «1 à 10» et «13» de ce cycle en V. Celles-ci couvrent les activités requises pour la réception du système faisant l'objet de l'évaluation;

(b) la MSC ne couvre pas les phases «11», «12» et «14» du cycle de vie du système:

(1) les phases «11» et «12» concernent respectivement l'«exploitation et la maintenance» et la «surveillance des performances» du système après sa réception sur la base de la MSC. Ces deux phases sont couvertes par le système de gestion de la sécurité (SGS) de l'EF et du GI – (voir CADRE 4 de la Figure 5). Si toutefois, pendant l'exploitation, la maintenance ou la surveillance des performances du système, il apparaît nécessaire de modifier et de mettre à niveau le système (phase 13 de la Figure 5) alors qu'il est déjà en opération, la MSC est appliquée à nouveau aux nouveaux changements requis conformément à l'Article 2. Par conséquent, si le changement est significatif:

(i) les processus de gestion et d'appréciation des risques de la MSC sont appliqués à ces nouveaux changements;
(ii) une réception de ces nouveaux changements est requise conformément à l'Article 6:

(2) le «retrait du service et l'élimination» d'un système déjà en opération (phase 14) peuvent être considérés comme un changement significatif, et la MSC peut donc être appliquée à nouveau conformément à l'Article 2 pour la phase 14 de la Figure 5.

Pour de plus amples informations sur la portée de chaque phase ou activité du cycle en V CENELEC repris à la Figure 5, voir la section § 6 de la norme EN 50 126-1 {Ref. 8}.

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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] En général, le proposant décide quel principe d'acceptation des risques est le plus approprié pour maîtriser les dangers identifiés sur la base des exigences spécifiques du projet et de l'expérience du proposant avec ces trois principes.

[G 2] Il n'est pas toujours possible d'évaluer l'acceptabilité des risques au niveau du système en utilisant un seul des trois principes d'acceptation des risques. L'acceptation des risques se basera souvent sur une combinaison de ces principes. Si, pour un danger significatif, il est nécessaire d'appliquer plus d'un principe d'acceptation des risques afin de contrôler le risque associé, le danger concerné doit être divisé en sous-dangers afin que chaque sous-danger individuel puisse être maîtrisé adéquatement par un seul principe d'acceptation des risques.

[G 3] La décision de maîtriser un danger au moyen d'un principe d'acceptation des risques doit tenir compte du danger et des causes du danger déjà identifiées lors de la phase d'identification des dangers. Ainsi, si deux causes différentes et indépendantes sont associées au même danger, celui-ci doit être divisé en deux sous-dangers différents. Chaque sous-danger est ensuite maîtrisé au moyen d'un seul principe d'acceptation des risques. Les deux sous-dangers doivent être enregistrés et gérés dans le registre des dangers. Si par exemple le danger est provoqué par une erreur de conception, il peut être géré par l'application d'un code de pratique. Si par contre la cause du danger est une erreur de maintenance, le code de pratique seul peut ne pas suffire; l'application d'un autre principe d'acceptation des risques est alors nécessaire.

[G 4] La réduction des risques à un niveau acceptable peut nécessiter plusieurs itérations entre les phases d'analyse et d'évaluation des risques jusqu'à ce que des mesures de sécurité adéquates aient été identifiées.

[G 5] Le risque résiduel présent sur la base de l'expérience sur le terrain pour les systèmes existants et pour les systèmes basés sur l'application de codes de pratique est considéré comme acceptable. Le risque résultant de l'estimation des risques explicites se base sur un avis d'experts et sur différentes hypothèses faites par l'expert pendant l'analyse, ou sur des bases de données liées aux expériences des accidents ou de l'exploitation. Par conséquent, le risque résiduel issu de l'estimation des risques explicites ne peut pas être confirmé immédiatement par le retour du terrain. Une telle démonstration nécessite du temps pour l'exploitation, le contrôle et l'obtention d'expériences de terrain représentatives pour le(s) système(s) concerné(s). En général, l'application de codes de pratique et la comparaison avec des systèmes de référence similaires présentent l'avantage d'éviter la surspécification d'exigences de sécurité inutilement strictes qui peuvent résulter d'hypothèses (de sécurité) excessivement prudentes dans l'estimation des risques explicites. Cependant, il peut arriver que certaines exigences de sécurité dérivées des codes de pratique ou des systèmes de référence similaires ne soient pas tenues d'être respectées pour le système faisant l'objet de l'évaluation. Dans ce cas, l'application d'une estimation des risques explicites aurait

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

l'avantage d'éviter une surconception inutile du système évalué et de permettre une conception plus économique jamais essayée auparavant.

[G 6] Si les dangers identifiés et les risques associés du système évalué ne peuvent pas être maîtrisés par l'application de codes de pratique ou de systèmes de référence similaires, une estimation des risques explicites est effectuée sur la base d'analyses quantitatives ou qualitatives d'événements dangereux. Cette situation se présente lorsque le système évalué est entièrement nouveau (ou présente une conception innovante) ou lorsqu'il y a des déviations par rapport à un code de pratique ou à un système de référence. L'estimation des risques explicites détermine alors si le risque est acceptable (c'est-à-dire si une analyse plus approfondie est inutile) ou si des mesures de sécurité supplémentaires sont nécessaires pour continuer à réduire le risque.

[G 7] La section § 8 de la ligne directrice EN 50 126-2 {Ref. 9} fournit également des recommandations en matière de réduction et d'acceptation des risques.

[G 8] Le principe d'acceptation des risques utilisé et son application doivent être évalués par l'organisme d'évaluation.

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] Par exemple, si l'application du processus de développement SIL 4 de la norme EN 50 128 est définie comme une exigence de sécurité pour le logiciel d'un composant, la démonstration devra prouver que le processus recommandé par la norme a bien été respecté. Ceci implique par exemple de démontrer que:

(a) les exigences en matière d'indépendance dans l'organisation de la conception, de la vérification et de la validation du logiciel ont été respectées;
(b) les méthodes correctes de la norme EN 50 128 pour le niveau d'intégrité de sécurité SIL 4 ont été appliquée;
(c) etc.

[G 2] Par exemple, si un code de pratique dédié doit être utilisé pour la fabrication de soupapes électriques pour frein d'urgence, la démonstration devra prouver que le processus de fabrication respecte toutes les exigences du code de sécurité.

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

[G 1] On peut distinguer deux types de mesures de sécurité:

(a) les «mesures de sécurité préventives» préviennent la survenance des dangers ou de leurs causes;
(b) les «mesures de sécurité atténuantes» évitent que les dangers ne se transforment en accidents, ou réduisent les conséquences des accidents qui se produisent (mesures de protection).

Pour l'exploitabilité, la prévention des causes est généralement plus efficace.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Le proposant considèrera comme les plus appropriées les mesures de sécurité qui permettent le meilleur compromis possible entre le coût lié à la réduction des risques et le niveau de risque résiduel. Les mesures de sécurité choisies deviennent les exigences de sécurité du système évalué.

[G 3] Il est important de vérifier que les mesures de sécurité sélectionnées pour maîtriser un danger ne sont pas en conflit avec d'autres dangers. Comme l'illustre la Figure 6, les deux cas suivants peuvent par exemple se présenter[13]:

(a) CAS 1: si la même mesure de sécurité (mesure A de la Figure 6) peut maîtriser différents dangers sans créer de conflits entre eux, et si cela se justifie du point de vue économique, la mesure de sécurité concernée peut être choisie seule comme l'«exigence de sécurité» associée. Le nombre total d'exigences de sécurité à respecter est plus petit que la mise en œuvre des mesures B et C;

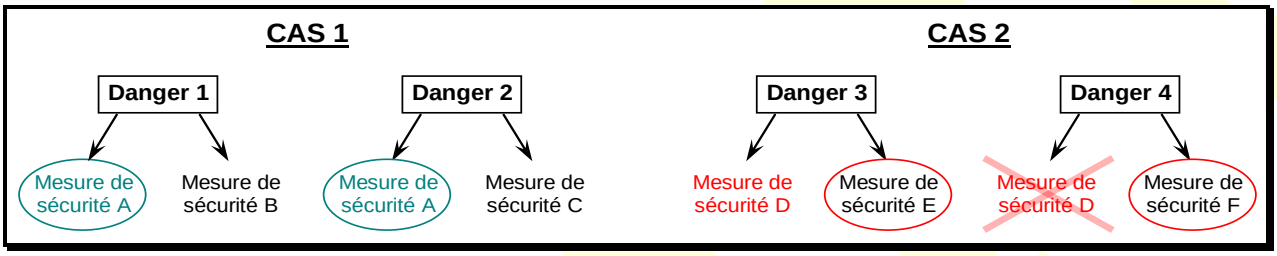


Figure 6: Sélection des mesures de sécurité adéquates pour maîtriser les risques.

(b) CAS 2: réciproquement, si une seule mesure de sécurité peut maîtriser un danger mais qu'elle crée un conflit avec un autre danger (mesure D sur la Figure 6), elle ne peut pas être choisie comme «exigence de sécurité». Les autres mesures de sécurité pour le danger envisagé doivent être utilisées (mesures E et F de la Figure 6):

(1) Un exemple typique dans le cadre du système de contrôle-commande est l'utilisation de l'emplacement du train sur la voie pour contrôler l'utilisation du frein ou pour autoriser l'accélération du train. L'utilisation de la partie avant (ou arrière) du train pour déterminer l'emplacement du train n'est pas sûre dans toutes les situations:

(i) lorsque le système ce contrôle-commande ETCS doit appliquer de façon sûre le frein d'urgence, il utilise la position sûre maximale de la partie avant (MAXIMUM SAFE FRONT END) afin de permettre au train de s'arrêter avant d'atteindre le point de danger;

(ii) réciproquement, quand le train est autorisé à accélérer après une limitation de vitesse par exemple, le système de contrôle-commande ETCS utilise la position sûre minimale de la partie arrière (MINIMUM SAFE REAR END);

(2) Un autre exemple est celui d'une mesure de sécurité qui pourrait être valide pour arrêter un train dans la plupart des circonstances, mais pas dans un tunnel ni sur un pont. Dans ce dernier cas, la mesure D du CAS 2 de la Figure 6 ne peut pas être prise.

(13) *Il convient de remarquer que le guide n'énumère pas toutes les situations dans lesquelles des mesures de sécurité peuvent entrer en conflit avec d'autres dangers identifiés. Seuls quelques exemples illustratifs sont fournis.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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] En fonction par exemple des choix techniques ayant présidé à la conception d'un système, de ses sous-systèmes et de ses équipements, de nouveaux dangers peuvent être identifiés pendant la «démonstration de conformité aux exigences de sécurité» (par ex., l'utilisation de certaines peintures pourrait provoquer des fumées toxiques en cas d'incendie). Ces nouveaux dangers ainsi que les risques associés doivent être considérés comme de nouveaux éléments pour une nouvelle boucle du processus itératif d'appréciation des risques. L'appendice A.4.3 de la norme EN 50 129 fournit d'autres exemples de cas où de nouveaux dangers sont susceptibles d'être introduits et doivent être maîtrisés.

2.2. Identification des dangers

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] Dans la mesure du possible, les dangers sont exprimés au même niveau de détail. Lors des analyses de danger préliminaires, il peut arriver que des dangers présentant différents niveaux de détail soient identifiés (par exemples, parce que l'HAZOP implique des personnes possédant des expériences différentes).
Le niveau de détail dépend également du principe d'acceptation des risques sélectionné pour maîtriser les dangers identifiés. Par exemple, si un danger est maîtrisé complètement par un code de pratique ou par un système de référence similaire, une identification plus détaillée des dangers ne sera pas nécessaire.

[G 2] Tous les dangers identifiés au cours du processus d'appréciation des risques (y compris ceux associés à des risques largement acceptables), les mesures de sécurité associées et les risques associés doivent être portés au registre des dangers.

[G 3] Selon la nature du système à analyser, différentes méthodes peuvent être utilisées pour l'identification des dangers:

(a) une identification empirique des dangers peut être utilisée, exploitant l'expérience passée (par ex. utilisation de listes de contrôle ou de listes génériques de dangers);
(b) une identification créative des dangers peut être utilisée pour les nouveaux domaines de préoccupation (prévision proactive, par ex. des études "WHAT-IF" structurées telles que FMEA ou HAZOP).

[G 4] Les méthodes empiriques et créatives d'identification des dangers peuvent être utilisées à titre complémentaire afin de garantir une liste complète de dangers potentiels et de mesures de sécurité.

[G 5] À titre préliminaire, l'identification des dangers pourrait commencer par une équipe de réflexion comprenant des experts possédant différentes compétences et couvrant tous les aspects pertinents du changement significatif. Lorsque le panel d'experts le juge nécessaire, il est possible d'utiliser des méthodes empiriques pour analyser une fonction ou un mode opérationnel spécifiques.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 6] Les méthodes utilisées pour l'identification des dangers dépend de la définition du système. L'appendice B en fournit quelques exemples.

[G 7] Les annexes A.2 & E de la ligne directrice EN 50 126-2 {Ref. 9} fournit de plus amples informations sur les techniques et méthodes d'identification des dangers.

[G 8] La section C.17 de l'appendice C donne un exemple d'une liste générique de dangers.

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

[G 1] Afin de contribuer au processus d'appréciation des risques, les dangers significatifs peuvent être regroupés dans différentes catégories. Par exemple, les dangers significatifs peuvent être classés ou ordonnés en fonction de leur gravité de risque attendue ou de leur fréquence de survenance. Les normes CENELEC donnent des lignes directrices pour cet exercice: voir la section A3 de l'appendice A.

[G 2] L'évaluation et l'analyse des risques décrites à la section 2.1.4 sont appliquées selon un ordre de priorité, en commençant par les dangers les plus importants.

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

[G 1] Par exemple, un risque associé à un danger peut être considéré comme largement acceptable:

(a) si le risque est inférieur à un certain pourcentage (par ex. x %) du risque maximum tolérable pour ce type de danger. La valeur de x % peut être basée sur les bonnes pratiques et sur l'expérience de plusieurs approches d'analyse des risques, par ex. le rapport entre les classifications des risques largement acceptables et les risques intolérables dans des courbes FN ou des matrices de risques. Ceci peut prendre la forme illustrée à la Figure 7;

(b) ou si le préjudice associé au risque est tellement minime qu'il n'est pas raisonnable de mettre en œuvre une mesure de sécurité pour le contrer.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

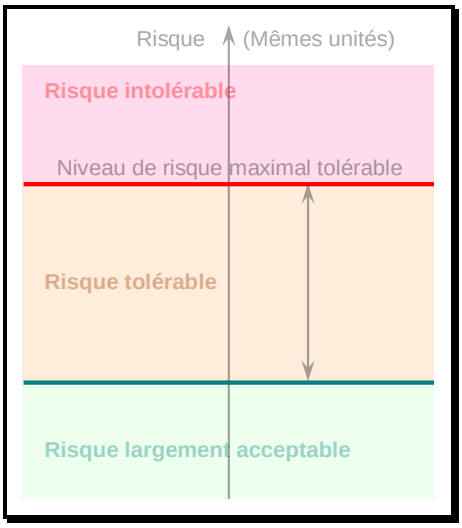


Figure 7: Risques largement acceptables

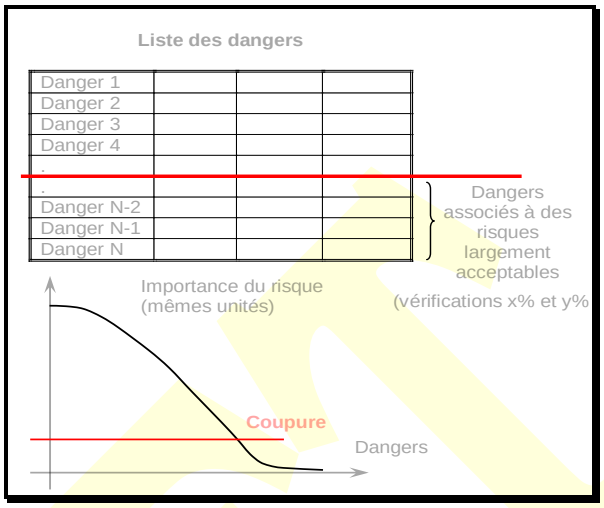


Figure 8: Filtrage des dangers associés à des risques largement acceptables.

[G 2] En outre, si des dangers sont identifiés avec différents niveaux de détail (des dangers de haut niveau d'un côté, des sous-dangers détaillés d'un autre côté), il convient de prendre des précautions pour éviter leur classification erronée en tant que dangers associés à des risques largement acceptables. La contribution de tous les dangers associés à des risques largement acceptables ne peut pas dépasser une certaine proportion (par ex. y %) du risque global au niveau du système. Cette vérification est nécessaire pour éviter de rendre la justification caduque en subdivisant les dangers en de nombreux sous-dangers de bas niveau. En effet, si un danger est exprimé sous la forme d'un grand nombre de sous-dangers «plus petits», chacun de ces sous-dangers peut facilement être classé comme étant associé à des risques largement acceptables s'il est évalué indépendamment, alors que ces sous-dangers évalués ensemble (en tant qu'un danger de haut niveau) sont associés à un risque significatif. La valeur de la proportion (par ex. y %) dépend des critères d'acceptation des risques applicables au niveau du système. Elle peut être estimée sur la base de l'expérience opérationnelle de systèmes de référence similaires.

[G 3] Les deux vérifications ci-dessus (par rapport à x % et y %) permettent de focaliser l'appréciation des risques sur les dangers les plus importants et de garantir la maîtrise de chaque risque significatif (voir Figure 8).
Sans préjudice des exigences légales en vigueur dans un État membre, le proposant est responsable de définir, sur la base d'un avis d'expert, les valeurs de x % et de y % et de les faire évaluer indépendamment par l'organisme d'évaluation. Un exemple d'ordre de grandeur peut être x = 1 % et y = 10 %, si l'avis d'expert considère ces valeurs comme acceptables.

[G 4] La section 2.2.2 exige que la classification en «risques largement acceptables» soit évaluée indépendamment par un organisme d'évaluation

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] L'objectif principal de cette activité est l'identification des dangers liés au changement. Si des mesures de sécurité ont déjà été identifiées, elles doivent être portées au registre des dangers. La nature de ces mesures dépend du changement; elles peuvent être de nature procédurale, technique, opérationnelle ou organisationnelle.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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] Même si un risque est maîtrisé à un niveau acceptable, le proposant peut encore décider qu'une identification plus détaillée des dangers est nécessaire. La raison peut en être, par exemple, qu'une identification plus détaillée des dangers est susceptible d'aboutir à des mesures de sécurité plus économiques pour la maîtrise des risques.

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] Aucune explication supplémentaire n'est considérée nécessaire.

2.3. Utilisation des codes de pratique et évaluation des risques

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] Aucune explication supplémentaire n'est considérée nécessaire.

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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] Aucune explication supplémentaire n'est considérée nécessaire.

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

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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] Aucune explication supplémentaire n'est considérée nécessaire.

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

2.4. Utilisation du système de référence et évaluation des risques

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] La section § 8 du guide EN 50 126-2 {Ref. 9} fournit de plus amples informations sur ces principes.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

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

[G 1] Par exemple, un ancien système de contrôle-commande dont l'utilisation a démontré le niveau de sécurité acceptable peut être remplacé par un autre système utilisant une technologie plus récente et offrant de meilleures performances de sécurité. Il convient donc, chaque fois que l'on applique un système de référence, de vérifier qu'il est toujours adéquat pour l'acceptation.

[G 2] Par exemple, étant donné que certains aspects de la sécurité des tunnels ou de la sécurité du transport de marchandises dangereuses peuvent être spécifiques et dépendre des conditions opérationnelles et environnementales, il est nécessaire de vérifier pour chaque projet que le système sera utilisé dans les mêmes conditions.

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

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

[G 1] La section § 8.1.3 du guide EN 50 1262 {Ref. 9} fournit de plus amples informations sur les analyses de similarité.

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] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

2.5. Estimation et appréciation des risques explicites

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] Aucune explication supplémentaire n'est considérée nécessaire.

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

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

[G 1] Afin d'évaluer si les risques du système évalué sont acceptables ou non, des critères d'acceptation des risques sont nécessaires (voir les cadres «évaluation des risques» à la Figure 1). Les critères d'acceptation des risques peuvent être implicites ou explicites:

(a) critères implicites d'acceptation des risques: selon les sections 2.3.5 et 2.4.3, les risques couverts par l'application des codes de pratique et par comparaison à des systèmes de référence sont considérés implicitement comme acceptables si, respectivement (voir le cercle en pointillé de la Figure 1):

(1) les conditions d'application des codes de pratique de la section 2.3.2 sont respectées;
(2) les conditions d'utilisation d'un système de référence de la section 2.4.2 sont respectées;

(b) critères explicites d'acceptation des risques: Afin d'évaluer si les risques maîtrisés par l'application de l'estimation des risques explicites sont acceptables ou non, des critères explicites d'acceptation des risques sont nécessaires (voir le cercle plein de la Figure 1 pour le troisième principe). Ceux-ci peuvent être définis à différents niveaux d'un système ferroviaire. Ils peuvent être considérés comme une « pyramide de critères » (voir Figure 9) partant des critères d'acceptation des risques de haut niveau (exprimés par exemple comme des risques sociétaux ou individuels) et descendant vers les sous-systèmes et composants (afin de couvrir les systèmes techniques) et comprenant les opérateurs humains pendant les activités d'exploitation et de maintenance du système et des sous-systèmes. Bien que les critères d'acceptation des risques contribuent à réaliser les performances de sécurité du système, et qu'ils soient donc liés aux OSC et NRV, il est très difficile d'élaborer un modèle mathématique entre eux: voir {Ref. 12} pour plus de détails à ce sujet.
Le niveau auquel sont définis les critères d'acceptation des risques doit correspondre à l'importance et à la complexité du changement significatif. Par exemple, il n'est pas nécessaire d'évaluer le risque global du système ferroviaire lorsque l'on modifie un type d'essieu sur le matériel roulant. La définition des critères d'acceptation des risques peut se focaliser sur la sécurité du matériel roulant. Réciproquement, des changements ou des ajouts importants apportés à un système ferroviaire important ne doivent pas être évalués uniquement sur la base des performances de sécurité des fonctions ou changements ajoutés. Il convient également de vérifier, au niveau du système ferroviaire, que le changement est acceptable dans son ensemble.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

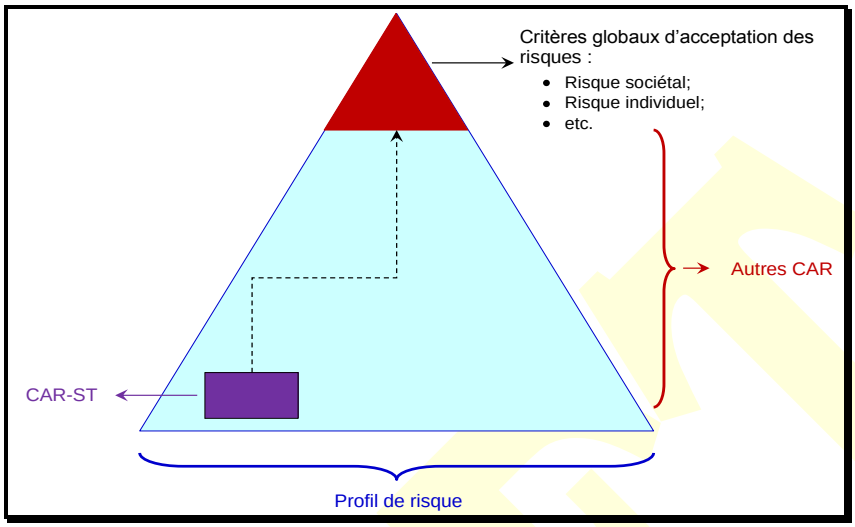


Figure 9: Pyramide des critères d'acceptation des risques (CAR).

