Europees Spoorwegbureau	
Verzameling van voorbeelden van risicobeoordelingen en van mogelijke hulpmiddelen ter onderbouwing van de CSM-verordening	
Referentie bij het ESB:	ERA/GUI/02-2008/SAF
Versie bij het ESB:	1.1
Datum:	06/01/2009

Document opgesteld door	Europees Spoorwegbureau Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Frankrijk
Soort document:	Leidraad
Status van het document:	Publiek

	Naam	**Functie**
Vrijgegeven door	Marcel VERSLYPE	Uitvoerend directeur
Gereviseerd door	Anders LUNDSTRÖM Thierry BREYNE	Hoofd eenheid Veiligheid Hoofd dienst Veiligheidsbeoordeling
Geschreven door (auteur)	Dragan JOVICIC	Projectmedewerker eenheid Veiligheid

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

DOCUMENTGEGEVENS

Wijzigingsoverzicht

Tabel 1: Status van het document.

Versie Datum	Auteur(s)	Documentver wijzing	Beschrijving wijziging
Vorige documenttitel en -structuur: *"Richtsnoer voor het gebruik van de aanbeveling over de 1ste reeks CSM"*			
Richtsnoer versie 0.1 15/02/2007	Dragan JOVICIC	Alles	Eerste versie van het "richtsnoer voor het gebruik" verbonden aan versie 1.0 van de "1ste reeks CSM-aanbevelingen". Dit is ook de eerste documentversie die voor formele herziening aan de CSM-werkgroep werd bezorgd.
Richtsnoer versie 0.2 07/06/2007	Dragan JOVICIC	Alles	Herschikken van het document om dit in overeenstemming te brengen met de structuur van versie 4.0 van de CSM-aanbeveling. Bijwerken van versie 1.0 van de aanbeveling op basis van het formele herzieningsproces door de CSM-werkgroep.
		Alles	Bijwerken van het document met aanvullende informatie die op interne vergaderingen van het ERA werd verzameld, alsook op verzoek van de CSM-actiegroep en -werkgroep om nieuwe punten uit te werken.
		Figuur 1	Wijzigen van de figuur met het "raamwerk voor risicobeheer van de eerste reeks gemeenschappelijke veiligheidsmethoden" in overeenstemming met de opmerkingen na herziening en de ISO-terminologie.
Richtsnoer versie 0.3 20/07/2007	Dragan JOVICIC	Aanhangsels	Herschikken van bestaande en aanmaken van nieuwe aanhangsels. Nieuw aanhangsel met daarin alle schema's ter illustratie en ter vereenvoudiging van de leesbaarheid en het begrip van de leidraad.
		Alle punten	Bijwerken van het document met als doel: • bestaande x punten zoveel mogelijk nader uit te werken; • nader toe te lichten wat wordt verstaan onder "aantonen dat het systeem aan de veiligheidsvereisten voldoet"; • een link te leggen met de CENELEC V-cyclus (dat wil zeggen figuur 8 en figuur 10 van EN 50 126); • verder de nadruk te leggen op de noodzaak van samenwerking en coördinatie tussen de verschillende actoren van de spoorwegsector wier activiteiten gevolgen kunnen hebben voor de veiligheid van het spoorwegsysteem; • duidelijkheid te verschaffen over het bewijsmateriaal (bijvoorbeeld gevarenlogboek of veiligheidsbewijs) dat de beoordelingsinstanties beoogt aan te tonen dat het CSM-risicobeoordelingsproces juist wordt toegepast; Verder bijwerken van het document na een eerste interne herziening bij het Spoorwegbureau.
Richtsnoer versie 0.4 16/11/2007	Dragan JOVICIC	Alle punten	Bijwerken van het document aansluitend aan de hand van het formele herzieningsproces, rekening houdend met de opmerkingen die over versie 0.3 werden gemaakt door de volgende leden van de CSM-werkgroep of organisaties en die telefonisch met hen werden afgesproken: • nationale veiligheidsinstanties van België, Spanje, Finland, Noorwegen, Frankrijk en Denemarken; • SIEMENS (lid van UNIFE); • Noorse infrastructuurbeheerder (Jernbaneverket – lid van EIM).
Richtsnoer versie 0.5 27/02/2008	Dragan JOVICIC	Alle punten	Bijwerken van het document rekening houdend met de opmerkingen die over versie 0.3 werden gemaakt door de volgende leden van de CSM-werkgroep of organisaties en die telefonisch met hen werden afgesproken: • CER

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

Tabel 1: Status van het document.