[G 2] Les critères explicites d'acceptation des risques nécessaires pour soutenir la reconnaissance mutuelle seront harmonisés entre les États membres via le travail en cours de l'Agence sur les critères d'acceptation des risques. Des informations complémentaires seront intégrées à ce document une fois disponibles.

[G 3] Entre-temps, il est possible d'évaluer les risques en utilisant par exemple la matrice des risques de la section § 4.6 de la norme EN 50 126-1 {Ref. 8}. D'autres types de critères appropriés peuvent également être utilisés, étant donné que ces critères sont considérés comme assurant un niveau de sécurité acceptable dans les cas concernés.

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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] De plus amples détails concernant les CAR-ST et les aspects et fonctions du système technique auxquels le critère s'applique sont fournis par une note séparée de l'Agence associée au présent document: voir la section A.3 de l'appendice A et le document de référence {Ref. 11}.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

3. DÉMONSTRATION DE LA CONFORMITÉ AUX EXIGENCES DE SÉCURITÉ

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] Comme l'expliquent les points [G 5] à [G 5] de la section 2.1.1, la «démonstration de la conformité du système aux exigences de sécurité» inclut les phases 6 à 10 du cycle en V CENELEC (voir CADRE 3 de la Figure 5). Voir le point [G 5] de la section 2.1.1.

[G 2] Voir également le point [G 5] de la section 2.1.1 de ce document.

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

[G 1] Un exemple d'évaluations et d'analyses de sécurité réalisables au niveau des sous-systèmes est constitué par les analyses causales: voir la Figure 10. N'importe quelle autre méthode peut cependant être utilisée pour démontrer la conformité du sous-système aux exigences de sécurité en entrée.

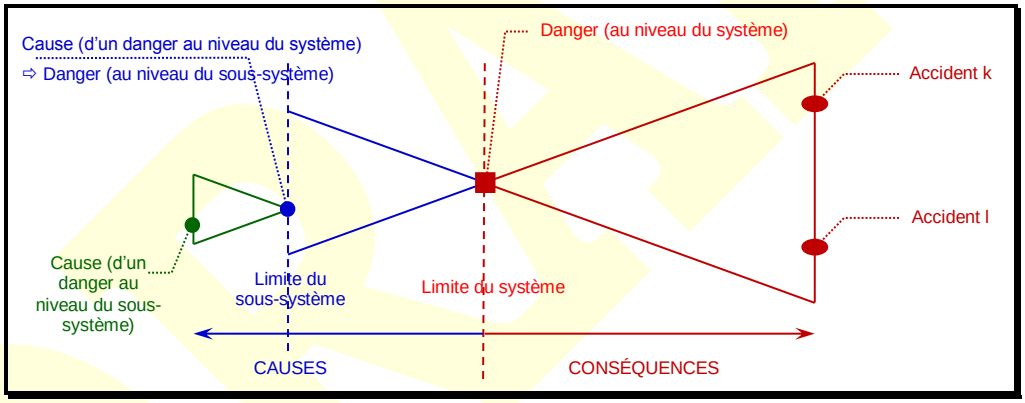


Figure 10: Figure A.4 de la norme EN 50 129: Définition des dangers par rapport aux limites du système.

[G 2] La structuration hiérarchique des dangers et des causes par rapport aux systèmes et aux sous-systèmes peut être répétée pour chaque phase inférieure du cycle en V CENELEC de la Figure 5. Les activités d'identification des dangers et d'analyse causale (ou toute méthode pertinente) ainsi que l'utilisation de codes de pratique, de systèmes de référence similaires et d'analyses et évaluations explicites peuvent également être répétées pour chaque phase du cycle de développement du système afin de dériver, depuis les mesures de sécurité identifiée au niveau du sous-système, les exigences de sécurité à respecter pour la phase suivante. Ce processus est également illustré par la Figure 11.

[G 3] Voir également le point [G 5] de la section 2.1.1 de ce document.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

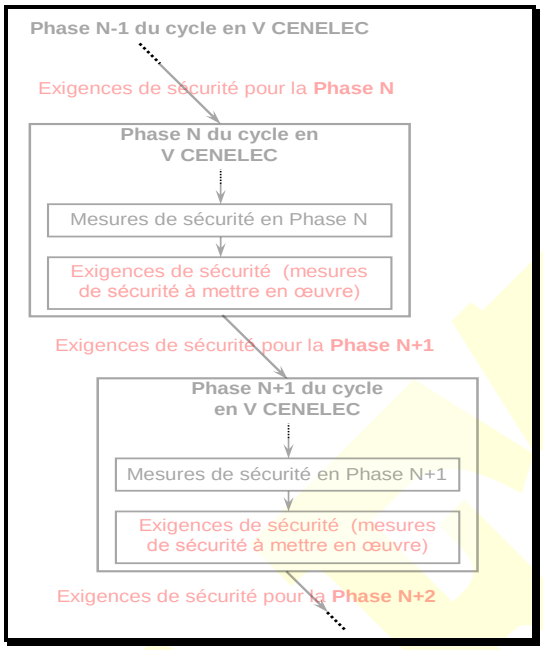


Figure 11: Dérivation des exigences de sécurité pour les phases inférieures.

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] Toutes les activités représentées à la CASE 3[(14)] du cycle en V CENELEC à la Figure 5 font donc elles aussi l'objet d'une évaluation indépendante.

[G 2] Les explications de l'Article 6 décrivent le type et le niveau de détail de l'évaluation indépendante réalisée par les organismes d'évaluation (évaluation détaillée ou macroscopique).

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] Par exemple, la méthode d'extinction des feux peut provoquer un nouveau danger (la suffocation) qui impose de nouvelles exigences de sécurité (par ex. une procédure spécifique d'évacuation des passagers). Un autre exemple est l'utilisation de verre trempé afin d'éviter le bris de vitres lors d'accidents et d'empêcher les blessures dues aux éclats de verre ou l'éjection des passagers. Le nouveau danger provoqué est que l'évacuation d'urgence des passagers par les fenêtres des voitures est nettement plus difficile. Il peut en découler une exigence de sécurité selon laquelle certaines fenêtres doivent être conçues spécialement pour permettre l'évacuation.

(14) *La correspondance des activités entre la MSC et la Figure 5 (c.-à-d. figure 10 du cycle en V de la norme EN 50 126 (cycle de vie CENELEC du système)) est décrite à la section 2.1.1. En particulier, le point [G3] à la section 2.1.1 répertorie les activités CENELEC qui sont incluses dans la phase MSC «démonstration de la conformité du système aux exigences de sécurité».*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

[G 2] Exemple de changement opérationnel: aucun transport de marchandises dangereuses ne peut emprunter une ligne passant par des zones à forte densité de population. Cela peut contraindre ces transports à emprunter un itinéraire alternatif avec des tunnels, ce qui crée de nouveaux types de dangers.

[G 3] L'appendice A.4.3 de la norme EN 50 129 fournit d'autres exemples de nouveaux dangers susceptibles d'être identifiés lors de la démonstration de la conformité du système aux exigences de sécurité.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

4. GESTION DES DANGERS

4.1. Processus de gestion des dangers

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] L'utilisation d'un registre des dangers pour l'enregistrement, la gestion et la maîtrise des informations relatives à la sécurité est également recommandée par les normes CENELEC 50 126-1 {Ref. 8} et 50 129 {Ref. 7}.

[G 2] Par exemple, selon la complexité du système, un acteur peut posséder un ou plusieurs registres des dangers. Dans les deux cas, les registres des dangers font l'objet d'une évaluation indépendante par l'organisme d'évaluation. Par exemple, une solution possible pourrait être de posséder:

(a) un «registre des dangers interne» pour la gestion de toutes les exigences de sécurité internes applicables au sous-système dont l'acteur est responsable. Sa taille et le volume de travail de gestion requis dépendent de sa structure et, bien entendu, de la complexité du sous-système. Cependant, étant donné qu'il est utilisé à des fins de gestion interne, le registre des dangers ne doit pas être communiqué à d'autres acteurs. Le registre interne des dangers contient tous les dangers identifiés maîtrisés ainsi que les mesures de sécurité associées qui ont été validées;

(b) un «registre des dangers externe» pour le transfert vers d'autres acteurs des dangers et des mesures de sécurité associées (que l'acteur ne peut mettre en œuvre complètement lui-même) conformément à la section 1.2.2. Généralement, ce deuxième registre des dangers est plus petit et nécessite un travail de gestion moindre (voir l'exemple à la section C.16.4 de l'appendice C).

[G 3] S'il semble compliqué de gérer plusieurs registres de dangers, une autre solution possible est de gérer tous les dangers et les mesures de sécurité associées couvertes par les points (a) et (b) ci-dessus dans un seul registre des dangers avec la possibilité de produire deux rapports de registres de dangers différents (voir l'exemple de la section C.16.3 de l'appendice C):

(a) un rapport de registre des dangers interne, qui n'est peut-être même pas nécessaire si le registre des dangers est bien structuré afin de permettre une évaluation indépendante;
(b) un rapport de registre des dangers externe destiné au transfert de dangers et des mesures de sécurité associées vers d'autres acteurs.

[G 4] Comme l'explique la section 4.2, lors de l'acceptation du système en fin de projet:

(a) tous les dangers transférés vers d'autres acteurs sont maîtrisés dans le registre des dangers externe de l'acteur qui les transfère. Étant donné qu'ils sont importés et gérés dans les registres des dangers internes des autres acteurs, ils n'ont pas à être gérés plus avant par l'acteur concerné durant le cycle de vie du (sous-)système;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) cependant, toutes les mesures de sécurité associées ne doivent pas être validées dans le registre des dangers pour les raisons expliquées au point (c) de la section 4.2. En effet, il est utile que l'organisation qui exporte les restrictions d'utilisation indique clairement dans son registre des dangers que les mesures de sécurité associées n'ont pas été validées.

[G 5] Réciproquement, tous les registres des dangers internes sont tenus à jour tout au long du cycle de vie du (sous-)système. Ceci permet de suivre le progrès du contrôle des risques associés aux dangers identifiés pendant l'exploitation et la maintenance du (sous-)système, donc même après sa mise en service: voir le CADRE 4 du cycle en V CENELEC à la Figure 5.

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

[G 1] Les informations sur les dangers et les mesures de sécurité associées reçues de la part d'autres acteurs (voir également la section 1.2.2) comprennent également toutes les hypothèses(15) et toutes les restrictions d'utilisation(15) (également appelées conditions d'applications liées à la sécurité) applicables aux différents sous-systèmes, les applications génériques et les cas génériques de sécurité des produits élaborés par les fabricants le cas échéant.

[G 2] La section C.16 de l'appendice C décrit une structure possible du registre des dangers.

4.2. Échange d'informations

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

[G 1] Par exemple, pour le sous-système odométrique de l'équipement embarqué ETCS, le fabricant peut valider les algorithmes en laboratoire en simulant les signaux théoriques susceptibles d'être générés par les capteurs odométriques associés. Toutefois, la validation complète du sous-système odométrique nécessite l'aide de l'EF ou du GI pour effectuer une validation au moyen d'un train réel et d'un réel contact entre la roue et la voie.

[G 2] D'autres exemples sont le transfert par le fabricant à l'entreprise ferroviaire des mesures de sécurité d'exploitation et de maintenance pour l'équipement technique. Ces mesures de sécurité devront être mises en œuvre par l'entreprise ferroviaire.

[G 3] Afin de permettre une réévaluation commune de ces dangers, des mesures de sécurité et des risques associés par les organisations impliquées, il est utile que l'organisation qui les a

(15) *Voir le point [G5] de la section 1.1.5 et les notes de bas de page (9) et (10) en page 31 de ce document pour une explication plus détaillée de la terminologie «dossiers de sécurité de produit générique et d'application générique», «hypothèses et restrictions d'utilisation».*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

identifiés fournisse toutes les explications nécessaires pour comprendre clairement le problème. Il se peut que la formulation initiale des dangers, des mesures de sécurité et des risques doive être modifiée pour les rendre compréhensibles sans devoir en rediscuter ensemble. La réévaluation commune des dangers peut entraîner l'identification de nouvelles mesures de sécurité.

[G 4] L'acteur réceptionnaire responsable de la mise en œuvre, de la vérification et de la validation des mesures de sécurité reçues ou nouvelles inscrit dans son propre registre des dangers tous les dangers concernés avec les mesures de sécurité associées (tant les dangers et mesures importés que ceux identifiés conjointement).

[G 5] Lorsqu'une mesure de sécurité n'est pas pleinement validée, il convient de définir une restriction claire d'utilisation (par exemple des mesures d'atténuation opérationnelle) et de la porter au registre des dangers. Il se peut que les mesures de sécurité techniques/de conception:

(a) ne soient pas mises en œuvre correctement;
(b) ne soient pas mises en œuvre complètement;
(c) ne soient pas mises en œuvre intentionnellement, par exemple parce que des mesures de sécurité autres que celles reprises au registre des dangers sont mises en œuvre (par ex. pour des raisons de coûts). Dans la mesure où elles ne sont pas validées, ces mesures de sécurité n'ont pas à être identifiées clairement dans le registre des dangers. Il faut prouver/justifier le fait que les mesures de sécurité mises en œuvre à leur place[16] sont appropriées, et démontrer qu'avec les mesures de sécurité de remplacement, le système respecte les exigences de sécurité;
(d) etc.

Dans ces cas, les mesures de sécurité techniques/de conception liées ne peuvent pas être vérifiées et validées lors de la gestion des dangers. Les dangers et les mesures de sécurité correspondants doivent rester ouverts dans le registre des dangers afin d'éviter l'utilisation abusive des mesures de sécurité pour d'autres systèmes par l'application du système d'acceptation des risques sur la base d'un «système de référence similaire»

[G 6] Généralement, les mesures de sécurité mises en œuvre de façon incorrecte et/ou incomplète sont détectées à un stade précoce du cycle de vie du système et corrigées avant l'acceptation du système. Cependant, si elles sont détectées trop tard pour une mise en œuvre correcte et complète de la mesure de sécurité technique, l'organisation responsable de la mise en œuvre et de la gestion doit identifier et porter au registre des dangers des restrictions d'utilisation claires pour le système évalué. Ces restrictions d'utilisation sont souvent des contraintes opérationnelles d'application pour le système évalué.

[G 7] Il pourrait également être utile de préciser dans le registre des dangers si les mesures de sécurité associées vont être mises en œuvre correctement à un stade ultérieur du cycle de vie du système ou si le système continuera d'être utilisé avec les restrictions d'utilisation identifiées. Il pourrait également être utile de noter au registre des dangers la justification de la mise en œuvre incorrecte/incomplète des mesures de sécurité techniques associées.

[G 8] L'acteur qui reçoit les restrictions d'utilisation:

(a) les importe dans son propre registre des dangers;

---

(16) *Si des mesures de sécurité différentes des mesures initialement spécifiées sont mises en œuvre, celles-ci doivent également être portées au registre des dangers.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) veille à ce que les conditions d'utilisation du système utilisé soient conformes à toutes les restrictions d'utilisation reçues;
(c) vérifie et valide que le système évalué est conforme à ces restrictions d'utilisation.

[G 9] Selon les décisions prises par les organisations impliquées:

(a) soit les mesures de sécurité techniques sont mises en œuvre correctement dans la conception à un stade ultérieur.
L'organisation qui exporte les restrictions d'utilisation continue à suivre la mise en œuvre technique correcte des mesures de sécurité associées. Par conséquent, les mesures de sécurité correspondantes ne peuvent pas être validées et les dangers qui leurs sont associés ne peuvent pas être maîtrisés dans le registre des dangers de cette organisation aussi longtemps que les mesures de sécurité techniques correspondantes n'ont pas été pleinement mises en œuvre. Il convient d'y veiller même si, entre-temps, les restrictions d'utilisation exportées ont été mises en place;

(b) soit les mesures de sécurité techniques ne seront pas mises en œuvre dans la conception à un stade ultérieur. Le système continuera donc à être utilisé durant tout son cycle de vie avec les restrictions d'utilisation associées. Dans ce cas, on peut faire ce qui suit:

(1) l'organisation qui exporte les restrictions d'utilisation n'enregistre pas les mesures de sécurité associées comme étant «validées» dans son registre des dangers. Ainsi, lorsque le système concerné est utilisé comme système de référence pour d'autres projets, les préoccupations de sécurité correspondantes ne seront pas ignorées. Par conséquent, même si un autre acteur accepte de gérer les risques associés différemment, il est utile que l'organisation qui exporte les restrictions d'utilisation indique clairement dans son registre des dangers que les mesures de sécurité associées n'ont pas été validées; ou

(2) la description du système peut être modifiée de façon à inclure les restrictions d'utilisation dans le champ d'application du système (c'est-à-dire les hypothèses pour le système) et dans les exigences de sécurité. Ceci permettra de maîtriser les dangers. Donc, en cas d'utilisation du système comme système de référence dans une autre application:

(i) le nouveau système devra être utilisé dans les mêmes conditions (c'est-à-dire respecter les restrictions d'utilisation associées à ces hypothèses); ou
(ii) une appréciation des risques supplémentaire devra être effectuée par le proposant pour les déviations par rapport à ces hypothèses.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

5. PREUVES D'APPLICATION DU PROCESSUS DE GESTION DES RISQUES

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

[G 1] Le système de gestion de la sécurité (SGS) de l'entreprise ferroviaire ou du gestionnaire d'infrastructure couvre déjà ces exigences. Quant aux autres acteurs du secteur ferroviaire impliqués dans le changement significatif, bien que le SGS ne soit pas obligatoire, ils possèdent en général au moins au niveau du projet un système de gestion de la qualité (SGQ) et/ou un processus de gestion de la sécurité (PGS). Ces deux processus se basent sur une hiérarchie structurée de la documentation à l'intérieur de la société ou au moins au sein du projet. Ils couvrent également les besoins documentaires de la gestion RAMS. Cette documentation structurée peut se composer principalement des éléments suivants (voir aussi la Figure 12):

(a) Des **plans de projet** élaborés afin de décrire l'organisation à mettre en place pour gérer une activité au sein d'un projet.

(b) Des **procédures de projet** élaborées afin de décrire en détail la façon d'accomplir une tâche dédiée. Généralement, les procédures et les instructions existent au sein de la compagnie et sont utilisées comme telles. De nouvelles procédures de projet ne sont élaborées que lorsqu'il est nécessaire de décrire une tâche spécifique au sein du projet envisagé.

(c) Des **documents de développement de projet** élaborés tout au long du cycle de vie du système illustré à la Figure 5.

(d) Des **modèles propres à la société ou au moins au projet** existent pour les différents types de documents à produire.

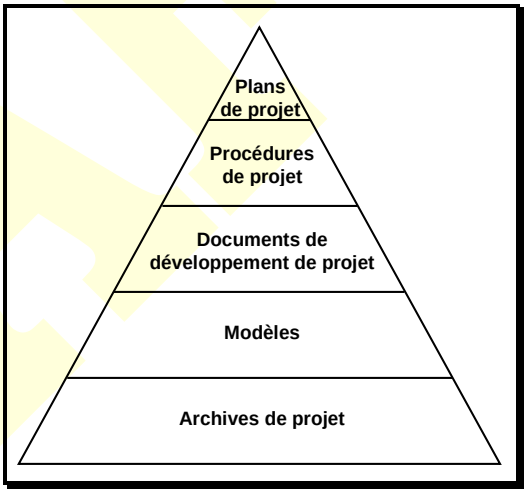


Figure 12: Hiérarchie de documentation structurée.

(e) Des **archives de projet** élaborées tout au long du projet et nécessaires afin de démontrer la conformité avec les processus de gestion de la qualité et de la sécurité de l'entreprise.

Il s'agit là d'une façon de répondre aux besoins de documentation. Il peut en exister d'autres pour autant qu'elles respectent les critères de la MSC.

[G 2] Les normes CENELEC recommandent de démontrer la conformité du système avec les exigences fonctionnelles et de sécurité dans un document de dossier de sécurité (ou dans

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

un rapport de sécurité). Même si cela n'est pas obligatoire, l'utilisation d'un dossier de sécurité fournit, dans un document de justification de sécurité structuré:

(a) la preuve de la gestion de la qualité;
(b) la preuve de la gestion de la sécurité;
(c) la preuve de la sécurité fonctionnelle et de sécurité.

Il présente également l'avantage de soutenir et de guider le ou les organisme(s) d'évaluation dans l'évaluation indépendante de l'application correcte de la MSC.

[G 3] Le dossier de sécurité décrit et résume la façon dont les documents de projet issus de l'application du processus de gestion de la qualité et/ou de la sécurité de l'entreprise ou du projet interagissent avec le processus de développement du système pour démontrer la sécurité du système. Généralement, le dossier de sécurité n'inclut pas de volumes importants de preuves détaillées ni de documentation, mais fournit des références précises à ces documents.

[G 4] **Dossier de sécurité pour les systèmes techniques:** Les normes CENELEC peuvent être utilisées en tant que lignes directrices pour la rédaction et/ou la structure des dossiers de sécurité:

(a) voir la norme EN 50 129 {Ref. 7} « Applications ferroviaires -- Systèmes de signalisation, de télécommunication et de traitement – Systèmes électroniques de signalement en matière de sécurité »;
L'appendice H.2 de la ligne directrice EN 50 126-2 {Ref. 9} propose également une structure pour le dossier de sécurité des systèmes de signalisation;
(b) voir l'appendice H.1 de la ligne directrice EN 50 126-2 {Ref. 9} pour la structure du dossier de sécurité pour le matériel roulant;
(c) voir l'appendice H.3 de la ligne directrice EN 50 126-2 {Ref. 9} pour la structure du dossier de sécurité des infrastructures;

Comme l'indiquent ces références, la structure du dossier de sécurité des systèmes techniques, ainsi que son contenu, dépendent du système dont il faut démontrer la conformité aux exigences de sécurité.

Le dossier de sécurité ébauché à l'appendice H de la ligne directrice EN 50 126-2 {Ref. 9} fournit uniquement des exemples et ne convient pas nécessairement à tous les systèmes du type donné. Il convient donc d'utiliser cette esquisse en évaluant de façon appropriée les éléments qui correspondent à chaque application spécifique.

[G 5] **Dossier de sécurité pour les aspects organisationnels et opérationnels des systèmes ferroviaires:**

Il n'existe actuellement aucune norme dédiée précisant la structure, le contenu et une ligne directrice pour la rédaction d'un dossier de sécurité pour les aspects organisationnels et opérationnels d'un système ferroviaire. Toutefois, dans la mesure où le dossier de sécurité a pour but de démontrer de façon structurée la conformité du système avec ses exigences de sécurité, il est possible d'utiliser le même type de structure de sécurité que pour les systèmes techniques. Les références au point [G 3] de la section 5.1 donnent des conseils et une liste de contrôle d'éléments à couvrir quel que soit le type de système évalué. La gestion des changements opérationnels et organisationnels nécessite le même genre de processus de gestion de la qualité et de la sécurité que les changements techniques, avec une démonstration de la conformité du système aux exigences de sécurité spécifiques. Les exigences des normes CENELEC qui ne s'appliquent pas aux aspects organisationnels et opérationnels sont celles qui sont liées purement à la conception des systèmes techniques, comme par exemple les principes de «protection inhérente du matériel contre les défaillances», la compatibilité électromagnétique (CEM), etc.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

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

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

(b) results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.

[G 1] Selon la complexité du système, ces preuves peuvent être rassemblées dans un ou plusieurs dossier(s) de sécurité. Voir respectivement les points [G 3] et 5.1.[G 5] de la section 5.1 pour la structure des dossiers de sécurité des systèmes techniques et pour les aspects opérationnels et organisationnels.