Versie Datum	Auteur(s)	Documentverwijzing	Beschrijving wijziging
			• nationale veiligheidsinstantie van Nederland
		Alle punten	Bijwerken van het document overeenkomstig de ondertekende versie van de CSM-aanbeveling. Bijwerken van het document rekening houdend met opmerkingen die naar aanleiding van de interne herziening bij het Spoorwegbureau werden gemaakt door Christophe CASSIR en Marcus ANDERSSON
		Alle punten Aanhangsels	Volledig hernummeren van de alinea's in het document conform de aanbeveling Toevoegen van toepassingsvoorbeelden van de CSM-aanbeveling.
Nieuwe documenttitel en -structuur: *"Verzameling van voorbeelden van risicobeoordelingen en bepaalde hulpmiddelen ter onderbouwing van de CSM-verordening"*			
Leidraad versie 0.1 23/05/2008	Dragan JOVICIC	Alles	Eerste versie van het document ontstaan uit de splitsing van het "richtsnoer voor het gebruik" versie 0.5 in twee aanvullende documenten.
Leidraad versie 02 03/09/2008	Dragan JOVICIC	Alles	Bijwerken van het document conform: • de CSM-verordening van de Europese Commissie {Ref. 3}; • opmerkingen van de workshop van 1 juli 2008 met leden van het "Railway Interoperability and Safety Committee" (RISC); • opmerkingen van de leden van de CSM-werkgroep (nationale veiligheidsinstanties van Noorwegen, Finland, het Verenigd Koninkrijk, Frankrijk, CER, EIM, Jens BRABAND [UNIFE] en Stéphane ROMEI [UNIFE].
Leidraad versie 1.0 10/12/2008	Dragan JOVICIC	Alles	Bijwerken van het document conform de CSM-verordening van de Europese Commissie inzake risico-evaluatie en –beoordeling {Ref. 3}, aangenomen door het "Railway Interoperability and Safety Committee" (RISC) op de plenaire vergadering van 25 november 2008
Leidraad versie 1.1 06/01/2009	Dragan JOVICIC	Alles	Bijwerken van het document rekening houdend met de opmerkingen bij de CSM-verordening door de juridische en taalkundige diensten van de Europese Commissie.

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

Inhoudsopgave

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

Figurenlijst

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

Tabellenlijst

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

0. INLEIDING

0.1. Toepassingsgebied

0.1.1. Voorliggend document bevat nadere informatie ter verduidelijking van de “Verordening van de Commissie betreffende de vaststelling van een gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling als bedoeld in artikel 6, lid 3, punt a), van Richtlijn 2004/49/EG van het Europees Parlement en de Raad” {Ref. 3}. In voorliggend document wordt naar deze verordening verwezen als “CSM-verordening”.

0.1.2. Dit is geen juridisch bindend document en de inhoud ervan kan in geen enkel opzicht worden geïnterpreteerd als enige manier om te voldoen aan de CSM-vereisten. Voorliggend document is bedoeld als aanvulling op de leidraad voor de toepassing van de CSM-verordening {Ref. 4} en verduidelijkt hoe het in de CSM-verordening genoemde proces moet worden gebruikt en toegepast. Dit document geeft aanvullende praktische informatie zonder evenwel verplicht na te leven procedures of juridisch bindende handelwijzen op te leggen. Deze informatie kan van nut zijn voor alle actoren[1] die activiteiten uitoefenen die gevolgen kunnen hebben voor de veiligheid van het spoorwegsysteem en die de CSM-verordening direct of indirect moeten toepassen. In dit document staan voorbeelden van risicobeoordelingen en worden mogelijke hulpmiddelen aangereikt ter onderbouwing van de toepassing van de CSM. Deze voorbeelden zijn alleen bedoeld als advies en toelichting. Actoren mogen alternatieve methoden toepassen of hun eigen, reeds bestaande methoden om de CSM-verordening na te leven, verder blijven gebruiken voor zover ze naar hun oordeel beter aangewezen zijn.
De voorbeelden en aanvullende informatie in dit document zijn niet volledig en bestrijken niet alle mogelijke situaties waarin belangrijke wijzigingen worden voorgesteld. Bijgevolg heeft dit document uitsluitend informatieve waarde.

0.1.3. Dit informatieve document mag uitsluitend worden gelezen als extra hulp bij de toepassing van de CSM-verordening. Voorliggend document dient samen met de CSM-verordening {Ref. 3} en de daarmee samenhangende leidraad {Ref. 4} te worden gebruikt met als doel de toepassing van de CSM te vergemakkelijken. Het beoogt geenszins de CSM-verordening te vervangen.

0.1.4. Dit document werd opgesteld door het Europees Spoorwegbureau (ERA) met de hulp van deskundigen van spoorwegverenigingen en nationale veiligheidsinstanties uit de CSM-werkgroep. Dit document bevat een uitvoerig overzicht van ideeën en informatie die het Spoorwegbureau heeft verzameld op interne vergaderingen en vergaderingen met de CSM-werkgroep en CSM-actiegroepen. Het Spoorwegbureau zal dit document indien nodig herzien en bijwerken zodat dit een afspiegeling blijft van de voortgang van de Europese normering, de wijzigingen in de CSM wat betreft de risicobeoordeling en eventueel opgedane ervaring met het gebruik van de CSM-verordening. Voor dit herzieningsproces kon bij het opstellen van dit document geen tijdschema worden vastgelegd. Daarom wordt de lezer aangeraden het Europees Spoorwegbureau te raadplegen voor informatie over de laatste uitgave van dit document.

---

(1) *De actoren waarvan sprake zijn de aanbestedende diensten bedoeld in artikel 2, onder r), van Richtlijn 2008/57/EG betreffende de interoperabiliteit van het spoorwegsysteem in de Gemeenschap, of de fabrikanten, in de verordening gezamenlijk “initiatiefnemer” genoemd, of hun leveranciers en dienstverleners.*

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

0.2. Beperking van het toepassingsgebied

0.2.1. Dit document bevat geen aanwijzingen over methoden voor het organiseren, exploiteren of ontwerpen (en vervaardigen) van een spoorwegsysteem of de samenstellende delen daarvan. Dit document bepaalt evenmin de contractuele overeenkomsten en afspraken die tussen bepaalde actoren kunnen bestaan voor de toepassing van het risicobeheerproces. Projectspecifieke contractuele afspraken vallen buiten het toepassingsgebied van de CSM-verordening en behoren dan ook niet tot de werkingssfeer van de daarmee samenhangende leidraad en het voorliggende document.

0.2.2. Ook al vallen ze buiten de werkingssfeer van dit document, de afspraken die tussen de betrokken actoren werden gemaakt, kunnen bij aanvang van het project in relevante contracten worden vastgelegd en doen geen afbreuk aan de bepalingen van de CSM. Dit kan bijvoorbeeld het geval zijn voor:

(a) de specifieke kosten voor het beheer van veiligheidsgerelateerde risico's bij de interfaces tussen de actoren;
(b) de specifieke kosten voor de overdracht van gevaren en daarmee samenhangende veiligheidsmaatregelen tussen actoren die nog onbekend zijn bij aanvang van het project;
(c) de manier om conflicten te beheren die tijdens het project kunnen ontstaan;
(d) enzovoort.

Indien tijdens de projectontwikkeling meningsverschillen of conflicten ontstaan tussen de initiatiefnemer en zijn onderaannemers, mogen de relevante contracten worden aangevoerd om conflictsituaties te helpen oplossen.

0.3. Opzet van dit document

0.3.1. Ook al lijkt dit een op zichzelf staand document voor leesdoeleinden, dit document beoogt geenszins de CSM-verordening {Ref. 3} te vervangen. Duidelijkheidshalve werd elk artikel van de CSM-verordening tekstueel in dit document overgenomen. Waar nodig wordt het desbetreffende artikel op voorhand uitgelegd in de leidraad voor de toepassing van de CSM-verordening {Ref. 4}. In de daarop volgende alinea's staat nadere uitleg om waar nodig opheldering te verschaffen en inzicht te geven in de CSM-verordening.

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

0.3.3. Om het de lezer makkelijker te maken, volgt de indeling van dit document de structuur van de CSM-verordening en de daarmee samenhangende leidraad.

0.4. Documentbeschrijving

0.4.1. Dit document is als volgt ingedeeld:

(a) hoofdstuk 0. bepaalt het toepassingsgebied van het document en geeft een overzicht van referentiedocumenten;

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

(b) bijlage I en bijlage II geven nadere uitleg over de corresponderende delen van de CSM-verordening {Ref. 3} en de daarmee samenhangende leidraad {Ref. 4};
(c) in nieuwe aanhangsels worden specifieke aspecten nader uitgewerkt en worden voorbeelden gegeven.

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

0.5. Referentiedocumenten

Tabel 2: Tabel met referentiedocumenten.

{Referentienr.}	Titel	Referentie	Versie
{Ref. 1}	Richtlijn 2004/49/EG van het Europees Parlement en de Raad van 29 april 2004 inzake de veiligheid op de communautaire spoorwegen en tot wijziging van Richtlijn 95/18/EG van de Raad betreffende de verlening van vergunningen aan spoorwegondernemingen, en van Richtlijn 2001/14/EG van de Raad inzake de toewijzing van spoorweginfrastructuurcapaciteit en de heffing van rechten voor het gebruik van spoorweginfrastructuur alsmede inzake veiligheidscertificering (Spoorwegveiligheidsrichtlijn)	2004/49/EG PB L 164 van 30.4.2004, blz. 44, gerectificeerd in PB L 220 van 21.6.2004, blz. 16.	-
{Ref. 2}	Richtlijn 2008/57/EG van het Europees Parlement en de Raad van 17 juni 2008 betreffende de interoperabiliteit van het spoorwegsysteem in de Gemeenschap	2008/57/EG PB L 191 van 18.7.2008, blz.1.	-
{Ref. 3}	Verordening (EG) nr. .../.. van de Commissie van [...] betreffende de vaststelling van een gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling, als bedoeld in artikel 6, lid 3, punt a), van Richtlijn 2004/49/EG van het Europees Parlement en de Raad	xxxx/jj/EG	aangenomen door RISC op 25.11.2008
{Ref. 4}	Leidraad voor de toepassing van de Verordening van de Commissie betreffende de vaststelling van een gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling als bedoeld in artikel 6, lid 3, punt a), van de Spoorwegveiligheidsrichtlijn	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Richtlijn 2008/57/EG van het Europees Parlement en de Raad van 17 juni 2008 betreffende de interoperabiliteit van het spoorwegsysteem in de Gemeenschap	2008/57/EG PB L 191 van 18.7.2008, blz.1.	-
{Ref. 6}	Veiligheidsbeheersysteem - Beoordelingscriteria voor spoorwegondernemingen en infrastructuurbeheerders	Beoordelingscriteria voor veiligheidsbeheersystemen Deel A Veiligheidscertificaten en -vergunningen	31/05/2007
{Ref. 7}	Spoorwegtoepassingen – Communicatie, signalering en processystemen – Elektronische signaleringssystemen met betrekking tot veiligheid	EN 50129	Februari 2003
{Ref. 8}	Spoorwegtoepassingen - De specificatie en het bewijs van de bruikbaarheid, beschikbaarheid, onderhoudbaarheid en veiligheid – Deel 1: de norm zelf	EN 50126-1	September 2006
{Ref. 9}	Spoorwegtoepassingen - De specificatie en het bewijs van de bruikbaarheid, beschikbaarheid, onderhoudbaarheid en veiligheid Deel 2: Richtsnoer voor de toepassing van EN 50126-1 voor veiligheidskwesties	EN 50126-2 (richtsnoer)	Definitief ontwerp (augustus 2006)
{Ref. 10}	Algemeen richtsnoer ter berekening van het risico inherent aan het vervoer van gevaarlijke goederen per spoor	OTIF-richtsnoer goedgekeurd door de commissie van deskundigen van het RID (reglement betreffende het internationale spoorwegvervoer van gevaarlijke goederen)	24 november 2005.
{Ref. 11}	Risicoaanvaardingscriterium voor technische systemen	Nota 01/08	1.1 (25/01/2008)

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

Tabel 2: Tabel met referentiedocumenten.