[G 2] Voir également la section A.4 de l'appendice A pour des exemples de preuves possibles.

[G 3] Dans le secteur ferroviaire, la durée de vie prévue des systèmes et sous-systèmes est généralement d'une trentaine d'années. Au cours d'une si longue période, il est raisonnable de s'attendre également à un certain nombre de changements significatifs apportés à ces systèmes. D'autres évaluations des risques pourraient donc être effectuées pour ces systèmes et leurs interfaces avec la documentation correspondante qui devra être revue, complémentée et transférée entre différents acteurs et organisation au moyen de registres de dangers. Ceci implique des exigences relativement strictes en matière de contrôle de la documentation et de gestion de la configuration.

[G 4] Il est donc utile que l'entreprise qui archive toutes les informations d'appréciation des risques et de gestion des risques garantisse le stockage des résultats/informations sur un support physique lisible/accessible durant tout le cycle de vie du système (c'est-à-dire pendant 30 ans).

[G 5] Les principales raisons de cette exigence sont, entre autres:

(a) de garantir l'accessibilité de toutes les analyses et de toutes les archives de sécurité du système évalué tout au long de sa vie. Donc:

(1) en cas de nouveaux changements significatifs apportés au même système, la dernière documentation du système est disponible;

(2) en cas de problème pendant la vie du système, il est utile de revenir aux analyses de sécurité associées et aux archives de sécurité;

(b) de garantir l'accessibilité de toutes les analyses et de toutes les archives de sécurité du système évalué au cas où il serait utilisé comme système de référence similaire pour une autre application.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

ANNEXE II DU RÈGLEMENT MSC

Critères à respecter par les organismes d'évaluation

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

[G 1] Aucune explication supplémentaire n'est considérée nécessaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

APPENDICE A: CLARIFICATIONS SUPPLÉMENTAIRES

A.1. Introduction

A.1.1. L'objectif de cet appendice est de faciliter la lecture du présent document. Au lieu de fournir des quantités importantes d'informations dans le corps du document, les sujets les plus complexes sont expliqués plus en détail dans le présent appendice.

A.2. Classification des dangers

A.2.1. Une ligne directrice est fournie à la section § 4.6.3 de la norme EN 50 126-1 {Ref. 8} ainsi qu'à l'appendice B.2 de la ligne directrice EN 50 126-2 {Ref. 9} pour la classification / le classement des dangers.

A.3. Critère d'Acceptation des Risques pour les Systèmes Techniques (CAR-ST)

A.3.1. Limite supérieure d'acceptabilité des risques pour les systèmes techniques

A.3.1.1. Le CAR-ST est décrit à la section 2.5.4 de {Ref. 4}:

A.3.1.2. L'objectif du CAR-ST est de définir une limite supérieure d'acceptabilité des risques pour les systèmes techniques dont les exigences de sécurité ne peuvent être définies ni par l'utilisation de codes de pratique ni par comparaison avec des systèmes de référence similaires. Il définit par conséquent un point de référence sur la base duquel les méthodes d'analyse des risques pour les systèmes techniques peuvent être calibrées. Comme le décrit la section A.3.6 de l'appendice A de ce document, cette valeur de référence ou limite supérieure d'acceptabilité du risque pourrait également être utilisée pour déterminer les critères d'acceptation des risques d'autres défaillances fonctionnelles de systèmes techniques qui ne présentent pas un potentiel crédible et direct de conséquences catastrophiques (c'est-à-dire pour d'autres gravités). Mais le CAR-ST n'est pas une méthode d'analyse des risques.

A.3.1.3. Le CAR-ST est un critère semi-quantitatif. Il s'applique aussi bien aux défaillances aléatoires du matériel qu'au défaillances/erreurs systématiques du système technique. Les défaillances/erreurs systématiques du système technique résultant potentiellement d'erreurs humaines pendant le processus de développement du système technique (c'est-à-dire la spécification, la conception, l'implémentation et la validation) sont donc couvertes également. Par contre, le CAR-ST ne couvre pas les erreurs humaines pendant l'exploitation et la maintenance des systèmes techniques.

A.3.1.4. Selon les appendices A.3 et A.4 de la norme CENELEC 50 129, les erreurs/défaillances systématiques ne sont pas quantifiables et l'objectif quantitatif doit donc être démontré pour les défaillances matérielles aléatoires uniquement, alors que les défaillances/erreurs

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

systématiques sont abordées par des méthodes qualitatives[17]. *«Étant donné qu'il n'est pas possible d'évaluer l'intégrité face aux défaillances systématiques par des méthodes quantitatives, les niveaux d'intégrité de sécurité sont utilisés pour regrouper des méthodes, outils et techniques dont on considère, lorsqu'ils sont utilisés efficacement, qu'ils fournissent un niveau adéquat de confiance dans la réalisation d'un système à un niveau d'intégrité défini.»*

A.3.1.5. De même, selon les normes CENELEC, l'intégrité du logiciel des systèmes techniques n'est pas quantifiable. La norme CENELEC 50 128 donne des recommandations pour le processus de développement de logiciels liés à la sécurité en fonction du niveau d'intégrité de sécurité requis. Ceci comprend les processus de conception, de vérification, de validation et d'assurance qualité pour les logiciels.
Selon la norme CENELEC 50 128, pour un système programmable de contrôle électronique mettant en œuvre des fonctions de sécurité, le niveau d'intégrité de sécurité le plus élevé possible pour le processus de développement de logiciels est SIL 4, ce qui correspond à un taux de danger quantitatif tolérable de 10^{-9} h^{-1}.

A.3.1.6. Par conséquent, étant donné que les défaillances/erreurs systématiques ne sont pas quantifiables, elles doivent être gérées de façon qualitative en mettant en place un processus de qualité et de sécurité compatible avec le niveau d'intégrité de sécurité pour le système évalué.

(a) l'objectif du processus de qualité est de «*minimiser l'incidence des erreurs humaines à chaque stade du cycle de vie, et donc de réduire le risque de défaillances systématiques du système*»;

(b) l'objectif du processus de sécurité est de «*réduire encore l'incidence des erreurs humaines en matière de sécurité tout au long du cycle de vie, et donc de réduire le risque de défaillances systématiques du système*»;

A.3.1.7. Les normes suivantes fournissent des recommandations quant à la gestion de l'incidence des erreurs/défaillances systématiques et quant à des mesures de conception possibles pour protéger contre les défaillances à cause/mode communs (Common Cause/Mode Failures, CCF/CMF) et pour garantir que les systèmes techniques passent en mode de sécurité en cas d'erreurs / de défaillances de cette nature:

(a) la norme CENELEC 50 126-1 {Ref. 8} et son guide 50 126-2 {Ref. 9} listent les clauses de la norme CENELEC 50 129 et indiquent leur applicabilité pour la preuve documentée de systèmes autres que ceux de signalisation: voir le tableau 9.1 du guide 50 126-2 {Ref. 9}. Cette liste fait références aux conseils relatifs à la façon de faire face aux erreurs provenant du système lui-même et aux effets de l'environnement sur le système évalué;

Par exemple, des techniques/mesures pour les caractéristiques de conception sont données au *«tableau E.5: Caractéristiques de conception (auxquelles il est fait référence en 5.4)»* de la norme CENELEC 50 129 {Ref. 7} *«pour éviter et maîtriser les défaillances provoquées par:*

(1) *«les défaillances conceptuelles résiduelles»;*

---

(17) *Selon les normes CENELEC 50 126 et 50 129, le chiffre quantitatif relatif aux défaillances matérielles aléatoires doit toujours être lié à un niveau d'intégrité de sécurité afin de gérer les erreurs/défaillances systématiques. Par conséquent, le chiffre de 10^{-9} h^{-1} du CAR-ST nécessite également la mise en place d'un processus adéquat de gestion des erreurs/défaillances systématiques. Mais pour faciliter la lecture de la note, il ne fait souvent référence qu'aux défaillances matérielles aléatoires du système technique.*

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(2) *«les conditions environnementales»;*
(3) *«une mauvaise utilisation ou des erreurs d'utilisation»;*
(4) *«les erreurs logicielles résiduelles»;*
(5) *«les facteurs humains»*

Les appendices D et E de la norme CENELEC 50 129 {Ref. 7} décrivent des techniques et des mesures destinées à éviter les défaillances systématiques et à contrôler les erreurs/défaillances matérielles aléatoires et systématiques pour les systèmes électroniques de sécurité en matière de signalement. Bon nombre de ces méthodes peuvent être étendues à des systèmes autres que les systèmes de signalement via une référence à ces lignes directrices au tableau 9.1 du guide 50 126-2 {Ref. 9}.

(b) La norme CENELEC 50 128 donne des recommandations pour le processus de développement de logiciels liés à la sécurité en fonction du niveau d'intégrité de sécurité (SIL 0 à SIL 4) requis pour le logiciel du système évalué.

A.3.1.8. Le CAR-ST représente également le niveau d'intégrité le plus élevé qui puisse être requis selon les normes CENELEC et IEC. Pour faciliter la référence, les exigences des normes IEC 61508-1 et CENELEC 50 129 sont citées:

(a) IEC 61508-1: «*Cette norme fixe une limite inférieure exigible pour les mesures de défaillances cibles, dans le cas d'un mode de défaillance dangereux. Ces limites inférieures déterminent le niveau d'intégrité de sécurité 4. Il peut être possible de réaliser des concepts de systèmes de sécurité possédant des valeurs limites inférieures pour les mesures de défaillances pour des systèmes non complexes, mais il est considéré que les chiffres de ce tableau représentent la limite de ce qui peut être atteint pour des systèmes relativement complexes (par exemple pour des systèmes électroniques de sécurité programmables) à l'heure actuelle*.»

(b) EN 50129: *«Une fonction présentant des exigences quantitatives plus strictes que 10^{-9} h^{-1} sera traitée de l'une des façons suivantes:*

(1) *s'il est possible de diviser cette fonction en sous-fonctions fonctionnellement indépendantes, le THR peut être divisé entre ces sous-fonctions et un SIL attribué à chaque sous-fonction;*
(2) *si la fonction n'est pas divisible, les mesures et méthodes requises pour SIL 4 seront, à tout le moins, respectées et la fonction sera utilisée en combinaison avec d'autres mesures techniques ou opérationnelles afin d'atteindre le THR nécessaire.»*

A.3.1.9. Tous les systèmes techniques doivent donc limiter l'exigence de sécurité quantitative à ce chiffre. Si un degré supérieur de protection est nécessaire, il ne peut être atteint avec un seul système. L'architecture du système doit être modifiée, par exemple en utilisant deux systèmes indépendants en parallèle qui effectuent des vérifications croisées entre eux pour générer des sorties sûres. Mais ceci augmente clairement les coûts de développement du système technique.

Remarque: s'il existe certaines fonctions existantes, par ex. des systèmes mécaniques dont l'expérience opérationnelle montre qu'ils ont atteint un niveau d'intégrité supérieur, le niveau de sécurité peut être décrit par un code de pratique particulier, ou les exigences de sécurité peuvent être déterminées par une analyse de similarité avec le système existant. Dans le contexte de la MSC, le CAR-ST ne doit être appliqué que s'il n'existe aucun code de pratique et aucun système de référence.

A.3.1.10. On peut résumer la situation comme suit:

(a) selon les normes CENELEC 50 126, 50 128 et 50 129, les erreurs/défaillances systématiques de développement ne sont pas quantifiables;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) l'incidence des erreurs/défaillances systématiques ainsi que leur risque résiduel doivent être maîtrisés et gérés par l'application d'un processus de qualité et de sécurité compatible avec le niveau d'intégrité de sécurité requis pour le système évalué;
(c) le niveau d'intégrité de sécurité maximal est SIL 4 tant pour les défaillances matérielles aléatoires que pour les défaillances/erreurs systématiques des systèmes techniques;
(d) cette limite du niveau d'intégrité de sécurité de SIL 4 implique que le taux de danger maximal tolérable (Tolerable Hazard Rate, THR), c'est-à-dire le taux de défaillance maximal des systèmes techniques doit également être limité à 10^{-9} h^{-1}.

A.3.1.11. Un taux de danger tolérable de 10^{-9} h^{-1} peut être atteint par le système technique soit par une «architecture protégée contre les défaillances» (qui réalise par définition ces performances de sécurité), soit par une «architecture redondante» (deux canaux de traitement indépendants qui se contrôlent mutuellement).

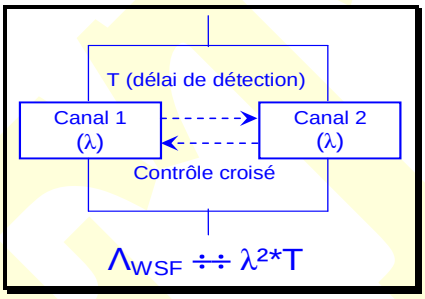


Figure 13: Architecture redondante d'un système technique.

Pour une architecture redondante, il peut être prouvé que le taux global de défaillance du mauvais côté (Λ_{WSF}) du système technique est proportionnel à λ^2*T, où:

(a) λ^2 représente le carré du taux de défaillance du mauvais côté d'un canal;l
(b) T représente le temps nécessaire pour qu'un canal détecte la défaillance de l'autre canal. Ceci est généralement un multiple du temps/cycle de traitement d'un canal. T est généralement largement inférieur à une seconde.

A.3.1.12. Sur la base de cette formule (λ^2*T), il peut être démontré théoriquement (en tenant compte uniquement des défaillances matérielles aléatoires du système technique – voir également le point A.3.1.13 de l'appendice A) qu'une exigence quantitative de 10^{-9} h^{-1} pour le CAR-ST peut être respectée. Les défaillances/erreurs systématiques doivent être gérées au moyen d'un processus: voir le point A.3.1.6 de l'appendice A. Par exemple:

(a) avec un MBTF de 10 000 heures pour le chiffre de fiabilité d'un canal, et l'hypothèse prudente que toute défaillance de canal est dangereuse, le taux de défaillance du mauvais côté d'un canal est 10^{-4} h^{-1};
(b) même avec un délai de 10 minutes (c'est-à-dire $\approx 2*10^{-3}$ heures) pour détecter les défaillances du mauvais côté de l'autre canal, ce qui est également une hypothèse prudente;

Le taux global de défaillance du mauvais côté $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}

A.3.1.13. Dans la pratique, pour une telle architecture redondante, l'évaluation du taux quantitatif global de défaillance du mauvais côté doit tenir compte des mesures prises au niveau de la conception pour protéger contre les défaillances à cause/mode communs (CCF/CMF) et pour garantir que les systèmes techniques passent en mode de sécurité en cas d'erreurs / de défaillances de cette nature. L'évaluation de ce taux global de défaillance du mauvais côté (Λ_{WSF}) doit donc tenir compte:

(a) des composants communs à tous les canaux: entrées simples ou communes vers tous les canaux, alimentation électrique commune, comparateurs, dispositifs en redondance majoritaire, etc;
(b) le délai requis pour détecter les défaillances dormantes ou latentes. Pour les systèmes techniques complexes, ce délai peut être supérieur à une seconde par plusieurs ordres de grandeur;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(c) l'impact des défaillances à cause/mode communs (CCF/CMF).

Des conseils relatifs à ces sujets sont fournis par les normes mentionnées au point A.3.1.7 de l'appendice A du présent document.

A.3.2. Diagramme du test d'applicabilité du CAR-ST

A.3.2.1. La Figure 14 illustre une façon possible d'appliquer le CAR-ST aux dangers provoqués par les défaillances des systèmes techniques.

A.3.2.2. La section C.15. de l'appendice C décrit l'application de ce diagramme à un exemple.

A.3.3. Définition d'un système technique selon la MSC

A.3.3.1. Le CAR-ST s'applique uniquement aux systèmes techniques. L'article 3, paragraphe 22, du règlement MSC définit le concept de «système technique» comme suit:

«système technique», un produit ou un ensemble de produits, y compris la conception, la mise en œuvre et la documentation; le développement d'un système technique débute par la spécification de ses exigences et se termine par son acceptation; bien que la conception des interfaces pertinentes avec le comportement humain soit prise en considération, les opérateurs humains et leurs actions ne font pas partie du système technique; le processus de maintenance est décrit dans les manuels d'entretien mais ne fait pas en soi partie du système technique.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

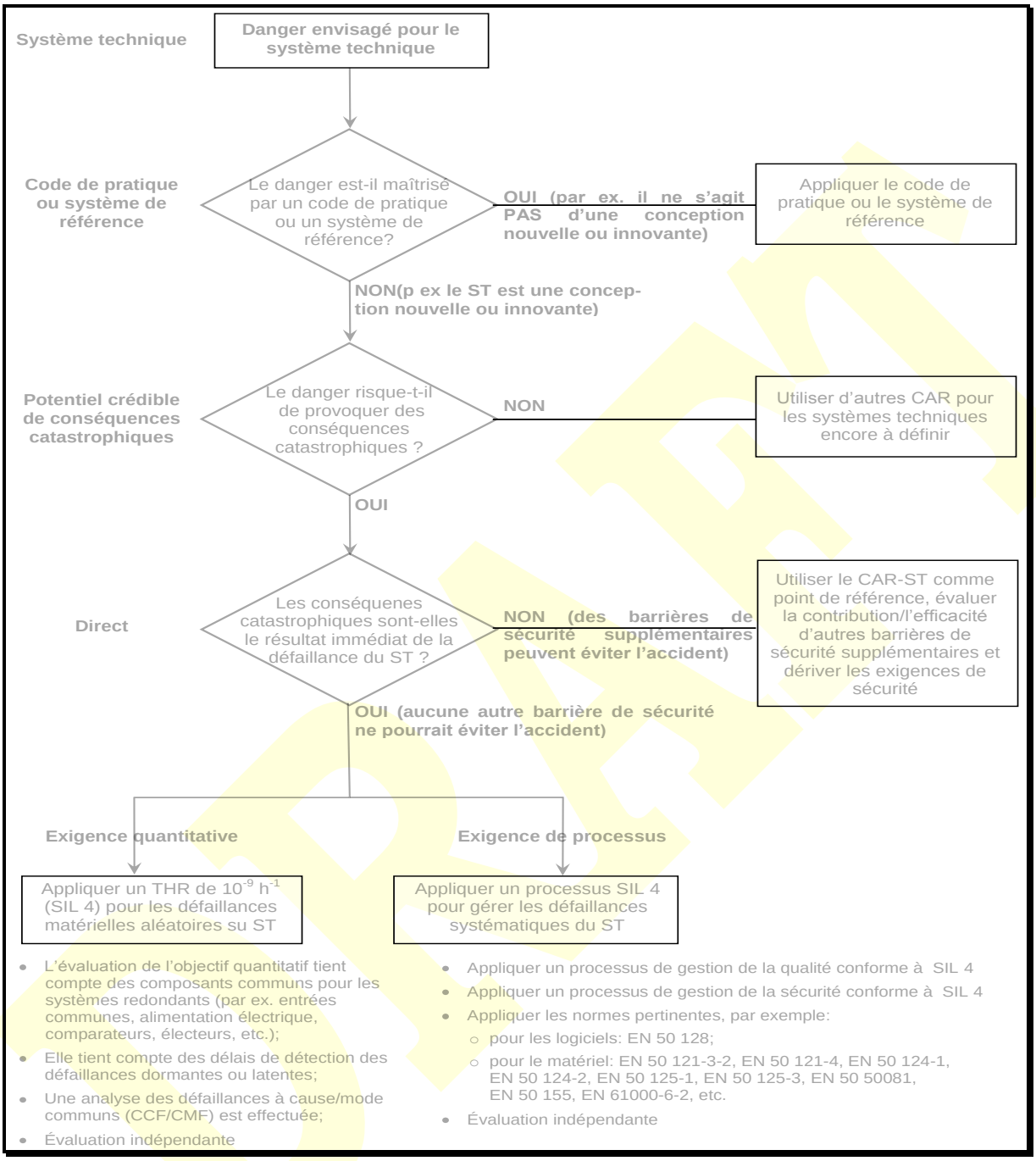


Figure 14: Diagramme pour le test d'applicabilité du CAR-ST.

A.3.4. Explication de la définition d'un «système technique»

A.3.4.1. Cette définition d'un système technique décrit la portée du système technique: *«un produit ou un ensemble de produits, y compris la conception, la mise en œuvre et la documentation.»* Il se compose donc des éléments suivants:

(a) les composants physiques du système technique;
(b) les logiciels associés éventuels;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(c) la conception et la mise en œuvre du système technique y compris, le cas échéant, la configuration et le paramétrage d'un produit générique en fonction des exigences spécifiques de l'application spécifique;
(d) la documentation nécessaire pour:

(1) le développement du système technique;
(2) l'exploitation et la maintenance du système technique;

A.3.4.2. Les notes associées à cette définition précisent la portée du système technique:

(a) *«le développement d'un système technique débute par la spécification de ses exigences et se termine par son acceptation».* Ceci inclut les phases 1 à 10 du cycle en V représenté à la figure 10 de la norme CELENEC 50 126-1 {Ref. 8};

(b) *«bien que la conception des interfaces pertinentes avec le comportement humain soit prise en considération, les opérateurs humains et leurs actions ne font pas partie du système technique».* Bien que les erreurs liées au facteur humain pendant l'exploitation et la maintenance du système technique ne fassent pas partie du système technique lui-même, la conception des interfaces avec les opérateurs humains doit en tenir compte. L'objectif est de minimiser la probabilité d'erreurs humaines liées à une mauvaise conception des interfaces concernées avec les opérateurs humains;

(c) *«Le processus de maintenance est décrit dans les manuels d'entretien mais ne fait pas en soi partie du système technique.»* Cela signifie que le CAR-ST ne doit pas être appliqué à l'exploitation et à la maintenance du système technique; celles-ci reposent dans une large mesure sur des processus et des actions pris en charge par du personnel humain.
Cependant, afin de soutenir la maintenance des systèmes techniques, la définition des systèmes techniques doit comprendre les éventuelles exigences pertinentes (par ex. maintenance préventive périodique, ou maintenance corrective en cas de défaillance) avec un niveau de détail suffisant. Toutefois, la façon dont la maintenance du système technique doit être organisée et réalisée ne fait pas partie de la définition du système technique mais des manuels de maintenance correspondants.

A.3.4.3. Voir également la section A.3.1. de l'appendice A.

A.3.5. Fonctions des systèmes techniques auxquels s'applique le CAR-ST

A.3.5.1. Selon la définition du CAR-ST, celui-ci s'applique aux défaillances fonctionnelles du système technique qui présentent *«un potentiel **direct** crédible de conséquences catastrophiques»*: voir la section 2.5.4 de {Ref. 4}.

A.3.5.2. Le CAR-ST peut également être appliqué à des fonctions impliquant des systèmes techniques mais dont la défaillance **ne présente** pas de *«potentiel **direct** de conséquences catastrophiques».* Dans ce cas, le CAR-ST doit être appliqué en tant qu'objectif global pour la série d'événements qui aboutissent aux conséquences catastrophiques. Sur la base de cet objectif global, la contribution effective de chaque événement, et donc des défaillances fonctionnelles du système technique impliqué dans le scénario envisagé, doit être dérivée de la section A.3.6 de l'appendice A.
Cette utilisation du CAS-ST doit encore faire l'objet de discussions et d'un accord avec le groupe de travail MSC.