{Referentienr.}	Titel	Referentie	Versie
{Ref. 12}	Eenheid Veiligheid van het ERA: Haalbaarheidsstudie – Verdeling van veiligheidsdoelen (aan technische specificaties inzake interoperabiliteit van subsystemen) en consolidatie van technische specificaties inzake interoperabiliteit vanuit veiligheidsoogpunt WP1.1 - Beoordeling of de verdeling van gemeenschappelijke veiligheidsdoelen haalbaar is	WP1.1	1.0
{Ref. 13}	"Railtoepassingen — Classificatiesysteem voor railvoertuigen — Deel 4: EN 0015380 Deel 4: Functiegroepen".	EN 0015380 Deel 4	

0.6. Standaarddefinities, -begrippen en -afkortingen

0.6.1. De in dit document gebruikte algemene definities, begrippen en afkortingen zijn terug te vinden in een gewoon woordenboek.

0.6.2. Nieuwe definities, begrippen en afkortingen in dit document worden hieronder uitgelegd.

0.7. Specifieke definities

0.7.1. Zie Artikel 3.

0.8. Specifieke begrippen en afkortingen

0.8.1. Hieronder worden nieuwe specifieke begrippen en afkortingen uitgelegd die veelvuldig in voorliggend document worden gebruikt.

Tabel 3: Tabel met begripsomschrijvingen.

Begrip	Omschrijving
Spoorwegbureau	het Europees Spoorwegbureau (ERA)
leidraad	voorliggende "leidraad voor de toepassing van de Verordening van de Commissie (EG) nr. .../.. van [...] betreffende de vaststelling van een gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling, als bedoeld in artikel 6, lid 3, punt a), van Richtlijn 2004/49/EG van het Europees Parlement en de Raad"
CSM-verordening	de "Verordening (EG) nr. .../.. van de Commissie van [...] betreffende de vaststelling van een gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling, als bedoeld in artikel 6, lid 3, punt a), van Richtlijn 2004/49/EG van het Europees Parlement en de Raad" {Ref. 3}

Tabel 4: Afkortingentabel.

Afkorting	Betekenis
CCS	Besturings- en seingevingssysteem
CSM	Gemeenschappelijke veiligheidsmethode(n)
CST	Gemeenschappelijke veiligheidsdoelen

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

Tabel 4: Afkortingentabel.

Afkorting	Betekenis
EC	Europese Commissie
ERA	Europees Spoorwegbureau
IM	Infrastructuuurbeheerder(s)
ISA	Onafhankelijke veiligheidsbeoordelaar
OTIF	Intergouvernementele Organisatie voor het internationale spoorwegvervoer
MS	Lidstaat
NOBO	Aangemelde instantie
NSA	Nationale veiligheidsinstantie
QMP	Kwaliteitsborgingsproces
QMS	Kwaliteitsborgingssysteem
RISC	Railway Interoperability and Safety Committee
RU	Spoorwegonderneming(en)
SMP	Veiligheidsbeheerproces
SMS	Veiligheidsbeheersysteem
SRT	Veiligheid in spoorwegtunnels
TBC	Wordt later aangevuld
TSI	Technische specificatie voor interoperabiliteit

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

VERDUIDELIJKING VAN DE ARTIKELEN IN DE CSM-VERORDENING

Artikel 1. Doelstelling

Artikel 1, lid 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] Dit behoeft geen verdere uitleg.

Artikel 1, lid 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] Dit behoeft geen verdere uitleg.

Artikel 2. Toepassingsgebied

Artikel 2, lid 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] De CSM geldt voor het volledige spoorwegsysteem en behelst de beoordeling van de volgende wijzigingen in spoorwegsystemen voor zover die als belangrijk worden aangemerkt conform het bepaalde in Artikel 4:

(a) aanleg van nieuwe spoorlijnen of wijzigingen van bestaande spoorlijnen;
(b) invoering van nieuwe en/of gewijzigde technische systemen;
(c) wijzigingen van operationele aard (zoals nieuwe of gewijzigde bedrijfsvoorschriften en onderhoudsprocedures);

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

(d) wijzigingen van organisatorische aard bij spoorwegondernemingen/infrastructuurbeheerders.

In de CSM behelst de term “systeem” alle aspecten van een systeem, waaronder mede begrepen ontwikkeling, exploitatie, onderhoud, enz. tot de buitenbedrijfstelling of verwijdering.

[G 2] De CSM bestrijkt de belangrijke wijzigingen die zowel verband houden met:

(a) “kleine en eenvoudige” systemen die uit een klein aantal technische subsystemen of elementen kunnen bestaan,
(b) als met “grote en complexere” systemen (bijvoorbeeld stations en tunnels).

Artikel 2, lid 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:

(c) 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;
(d) 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] Overeenkomstig de Spoorwegveiligheidsrichtlijn {Ref. 1} en de spoorweginteroperabiliteitsrichtlijn {Ref. 2} moet rollend materieel van een nieuw type voor hogesnelheidslijnen bijvoorbeeld voldoen aan de technische specificatie voor interoperabiliteit voor hogesnelheidsmateriaal. Hoewel het beoordeelde systeem grotendeels wordt bestreken door de technische specificatie voor interoperabiliteit, komt het kernvraagstuk van menselijke factoren die verband houden met de stuurcabine daar niet aan bod. Bijgevolg moet het CSM-proces worden toegepast om zeker te stellen dat alle redelijkerwijs voorzienbare gevaren te wijten aan menselijke factoren (dat wil zeggen bij de interfaces tussen treinbestuurder, rollend materieel en de rest van het spoorwegsysteem) worden geïnventariseerd en op gepaste wijze worden beheerst.

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

Artikel 2, lid 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] Dit behoeft geen verdere uitleg.

Artikel 2, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 3. Definities

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 0;

(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

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

company safety targets;

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

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

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

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

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

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

(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[2], Directive 2001/16/EC of the European Parliament and the Council[3] and Directives2004/49/EC and 2008/57/EC.

---

(2) *PB L 235 van 17.9.1996, blz. 6.*

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

[G 1] Dit behoeft geen verdere uitleg.

Artikel 4. Belangrijke wijzigingen

Artikel 4, lid 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] Bestaat er geen aangemeld nationaal voorschrift, dan valt de beslissing onder de verantwoordelijkheid van de initiatiefnemer. De mate van belangrijkheid van de wijziging wordt bepaald op basis van deskundig oordeel. Heeft de voorgenomen wijziging in een bestaand systeem een hoge moeilijkheidsgraad, dan kan deze als belangrijk worden aangemerkt in zoverre de kans groot is dat bestaande systeemfuncties(4) daardoor worden beïnvloed, ook al houdt de wijziging zelf geen verband met de veiligheid.

Artikel 4, lid 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] **Voorbeeld van kleine wijzigingen:** Als de maximale baanvaksnelheid na inbedrijfstelling van het systeem eenmaal met 5 km/uur wordt verhoogd, gaat het niet om een belangrijke

Voortzetting van de voetnoot

(3) *PB L 110 van 20.4.2001, blz. 1.*

(4) *De functies in een systeem staan niet altijd los van elkaar. Bijgevolg kunnen wijzigingen van bepaalde functies ook andere systeemfuncties beïnvloeden, ook al hebben die wijzigingen op het eerste gezicht geen betrekking op deze functies.*

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

wijziging. Wordt de maximale baanvaksnelheid echter verder verhoogd in stappen van 5 km/uur, dan kan de som van de opeenvolgende wijzigingen (die afzonderlijk genomen geen belangrijke wijziging uitmaken) als belangrijke wijziging worden aangemerkt ten opzichte van de oorspronkelijke veiligheidsvereisten van het systeem.

[G 2] Om te bepalen of een reeks opeenvolgende (niet-belangrijke) wijzigingen als belangrijk moet worden aangemerkt, moet alle gevaren en daarmee samenhangende risico's worden bezien die door de gezamenlijke wijzigingen als geheel genomen worden teweeggebracht. De reeks voorgenomen wijzigingen mag als niet-belangrijk worden aangemerkt in zoverre het daaruit voortvloeiende risico algemeen aanvaardbaar is.

[G 3] Uit de werkzaamheden van het Spoorwegbureau inzake belangrijke wijzigingen is het volgende gebleken:

(a) het is niet mogelijk geharmoniseerde drempelwaarden of voorschriften vast te leggen waarmee voor een gegeven wijziging een beslissing over de mate van belangrijkheid van de wijziging kan worden genomen, en
(b) het is niet mogelijk een volledige, limitatieve lijst van belangrijke wijzigingen te geven;
(c) het kan zijn dat de beslissing niet van toepassing is op alle initiatiefnemers en op alle technische, operationele, organisatorische en milieutechnische condities.

Bijgevolg is het van cruciaal belang de beslissingsverantwoordelijkheid over de veilige exploitatie en beheersing van de daarmee samenhangende risico's over te laten aan de initiatiefnemer die voor het desbetreffende deel van het systeem verantwoordelijk is, overeenkomstig het bepaalde in artikel 4, lid 3, van de Spoorwegveiligheidsrichtlijn {Ref. 1}.

[G 4] Om de initiatiefnemer daarbij te helpen, staat onder C.2. in aanhangsel C een voorbeeld van "beoordeling en gebruik van criteria".

[G 5] De CSM mag niet worden toegepast wanneer een veiligheidsgerelateerde wijziging als niet-belangrijk wordt aangemerkt. Dat wil echter niet zeggen dat geen actie moet worden ondernomen: de initiatiefnemer moet (voorafgaande) risicoanalyses uitvoeren om te beslissen of het gaat om een belangrijke wijziging. Deze risicoanalyses moeten samen met de rechtvaardigingsgronden en argumenten worden gedocumenteerd met het oog op een controle door de nationale veiligheidsinstantie. Het oordeel betreffende de mate van belangrijkheid van een wijziging, en de beslissing dat het om een niet-belangrijke wijziging gaat, behoeven niet onafhankelijk te worden beoordeeld door een beoordelingsinstantie.

Artikel 5. Risicobeheerproces

Artikel 5, lid 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] Dit behoeft geen verdere uitleg.