A.3.5.3. À quelles fonctions du système technique le CAR-ST s'applique-t-il ? Selon la norme IEC 61226:2005:

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(a) une fonction est définie dans ce contexte comme «*un objectif spécifique à réaliser qui peut être spécifié ou décrit sans référence au moyen physique de le réaliser*».
(b) une fonction (considérée comme une boîte noire) transfère des paramètres d'entrée (par ex. matériaux, énergie, informations) en paramètres de sorties liés à l'objectif (par ex. matériaux, énergie, informations);
(c) l'analyse de la fonction est indépendante de sa réalisation technique.

A.3.5.4. Le CAR-ST est applicable aux types de fonctions suivants:

(a) exemples pour le sous-système embarqué ETCS:

(1) « fournir au conducteur les informations nécessaires pour lui permettre de conduire le train en toute sécurité et utiliser les freins en cas de survitesse ». Sur la base d'informations reçues depuis la voie (vitesse autorisée) et du calcul de la vitesse du train par l'ETCS embarqué, le conducteur et l'ETCS embarqué sont en mesure de veiller à ce que le train ne dépasse pas la vitesse autorisée. Le CAR-ST s'applique à l'évaluation de la vitesse du train par le système embarqué étant donné:

(i) qu'il n'existe pas de barrière (directe) supplémentaire puisque les informations fournies au conducteur sont également sous-évaluées;
(ii) la survitesse du train pourrait provoquer un déraillement, c'est-à-dire un accident présentant un potentiel de conséquences catastrophiques;

(2) «fournir au conducteur les informations nécessaires pour lui permettre de conduire le train en toute sécurité et utiliser les freins en cas de violation de l'autorité de mouvement permise».

(b) exemple pour un circuit de voie: «détecter l'occupation de la section de voie». Le CAR-ST sera applicable tel quel à cette fonction uniquement si l'aiguillage n'implémente pas de fonction de «monitoring de séquence».
(c) exemple pour un point: «contrôler la position de point»;

A.3.5.5. Certaines normes définissent également des fonctions auxquelles le CAR-ST pourrait s'appliquer. Par exemple:

(a) La norme prEN 0015380-4 {Ref. 13} (ModTrain Work) définit dans sa partie normative trois niveaux de fonction hiérarchiques (étendus jusqu'à cinq niveaux dans les annexes informatives). Au total, prEN 0015380-4 définit plusieurs centaines de fonctions relatives aux trains;
(b) en général, il est recommandé de sélectionner les fonctions depuis les trois premiers niveaux de prEN 0015380-4 (mais pas plus bas) en tenant compte également de l'éventail structurel des produits:
(c) pour les fonctions qui ne tombent pas sous le coup de la norme prEN 0015380-4, le niveau fonctionnel approprié doit être défini par comparaison sur la base d'un avis d'expert.

L'Agence doit poursuivre son travail sur ces exemples de fonctions issus de la norme prEN 0015380-4 dans le cadre du travail relatif aux risques largement acceptables et aux critères d'acceptation des risques.

A.3.5.6. Le CAR-ST s'applique également, par exemple, aux fonctions suivantes de prEN 0015380-4: *«Contrôle de l'inclinaison»* (code = CLB). Cette fonction peut être utilisée au niveau du système des deux façons suivantes:

(a) premier cas: le train doit s'incliner dans les courbes pour le confort des passagers et doit surveiller la conformité du gabarit avec l'infrastructure de voie;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(b) deuxième cas: le train doit s'incliner dans les courbes pour le confort des passagers uniquement, mais ne doit pas surveiller la conformité du gabarit avec l'infrastructure de voie;

Le CAR-ST sera appliqué dans le premier cas mais pas dans le second, puisque dans le second cas la défaillance de la fonction d'inclinaison n'a pas de conséquences catastrophiques.

A.3.5.7. Cet exemple (b) au point A.3.5.4 et les exemples du point A.3.5.6 de l'appendice A montrent clairement qu'il ne sera pas possible de dresser une liste prédéfinie de fonctions auxquelles le CAR-ST s'applique dans tous les cas. Cela dépendra toujours de la façon dont le système utilise ces fonctions de sous-systèmes.

A.3.5.8. La section C.15. de l'appendice C donne un exemple d'application du CAR-ST.

A.3.6. Exemples d'application du CAR-ST

A.3.6.1. Introduction

(a) Ce chapitre donne des exemples de la façon de déterminer les taux de défaillance pour les autres gravités de dangers et montre comment définir des exigences de sécurité inférieures à $10^{-9}\,h^{-1}$. Ce document ne recommande ni n'impose aucune méthode particulière. Il montre seulement à titre informatif comment le CAR-ST peut être utilisé pour calibrer certaines méthodes largement utilisées. Ce point doit faire l'objet d'un développement plus approfondi dans le cadre du travail de l'Agence sur les risques largement acceptables et sur les critères d'acceptation des risques.

(b) En fait, le CAR-ST ne peut être appliqué directement que dans un petit nombre de cas vu que, dans la pratique, peu de défaillances fonctionnelles des systèmes techniques provoquent directement des accidents ayant des conséquences potentiellement catastrophiques. Par conséquent, afin d'appliquer les critères aux dangers sans conséquences catastrophiques et de déterminer le taux de défaillance visé, il est possible de faire des compromis (par ex. en calibrant une matrice de risques sur la base de ce critère) entre différents paramètres, par ex. gravité vs. fréquence.

A.3.6.2. Exemple 1: Compromis de risque direct

(a) le CAR-ST peut être appliqué facilement aux scénarios qui ne diffèrent que par quelques paramètres indépendants des conditions de référence définies pour le CAR-ST à la section 2.5.4 du règlement MSC {Ref. 3};

(b) supposons que, pour un paramètre donné p, la relation avec le risque soit multiplicative. Supposons que p* soit présent dans les conditions de référence, alors que p' soit applicable dans le scénario alternatif. Dans ce cas, seul le rapport p*/p' est pertinent et le taux de survenance peut être réduit. Cette procédure peut faire l'objet d'une itération si les paramètres sont indépendants.

(c) Exemple:

(1) supposons que le potentiel réel de conséquences catastrophiques ait été évalué, sur la base d'un avis d'expert, à une valeur dix fois inférieure au potentiel dans les conditions de référence de la section 2.5.4 du règlement MSC {Ref. 3}. L'exigence est alors $10^{-8}\,h^{-1}$ au lieu de $10^{-9}\,h^{-1}$.

(2) supposons qu'une barrière de sécurité supplémentaire assurée par un autre système technique (indépendamment des conséquences) et efficace dans 50 % des cas ait été identifiée;

(3) l'exigence de sécurité serait alors $5*10^{-7}\,h^{-1}$ (soit $0.5*10^{-8}\,h^{-1}$) au lieu de $10^{-9}\,h^{-1}$.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

A.3.6.3. Exemple 2: Calibrage de la matrice des risques

(a) pour utiliser correctement le CAR-ST dans une matrice de risques, il faut que la matrice concerne le niveau de système correct (comparable à celui fourni à la section A.3.5 de l'appendice A).

(b) le CAR-ST définit un champ de la matrice de risques comme étant tolérable. Celui-ci correspond à la coordonnée (gravité catastrophique; 10^{-9} h^{-1} fréquence de survenance): voir le champ rouge dans le tableau 5. Tous les champs qui concernent une fréquence supérieure doivent être identifiés comme «intolérables». Il convient de noter que la fréquence des accidents n'est identique à la fréquence des défaillances fonctionnelles qu'en cas de potentiel direct crédible de conséquences catastrophiques.

(c) ensuite le reste de la matrice peut être complété en tenant compte d'effets tels que l'aversion au risque et la mise à l'échelle des catégories. Dans le cas le plus simple d'une mise à l'échelle linéaire décennale (comme l'indique la flèche dans le tableau 5), le champ qui peut être identifié comme «acceptable» par le CAR-ST est extrapolé de façon linéaire au reste de la matrice. Cela signifie que tous les champs qui appartiennent à la même diagonale (ou qui se trouvent sous la diagonale) sont également identifiés comme «acceptables». Les champs situés en-dessous peuvent également être identifiés comme «acceptables».

Tableau 5: Exemple typique d'une matrice de risques calibrée

Fréquence de survenance d'un accident (provoqué par un danger)	**Niveaux de risque**			
Fréquent (10^{-4} par heure)	**Intolérable**	**Intolérable**	**Intolérable**	**Intolérable**
Probable (10^{-5} par heure)	**Intolérable**	**Intolérable**	**Intolérable**	**Intolérable**
Occasionnel (10^{-6} par heure)	**Acceptable**	**Intolérable**	**Intolérable**	**Intolérable**
Distant (10^{-7} par heure)	**Acceptable**	**Acceptable**	**Intolérable**	**Intolérable**
Improbable (10^{-8} par heure)	**Acceptable**	**Acceptable**	**Acceptable**	**Intolérable**
Incroyable (10^{-9} par heure)	**Acceptable**	**Acceptable**	**Acceptable**	**Acceptable**
	Insignifiant	Marginal	Critique	Catastrophique
	Niveaux de gravité des conséquences du danger (c'est-à-dire de l'accident)			

Évaluation des risques	**Réduction/contrôle des risques**
Intolérable	Le risque doit être éliminé.
Acceptable	Le risque est acceptable. Une évaluation indépendante est requise.

(d) une fois la matrice complétée, elle peut également être appliquée aux dangers non catastrophiques. Si par exemple une autre défaillance fonctionnelle présente une gravité classée comme «critique», selon la matrice de risques calibrée, la fréquence tolérable d'accidents devrait être inférieure ou égale à «improbable».

(e) il convient de noter que l'utilisation de la matrice de risques peut donner des résultats exagérément prudents lorsque l'on applique des fréquences de défaillances fonctionnelles (c'est-à-dire pour des défaillances fonctionnelles qui ne provoquent pas directement d'accidents).

A.3.6.4. Principe de calibrage d'autres méthodes d'analyse des risques

D'autres méthodes d'analyse des risques, par exemple le mécanisme proposé de numéro de priorité des risques ou le graphique de risques de VDV 331 ou d'IEC 61508, peuvent

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

également être calibrées selon des procédures semblables à celle décrite pour la matrice de risques:

(a) première étape: classifier le point de référence du CAR-ST comme tolérable et les points présentant une fréquence ou une gravité supérieure comme un CAR-ST intolérable.
(b) deuxième étape: utiliser les mécanismes de compromis de la méthode concernée pour extrapoler la tolérabilité des risques aux dangers non catastrophiques (en utilisant comme point de départ un compromis de risque linéaire).
(c) troisième étape: pour les dangers non catastrophiques, le CAR-ST peut ensuite être dérivé de la méthode calibrée d'analyse des risques en comparant la coordonnée (fréquence, gravité) à la courbe FN ainsi obtenue.

A.3.7. Conclusions relatives au CAR-ST

A.3.7.1. Dans le cadre général d'appréciation des risques proposé par le MSC, les critères d'acceptation des risques sont nécessaires pour déterminer quand le niveau de risque(s) résiduel devient acceptable et donc quand on peut mettre fin à l'estimation des risques explicites.

A.3.7.2. Le CAR-ST est un objectif de conception ($10^{-9}\,h^{-1}$) pour les systèmes techniques.

A.3.7.3. Les finalités premières du CAR-ST sont:

(a) de spécifier une limite supérieure d'acceptabilité des risques et par conséquent un point de référence sur la base duquel les méthodes d'analyse des risques pour les systèmes techniques peuvent être calibrées.
(b) de permettre la reconnaissance mutuelle des systèmes techniques, puisque les évaluations de sécurité et des risques associés seront appréciées sur la base du même critère d'acceptation des risques dans tous les EM;
(c) de réduire les coûts, dans la mesure où il ne nécessite pas d'exigences de sécurité quantitatives inutilement élevées;
(d) de faciliter la concurrence entre les constructeurs. L'utilisation de différents critères d'acceptation des risques en fonction du proposant ou de l'État membre obligerait le secteur à effectuer de nombreuses démonstrations différentes sur les mêmes systèmes techniques. Ceci mettrait en danger la compétitivité des constructeurs et augmenterait inutilement le prix des produits.

A.3.7.4. L'exigence semi-quantitative contenue dans le CAR-ST n'a pas toujours à être démontrée pour les systèmes techniques. En effet, dans le cadre de la MSC, le CAR-ST ne doit être appliqué qu'aux systèmes techniques dont les dangers identifiés ne peuvent pas être maîtrisés adéquatement par l'utilisation de codes de pratique ni par comparaison avec des systèmes de référence. Ceci permet de définir des exigences de sécurité moins élevées pour autant que le niveau de sécurité global soit maintenu.

A.3.7.5. Un critère semi-quantitatif harmonisé d'acceptation des risques pour les systèmes techniques n'est nécessaire que lorsqu'il n'existe aucun code de pratique et aucun système de référence.

A.3.7.6. Étant donné que le niveau d'intégrité de sécurité pour les défaillances/erreurs systématiques est limité à SIL 4, le niveau d'intégrité de sécurité pour les défaillances matérielles aléatoires des systèmes techniques doit également être limité à SIL 4. Ceci correspond à un taux de danger maximal tolérable (THR) de $10^{-9}\,h^{-1}$ (soit le taux de défaillance maximal). Selon la norme CENELEC 50 129, si des exigences de sécurité plus strictes sont nécessaires, un seul système ne peut y parvenir; l'architecture du système doit être modifiée, par exemple en

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

utilisant deux systèmes, ce qui augmente inévitablement de façon considérable le coût du système technique. Pour plus de détails, voir la section A.3.1. de l'appendice A.

A.3.7.7. Enfin, la section A.3.6. de l'appendice A montre comment le CAR-ST peut être utilisé comme point de référence pour calibrer des méthodes particulières de matrice de risques lorsque les systèmes techniques présentent un potentiel de conséquences non catastrophiques.

A.4. Preuve de l'évaluation de sécurité

A.4.1. Cette section décrit les preuves généralement fournies à l'organisme d'évaluation afin de permettre l'évaluation indépendante et l'acceptation de sécurité sans préjudice des exigences nationales d'un État membre. Elle peut être utilisée comme une liste de contrôle pour vérifier que tous les aspects associés sont couverts et documentés si nécessaire pendant l'application de la MSC.

A.4.2. Plan de sécurité: CENELEC recommande de créer un plan de sécurité en début de projet ou, si le projet ne s'y prête pas, d'inclure la description correspondante dans tout autre document pertinent. Si des organismes d'évaluation sont désignés en début de projet, le plan de sécurité peut également leur être soumis pour avis. En principe, le plan de sécurité décrit:

(a) l'organisation mise en place et les compétences des personnes impliquées dans le développement et dans l'appréciation des risques;
(b) toutes les activités de sécurité prévues lors des différentes phases du projet ainsi que les résultats attendus;

A.4.3. Preuves requises lors de la phase de définition du système:

(a) description du système:
    (1) définition de la portée / des limites du système;
    (2) description des fonctions;
    (3) description de la structure du système;
    (4) description des conditions opérationnelles et environnementales;
(b) description des interfaces externes;
(c) description des interfaces internes;
(d) description des phases du cycle de vie;
(e) description des principes de sécurité;
(f) description des hypothèses qui déterminent les limites de l'appréciation des risques;

A.4.4. Pour permettre l'appréciation des risques, le contexte du changement prévu est pris en compte dans la définition du système:

(a) si la modification prévue constitue une modification d'un système existant, la définition du système décrit le système avant le changement ainsi que le changement prévu:
(b) si la modification prévue est la construction d'un nouveau système, cette description se limite à la définition du système dans la mesure où il n'y a aucune description de système existant.

A.4.5. Preuves requises lors de la phase d'identification des dangers:

(a) description et justification (y compris les restrictions) des méthodes et outils d'identification des dangers (méthode de haut en bas, de bas en haut, HAZOP, etc.);
(b) résultats:
    (1) liste des dangers:
    (2) dangers du système (et de ses limites);

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) dangers des sous-systèmes;
(4) dangers aux interfaces;
(5) les mesures de sécurité susceptibles d'être identifiée au cours de cette phase;

A.4.6. Les preuves suivantes sont également requises depuis la phase d'analyse des risques:

(a) lorsque des codes de pratique sont utilisés pour maîtriser les dangers, démonstration que toutes les exigences pertinentes des codes de pratique sont respectées pour le système évalué. Ceci inclut la démonstration de l'application correcte de tous les codes de pratique concernés;

(b) lorsque des systèmes de référence similaires sont utilisés pour la maîtrise des dangers:

(1) définition, pour le système évalué, des exigences de sécurité des systèmes de référence pertinents;
(2) démonstration que le système évalué est utilisé dans des conditions fonctionnelles, opérationnelles et environnementales similaires à celles du système de référence. Si cela n'est pas possible, démonstration que les déviations par rapport au système de référence sont évaluées correctement;
(3) preuve que les exigences de sécurité des systèmes de référence ont été mises en œuvre correctement dans le système évalué;

(c) lorsqu'une estimation des risques explicites est utilisée pour la maîtrise des dangers:

(1) description et justification (y compris les restrictions) des méthodes et outils d'analyse des risques (analyse qualitative, quantitative, semi-quantitative, de non-régression...);
(2) identification des mesures de sécurité existantes et des facteurs de réduction des risques pour chaque danger (y compris les facteurs humains);
(3) évaluation et classement du risque pour chaque danger:

(i) estimation des conséquences du danger et justification (avec hypothèse et conditions);
(ii) estimation de la fréquence du danger et justification (avec hypothèse et conditions);
(iii) classement des dangers selon leur gravité et leur fréquence de survenance;

(4) identification de mesures de sécurité appropriées supplémentaires permettant d'obtenir des risques acceptables pour chaque danger (processus itératif après la phase d'évaluation des risques);

A.4.7. Preuves requises de l'évaluation des risques:

(a) en cas d'estimation des risques explicites:

(1) définition et justification des critères d'évaluation des risques pour chaque danger;
(2) démonstration/justification que les mesures de sécurité et les exigences de sécurité couvrent chaque danger à un niveau acceptable (sur la base du critère d'évaluation des risques ci-dessus);

(b) selon les sections 2.3.5 et 2.4.3, du règlement MSC, les risques couverts par l'application de codes de pratique et par comparaison à des systèmes de référence sont considérés implicitement comme acceptables si, respectivement (voir le cercle en pointillé de la Figure 1):

(1) les conditions d'application des codes de pratique de la section 2.3.2 sont respectées;
(2) les conditions d'utilisation d'un système de référence de la section 2.4.2 sont respectées;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

Les critères d'acceptation des risques sont implicites pour ces deux principes d'acceptation des risques.

A.4.8. Preuves de la gestion des dangers:

(a) enregistrement de tous les dangers dans un registre des dangers contenant les éléments suivants:

(1) danger identifié;
(2) mesures de sécurité empêchant la survenance du danger ou atténuant ses conséquences;
(3) exigences de sécurité des mesures;
(4) partie concernée du système;
(5) acteur responsable des mesures de sécurité;
(6) état du danger (par ex. ouvert, résolu, supprimé, transféré, maîtrisé, etc.);
(7) date d'enregistrement, de réexamen et de maîtrise de chaque danger;

(b) description de la façon dont les dangers seront gérés efficacement pendant toute la durée du cycle de vie;
(c) description des échanges d'informations entre les parties pour les dangers aux interfaces et attribution des responsabilités.

A.4.9. Preuves liées à la qualité du processus d'évaluation et d'appréciation des risques:

(a) description des personnes impliquées dans le processus et de leurs compétences;
(b) pour les estimations de risques explicites, description des informations, des données et d'autres statistiques utilisées dans le processus et justification de leur adéquation (par ex. étude de sensibilité sur les données utilisées).

A.4.10. Preuve de la conformité aux exigences de sécurité:

(a) liste des normes utilisées;
(b) description de la conception des principes opérationnels;
(c) preuve de l'application d'un bon système de gestion de la qualité et de la sécurité pour le projet: voir le point (b) de la section 1.1.2;
(d) résumé des rapports d'analyses de sécurité (par ex. analyse de cause des dangers) démontrant le respect des exigences de sécurité;
(e) description et justification des méthodes et outils (FMECA, FTA...) utilisés pour l'analyse de la cause des dangers;
(f) synthèse des tests de vérification et de validation de sécurité.

A.4.11. Dossier de sécurité: CENELEC recommande de regrouper toutes les preuves susmentionnées et de les synthétiser dans un document soumis à l'organisme d'évaluation: voir les points [G 3] et [G 3] de la section 5.1.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

APPENDICE B: EXEMPLES DE TECHNIQUES ET D'OUTILS D'AIDE AU PROCESSUS D'APPRÉCIATION DES RISQUES

B.1. L'annexe E du guide EN 50 126-2 {Ref. 9} fournit des exemples de techniques et d'outils destinés aux activités d'appréciation des risques couvertes par la MSC. Le tableau E.1 présente une synthèse des techniques et des outils. Chaque technique est décrite et, si nécessaire, une référence à d'autres normes est donnée pour de plus amples informations.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

APPENDICE C: EXEMPLES

C.1. Introduction

C.1.1. L'objectif de cet appendice est de faciliter la lecture du présent document. Il regroupe tous les exemples rassemblés dans le but de faciliter l'application de la MSC.

C.1.2. Les exemples d'appréciations des risques donnés dans cet appendice ne résultent pas de l'application du processus MSC, dans la mesure où elles ont eu lieu avant la création du règlement MSC. Ces exemples peuvent être classés dans les catégories suivantes:

(a) exemples fournis par les experts du groupe de travail MSC avec référence d'origine;
(b) exemples fournis par les experts du groupe de travail MSC en omettant intentionnellement la référence d'origine. Les experts concernés ont demandé à ce que l'origine reste confidentielle;
(c) exemples dont l'origine n'est pas mentionnée et qui ont été produits par des membres du personnel de l'Agence sur la base de leur propre expérience professionnelle antérieure.

Chaque exemple établit la correspondance entre le processus appliqué et le processus requis par la MSC et fournit l'argumentation et la valeur ajoutée de la réalisation des étapes supplémentaires (le cas échéant) requises par la MSC.

C.2. Exemples d'application des critères relatifs aux changements significatifs selon l'article 4, paragraphe 2

C.2.1. L'Agence travaille à la définition de ce qui peut être considéré comme un «changement significatif». Cette section consacrée à la façon d'appliquer les critères de l'Article 4 (2) donne un exemple de ce travail.

C.2.2. Le changement consiste à modifier, pour un passage à niveau à commande manuelle, la façon dont les garde-signaux communiquent à l'opérateur du passage à niveau la direction d'un train en approche. Ce changement est illustré par la Figure 15.

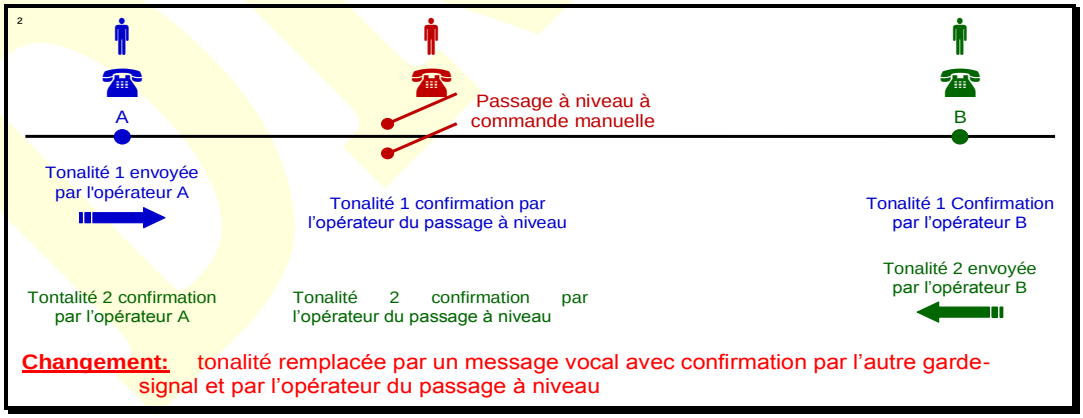


Figure 15: Exemple de changement non significatif
Message téléphonique pour le contrôle d'un passage à niveau.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.2.3. Système existant: avant le changement prévu, les informations relatives à la direction d'un train en approche étaient indiquées automatiquement à l'opérateur du passage à niveau par la sonnerie du téléphone. La tonalité variait en fonction de l'origine de l'appel.