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

Artikel 5, lid 2

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

[G 1] Dit behoeft geen verdere uitleg.

Artikel 5, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 6. Onafhankelijke beoordeling

Artikel 6, lid 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] De vereiste mate van onafhankelijkheid van de beoordelingsinstantie hangt af van het voor het beoordeelde systeem vereiste veiligheidsniveau. In afwachting dat dit onderwerp nader wordt geharmoniseerd, is de desbetreffende beste praktijk terug te vinden in artikel 8 van IEC61508-1:2001 of in punt 5.3.9. van de norm EN 50 129 {Ref. 7}. De mate van onafhankelijkheid wordt niet alleen bepaald door de ernstgraad van de gevolgen van het aan de uitrusting verbonden gevaar, maar ook door de nieuwheidsfactor daarvan. In punt 9.7.2 van EN 50 126-2 en in EN 50129 wordt de mate van onafhankelijkheid voor seingevingssystemen gedefinieerd. Deze definitie is in beginsel ook bruikbaar voor andere systemen.

[G 2] Het Spoorwegbureau is bezig met het nader definiëren van de functies en verantwoordelijkheden van de verschillende beoordelingsinstanties (nationale veiligheidsinstantie, aangemelde instantie en onafhankelijke veiligheidsbeoordelaar) alsook van de vereiste interfaces tussen deze beoordelingsinstanties. Daarbij zal in de mate van het mogelijke worden bepaald wie van deze beoordelingsinstanties wat moet doen en hoe. Uiteindelijk zal deze definitie:

(a) het mogelijk maken te bepalen hoe op basis van bewijsmateriaal moet worden nagegaan of de in de CSM genoemde risicobeheer- en risicobeoordelingsprocessen juist worden toegepast, en
(b) steun bieden aan de initiatiefnemer bij de beslissing om de belangrijke wijziging voor het beoordeelde systeem goed te keuren.

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

Artikel 6, lid 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 3] De werkzaamheden van het Spoorwegbureau zullen aanvullende informatie verschaffen over de functies en verantwoordelijkheden van de beoordelingsinstanties.

Artikel 6, lid 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] Dit behoeft geen verdere uitleg.

Artikel 6, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 7. Veiligheidsbeoordelingsverslagen

Artikel 7, lid 1

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

[G 1] Dit behoeft geen verdere uitleg.

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

Artikel 7, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 7, lid 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 3] Dit behoeft geen verdere uitleg.

Artikel 7, lid 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 4] Dit beginsel van wederzijdse erkenning wordt reeds aanvaard in de CENELEC-normen: zie punt 5.5.2 in EN 50 129, en punt 5.9 in EN 50 126-2. In CENELEC wordt het beginsel van de onderlinge erkenning toegepast door initiatiefnemers of onafhankelijke veiligheidsbeoordelaars op generieke producten en generieke toepassingen[(5)] mits de veiligheid wordt beoordeeld en aangetoond overeenkomstig het vereiste in de CENELEC-norm.

[G 5] Het beginsel van de wederzijdse erkenning moet ook worden toegepast voor de goedkeuring van nieuwe of gewijzigde systemen voor zover de daarmee samenhangende risicobeoordeling en het bewijs dat het systeem voldoet aan de veiligheidsvereisten beantwoorden aan het bepaalde in de CSM-verordening {Ref. 3}.

(5) *Zie onder [G 5] in punt 1.1.5 en de voetnoten (7) en (8), alsook Figuur 3, van voorliggend document voor meer uitleg over de termen "generiek product en generieke toepassing" en de daaraan inherente beginselen.*

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

Artikel 8. Risicobeheersingsmanagement/interne en externe audits

Artikel 8, lid 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] Dit behoeft geen verdere uitleg.

Artikel 8, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 9. Feedback en technische vooruitgang

Artikel 9, lid 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] Dit behoeft geen verdere uitleg.

Artikel 9, lid 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 2] Dit behoeft geen verdere uitleg.

Artikel 9, lid 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 3] Dit behoeft geen verdere uitleg.

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

Artikel 9, lid 4

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

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

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

[G 1] Dit behoeft geen verdere uitleg.

Artikel 10. Inwerkingtreding

Artikel 10, lid 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] Dit behoeft geen verdere uitleg.

Artikel 10, lid 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] Dit behoeft geen verdere uitleg.

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

BIJLAGE I - VERDUIDELIJKING VAN HET PROCES IN DE CSM-VERORDENING

1. ALGEMENE BEGINSELEN DIE VAN TOEPASSING ZIJN OP HET RISICOBEHEERPROCES

1.1. Algemene beginselen en verplichtingen

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] Het raamwerk voor risicobeheer van de CSM en het daarmee samenhangende risicobeoordelingsproces worden geïllustreerd in Figuur 1. Waar nodig worden alle kaders en activiteiten in deze figuur nader toegelicht in een specifiek punt van dit document.

[G 2] CENELEC adviseert de risicobeheer- en risicobeoordelingsprocessen te beschrijven in een veiligheidsplan. Als dat praktisch niet haalbaar is, mag de bijbehorende beschrijving in elk ander relevant document worden opgenomen. Zie punt 1.1.6.