C.2.4. Changement prévu: étant donné que l'ancien système téléphonique est devenu obsolète et doit être remplacé par un système numérique, il n'est techniquement plus possible d'intégrer les informations pertinentes à la sonnerie. La tonalité est exactement la même quel que soit le garde-signal qui passe l'appel. Il a donc été décidé de remplacer cette fonction par une procédure opérationnelle:

(a) lors du départ du train, le garde-signal informe oralement l'opérateur du passage à niveau de la direction du train en approche;
(b) l'information est vérifiée par rapport aux horaires et confirmée à la fois par l'opérateur du passage à niveau et par l'autre garde-signal afin d'éviter tout malentendu dans le chef de l'opérateur.

Le changement prévu et la procédure opérationnelle associée sont illustrés à la Figure 15.

C.2.5. Bien que le changement semble avoir un impact potentiel sur la sécurité (risque de ne pas baisser la barrière du passage à niveau à temps), d'autres critères de l'Article 4 (2) tels que:

(a) la faible complexité;
(b) le manque d'innovation et
(c) la facilité de suivi

suggèrent que le changement prévu n'est pas significatif.

C.2.6. Dans cet exemple, une analyse ou un argument de sécurité est de toute façon nécessaire pour montrer que, pour cette tâche critique en matière de sécurité, le remplacement d'un ancien système technique par une procédure opérationnelle (avec contrôle mutuel d'acteurs humains) permettrait de maintenir un niveau de sécurité similaire. La question est de savoir si cela nécessiterait l'application du processus MSC complet, avec registre des dangers, évaluation indépendante par un organisme d'évaluation, etc. Dans ce cas, il est douteux que ce processus apporte une valeur ajoutée quelconque, ce qui implique que ce changement ne serait pas considéré comme significatif.

C.3. Exemples d'interfaces entre acteurs du secteur ferroviaire

C.3.1. Ci-dessous quelques exemples d'interfaces et les raisons de coopération entre différents acteurs du secteur ferroviaire:

(a) GI -- GI: par exemple, les deux infrastructures doivent prévoir des mesures de sécurité afin de garantir la transition en toute sécurité des trains d'une infrastructure à l'autre;

(b) GI -- EF: par exemple, il pourrait y avoir des règles opérationnelles spécifiques dépendant de l'infrastructure et que le conducteur du train doit respecter;

(c) GI – constructeur: par exemple, les sous-systèmes du constructeur pourraient s'accompagner de restrictions d'utilisation à respecter par le GI;

(d) GI – prestataire de service: par exemple, il pourrait y avoir des contraintes spécifiques de maintenance de l'infrastructure à respecter par le sous-traitant chargé des activités de maintenance;

(e) EF – constructeur: par exemple, les sous-systèmes du constructeur pourraient s'accompagner de restrictions d'utilisation à respecter par l'EF;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(f) EF – prestataire de services: par exemple, il pourrait y avoir des contraintes spécifiques de maintenance de l'infrastructure à respecter par le sous-traitant chargé des activités de maintenance;

(g) EF – détenteurs: par exemple, il pourrait exister des restrictions d'utilisation spécifiques aux véhicules à respecter par l'entreprise ferroviaire qui exploite ces véhicules;

(h) Constructeur – constructeur: par exemple, la gestion d'interfaces techniques liées à la sécurité entre sous-systèmes provenant de deux constructeurs différents;

(i) Constructeur – prestataire de services: par exemple, la gestion par le constructeur du registre des dangers lorsqu'il sous-traite certains travaux à une société trop petite pour posséder une organisation de sécurité dédiée sur le projet envisagé;

(j) Prestataire de services – prestataire de services: exemple semblable au point (i) ci-dessus;

C.3.2. Les prestataires de services couvrent toutes les activités sous-traitées par l'EF, le FI ou le constructeur, comme par exemple la maintenance, le ticketing, les services techniques, etc.

C.3.3. L'exemple suivant illustre la gestion des interfaces et l'identification des dangers associés. Il envisage une interface entre un constructeur de trains et un proposant (EF). Il décrit la manière dont les principaux critères requis au point [G 2] de la section 1.2.1 peuvent être respectés:

(a) Direction: le proposant (EF);

(b) Entrées:

(1) liste(s) de dangers pertinents issus de projets similaires;
(2) description de toutes les entrées et sorties (input/output, I/O) de l'interface, y compris les caractéristiques de performances;

(c) Méthodes: voir l'appendice A.2 de la ligne directrice EN 50 126-2 {Ref. 9};

(d) Participants requis:

(1) responsable d'assurance de sécurité de l'EF;
(1) responsable d'assurance de sécurité du constructeur de trains;
(2) autorité de conception du proposant;
(3) autorité de conception du constructeur de trains;
(4) personnel de maintenance du proposant (déterminé en partie par les I/O analysées);
(5) conducteurs de trains (déterminé en partie par les I/O analysées);

(e) Sorties:

(1) rapport d'identification des dangers défini conjointement;
(2) mesures de sécurité pour le registre des dangers avec une description claire des responsabilités.

C.4. Exemples de méthodes pour la définition des risques largement acceptables

C.4.1. Introduction

C.4.1.1. Le règlement MSC définit les risques largement acceptables comme des risques *«tellement faible[s] qu'il n'est pas raisonnable de mettre en œuvre des mesures de sécurité supplémentaires».* Dans l'identification des dangers, la classification de certains dangers comme étant associés à des risques largement acceptables permet de ne pas poursuivre

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

l'analyse de ces dangers dans le processus d'appréciation des risques. La définition des risques largement acceptables citée ci-dessus laisse toutefois une certaine marge d'interprétation. C'est pourquoi le règlement indique que la décision de classer les dangers présentant des risques largement acceptables est confiée à un avis d'expert.

C.4.1.2. Il est en effet difficile de définir de façon commune un critère plus explicite définissant les risques largement acceptables, qui s'appliquerait à tous les niveaux possibles des systèmes où ces dangers sont susceptibles d'être identifiés et qui tienne également compte des différents facteurs d'aversion aux risques qui prévalent pour différentes applications. Cependant, étant donné qu'il est important d'assurer que les avis d'experts soient facilement compréhensibles et traçables, il est utile de fournir certaines recommandations sur la façon de définir des risques comme étant largement acceptables. Les critères permettant de définir des risques largement acceptables peuvent être quantitatifs, qualitatifs ou semi-qualitatifs. Les sections ci-dessous donnent quelques exemples de la façon de définir des critères permettant l'évaluation de risques largement acceptables d'une façon quantitative ou semi-quantitative.

C.4.1.3. Les exemples ci-dessous illustrent ce principe. Ils sont issus de l'article *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Définition d'un critère quantitatif

C.4.2.1. On pourrait définir les risques largement acceptables comme des risques nettement inférieurs au risque acceptable pour une classe de dangers donnée. Sur la base de données statistiques, il est possible de calculer le niveau de risque actuel des systèmes ferroviaires et donc de déclarer le niveau ainsi calculé comme acceptable. En divisant ce niveau de risque par le nombre (N) de dangers (par exemple, on pourrait considérer arbitrairement qu'il existe environ N = 100 catégories principales de dangers dans le système ferroviaire), on obtient le niveau de risque acceptable par catégorie de danger. On pourrait ensuite déclarer qu'un danger associé à un risque inférieur de deux ordres de grandeur au niveau de risque acceptable par danger (le paramètre x % du point [G 1] de la section 2.2.3) serait considéré comme un risque largement acceptable.

C.4.2.2. Il faudra toutefois vérifier que la contribution de tous les dangers associés à des risques largement acceptables dépasse une certaine proportion (par ex. y %) du risque global au niveau du système: voir la section 2.2.3 et l'explication au point [G 2] de la section 2.2.3.

C.4.3. Évaluation des risques largement acceptables

C.4.3.1. Les valeurs limites des risques largement acceptables tels qu'ils sont définis dans les exemples ci-dessus peuvent ensuite servir à calibrer des outils qualitatifs comme une matrice des risques, un graphique des risques ou des chiffres de priorité des risques afin d'aider l'expert à prendre sa décision de classifier le risque comme largement acceptable. Il est important de souligner que le fait d'avoir des valeurs quantitatives comme critères pour les risques largement acceptables n'implique pas qu'il soit nécessaire de faire une estimation ou une analyse précise des risques afin de décider si un risque est largement acceptable. C'est ici que le jugement de l'expert intervient afin de faire cette estimation lors de la phase d'identification des dangers.

C.4.3.2. Il est également important de vérifier que la contribution de tous les dangers associés à des risques largement acceptables dépasse une certaine proportion (par ex. y %) du risque

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

global au niveau du système: voir la section 2.2.3 et l'explication au point [G 2] de la section 2.2.3.

C.5. Exemple d'appréciation des risques pour un changement organisationnel significatif

C.5.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.5.2. Cet exemple concerne un changement organisationnel. Le proposant concerné l'a considéré comme significatif. Ce changement a été évalué au moyen d'une approche basée sur l'appréciation des risques.

C.5.3. Une filiale de l'organisation du gestionnaire d'infrastructure chargée avant le changement d'effectuer certaines activités de maintenance (autres que la signalisation et la télématique) a dû être mise en concurrence avec d'autres entreprises actives dans le même secteur. L'impact direct fut la nécessité de réduire et de réorganiser le personnel et les tâches au sein de la filiale du GI mise en compétition.

C.5.4. Préoccupations pour le gestionnaire d'infrastructure concerné:

(a) le personnel du GI touché par le changement était chargé des opérations de maintenance et de réparation d'urgence en cas d'erreurs soudaines dans l'infrastructure. Ce personnel était également chargé de certaines activités de maintenance planifiées ou à base de projets comme le garnissage de voie, le nettoyage du ballast et le contrôle de la végétation;
(b) ces tâches étaient considérées critiques pour la sécurité et la ponctualité des opérations. Il a donc fallu les analyser afin de trouver les mesures correctes permettant d'éviter que la situation ne se détériore, étant donné que de nombreuses personnes chargées des questions de sécurité quittent l'organisation du GI;
(c) le même niveau de sécurité et de ponctualité devait être maintenu pendant et après le changement apporté à l'organisation.

C.5.5. Par comparaison au processus MSC, les étapes suivantes ont été suivies (voir également Figure 1):

(a) description du système [section 2.1.2]:
    (1) description des tâches effectuées par l'organisation existante (c'est-à-dire par l'organisation du GI avant le changement);
    (2) description des modifications prévues dans l'organisation du GI;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) les interfaces de la «filiale à détacher» avec les organisations avoisinantes ou avec l'environnement physique n'ont pu être décrites que brièvement. Les limites n'ont pas pu être définies clairement à 100 %;

(b) identification des dangers [section 2.2]:

(1) brainstorming par un groupe d'experts:

(i) afin d'identifier tous les dangers provoqués par le changement organisationnel prévu et ayant une incidence sur le risque;
(ii) afin d'identifier les actions possibles pour maîtriser le risque;

(2) classification des dangers:

(i) en fonction de la gravité du risque associé: risque important, modéré, faible;
(ii) en fonction de l'impact du changement: augmentation ou réduction du risque, risque inchangé;

(c) utilisation d'un système de référence [section 2.4]:

Le système antérieur au changement a été considéré comme ayant un niveau de sécurité acceptable. Il a donc servi de «système de référence» afin de dériver les critères d'acceptation des risques (CAR) pour la modification de l'organisation;

(d) estimation et appréciation des risques explicites [section 2.5]:

Pour chaque danger présentant des risques accrus suite à la modification de l'organisation, des mesures de réduction des risques ont été identifiées. Le risque résiduel est comparé aux CAR du système de référence afin de vérifier la nécessité d'identifier des mesures supplémentaires;

(e) démonstration de la conformité du système aux exigences de sécurité [section 3]:

(1) l'analyse des risques et le registre des dangers montrent que les dangers ne peuvent pas être maîtrisés tant qu'ils n'ont pas été vérifiés et qu'il n'a pas été prouvé que les exigences de sécurité (c'est-à-dire les mesures de sécurité sélectionnées) ont été mises en œuvre;
(2) l'analyse des risques et le registre des dangers étaient des documents vivants. L'efficacité des actions décidées a été vérifiée à intervalles réguliers afin de vérifier si les conditions avaient changé et si l'analyse des risques et l'évaluation des risques devaient être mise à jour;
(3) si les mesures implémentées n'étaient pas suffisamment efficaces, l'analyse des risques, l'appréciation des risques et le registre des dangers ont été mis à jour et contrôlés à nouveau;

(f) gestion des dangers [section 4.1]:

Les dangers identifiés et les mesures de sécurité ont été enregistrés et gérés dans un registre des dangers. L'une des conclusions de l'exemple fut de mettre à jour en continu l'analyse des risques et le registre des dangers lorsque des décisions et des actions étaient prises pendant le changement de l'organisation. L'analyse des risques couvrait également le risque aux interfaces, par exemple avec les sous-traitants.

La section C.16.2 de l'appendice C précise la structure et les champs utilisés pour le registre des dangers ainsi qu'un extrait de quelques lignes.

(g) évaluation indépendante [Article 6]:

Une évaluation indépendante a également été effectuée par une partie tierce afin:

(1) de vérifier que la gestion et l'appréciation des risques avaient été effectuées correctement;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(2) de vérifier que le changement organisationnel était adéquat et qu'il permettrait de maintenir un niveau de sécurité identique à celui antérieur au changement.

C.5.6. Cet exemple montre que les principes requis par la méthode de sécurité commune existent déjà dans le secteur ferroviaire et qu'ils sont déjà appliqués pour évaluer les risques liés aux changements organisationnels. L'appréciation des risques décrite dans cet exemple remplit toutes les exigences de la MSC. Elle utilise deux des trois principes d'appréciation des risques permis par l'approche harmonisée de la MSC:

(a) un «système de référence» est utilisé pour définir les critères d'acceptation des risques nécessaires pour évaluer l'acceptation des risques du changement organisationnel;
(b) «estimation et appréciation des risques explicites»:

(1) pour analyser les déviations du changement par rapport au système de référence;
(2) pour identifier les mesures de réduction des risques face aux risques accrus engendrés par le changement;
(3) pour évaluer si un niveau de risque acceptable a été atteint.

C.6. Exemple d'appréciation des risques pour un changement opérationnel significatif – modification des temps de conduite

C.6.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.6.2. Cet exemple concerne un changement opérationnel par lequel l'entreprise ferroviaire souhaitait attribuer de nouveaux itinéraires et, potentiellement, de nouveaux horaires de travail (y compris des rotations et des systèmes de pause) à ses conducteurs.

C.6.3. Par comparaison au processus MSC, les étapes suivantes ont été suivies (voir également Figure 1):

(a) Importance du changement [Article 4]:

L'entreprise ferroviaire a réalisé une appréciation des risques préliminaire qui a conclu que le changement opérationnel était significatif. Étant donné que les conducteur allaient devoir suivre de nouveaux tracés, parfois en dehors de leurs heures de travail habituelle, il y avait un risque réel qu'ils passent des signaux de danger, qu'ils roulent trop vite ou qu'ils ignorent les limitations de vitesse provisoires.

En comparant cette appréciation des risques préliminaire aux critères de l'Article 4 (2) du règlement MSC, le changement peut également être catégorisé comme significatif sur la base des critères suivants:

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(1) lien avec la sécurité: le changement est lié à la sécurité dans la mesure où la modification de la façon de travailler des conducteurs peut avoir un impact catastrophique;
(2) conséquence d'une défaillance: les erreurs dans le chef des conducteurs mentionnées ci-dessus peuvent éventuellement avoir des conséquences catastrophiques;
(3) nouveauté: l'EF peut potentiellement instaurer de nouvelles façons de travailler pour les conducteurs;
(4) complexité du changement: la modification des heures de conduite pourrait être complexe dans la mesure où elle nécessite une évaluation et une modification complète des conditions de travail existantes;

(b) définition du système [section 2.1.2]:

La définition du système décrivait initialement:

(1) les conditions de travail existantes: horaires de travail, organisation des équipes, etc;
(2) la modification des horaires de travail;
(3) les problèmes d'interface (par ex. avec le gestionnaire d'infrastructure)

Au cours des différentes itérations, la définition du système a été mise à jour sur la base des exigences de sécurité découlant du processus d'appréciation des risques. Des représentants essentiels du personnel ont été impliqués dans ce processus itératif pour l'identification des dangers et la mise à jour de la définition du système.

(c) identification des dangers [section 2.2]:

Les dangers et les mesures de sécurité possibles ont été identifiés en organisant un brainstorming par un groupe d'experts comprenant des représentants des conducteurs, pour les nouvelles routes et les nouvelles pauses. Les tâches des conducteurs dans les nouvelles conditions ont été analysées afin d'évaluer si elles avaient un impact sur les conducteurs, leur charge de travail, l'étendue géographique et les horaires du système de travail par équipes.
L'EF a également consulté les syndicats de travailleurs pour voir s'ils pouvaient fournir des informations complémentaires et a examiné le risque de fatigue et de maladie susceptible d'être provoqué par une augmentation possible des heures supplémentaires suite à des trajets prolongés sur des routes inconnues.
Chacun de ces dangers a reçu un niveau de gravité des risques et des conséquences (élevé, modéré, faible) et l'impact du changement proposé a été examiné par rapport à ce niveau (augmentation, réduction, pas de changement du risque).

(d) utilisation de codes de pratique [section 2.3]:

Des codes de pratique relatifs aux heures de travail et aux risques de fatigue humaine ont été utilisés afin de réviser les conditions de travail existantes et de définir les nouvelles exigences de sécurité. Les règles opérationnelles nécessaires ont été écrites sur la base des codes de pratique du nouveau système d'équipes. Toutes les parties nécessaires ont été impliquées dans les procédures opérationnelles révisées et dans l'accord de procéder au changement.

(e) démonstration de la conformité du système aux exigences de sécurité [section 3]:

Les procédures opérationnelles révisées ont été introduites dans le système de gestion de la sécurité de l'EF. Elles ont été contrôlées, et un processus de réexamen a été mis en place afin de veiller à ce que les dangers identifiés continuent à être maîtrisés correctement durant l'exploitation du système ferroviaire.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(f) gestion des dangers [section 4.1]:

Voir le point ci-dessus, étant donné que pour les entreprises ferroviaires, le processus de gestion des dangers peut faire partie de leur système de gestion de la sécurité pour l'enregistrement et la gestion des risques. Les dangers identifiés ont été enregistrés dans un registre de dangers avec les exigences de sécurité (référence aux procédures opérationnelles révisées) maîtrisant le risque associé.
Les procédures révisées ont été contrôlées et réexaminées si nécessaire afin de veiller à ce que les dangers identifiés continuent à être maîtrisés correctement durant l'exploitation du système ferroviaire.

(g) évaluation indépendante [Article 6]:

Les processus d'appréciation et de gestion des risques ont été évalués par une personne compétente au sein de la société de l'EF qui était indépendante du processus d'appréciation. Cette personne compétente a évalué tant le processus que les résultats, c'est-à-dire les exigences de sécurité identifiées.

L'EF a fondé sa décision de mettre en œuvre le nouveau système sur le rapport d'évaluation indépendante produit par cette personne compétente.

C.6.4. L'exemple montre que les principes et les processus utilisés par l'entreprise ferroviaire sont conformes à la méthode de sécurité commune. Le processus de gestion et d'appréciation des risques respectait toutes les exigences de la MSC.

C.7. Exemple d'appréciation des risques pour un changement technique significatif (SCC)

C.7.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.7.2. Cet exemple concerne une modification technique du système de contrôle-commande. Le constructeur concerné l'a considéré comme significatif. Ce changement a été évalué au moyen d'une approche basée sur l'appréciation des risques.

C.7.3. Description du changement: le changement consiste à remplacer une boucle de voie située devant un signal par un sous-système «radio+GSM» (voir Figure 16).

C.7.4. Préoccupation: maintenir le niveau de sécurité du système après le changement.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

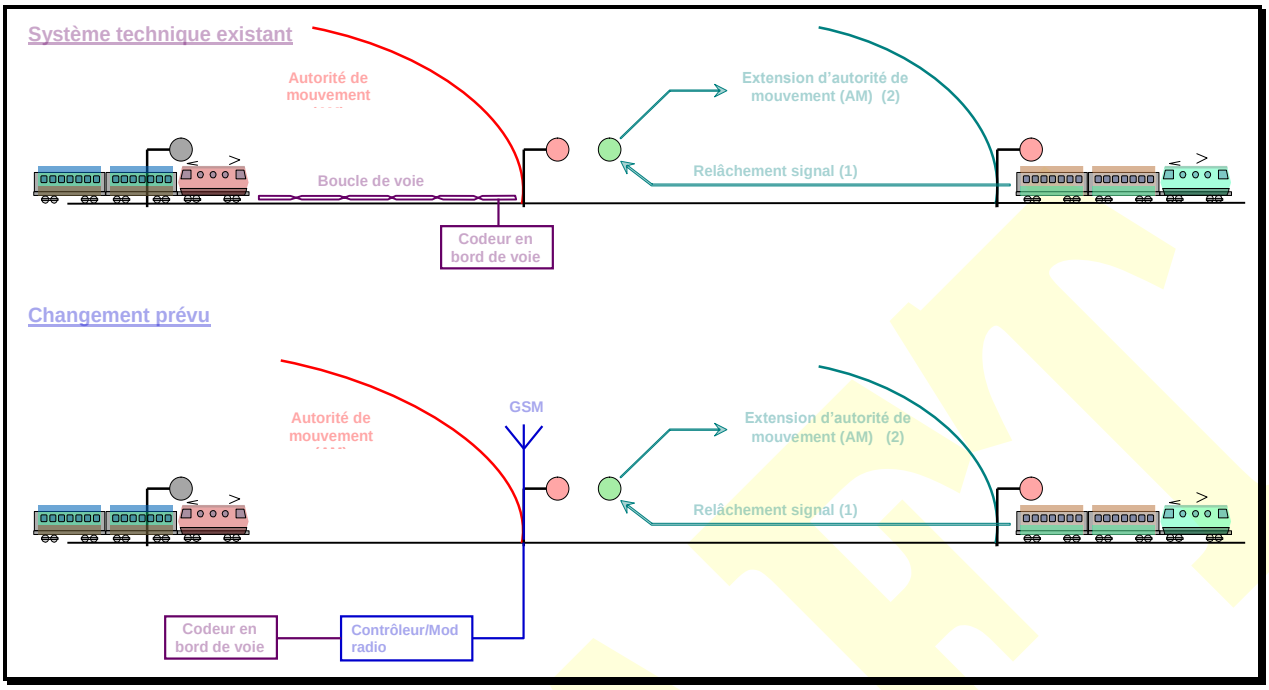


Figure 16: Remplacement d'une boucle de voie par un système radio.

C.7.5. Par comparaison au processus MSC, les étapes suivantes ont été suivies (voir également Figure 1):

(a) évaluation de l'importance du changement [Article 4]

Les critères de l'Article 4 (2) sont utilisés pour évaluer l'importance du changement. Les critères de complexité et de nouveauté sont utilisés principalement pour déterminer si le changement est significatif.

(b) description du système [section 2.1.2]:

(1) description du système existant: boucle et ses fonctions dans le système de contrôle-commande;
(2) description du changement prévu par le proposant et le constructeur;
(3) description des interfaces fonctionnelles et physiques de la boucle avec le reste du système;

La fonction du composant «boucle+codeur» dans le système existant est de libérer le signal à l'approche d'un train lorsque la section derrière le signal (c'est-à-dire devant le train en approche) devient inoccupée: voir la Figure 16.

(c) identification des dangers [section 2.2]:

Le processus itératif d'appréciation des risques et d'identification des dangers (voir section 2.1.1) est appliqué sur la base du brainstorming d'un groupe d'experts afin:

(1) d'identifier les dangers provoqués par le changement prévu et ayant une incidence sur le risque;
(2) d'identifier les actions possibles pour maîtriser le risque;

Étant donné que la boucle, et donc le signal radio, libère le signal, il existe un risque de donner une autorité de mouvement non sûre au train en approche alors que le train

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

précédent occupe encore la section en face du signal. Ce risque doit être maîtrisé à un niveau acceptable.

(d) utilisation d'un système de référence [section 2.4]:

Le système antérieur au changement (boucle) est considéré comme ayant un niveau de sécurité acceptable. Il sert donc de «système de référence» afin de dériver les exigences de sécurité pour le sous-système radio.

(e) estimation et appréciation des risques explicites [section 2.5]:

(1) les différences entre les systèmes à «boucle» et à «signal radio + GSM» sont analysées au moyen d'une estimation et d'une appréciation des risques explicites. Les dangers suivants sont identifiés pour le sous-système «signal radio + GSM»:

(i) transmission par des pirates informatiques d'informations non sûres par l'entrefer, puisque le sous-système «signal radio + GSM» est basé sur des transmissions ouvertes;
(ii) retard de transmission ou transmission de paquets de données mémorisés dans l'entrefer;

(2) estimation des risques explicites et utilisation du CAR-ST pour le contrôleur radio;

(f) utilisation de codes de pratique [section 2.3]:

(1) la norme EN 50 129-2 (*«Applications ferroviaires: Partie 2: communications de sécurité dans les systèmes de transmission ouverts»)* fournit les exigences de sécurité nécessaires pour maîtriser les nouveaux dangers à un niveau acceptable, par ex.:

(i) cryptage et protection des données;
(ii) séquencement des messages et enregistrement de l'heure;

(2) utilisation, par exemple, de la norme EN 50 128 pour le développement logiciel du contrôleur de signal radio;

(g) démonstration de la conformité du système aux exigences de sécurité [section 3]:

(1) suivi de la mise en œuvre des exigences de sécurité par le processus de développement du sous-système «radio+GSM»;
(2) vérification que le système, tel qu'il a été conçu et installé, est conforme aux exigences de sécurité;

(h) gestion des dangers [section 4.1]:

Les dangers identifiés, les mesures de sécurité et les exigences de sécurité qui en résultent issues de l'appréciation des risques et de l'application des trois principes d'acceptation des risques sont enregistrés et gérés dans un registre des dangers;

(i) évaluation indépendante [Article 6]:

Une évaluation indépendante est également effectuée par une partie tierce afin:

(1) de vérifier que la gestion et l'appréciation des risques ont été effectuées correctement;
(2) de vérifier que le changement technique est adéquat et qu'il permet de maintenir un niveau de sécurité identique à celui antérieur au changement.

C.7.6. Cet exemple montre que les trois principes d'acceptation des risques requis par la méthode de sécurité commune sont utilisés de façon complémentaire pour définir les exigences de sécurité du système évalué. L'appréciation des risques de l'exemple respecte toutes les exigences pour la MSC synthétisées à la Figure 1, y compris la gestion du registre des dangers et l'évaluation de sécurité indépendante effectuée par un tiers.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.8. Exemple de la ligne directrice suédoise BVH 585.30 pour l'appréciation des risques des tunnels ferroviaires

C.8.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.8.2. L'objectif de cet exemple est de comparer le processus de la MSC avec la ligne directrice BVH 585.30 utilisée par le gestionnaire d'infrastructure suédois Banverket pour concevoir et vérifier la réalisation d'un niveau de sécurité suffisant dans la planification et la construction de nouveaux tunnels ferroviaires. Les points communs et les différences par rapport à la MSC sont énumérés ci-dessous; les exigences détaillées en matière d'appréciation des risques sont fournis par la ligne directrice BVH 585.30.

C.8.3. Par comparaison au processus de la MSC illustré à la Figure 1:

(a) la ligne directrice BVH 585.30 présente les points communs suivants:

(1) description du système [section 2.1.2]:

La ligne directrice requiert une description détaillée du système comprenant:

(i) une description du tunnel;
(ii) une description de la voie;
(iii) une description du type de matériel roulant (y compris personnel à bord);
(iv) une description du trafic et des opérations prévues;
(v) une description de l'aide extérieure (y compris les services de secours);

(2) identification des dangers [section 2.2]:

La ligne directrice ne requiert pas explicitement une identification des dangers. Elle requiert l'identification des risques et un «catalogue des accidents» reprenant les types d'accidents potentiels identifiés dont on pense qu'ils ont un impact significatif sur le niveau de risque du tunnel et qui doivent être couverts par l'évaluation ultérieure. Exemples d'accidents:

(i) déraillement d'un train de passagers;
(ii) déraillement d'un train de marchandises;
(iii) accident impliquant des marchandises dangereuses;
(iv) incendie dans un véhicule;
(v) collision entre un train de passagers et un objet léger/lourd;
(vi) etc.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) il n'existe pas de disposition pour l'application de codes de pratique ou de systèmes de référence similaire. Il est entendu qu'une analyse des risques doit toujours être effectuée;

(4) estimation et appréciation des risques explicites [section 2.5]:

(i) de façon générale, la ligne directrice recommande d'élaborer une arborescence d'événements complète pour chaque type d'accident sur la base d'une analyse quantitative des risques. Mais, étant donné que l'intention de l'analyse des risques est d'analyser le niveau de sécurité global plutôt que d'analyser la sécurité individuellement aux niveaux plus détaillés, les conséquences de tous les scénarios sont additionnées afin de définir le niveau de risque global du tunnel;

(ii) l'acceptabilité de ce niveau de risque global pour le tunnel doit être comparée au critère quantitatif explicite d'acceptation des risques suivant: «*le trafic ferroviaire au kilomètre parcouru dans les tunnels doit être aussi sûr que le trafic ferroviaire au kilomètre à l'air libre, à l'exception des passages à niveau*». Ce critère est traduit en une courbe FN basée sur les données historiques des accidents ferroviaires en Suède et est extrapolé pour couvrir également les conséquences qui ne sont pas présentes dans les statistiques;

(iii) outre ce critère relatif au niveau de risque global du tunnel, il convient également de respecter des exigences complémentaires relatives notamment à l'évacuation des tunnels et aux possibilités d'intervention des services de secours:

- vérifier que l'évacuation est possible en cas d'incendie dans un train pour un «pire cas crédible» (des critères sont également donnés pour cette évaluation);
- le tunnel doit être planifié pour permettre l'intervention des secours dans une série donnée de scénarios;

(5) résultat de l'appréciation des risques [section 2.1.6]:

Les résultats de l'appréciation des risques sont les suivants:

(i) une liste de mesures de sécurité de la norme minimale basée sur la STI-SRT et sur les règles nationales à respecter pour la conception des tunnels;

(ii) toutes les mesures de sécurité supplémentaires identifiées comme nécessaires par l'analyse des risques, avec mention de leur objectif. Il est indiqué que les mesures doivent être définies selon l'ordre de priorité suivant:

- prévenir les accidents;
- réduire les conséquences des accidents;
- faciliter l'évacuation;
- faciliter les efforts de sauvetage;

(6) gestion des dangers [section 4.1]:

La ligne directrice ne requiert pas explicitement la tenue d'un registre des dangers. Ceci s'explique par le fait que le niveau d'appréciation est global et que les dangers ne sont donc pas évalués et maîtrisés individuellement. L'acceptabilité du risque global du tunnel est évaluée sans répartition du critère global d'acceptation du risque entre les différents types d'accidents et les dangers sous-jacents.

Il existe cependant une liste de toutes les mesures de sécurité, tant celles résultant de la «norme minimale» que elles identifiées comme indispensables par l'analyse des risques: voir le point (a)(5)(i) ci-dessus. Il faut indiquer dans la liste des mesures de sécurité si celles-ci concernent l'infrastructure du tunnel, la voie, les opérations ou le matériel roulant, ainsi que leurs effets prévus selon la liste numérotée du point (a)(5)(i). Mais la ligne directrice n'impose pas de spécifier

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

explicitement quels dangers les mesures de sécurité maîtrisent et qui est responsable de quelles mesures.

(7) évaluation indépendante [Article 6]:

Une évaluation indépendante effectuée par une partie tierce est obligatoire pour:

(i) vérifier que le processus d'appréciation des risques recommandé par la ligne directrice BVH 585.30 a été mis en œuvre correctement;
(ii) pouvoir considérer l'analyse des risques comme acceptable;
(iii) vérifier qu'il est indiqué clairement comment la gestion future de la sécurité doit être effectuée sur le projet;

Le document final d'analyse des risques est signé par l'évaluateur indépendant ainsi que par le coordinateur de sécurité au sein du projet.

(b) la ligne directrice BVH 585.30 diffère par les aspects suivants:

(1) démonstration de la conformité du système aux exigences de sécurité [section 3]:

La ligne directrice BVH 585.30 n'exige pas de faire le suivi de la mise en œuvre des exigences de sécurité, ni de vérifier que la conception finale du tunnel respecte toutes les exigences de sécurité identifiées. Elle décrit uniquement la façon dont cette exigence doit être transférée pour garantir leur implémentation en phase de construction.

La ligne directrice prévoit les exigences de sécurité à utiliser pour vérifier que l'analyse des risques a été effectuée d'une façon adéquate et transparente et qu'elle peut être acceptée par le projet.

C.8.4. En conclusion, la comparaison avec la MSC montre que:

(a) la ligne directrice BVH 585.30 respecte les parties pertinentes de la MSC même si leur portée et leurs objectifs ne sont pas exactement identiques;
(b) la ligne directrice BVH 585.30 évalue le niveau de risque global du tunnel ferroviaire;
(c) les dangers ne sont pas maîtrisés individuellement et il y a donc une focalisation moindre sur la gestion des dangers.
(d) la démonstration de la conformité et la vérification de la mise en œuvre correcte de toutes les mesures de sécurité ne sont pas imposées explicitement. La ligne directrice précise cependant que le rôle du coordinateur de sécurité au sein du projet (un rôle et une compétence que BVH 595.30 requiert) est de vérifier que les conclusions de l'analyse des risques sont mises en œuvre dans les documents schémas de conception et de vérifier qu'elles sont mises en œuvre correctement lors de la phase de construction;

C.8.5. Les MSC sont plus générales que la ligne directrice BVH 585.30 au sens où elles proposent l'application de trois principes différents d'acceptation des risques. Cependant, l'application de la ligne directrice BVH 585.30 dans le cadre de la MSC ne pose aucun problème dans la mesure où elle est compatible avec l'utilisation du troisième principe d'estimation des risques explicites.

C.9. Exemple d'appréciation des risques au niveau du système pour le métro de Copenhague

C.9.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.9.2. Cet exemple concerne un système de métro sans conducteur, complet et complexe, notamment les sous-systèmes techniques sous-jacents (par ex. matériel roulant et protection automatique des trains) ainsi que l'exploitation et la maintenance du système. Le système et les sous-systèmes ont été évalués au moyen d'une approche basée sur l'appréciation des risques. Le projet couvrait également la certification du SGS de la société qui devait exploiter le système. Ceci concerne la capacité de l'EF et du GI à exploiter et à maintenir en toute sécurité l'ensemble du système tout au long de sa durée de vie.

C.9.3. Par comparaison au processus MSC, les étapes suivantes ont été suivies (voir également Figure 1):

(a) description du système [section 2.1.2]:

(1) description des exigences de performances du système;
(2) description des règles opérationnelles;
(3) description claire des interfaces et des responsabilités entre les différents acteurs, notamment entre les sous-systèmes techniques;
(4) définition des exigences de haut niveau pour le système (en termes de fréquence acceptable des accidents et de définition d'une région ALARP);

(b) identification des dangers [section 2.2]:

(1) une analyse préliminaire des dangers au niveau du système;
(2) analyse fonctionnelle au niveau du système mettant en évidence tous les sous-systèmes, et pas seulement ceux dont l'importance en matière de sécurité est évidente (par ex. matériel roulant et protection automatique des trains), qui participent aux fonctions de sécurité et qui jouent un rôle actif dans la sécurité des passagers et du personnel;
(3) coordination intense entre les acteurs (sous-traitants, fournisseurs des sous-systèmes et des travaux d'ingénierie civile):

(i) pour identifier systématiquement tous les dangers raisonnablement prévisibles;
(ii) pour identifier les actions possibles afin de contrôler les risques associés aux dangers identifiés à un niveau acceptable;

(c) utilisation de codes de pratique [section 2.3]:

Différents codes de pratique, normes et règlements ont été utilisés, par ex.:

(1) règlement BOStrab pour la construction et l'exploitation de voitures de rue (règlement allemand applicable aux systèmes ferroviaires urbains) et pour l'exploitation sans conducteur;
(2) documents VDV (codes de pratique allemands) concernant les exigences en matière d'équipement pour garantir la sécurité des passagers dans les gares pour des opérations sans chauffeurs;
(3) normes CENELEC pour les systèmes ferroviaires (EN 50 126, 50 128 et 50 129). Ces normes abordent en particulier les systèmes ferroviaires techniques. Mais

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

étant donné qu'elles contiennent une approche méthodologique présentant une validité générale, elles ont été largement adoptées pour le métro de Copenhague:

(i) la norme EN 50 126 a été utilisée pour les activités de gestion de la sécurité et d'appréciation des risques de l'ensemble du système ferroviaire;
(ii) la norme EN 50 129 a été utilisée pour l'ensemble du système de signalisation;
(iii) la norme EN 50 128 a été utilisée pour le développement des logiciels (y compris leur vérification et validation) des sous-systèmes techniques;

(4) normes de protection contre l'incendie des tunnels (NEPA 130);
(5) normes pour l'ingénierie civile et les travaux de construction (Codes Euro);

(d) utilisation d'un système de référence [section 2.4]:

Le métro devait parvenir au niveau de sécurité des installations modernes correspondantes en Allemagne, en France et en Grande-Bretagne. Ces systèmes existants ont été utilisés comme systèmes de référence afin de définir les critères d'acceptation des risques en termes de fréquence acceptable des accidents pour le métro de Copenhague;

(e) estimation et appréciation des risques explicites [section 2.5]:

(1) pour l'estimation des risques liés à des dangers spécifiques;
(2) pour le contrôle de la ventilation d'urgence des tunnels (y compris le facteur humain impliquant les services de pompiers);
(3) pour identifier les mesures de réduction des risques;
(4) pour évaluer si un niveau de risque acceptable a été atteint pour l'ensemble du système;

(f) démonstration de la conformité du système aux exigences de sécurité [section 3]:

(1) efforts managériaux et techniques conformes à la complexité du système afin de démontrer la sécurité du système;
(2) attribution des exigences de sécurité du système jusqu'aux sous-systèmes techniques et aux travaux d'ingénierie civile ainsi qu'à toutes les fonctions liées à la sécurité du métro;
(3) démonstration que chaque sous-système, tel qu'il a été construit, respecte ses exigences de sécurité;
(4) pour les fonctions de sécurité assurées par plusieurs sous-systèmes, la démonstration de la conformité aux exigences de sécurité n'a pu être apportée au niveau des sous-systèmes. Elle a effectuée au niveau du système en intégrant les différents sous-systèmes, outils et procédures;
(5) démonstration que le système complet respecte les exigences de sécurité de haut niveau;

(g) gestion des dangers [section 4.1]:

Les dangers identifiés, les mesures de sécurité associées et les exigences de sécurité qui en découlent ont été enregistrés et gérés dans un registre central des dangers. Le responsable global de la sécurité du projet était responsable de ce registre des dangers. Les dangers opérationnels identifiés durant la conception et l'installation ainsi que les dangers liés à l'exploitation et à la maintenance ont été portés au registre des dangers;

(h) preuves de la gestion et de l'appréciation des risques [section 5]:

Les résultats de l'appréciation des risques ont été formellement documentés et étayés par un dossier de sécurité conformément aux exigences des normes CENELEC:

(1) dossier de sécurité global du système;
(2) dossier de sécurité pour chaque sous-système technique (y compris les sous-systèmes de signalisation et les travaux d'ingénierie civile);

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(3) dossier de sécurité pour les travaux d'ingénierie civile (gares, tunnels, viaducs, talus);
(4) dossier de sécurité d'installation;
(5) dossier de sécurité des véhicules;
(6) dossier de sécurité de l'opérateur (en appui de la certification du SGS de l'EF et du GI, c'est-à-dire la démonstration de la capacité à exploiter et à maintenir le système en toute sécurité);

(i) évaluation indépendante [Article 6]:

L'ensemble du processus a été suivi et évalué par un évaluateur de sécurité indépendant agissant avec une délégation de l'Autorité Technique de Supervision (Ministère danois des transports). Les rôles de l'évaluateur de sécurité indépendant sont décrits dans un code de pratique correspondant. Cette vérification couvre:

(1) la vérification de l'exécution correcte de la gestion et de l'appréciation des risques;
(2) la vérification que le système est adapté à son utilisation prévue et qu'il sera exploité et maintenu en toute sécurité tout au long de son cycle de vie;
(3) recommandation d'approbation par l'Autorité Technique de Supervision.

C.9.4. L'ensemble du projet s'appuyait sur un processus adéquat de gestion de la qualité.

C.9.5. Dans ce projet, les preuves apportées par les fournisseurs (à savoir dossiers de sécurité et documentation justificative détaillée pour les sous-systèmes techniques et les travaux d'ingénierie civile) ont été fournies au responsable de sécurité du proposant. Ces preuves ont ensuite été examinées par l'organisation de gestion de la sécurité ainsi que par un évaluateur de sécurité indépendant dont les conclusions ont été communiquées dans un rapport d'évaluation.
Le rapport d'évaluation indépendante de la sécurité a été examiné par les responsable de la sécurité du proposant et soumis au proposant, qui a transmis tous les fichiers à l'Autorité Technique de supervision (c'est-à-dire au Ministère danois des transports) pour l'approbation finale.

C.9.6. Cet exemple montre que les principes requis par la méthode de sécurité commune existent déjà dans le secteur ferroviaire. L'appréciation des risques décrite dans cet exemple remplit toutes les exigences de la MSC. En particulier, elle repose sur les trois principes d'acceptation des risques autorisés par l'approche harmonisée de la MSC.

C.10. Exemple de fil conducteur OTIF pour le calcul de risques lors du transport ferroviaire de marchandises dangereuses

C.10.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.10.2. La philosophie générale du fil conducteur OTIF est conforme à l'objectif de la MSC, mais le fil conducteur a un champ d'application plus restreint. L'objectif du fil conducteur OTIF est *«d'obtenir une approche plus uniforme pour l'évaluation du risque du transport (ferroviaire) de marchandises dangereuses dans les États membres de COTIF et de rendre en conséquence les évaluations individuelles de risques comparables».* Elle soutient donc l'acceptation mutuelle, entre les États membres de COTIF, des évaluations des risques relatives au transport ferroviaire de marchandises dangereuses.

C.10.3. Par comparaison avec la MSC et avec le diagramme de la Figure 1:

(a) le fil conducteur OTIF présente les points communs suivants:

(1) il s'agit d'une approche commune pour l'appréciation des risques, mais elle se base uniquement sur une estimation des risques explicites (c'est-à-dire le troisième principe d'acceptation des risques de la MSC);

(2) l'appréciation des risques de l'OTIF comprend les éléments suivants:

(i) une phase d'analyse des risques comprenant:

- une phase d'identification des dangers;
- une phase d'estimation des risques;

(ii) une phase d'évaluation des risques basée sur des critères d'acceptation des risques qui ne sont pas encore harmonisés. Dans la pratique, de nombreuses spécificités nationales sont susceptibles d'influencer ces critères;

(b) le fil conducteur diffère par les aspects suivants:

(1) son champ d'application est différent. Alors que les MSC doivent être appliquées uniquement aux changements significatifs apportés au système ferroviaire, le fil conducteur OTIF doit être appliqué pour évaluer les risques liés au transport ferroviaire de marchandises dangereuses, que cela constitue ou non un changement significatif au système ferroviaire;

(2) il n'y a pas de possibilité de choisir entre trois principes d'acceptation des risques pour maîtriser les risques. Le troisième principe, celui de l'estimation des risques explicites, est le seul permis. En outre, il doit se baser exclusivement sur une estimation quantitative plutôt que sur une estimation qualitative. L'analyse qualitative des risques peut convenir uniquement pour comparer différentes possibilités de mesures (de sécurité) pour la réduction des risques;

(3) l'application du principe ALARP est requise pour déterminer si des mesures de sécurité supplémentaires seraient susceptibles de réduire encore le risque évalué moyennant un coût raisonnable;

(4) il n'existe pas de concept de «dangers associés à des risques largement acceptables» permettant de focaliser l'appréciation des risques sur les dangers qui ont la plus grande contribution. Néanmoins, le fil conducteur recommande de réduire le nombre de scénarios d'accidents possibles à un nombre raisonnable de scénarios de base (voir la section § 3.2 de {Ref. 10});

(5) le processus se concentre sur l'appréciation des risques mais il n'inclut pas:

(i) le processus de sélection et de mise en œuvre des mesures (de sécurité) destinées à modifier le risque;

(ii) le processus d'acceptation des risques;

(iii) le processus visant à démontrer la conformité du système aux exigences de sécurité;

(iv) le processus de communication du risque aux autres acteurs concernés (voir le point ci-dessous);

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(6) il ne donne pas de consignes quant aux preuves à fournir par le processus d'appréciation des risques.
(7) il n'y a pas de demande de gestion des dangers;
(8) il n'y a pas de demande d'une évaluation indépendante par un tiers de l'application correcte de l'approche commune.

C.10.4. La comparaison entre le fil conducteur OTIF et la MSC montre que ces deux mesures sont compatibles même si leur portée et leurs objectifs ne sont pas exactement identiques. La MSC est plus générale que le fil conducteur OTIF, et en ce sens plus flexible. D'un autre côté, la MSC couvre davantage d'activités de gestion des risques:

(a) elle permet l'utilisation de trois principes d'acceptation des risques basées sur les pratiques existantes dans le secteur ferroviaire: voir la section 2.1.4;
(b) son application est requise uniquement pour les changements significatifs, et une analyse plus poussée des risques est requise uniquement pour les dangers qui ne sont pas associés à un risque largement acceptable;
(c) elle couvre la sélection et la mise en œuvre des mesures de sécurité nécessaires pour maîtriser les dangers identifiés et les risques associés;
(d) elle harmonise le processus de gestion des risques, y compris:

(1) l'harmonisation des critères d'acceptation des risques prévue dans le cadre du travail de l'Agence sur les risques largement acceptables et les critères d'acceptation des risques;
(2) la démonstration de la conformité du système aux exigences de sécurité;
(3) les résultats et les preuves du processus d'évaluation des risques;
(4) l'échange d'informations liées à la sécurité entre les acteurs impliqués aux interfaces;
(5) la gestion dans un registre des dangers de tous les dangers identifiés et des mesures de sécurité associées;
(6) l'évaluation indépendante par un tiers de l'application correcte de la MSC.

C.10.5. L'application du fil conducteur OTIF dans le cadre de la MSC (lorsque le transport de marchandises dangereuses constitue un changement significatif pour un GI ou une EF) ne pose toutefois aucun problème dans la mesure où ce fil conducteur est compatible avec l'utilisation du troisième principe d'estimation des risques explicites.