[G 3] Uitgangspunt voor het risicobeoordelingsproces is een voorafgaande systeemomschrijving. Tijdens de projectontwikkeling wordt de voorlopige systeemomschrijving gaandeweg bijgewerkt en vervangen door de systeemomschrijving. Is er geen voorafgaande systeemomschrijving, dan wordt de risicobeoordeling uitgevoerd met behulp van de formele systeemomschrijving. In dat geval is het nuttig dat alle bij de belangrijke wijziging betrokken actoren elkaar bij aanvang van het project ontmoeten met als doel:

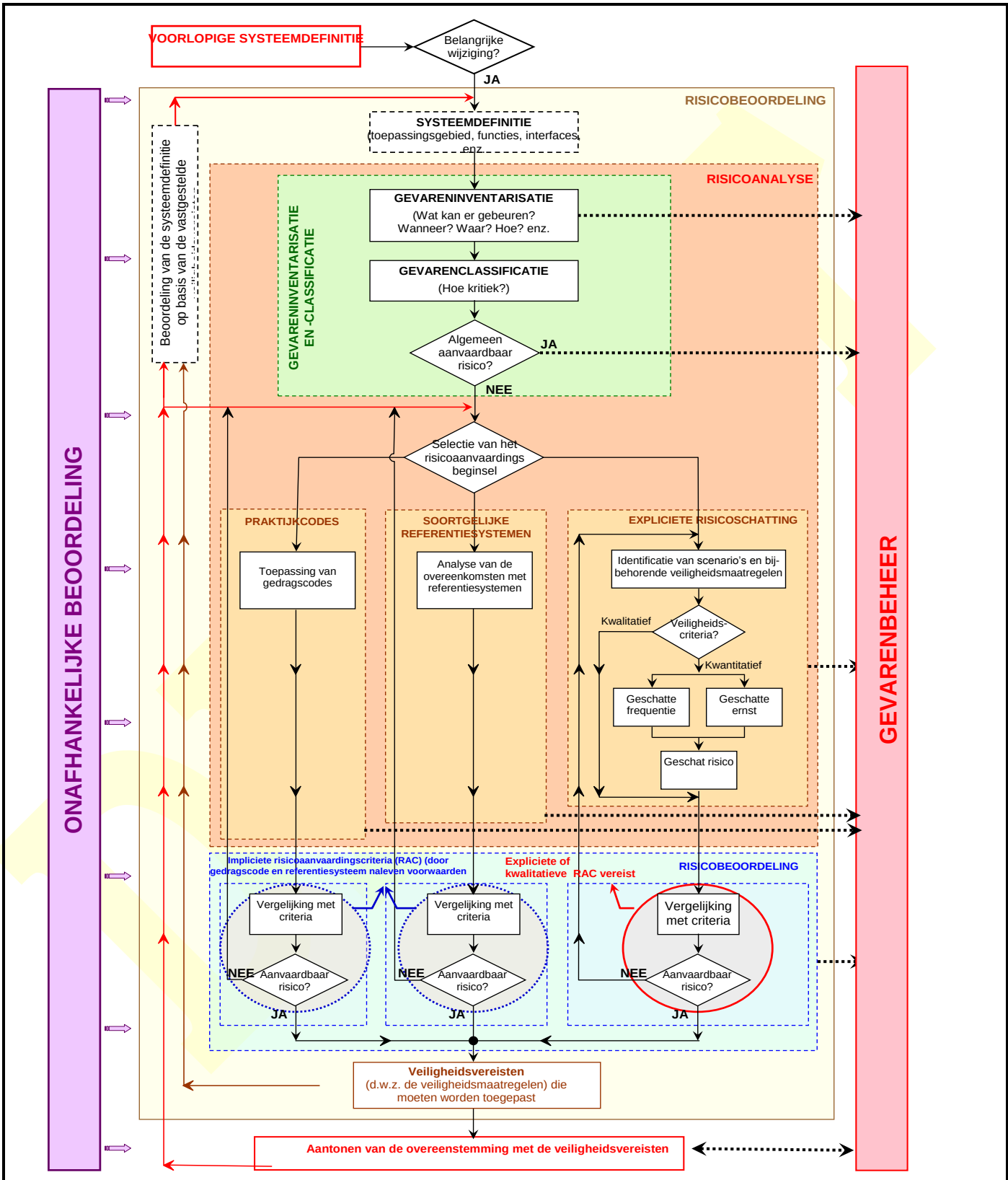
(a) het eens te worden over de alomvattende grondslagen, functies e.d. van het systeem. In beginsel mag dit nader worden omschreven in een voorafgaande systeemomschrijving;
(b) het eens te worden over de projectorganisatie;
(c) het eens te worden over het delen van functies en verantwoordelijkheden tussen de verschillende reeds betrokken actoren, waar nodig met inbegrip van de nationale veiligheidsinstantie, aangemelde instantie en onafhankelijke veiligheidsbeoordelaar.

Deze coördinatie, bijvoorbeeld tijdens de voorafgaande systeemomschrijving, geeft de initiatiefnemer, de onderaannemers, de nationale veiligheidsinstantie, de aangemelde instantie en de onafhankelijke veiligheidsbeoordelaar zo nodig de gelegenheid het in een

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

vroeg stadium eens te worden over de praktijkcodes of referentiesystemen waarvan het gebruik in projectverband aanvaardbaar is.

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



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

Figuur 1: Raamwerk voor risicobeheer van de CSM-verordening {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] Het veiligheidsbeheersysteem van de spoorwegonderneming en infrastructuurbeheerder geeft nauwkeurig het proces en de procedures aan om:

(a) erop toe te zien dat het systeem veilig blijft tijdens de volledige levenscyclus (dat wil zeggen tijdens exploitatie en onderhoud);
(b) te zorgen dat het bijbehorende systeem veilig wordt ontmanteld of vervangen.