C.11. Exemple d'appréciation des risques de la demande d'approbation d'un nouveau type de matériel roulant

C.11.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.11.2. Cet exemple d'appréciation des risques concerne la demande d'approbation d'un nouveau type de matériel roulant. Une analyse des risques a été effectuée afin d'évaluer les risques liés au lancement d'un nouveau wagon de marchandises.

C.11.3. L'objectif du changement était d'améliorer l'efficacité, la capacité, les performances et la fiabilité du transport de marchandises en vrac sur une ligne de marchandises donnée. Tous les wagons étaient destinés à un trafic transfrontalier, et l'approbation de deux ANS différentes était donc nécessaire. Le proposant était l'opérateur de transport de marchandises. Il était lui-même détenu par la société produisant les marchandises à transporter.

C.11.4. Le développement du projet comprenait la construction, la fabrication, le montage, la mise en service et la vérification du nouveau matériel roulant. L'analyse des risques a été réalisée pour vérifier que la nouvelle conception respectait les exigences de sécurité de chacun des sous-systèmes ainsi que du système complet.

C.11.5. L'analyse des risques fait référence aux procédures et définitions de CENELEC EN 50 126 et l'évaluation des risques est effectuée conformément à cette norme.

C.11.6. Par comparaison au processus MSC, les étapes suivantes ont été suivies

(a) description du système [section 2.1.2]:

Pour chacune des phases de conception, des exigences ont été exprimées quant à la documentation de vérification de sécurité et à la description de la conception du système:

(1) phase conceptuelle: description préliminaire des exigences opérationnelles de l'opérateur;

(2) phase de spécification: spécifications fonctionnelles, normes techniques applicables, plan de test et de vérification. Les exigences de l'opérateur quant à l'utilisation et à la maintenance des wagons ont été inclues également;

(3) phase de construction: documentation technique du constructeur, y compris les schémas, normes, calculs, analyses, etc. Analyse approfondie pour les conceptions nouvelles ou innovantes et pour les nouveaux domaines d'utilisation;

(4) phase de vérification:

(i) la vérification par le constructeur des performances techniques du wagon (rapports de tests, calculs, vérifications conformément aux normes et aux exigences fonctionnelles);
(ii) documentation des mesures de réduction des risques et rapports de tests prouvant la compatibilité des wagons avec l'infrastructure ferroviaire;
(iii) documents de maintenance et de formation, manuels d'utilisateur, etc.

(5) phase de réception:

(i) déclaration de sécurité et preuves de sécurité du constructeur (dossier de sécurité);
(ii) acceptation par l'opérateur du wagon de fret et de sa documentation;

(b) identification des dangers [section 2.2]:

Cette identification a été effectuée de façon continue lors de toutes les phases de conception. Tout d'abord, une approche «de bas en haut» a été utilisée, par laquelle les différents constructeurs ont évalué les séquences de risques provoquées par la défaillance des composants de leur sous-système. Les sous-systèmes étaient répartis comme suit:

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(1) châssis;
(2) système de freinage;
(3) accouplement central;
(4) etc.

Une approche complémentaire «de haut en bas» a ensuite été appliquée pour tenter de détecter les lacunes ou les informations manquantes. Les risques qui n'ont pas pu être acceptés immédiatement ont été transférés au registre des dangers pour la suite du traitement et la classification.

(c) utilisation des principes d'acceptation des risques [section 2.1.4]:

Une estimation des risques explicites a été réalisée sur l'ensemble du système. Cependant, des codes de pratiques ou des systèmes de références similaires ont pu être utilisés pour évaluer des dangers individuels. Le principe est que chaque nouveau sous-système doit être au moins aussi sûr que le sous-système qu'il remplace, ce qui aboutit à un nouveau système complet offrant un niveau de sécurité supérieur au précédent. La matrice de risque de la norme EN 50 126 a été utilisée pour positionner les risques identifiés. Plusieurs autres critères d'acceptation des risques ont également été utilisés, notamment:

(1) une défaillance unique ne doit pas provoquer une situation dans laquelle les personnes, le matériel ou l'environnement risquent d'être sérieusement touchés.
(2) si une telle situation ne peut être évitée par des moyens techniques de construction, elle doit être évitée par le biais de règles opérationnelles ou d'exigences de maintenance. Ceci n'était applicable qu'aux dangers pour lesquels il était possible d'identifier la défaillance survenue avant que celle-ci n'engendre une situation dangereuse;
(3) pour les composants présentant une probabilité de défaillance élevée, ou dont les défaillances ne peuvent être détectées au préalable ou prévenues par le biais de règles opérationnelles ou de maintenance, il convient d'envisager des fonctions et des barrières de sécurité supplémentaires;
(4) les systèmes redondants dont les composants sont susceptibles de développer des défaillances indétectables en cours d'exploitation doivent être protégés par des mesures de maintenance destinées à prévenir la redondance ainsi réduite;
(5) le niveau de sécurité final convenu fut le fruit d'une décision de la direction basée sur une analyse quantitative et qualitative des risques;

(d) démonstration de la conformité du système aux exigences de sécurité [section 3]:

Tous les risques et dangers identifiés ont été enregistrés, et la liste a été consultée et mise à jour de façon continue. Les dangers restants ont été portés au registre des dangers en même temps que la liste correspondante de mesures de réduction des risques à prendre lors de la construction, de l'exploitation et de la maintenance. Sur cette base, un rapport de sécurité définitif a été produit en vérifiant que les exigences de sécurité avaient bien été respectées;

(e) gestion des dangers [section 4.1]:

Comme indiqué ci-dessus, les dangers et les mesures de sécurité correspondantes ont été enregistrés dans un registre des dangers qui garde la trace de tous les dangers identifiés et de toutes les mesures de sécurité. Cependant, les dangers liés à des risques acceptables dans la prise de mesures spécifiques n'ont pas été portés au registre des dangers;

(f) évaluation indépendante [Article 6]:

Les documents reçus concernant ce changement significatif ne mentionnent pas de changement significatif.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.11.7. Cet exemple d'appréciation des risques se base sur la norme CENELEC EN 50 126 et correspond donc bien au processus MSC. L'appréciation des risques de l'exemple respecte toutes les exigences de la MSC à l'exception de l'exigence d'un évaluation indépendante, qui n'est pas clarifiée explicitement dans les documents reçus. Des critères d'acceptation des risques explicites ont été utilisés et indiqués clairement.

C.12. Exemple d'appréciation des risques pour un changement opérationnel significatif – opération par le conducteur seul

C.12.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.12.2. Cet exemple concerne un changement opérationnel par lequel l'entreprise ferroviaire a décidé de confier l'opération du train au conducteur seul (Driver-Only Operation – DOO) sur une route où, précédemment, un garde aidait le conducteur dans la gestion du train.

C.12.3. Par comparaison au processus MSC, les étapes suivantes ont été suivies (voir également la Figure 1):

(a) Importance du changement [Article 4]:

L'entreprise ferroviaire a réalisé une appréciation des risques préliminaire qui a conclu que le changement opérationnel était significatif. Dans la mesure où le conducteur devait travailler seul et sans aide, le risque que des passagers se trouvent pris entre les portes ou tombent sur la voie (en cas d'ouverture des portes du mauvais côté) ne pouvait être négligé.

En comparant cette appréciation des risques préliminaire aux critères de l'Article 4 du règlement MSC, le changement peut également être catégorisé comme significatif sur la base des critères suivants:

(1) lien avec la sécurité: le changement est lié à la sécurité dans la mesure où la modification radicale de la gestion de l'exploitation du train peut avoir un impact catastrophique;
(2) conséquence d'une défaillance: l'effet potentiel des actions du conducteur peut avoir des conséquences catastrophiques si l'opération n'est pas contrôlée correctement;
(3) nouveauté: l'exploitation avec conducteur seul pourrait nécessiter de nouvelles façons d'exploiter un train dont le risque doit être évalué;

(b) définition du système [section 2.1.2]:

La définition du système décrivait:

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(1) le système existant, décrivant clairement quelles tâches étaient prises en charge par le conducteur et quelles autres étaient effectuées par le personnel embarqué (ou de garde) afin d'aider le conducteur;
(2) la modification des responsabilités du conducteur suite à la suppression du personnel auxiliaire embarqué;
(3) les exigences techniques permettant au système de couvrir la modification des opérations;
(4) les interfaces existantes entre le personnel auxiliaire embarqué, le conducteur et le personnel côté voie du gestionnaire d'infrastructure;

Au cours des différentes itérations, la définition du système a été mise à jour sur la base des exigences de sécurité découlant du processus d'appréciation des risques. Des personnes clés (notamment des conducteurs, des représentants du personnel et du gestionnaire d'infrastructure) ont été impliquées dans ce processus itératif pour l'identification des dangers et la mise à jour de la définition du système.

(c) identification des dangers [section 2.2]:

Les dangers et les mesures de sécurité possibles ont été identifiés en organisant un brainstorming d'experts, parmi lesquels:

(1) des représentants des conducteurs et du personnel pour leur expérience opérationnelle;
(2) des représentants du GI, dans la mesure où l'infrastructure risquait également d'être impactée par le changement, ce qui impliquait par exemple de modifier les gares (par ex.: installation de miroirs et de système de vidéosurveillance sur les quais);

Les tâches supplémentaires à accomplir par le conducteur ont été examinées afin d'identifier tous les dangers prévisibles susceptibles de survenir suite à la suppression du personnel auxiliaire embarqué. L'identification des dangers s'est penchée plus particulièrement sur les principaux dangers opérationnels possibles dans les gares, sur les routes existantes qui bénéficiaient précédemment d'une aide de la part de personnel embarqué ou côté voie (y compris pour le départ des trains), sur les problèmes spécifiques liés au conducteurs, au matériel roulant (par ex. vérification de l'ouverture / de la fermeture des portes), les exigences de maintenance, etc.

Chacun des dangers identifiés a reçu un niveau de gravité des risques et des conséquences (élevé, modéré, faible) et l'impact du changement proposé a été examiné par rapport à ce niveau (augmentation, réduction, pas de changement du risque).

(d) utilisation de codes de pratique [section 2.3] et utilisation de systèmes de référence similaires [section 2.4]:

Des codes de pratique (à savoir un ensemble de normes pour le fonctionnement avec conducteur seul) et des systèmes de référence similaires ont été utilisés pour définir les exigences de sécurité des dangers identifiés. Les exigences de sécurité comprenaient:

(1) les procédures opérationnelles révisées pour le conducteur et requises pour exploiter en toute sécurité un train sans assistance embarquée;
(2) tous les équipements supplémentaires requis à bord ou sur la voie pour assurer un départ sûr et fiable des trains;
(3) une liste de contrôle garantissant l'adéquation du poste de conduite en tenant compte de l'interface entre le système ferroviaire (à bord et sur la voie) et le conducteur;

Les règles opérationnelles nécessaires ont été révisées conformément aux exigences des codes de pratique applicables et aux systèmes de référence concernés. Toutes les

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

parties nécessaires ont été impliquées dans les procédures opérationnelles révisées et dans la perspective de procéder au changement.

(e) démonstration de la conformité du système aux exigences de sécurité [section 3]:

Le système a été implémenté conformément aux exigences de sécurité identifiées (équipements supplémentaires et procédures révisées). Celles-ci ont été vérifiées comme constituant un moyen approprié de garantir un niveau de sécurité suffisant pour le système évalué.

Les procédures opérationnelles révisées ont été introduites dans le système de gestion de la sécurité de l'EF. Elles ont été contrôlées et réexaminées si nécessaire afin de veiller à ce que les dangers identifiés continuent à être maîtrisés correctement durant l'exploitation du système ferroviaire.

(f) gestion des dangers [section 4.1]:

Voir le point ci-dessus, étant donné que pour les entreprises ferroviaires, le processus de gestion des dangers peut faire partie de leur système de gestion de la sécurité pour l'enregistrement et la gestion des risques. Les dangers identifiés ont été enregistrés dans un registre de dangers avec les exigences de sécurité (à savoir référence aux équipements supplémentaires à bord et côté voie et aux procédures opérationnelles révisées) maîtrisant le risque associé.
Les procédures révisées ont été contrôlées et réexaminées si nécessaire afin de veiller à ce que les dangers identifiés continuent à être maîtrisés correctement durant l'exploitation du système ferroviaire.

(g) évaluation indépendante [Article 6]:

Les processus d'appréciation et de gestion des risques ont été évalués par une personne compétente au sein de la société de l'EF qui était indépendante du processus d'appréciation. Cette personne compétente a évalué tant le processus que les résultats, c'est-à-dire les exigences de sécurité identifiées.

L'EF a basé sa décision de mettre en œuvre le nouveau système sur le rapport d'évaluation indépendante produit par cette personne compétente.

C.12.4. Cet exemple montre que les principes et les processus utilisés par l'entreprise ferroviaire sont conformes à la méthode de sécurité commune. Le processus de gestion et d'appréciation des risques respectait toutes les exigences de la MSC.

C.13. Exemple d'utilisation d'un système de référence pour la définition d'exigences de sécurité destinées à de nouveaux systèmes d'aiguillages électroniques en Allemagne.

C.13.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.13.2. Afin de définir des exigences standard de sécurité pour les futurs systèmes d'aiguillages électroniques, Deutsche Bahn avait réalisé une analyse des risques sur un système électronique déjà agréé. Ce système avait été approuvé précédemment conformément aux codes de pratique allemands (Mü 8004).

C.13.3. L'analyse de risques a été effectuée conformément aux normes CENELEC (EN 50126 et EN 50129), et a couvert les étapes suivantes:

(a) définition du système;
(b) identification des dangers;
(c) analyse et quantification des dangers.

C.13.4. Pour la définition du système, il a été pris soin de définir les limites du système, ses fonctions et ses interfaces. Le principal défi fut de définir le système de telle façon qu'il soit indépendant de l'architecture interne d'un système d'aiguillage tout en restant compatible avec les systèmes d'aiguillage existants. Une attention particulière a donc été accordée à la définition claire des interfaces avec les systèmes externes interagissant avec l'aiguillage sans détailler les fonctions internes de l'aiguillage.

C.13.5. Les dangers ont été ensuite identifiés uniquement aux interfaces afin de rester génériques (c.-à-d. d'éviter toute dépendance par rapport à une architecture spécifique). Seuls les dangers provoqués par des défaillances techniques ont été envisagés. Pour chaque interface, deux dangers génériques ont ainsi été identifiés:

(a) mauvaise sortie de l'aiguillage transmise à l'interface
(b) entrée (correcte) corrompue au niveau de l'interface

C.13.6. Des caractéristiques plus spécifiques ont ensuite été attribuées à ces dangers génériques pour chaque interface.

C.13.7. Au cours de la phase suivante, les contributions des composants du système existant à chaque danger identifié ont été analysées et regroupées dans un arbre de défaillances. Ceci a permis, sur la base du taux de défaillance estimé des composants, de calculer le taux d'occurrence de chaque danger et d'utiliser ces dangers en tant que taux de danger tolérables (Tolerable Hazard Rates, THR) pour les futures générations d'aiguillages électroniques.

C.13.8. L'analyse des risques a été suivie et évaluée par l'autorité nationale de sécurité (EBA).

C.13.9. Dans le cadre de l'analyse des risques, une analyse des fonctionnalités de contrôle et d'affichage du système électronique a également été réalisée. De nouveau, un système agréé d'aiguillage électronique a été utilisé comme référence afin de définir les exigences de sécurité des fonctions d'interface homme-machine (man-machine interface, MMI) destinées à maîtriser les défaillances ou erreurs aléatoires et à maîtriser les défaillances systématiques. Ceci a permis de définir les niveaux d'intégrité de sécurité (SIL) pour différentes fonctions: pour les fonctions MMI en fonctionnement standard, pour les fonctions MMI en mode de commande-relâchement (mode dégradé) ou pour la fonctionnalité d'affichage.

C.13.10. Cette analyse des risques a également été suivie et évaluée par l'autorité nationale de sécurité (EBA).

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.13.11. Ces exemples d'appréciation des risques illustrent la manière dont le deuxième principe d'acceptation des risques (système de référence) peut être utilisé pour définir les exigences de sécurité des nouveaux systèmes. Ils sont en outre basés sur la norme CENELEC EN 50 126 et correspondent donc bien au processus MSC. L'appréciation des risques décrite dans ces exemples remplit toutes les exigences de la MSC relatives aux phases concernées. Cependant, étant donné qu'aucune activité de conception n'est concernée, il n'y a aucune référence à la gestion d'un registre des dangers ni à la démonstration de la conformité du système évalué aux exigences de sécurité identifiées.

C.13.12. Les documents suivants fournissent de plus amples informations sur ces analyses de risques:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15;

(b) Bock, H., Braband, J., et Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

C.14. Exemple d'un critère d'acceptation de risque explicite pour l'exploitation de trains à base de radio FFB en Allemagne

C.14.1. **Remarque:** cet exemple d'appréciation des risques n'a pas été produit suite à l'application du processus MSC; il est antérieur à l'existence de la MSC. Cet exemple a les objectifs suivants:

(a) identifier les similitudes entre les méthodes existantes d'appréciation des risques et le processus MSC;
(b) assurer la traçabilité entre le processus existant et celui requis par la MSC;
(c) justifier la valeur ajoutée de l'exécution des étapes supplémentaires (le cas échéant) requises par la MSC.

Il convient de souligner que cet exemple est fourni à titre informatif uniquement. Il a pour but d'aider le lecteur à comprendre le processus MSC. Cependant, l'exemple lui-même ne peut être transposé ni utilisé en tant que système de référence pour un autre changement significatif. L'appréciation des risques sera réalisée pour chaque changement significatif conformément au règlement MSC.

C.14.2. Une analyse des risques conforme aux normes CENELEC a été effectuée pour une toute nouvelle procédure opérationnelle qui avait été envisagée (mais jamais introduite) en Allemagne pour les lignes ferroviaires conventionnelles. Le concept consistait à faire fonctionner les trains uniquement via un contrôle radio (du train et des itinéraires). Étant donné qu'il n'y avait pas de codes de pratique existants (règles techniques reconnues) ni de systèmes de référence pour un tel nouveau système, une estimation des risques explicites a été effectuée afin de démontrer la sécurité de la nouvelle procédure. Il était nécessaire de démontrer que le niveau de risque auxquels les passagers seraient exposés dans le nouveau système ne dépasserait pas une valeur de risque acceptable (critère explicite d'acceptation des risques).

C.14.3. Ce critère explicite d'acceptation des risques a été estimé sur la base des statistiques des accidents attribués aux systèmes de signalement et de contrôle en Allemagne, et sa plausibilité a également été vérifiée par rapport au critère MEM. Cette démonstration de sécurité est conforme à l'exigence de l'EBO allemand d'assurer «le même niveau de

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

sécurité» en cas de déviation par rapport aux règles techniques. L'analyse des risques a également été suivie et évaluée par l'autorité nationale de sécurité (EBA).

C.14.4. Cet exemple d'appréciation des risques montre comment un critère explicite global (pour le troisième principe d'acceptation des risques de la MSC) peut être défini pour de nouveaux systèmes sans utiliser de codes de pratique ni de système de référence. L'analyse de risque réalisée ensuite pour le nouveau système se base sur les normes CENELEC et correspond donc bien au processus MSC. L'appréciation des risques de cet exemple respecte les exigences de la MSC, mais il n'y a aucune référence à la gestion d'un registre des dangers ni à la démonstration de la conformité du système évalué aux exigences de sécurité identifiées.

C.14.5. Le document suivant fournit de plus amples informations sur cette analyse de risque: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, 10-15

C.15. Exemple de test d'applicabilité du CAR-ST

C.15.1. L'objectif de cet appendice est de montrer, par l'exemple de la fonction du sous système ETCS embarqué, comment utiliser le critère décrit à la section 2.5.4 et comment déterminer si le CAR-ST est applicable.

C.15.2. Le sous-système embarqué ETCS est un système technique. La fonction suivante est envisagée: *«fournir au conducteur les informations nécessaires pour lui permettre de conduire le train en toute sécurité et utiliser les freins en cas de survitesse».*

Description de la fonction: sur la base des informations reçues de l'infrastructure de voie (vitesse autorisée) et de la vitesse du train calculée par le sous-système embarqué ETCS:

(a) le conducteur conduit le train et veille à ce que la vitesse du train ne dépasse pas la vitesse autorisée;
(b) parallèlement, le sous-système ETCS embarqué vérifie que le train ne dépasse jamais la vitesse maximale autorisée. En cas de survitesse, le système freine automatiquement.

Tant le conducteur que le sous-système ETCS embarqué utilisent l'évaluation de la vitesse du train calculée par le sous-système ETCS embarqué.

C.15.3. Question: «Le CAR-ST s'applique-t-il à l'évaluation de la vitesse du train par le sous-système embarqué ?»

C.15.4. Application du diagramme de la Figure 14 et réponses aux différentes questions:

(a) Danger envisagé pour le système technique:

«Dépassement de la vitesse de sécurité recommandée par l'ETCS» (voir UNISIG, sous-ensemble 091).

(b) Ce danger peut-il être maîtrisé par un code de pratique ou par un système de référence ?

NON. Il est supposé que le système ETCS est de conception nouvelle et innovante. Il n'existe donc pas de codes de pratique ni de systèmes de référence capables de maîtriser le danger à un niveau de risque acceptable.

(c) Est-il probable que ce danger ait des conséquences catastrophiques ?

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

OUI puisque le *«dépassement de la vitesse de sécurité recommandée par l'ETCS»* peut provoquer un déraillement et donc *«des morts et/ou blessures graves multiples et/ou un préjudice majeur pour l'environnement».*

(d) La conséquence catastrophique est-elle le résultat direct de la défaillance du système technique?

OUI s'il n'existe pas de barrières de sécurité supplémentaires. La même évaluation de la vitesse du train calculée par le sous-système ETCS embarqué est fournie au conducteur et à la fonction de contrôle du frein du sous-système ETCS embarqué. Par conséquent, en supposant que le conducteur, pour des raisons de performances, conduise le train à la vitesse maximale autorisée par l'infrastructure, ni le conducteur ni le sous-système ETCS ne détecteront que le train est en survitesse en cas de sous-estimation de la vitesse du train. Ceci peut potentiellement provoquer un déraillement avec des conséquences catastrophiques.

(e) Conclusions:

(1) pour les exigences quantitatives: appliquer un THR de 10^{-9} h^{-1} pour les défaillances matérielles aléatoires du sous-système ETCS embarqué, en respectant les conditions suivantes:

(i) l'évaluation de cet objectif quantitatif tient compte des composants communs pour les systèmes redondants (par ex. entrées communes ou uniques pour tous les canaux, alimentation électrique commune, comparateurs, dispositifs en redondance majoritaire, etc.);
(ii) les délais de détection des défaillances dormantes ou latentes sont couverts;
(iii) une analyse des défaillances à cause/mode communs (CCF/CMF) est effectuée;
(iv) une évaluation indépendante est effectuée;

(2) pour les exigences de processus: appliquer un processus SIL 4 pour la gestion des défaillances systématiques du sous-système ETCS embarqué. Ceci nécessite l'application:

(i) d'un processus de gestion de la qualité conforme à SIL 4;
(ii) d'un processus de gestion de la sécurité conforme à SIL 4;
(iii) des normes pertinentes, par ex.:

- pour le développement logiciel, utiliser la norme EN 50 128;
- pour le développement matériel, utiliser les normes 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) une évaluation indépendante du/des processus.

C.16. Exemples de structures possibles pour le registre des dangers

C.16.1. Introduction

C.16.1.1. Les exigences minimales à porter au registre des dangers sont identifiées à la section 4.1.2 du règlement MSC. Celles-ci sont indiquées sur fond grisé dans les exemples de registres de dangers ci-dessous.

C.16.1.2. Il existe de nombreuses façons différentes de structurer un registre des dangers et les informations complémentaires susceptibles de caractériser les dangers et les mesures de sécurité associées. Par exemple, les dangers et les mesures de sécurité associées peuvent présenter un champ par élément d'information. Toutefois, quelle que soit la structure utilisée,

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

il est important que le registre des dangers fournisse des liens clairs entre les dangers et les mesures de sécurité associées. Une solution possible est que le registre des dangers contienne, pour chaque danger et pour chaque mesure de sécurité, au moins un champ avec:

(a) une description claire y compris les références de son origine et du principe d'acceptation des risques sélectionné pour maîtriser le danger associé. Ce champ permet de comprendre le danger et les mesures de sécurité associées, et de savoir dans quelles analyses de sécurité ils ont été identifiés.

Étant donné que le registre des dangers est utilisé et maintenu durant tout le cycle de vie du système (c'est-à-dire pendant l'exploitation et la maintenance du système), il est utile d'assurer la traçabilité et de fournir un lien clair entre chaque danger et:

(1) le risque associé;
(2) les causes du danger si elles ont déjà été identifiées;
(3) les mesures de sécurité associées ainsi que les hypothèses qui définissent les limites du système évalué;
(4) les analyses de sécurité associées là où le danger est identifié;

En outre, la formulation des mesures de sécurité (notamment de celles qui doivent être transférées à d'autres acteurs comme le proposant) ainsi que la formulation des dangers associés et des risques doivent être claires et suffisantes. On entend par «claires et suffisantes» qu'il doit être possible de comprendre les mesures de sécurité, les dangers associés et les risques qu'elles sont censées maîtriser sans devoir revenir aux analyses de sécurité correspondantes.

(b) le principe d'acceptation des risques utilisé pour maîtriser le danger afin de soutenir la reconnaissance mutuelle et d'aider l'organisme d'évaluation à évaluer l'application correcte de la MSC;

(c) des informations claires quant à son statut: ce champ indique si le danger / la mesure de sécurité concerné(e) est ouvert(e) ou déjà maîtrisé(e)/validé(e).

(1) les dangers et mesures de sécurité ouverts sont suivis jusqu'à ce qu'ils soient maîtrisés/validés.
(2) réciproquement, les dangers / mesures de sécurité maîtrisés/validés ne sont plus suivis sauf en cas de changement significatif dans l'exploitation ou la maintenance du système: voir le point [G 5](a) de la section 2.1.1. Dans ce cas:

(i) la MSC est appliquée à nouveau aux changements requis conformément à l'Article 2. Voir également le point [G 5](a)(b) de la section 2.1.1;
(ii) tous les dangers et toutes les mesures de sécurité maîtrisés sont réexaminés afin de vérifier s'ils sont concernés par les changements. En cas d'impact, les dangers correspondants et les mesures de sécurité associées sont rouverts et gérés à nouveau dans le registre des dangers;

Il peut arriver que des mesures de sécurité autres que celles reprises au registre des dangers soient mises en œuvre (par ex. pour des raisons de coûts). Les mesures de sécurité mises en œuvre sont alors portées au registre des dangers avec la preuve/justification de leur adéquation et la démonstration qu'avec ces mesures, le système est conforme aux exigences de sécurité.

(d) la référence à la preuve associée maîtrisant un danger ou validant une mesure de sécurité. Ce champ permet de retrouver ultérieurement les preuves ayant permis de maîtriser le danger et de valider les mesures de sécurité associées;

Un danger ne peut être maîtrisé dans le registre des dangers qu'une fois que toutes les mesures de sécurité associées à ce danger ont été validées;

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

(e) l'organisation ou l'entité responsable de sa gestion.

C.16.1.3. L'appendice A.3 de la ligne directrice EN 50 126-2 {Ref. 9} donne un autre exemple de contenu possible d'un registre des dangers.

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

C.16.2. Exemple de registre des dangers pour le changement organisationnel de la section C.5 de l'appendice C

Tableau 6: Exemple de registre des dangers pour le changement organisationnel de la section C.5 de l'appendice C.

Description du danger	Mesures de sécurité	Priorité/sécurité Ponctualité	Mise en œuvre(18)	Notes	Responsabilité(18)	Origine	Principe d'acceptation des risques utilisé	Responsabilité de la vérification	Mode de vérification	Statut xx.xx.xx
Baisse de la motivation des employés restant dans la société. D'où continuation des départs. Managers démotivés/usés	Nouveau cycle de travail de motivation pour le personnel, à effectuer en petits groupes. Réallocation des fonds pour que la société ait des tâches utiles à effectuer. Inspections plus fréquentes par le responsable des voies. Prévoir les fonds nécessaires pour assurer que les personnes clés restent jusqu'au bout du processus. Attention particulière pour assurer le transfert des informations et des connaissances entre les employés qui partent et ceux qui reprennent leurs tâches. etc.	Élevée/Élevée	Coordonné par XYZ. Les régions doivent envisager des mesures pour augmenter le contrôle des voies, le double emploi des employés et le suivi par le responsable des lignes	Inspections accrues à préciser par contrat. Etc.	Responsable de la société	Brainstorming Rapport HAZID Rx	S.O.			L'évolution des conditions et des circonstances a réduit considérablement ce risque. Analyse de l'environnement de travail effectuée, formation du personnel.
Les sous-traitants de l'entrepreneur manquent de compétences, de capacités et de contrôle qualité	Demande accrue de compétences documentées. Contrôle systématique des tâches accomplies	Élevée/ Moyenne	Le GI doit coordonner. Les régions doivent implémenter des mesures pour exiger des compétences et contrôler le travail	Implémentation par suivi contractuel. Donnée d'entrée au planning de révision.	Gestionnaire d'infrastructure	Brainstorming Rapport HAZID Rx	S.O.	Responsable de sécurité		Focalisation accrue sur les routines de contrôle (2 contrôles opératifs par mois et par région opérative)

(18) *Ces deux colonnes concernent les informations / les champs relatifs aux acteurs chargés de maîtriser les dangers identifiés.*

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

Tableau 6: Exemple de registre des dangers pour le changement organisationnel de la section C.5 de l'appendice C.

Description du danger	Mesures de sécurité	Priorité/sécurité Ponctualité	Mise en œuvre(18)	Notes	Responsabilité(18)	Origine	Principe d'acceptation des risques utilisé	Responsabilité de la vérification	Mode de vérification	Statut xx.xx.xx
Incertitude quant aux rôles et responsabilités à l'interface entre la société et le GI (gestionnaire de voie).	Définir les rôles et responsabilités. Décrire toutes les interfaces et définir qui est responsable des interfaces.	Moyenne/Moyenne	Dans chaque région séparément	Mis en œuvre par le contrat de maintenance et le plan stratégique de la réorganisation	Directeur régionaux	Brainstorming Rapport HAZID Rx	S.O.	Responsable de sécurité		Les régions ont présenté leur stratégie.

C.16.3. Exemple d'un registre des dangers complet pour un sous-système embarqué de contrôle-commande

C.16.3.1. Cette section fournit un exemple de registre des dangers unique (voir le point [G 3] de la section 4.1.1) permettant de gérer à la fois:

(a) toutes les exigences de sécurité internes applicables au sous-système dont l'acteur est responsable;
(b) tous les dangers identifiés et toutes les mesures de sécurité associées que l'acteur n'est pas en mesure de mettre en œuvre et qu'il doit transférer à d'autres acteurs.

Tableau 7: Exemple du registre des dangers d'un constructeur pour un sous-système embarqué de contrôle-commande.

N° DGR	Origine	Description du danger	Informations complémentaires	Acteur responsable	Mesure de sécurité	Principe d'acceptation des risques utilisé	Exporté	Statut
1	Rapport HAZOP R_x	Vitesse maximale définie pour le train (Vmax) trop élevée	Configuration spécifique erronée du sous-système embarqué (personnel de maintenance). Mauvaise saisie de données à bord (conducteur)	Entreprise ferroviaire	• Définir une procédure d'approbation des données de configuration du sous-système embarqué; • Définir une procédure opérationnelle pour le processus de saisie des données par le	Estimation explicite des risques	Oui	Maîtrisé (exporté vers l'EF) Voir également la section C.16.3 à l'annexe C.

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

Tableau 7: Exemple du registre des dangers d'un constructeur pour un sous-système embarqué de contrôle-commande.

N° DGR	Origine	Description du danger	Informations complémentaires	Acteur responsable	Mesure de sécurité	Principe d'acceptation des risques utilisé	Exporté	Statut
					conducteur;			
2	Rapport HAZOP R_x	Courbes de freinage (autorité de mouvement) trop permissives dans les données de configuration du sous-système embarqué	La procédure de configuration spécifique du sous-système embarqué dépend: • des marges de sécurité adoptées pour le système de freinage du train; • du délai de réaction du système de freinage du train (celui-ci dépend directement de la longueur du train, surtout pour les trains de marchandises)	Entreprise ferroviaire	• Spécifier correctement les exigences du système dans la définition du système; • Adopter des marges de sécurité suffisantes pour le système de freinage du train concerné;	Estimation explicite des risques	Oui	Maîtrisé (exporté vers l'EF) Voir également la section C.16.4 à l'annexe C.
3	Rapport HAZOP R_x	• Vitesse maximale du train (Vmax) trop importante • Courbes de freinage (autorité de mouvement) trop permissives dans les données de configuration du sous-système embarqué	Défaut de mise à jour du diamètre des roues dans la configuration spécifique du sous-système embarqué (personnel de maintenance).	Entreprise ferroviaire	• Définir une procédure pour la mesure du diamètre des roues du train par le personnel de maintenance; • Définir une procédure pour la mise à jour régulière du diamètre des roues dans le sous-système embarqué;	Estimation explicite des risques	Oui	Maîtrisé (exporté vers l'EF) Voir également la section C.16.4 à l'annexe C.
			Défaillance de la procédure du constructeur pour la préparation et le chargement des données de configuration dans le sous-système embarqué	Constructeur	Définir une procédure pour la mise à jour du diamètre des roues dans les données de configuration embarquées	Estimation explicite des risques	Oui	Maîtrisé par la procédure P_x
4	Rapport HAZOP R_x	Entrée du train à grande vitesse (160 km/h si le signal de ligne est libre) sur la voie sans que le sous-système embarqué soit actif et sans signalisation de ligne.	Susceptible d'être maîtrisé uniquement par la vigilance du conducteur. L'entrée dans une zone avec ATP côté ligne nécessite une procédure de confirmation par le conducteur avant l'emplacement de transition. En l'absence d'une confirmation, il y a freinage automatique par le sous-système embarqué de contrôle-commande.	Gestionnaire d'infrastructure	Le gestionnaire d'infrastructure doit veiller à ce qu'aucun train non équipé d'un sous-système embarqué de contrôle-commande actif n'accède à la voie concernée. Définir une procédure de gestion du trafic.	Estimation explicite des risques	Oui	Maîtrisé (exporté vers le GI) Voir également la section C.16.4 à l'annexe C.
				Entreprise ferroviaire	Assurer la formation des conducteurs pour l'entrée dans une zone avec ATP côté voie	Estimation explicite des risques	Oui	Maîtrisé (exporté vers l'EF) Voir également la section C.16.4 à l'annexe C.

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

Tableau 7: Exemple du registre des dangers d'un constructeur pour un sous-système embarqué de contrôle-commande.

N° DGR	Origine	Description du danger	Informations complémentaires	Acteur responsable	Mesure de sécurité	Principe d'acceptation des risques utilisé	Exporté	Statut
5	Rapport HAZOP R_x	Vitesse maximale du train (Vmax) communiquée au conducteur trop élevée	Les informations affichées sur l'interface du conducteur sont contrôlées par le sous-système de contrôle-commande SIL 4 embarqué qui actionne le frein d'urgence en cas de divergence entre la valeur attendue et la valeur affichée. En cas de non-conformité avec l'autorité de mouvement, le sous-système de contrôle-commande embarqué actionne le frein d'urgence.	Constructeur	Développer un système de contrôle-commande embarqué SIL 4	Estimation explicite des risques	Oui	Dossier de sécurité attestant d'un sous-système SIL 4 évalué par un évaluateur de sécurité indépendant
6	Rapport HAZOP R_x	Départ du train sans interface conducteur-machine	Perte d'architecture redondante du sous-système embarqué	Constructeur	Développer un système de contrôle-commande embarqué SIL 4	Estimation explicite des risques	Oui	Dossier de sécurité attestant d'un sous-système SIL 4 évalué par un évaluateur de sécurité indépendant
etc.								

C.16.4. Exemple de registre des dangers pour le transfert d'informations vers d'autres acteurs

C.16.4.1 Cette section donne un exemple de registre des dangers destiné au transfert vers d'autres acteurs des dangers identifiés et des mesures de sécurité associées qu'un acteur envisagé n'est pas capable de mettre en œuvre. Voir le point 4.1.1 de la section 4.1.1.
Cet exemple est identique à celui de la section C.16.3 de l'appendice C. La seule différence est que tous les dangers internes et les mesures de sécurité susceptibles d'être contrôlés par l'acteur concerné ont été supprimés.

C.16.4.2. La dernière colonne du tableau 8 permet de respecter les exigences de la section 4.2 du règlement MSC. Il existe différents moyens d'y parvenir. Une façon possible est de se référer aux preuves utilisées par l'acteur qui reçoit les informations de sécurité exportées. Une autre façon est d'organiser une réunion entre les deux acteurs afin de trouver ensemble la solution adéquate pour maîtriser les risques associés. Les résultats de cette réunion peuvent être communiqués dans un document convenu (par exemple un compte-rendu de réunion) auquel l'acteur qui exporte les informations de sécurité concernées peut faire référence pour clôturer les dangers associés dans son registre des dangers.

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

Tableau 8: Exemple d'un registre des dangers pour le transfert d'informations de sécurité vers d'autres acteurs

N° DGR	Origine du danger		Description du danger	Informations complémentaires	Acteur responsable	Mesure de sécurité	Commentaire du destinataire
	N° au tableau 11	Autre					
1	N° 1	Rapport HAZOP R_x	Vitesse maximale du train (Vmax) trop importante	Configuration spécifique erronée du sous-système embarqué (personnel de maintenance). Mauvaise saisie de données à bord (conducteur)	Entreprise ferroviaire	• Définir une procédure d'approbation des données de configuration du sous-système embarqué; • Définir une procédure opérationnelle pour le processus de saisie des données par le conducteur;	• Les données de configuration du sous-système de contrôle-commande embarqué dépendent des caractéristiques physiques du matériel roulant. • Les marges de sécurité sont ensuite appliquées à ces données en coordination entre le gestionnaire d'infrastructure et l'entreprise ferroviaire. • Ces données sont ensuite chargées dans le sous-système embarqué conformément à la procédure appropriée du constructeur pendant l'installation, l'intégration au matériel roulant et la réception du sous-système de contrôle-commande. • Les conducteurs sont formés et évalués par rapport à la procédure D_P. • Les conducteurs sont également évalués par le GI par rapport aux règles applicables à l'infrastructure du GI.
2	N° 2	Rapport HAZOP R_x	Courbes de freinage (autorité de mouvement) trop permissives dans les données de configuration du sous-système embarqué	La procédure de configuration spécifique du sous-système embarqué dépend: • des marges de sécurité adoptées pour le système de freinage du train; • du délai de réaction du système de freinage du train (celui-ci dépend directement de la longueur du train, surtout pour les trains de marchandises)	Entreprise ferroviaire	• Spécifier correctement les exigences du système dans la définition du système; • Adopter des marges de sécurité suffisantes pour le système de freinage du train concerné;	Voir le commentaire à la ligne 1 ci-dessus.
3	N° 3	Rapport HAZOP R_x	• Vitesse maximale du train (Vmax) trop importante • Courbes de freinage (autorité de mouvement) trop permissives dans les données de configuration du sous-système embarqué	Défaut de mise à jour du diamètre des roues dans la configuration spécifique du sous-système embarqué (personnel de maintenance).	Entreprise ferroviaire	• Définir une procédure pour la mesure du diamètre des roues du train par le personnel de maintenance; • Définir une procédure pour la mise à jour régulière du diamètre des roues dans le sous-système embarqué;	• La maintenance du sous-système de contrôle-commande embarqué est effectuée conformément à la «procédure de maintenance MP_Z». • Le diamètre de roue du train est mis à jour à intervalles bien définis selon la procédure P_W. • Pour le processus de saisie des données, les conducteurs sont formés et évalués par rapport à la «procédure P_{DE}».
4	N° 4	Rapport	Entrée du train à	Susceptible d'être maîtrisé	Gestionnaire	Le gestionnaire d'infrastructure	La gestion du trafic sur l'infrastructure du GI est régie par l'ensemble de

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

Tableau 8: Exemple d'un registre des dangers pour le transfert d'informations de sécurité vers d'autres acteurs

N° DGR	Origine du danger		Description du danger	Informations complémentaires	Acteur responsable	Mesure de sécurité	Commentaire du destinataire
	N° au tableau 11	Autre					
		HAZOP R_x	grande vitesse (160 km/h si le signal de ligne est libre) sur la voie sans que le sous-système embarqué soit actif et sans signalisation de ligne.	uniquement par la vigilance du conducteur. L'entrée dans une zone avec ATP côté ligne nécessite une procédure de confirmation par le conducteur avant l'emplacement de transition. En l'absence d'une confirmation, il y a freinage automatique par le sous-système embarqué de contrôle-commande.	d'infrastructure	doit veiller à ce qu'aucun train non équipé d'un sous-système embarqué de contrôle-commande actif n'accède à la voie concernée. Définir une procédure de gestion du trafic.	règles R_{TM}.
					Entreprise ferroviaire	Assurer la formation des conducteurs pour l'entrée dans une zone avec ATP côté voie	• Les conducteurs sont formés régulièrement selon la procédure P_{IM_DP} du GI. • Les conducteurs sont également évalués par le GI par rapport aux règles (S_R) applicables à l'infrastructure du GI.
etc.							

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 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. Exemple d'une liste générique de dangers pour l'exploitation d'un système ferroviaire

C.17.1. L'objectif de ROSA (Rail Optimisation Safety Analysis), un projet réalisé dans le cadre de DEUFRAKO (coopération franco-allemande), était de dresser une liste complète et générique de dangers couvrant l'exploitation normale d'un système ferroviaire. La finalité et la difficulté consistaient à définir ces dangers au niveau de détail le plus élevé possible sans refléter les spécificités des chemins de fer français et allemands. La liste a été créée sur la base de liste de dangers existants en provenance des deux pays (SNCF et DB) et vérifiée en utilisant des listes de dangers en provenance d'autres pays. Malgré l'objectif déclaré d'être complète et générique, la liste n'est donnée ici qu'à titre d'exemple indicatif susceptible d'aider les acteurs chargés d'identifier les dangers d'un projet particulier. Il faut probablement s'attendre à ce que les dangers repris dans cette liste doivent être précisés ou complétés pour refléter les particularités de chaque projet.

C.17.2. Les dangers repris dans le projet de liste ci-dessous sont appelés «dangers de départ» (starting point hazards, SPH), c'est-à-dire qu'il s'agit de dangers sur la base desquels une analyse des causes et des conséquences pourrait être réalisée afin de déterminer les mesures/barrières de sécurité et les exigences de sécurité pour maîtriser les dangers.

C.17.3. Liste des dangers du projet ROSA:

SPH 01	Mauvaise définition initiale de la vitesse limite (en fonction de l'infrastructure)
SPH 02	Mauvaise définition de la vitesse limite (en fonction du train)
SPH 03	Mauvaise définition de la distance de freinage / du profil de vitesse / des courbes de freinage
SPH 04	Décélération insuffisante (causes physiques)
SPH 05	Commande de vitesse / de freinage incorrecte / inadéquate
SPH 06	Vitesse enregistrée incorrecte (mauvaise vitesse du train)
SPH 07	Erreur de communication de la vitesse du train
SPH 08	Démarrage du train
SPH 09	Direction de déplacement incorrecte / mouvement intentionnel en sens inverse (combinaison de SPH 08 et SPH 14)
SPH 10	Enregistrement incorrect de la position relative/absolue
SPH 11	Erreur de détection du train
SPH 12	Perte d'intégrité du train
SPH 13	Itinéraire incorrect possible du train
SPH 14	Erreur de transmission / de communication de l'horaire/ de l'AM (autorité de mouvement)
SPH 15	Défaillance structurelle de la voie
SPH 16	Composant d'aiguillage cassé
SPH 17	Commande d'aiguillage incorrecte
SPH 18	État incorrect de l'aiguillage
SPH 19	Objet de système sur la voie / dans l'enveloppe de dégagement (ED) (hormis ballast)
SPH 20	Objet étranger sur la voie / dans l'ED
SPH 21	Usager de la route sur PN
SPH 22	Effet de sillage sur le ballast
SPH 23	Impact de forces aérodynamiques sur le train
SPH 24	Équipement / élément / chargement du train enfreint l'ED du train
SPH 25	Dimensions incorrectes de l'ED du train (bord de voie)
SPH 26	Distribution incorrecte de la charge
SPH 27	Roue cassée, essieu cassé
SPH 28	Échauffement d'un essieu / d'une roue / d'un appui

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu

SPH 29	Défaillance d'un bogie / d'une suspension / d'un amortisseur
SPH 30	Défaillance du châssis / de la carrosserie d'une voiture
SPH 31	Accès non autorisé (du point de vue de la sécurité)
SPH 32	Personne autorisée traverse la voie
SPH 33	Personnel au travail sur la voie
SPH 34	Personne non autorisée accède à la voie (négligence)
SPH 35	Chute d'une personne depuis le quai sur la voie
SPH 36	Sillage / personne trop proche du bord du quai
SPH 37	Personnel au travail près de la voie, par exemple sur la voie voisine
SPH 38	Personne quitte le train intentionnellement (hormis échange de passagers)
SPH 39	Personne tombe par une porte (latérale)
SPH 40	Personne tombe par la porte arrière de la dernière voiture
SPH 41	Train démarre / roule avec des portes ouvertes (sans enfreindre l'ED)
SPH 42	Personne tombe sur la passerelle entre deux voitures
SPH 43	Passager se penche par la porte
SPH 44	Passager se penche par la fenêtre
SPH 45	Personnel / accompagnant de train se penche par la porte
SPH 46	Personnel / accompagnant de train se penche par la fenêtre
SPH 47	Personnel de manœuvre sur véhicule se penche depuis le marchepied
SPH 48	Personne tombe/descend du quai dans l'écart entre le véhicule et le quai
SPH 49	Personne tombe du train / quitte le train en l'absence d'un quai
SPH 50	Personne tombe dans la zone de porte lors d'un échange de passagers
SPH 51	Fermeture des portes alors qu'une personne se trouve entre les portes
SPH 52	Mouvement du train pendant échange de passagers
SPH 53	Possibilité de personne blessée à bord
SPH 54	Risque d'incendie / d'explosion (dans le train / à proximité du train) - catégorie accident, conséquence de SPH 55, SPH 56
SPH 55	Température inappropriée (dans le train)
SPH 56	Intoxication / asphyxie (dans le train / à proximité du train)
SPH 57	Électrocution (dans le train / à proximité du train)
SPH 58	Personne tombe sur le quai (hormis échange de passagers)
SPH 59	Température inappropriée (sur le quai)
SPH 60	Intoxication / asphyxie (sur le quai)
SPH 61	Électrocution (sur le quai)

Agence ferroviaire européenne ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33(0)327096500 ● Fax +33(0)327334065 ● http://www.era.europa.eu