Dit proces maakt geen deel uit van de CSM inzake risicobeoordeling.

[G 2] Om de CSM ten uitvoer te leggen, moeten alle betrokken partijen competent zijn (dat wil zeggen beschikken over de juiste vaardigheden, kennis en ervaring). Binnen de organisaties van de actoren in de spoorwegsector is voortdurend behoefte aan beheer van vakbekwaamheid:

(a) voor de infrastructuurbeheerders en spoorwegondernemingen is dit de taak van hun veiligheidsbeheersysteem overeenkomstig bijlage III, punt 2, onder e), van de Spoorwegveiligheidsrichtlijn {Ref. 1};
(b) ook al is het veiligheidsbeheersysteem niet verplicht, de andere actoren die activiteiten uitoefenen die gevolgen kunnen hebben voor de veiligheid van het spoorwegsysteem beschikken doorgaans minstens op projectniveau (zie onder 5 in punt 5.1) over een kwaliteitsborgingsproces en/of veiligheidsbeheerproces dat aan deze eis voldoet.

[G 3] Volgende punten van de CENELEC-norm EN 50 126-1 {Ref. 8} bevatten richtsnoeren inzake vakbekwaamheid:

(a) punt 5.3.5.(b): *"het voltallige personeel dat verantwoordelijkheden draagt"* in het risico*"beheerproces"* moet *"over voldoende vakbekwaamheid beschikken om deze verantwoordelijkheden te volbrengen"*;
(b) punt 5.3.5.(d): de voorschriften inzake risicobeheer en risicobeoordeling moeten *"ten uitvoer worden gelegd in het kader van bedrijfsprocessen onderbouwd door een kwaliteitsborgingssysteem dat voldoet aan de vereisten in EN ISO 9001, EN ISO 9002 of EN ISO 9003 die toepasselijk zijn voor het systeem"* dat wordt beoordeeld. Punt 5.2. van de norm EN 50 129 {Ref. 7} geeft een voorbeeld van de aspecten die onder het kwaliteitsborgingssysteem vallen.

Het gaat hier om kwaliteitsborgingsactiviteiten alsook om de vakbekwaamheid van en opleiding voor personeel/medewerkers ter onderbouwing van het door de CSM bestreken proces.

[G 4] Vaak wordt in de beginfase van het project follow-up aan het risicobeoordelingsproces gegeven door een beoordelingsinstantie. Tenzij anders voorgeschreven in de nationale wetgeving van een lidstaat, is deze deelneming van de beoordelingsinstantie in de beginfase niet verplicht, maar wel aan te raden. Het oordeel van de onafhankelijke beoordelingsinstantie kan van pas komen alvorens naar de volgende stap in het

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

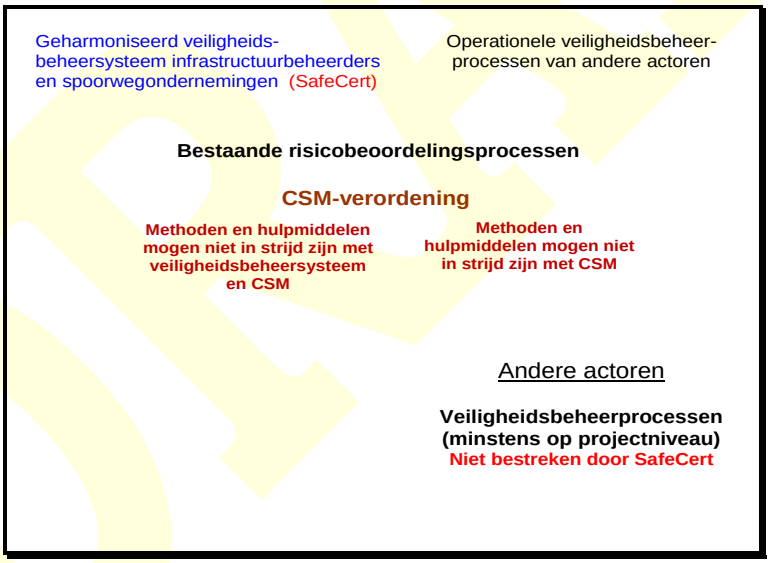
risicobeoordelingsproces te gaan. Zie Artikel 6 voor meer informatie over de onafhankelijke beoordeling.

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] Dit behoeft geen verdere uitleg.

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] Figuur 2 toont het verband tussen de CSM en de “veiligheidsbeheersystemen en risicobeoordelingsprocessen”.



Figuur 2: Geharmoniseerd veiligheidsbeheersysteem en CSM.

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

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] Is de initiatiefnemer een infrastructuurbeheerder of spoorwegonderneming, dan kan het soms nodig zijn andere actoren bij het proces te betrekken(6) (zie punt 1.2.1). In bepaalde gevallen kan de infrastructuurbeheerder of spoorwegonderneming de risicobeoordelingsactiviteiten volledig of gedeeltelijk uitbesteden. Doorgaans worden de betrokken actoren het in de beginfase van het project eens over de functies en verantwoordelijkheden van elke actor.

[G 2] Op te merken valt dat de initiatiefnemer te allen tijde verantwoordelijk blijft voor de toepassing van de CSM, voor de acceptatie van het risico en zodoende voor de veiligheid van het systeem. Daarbij moet erop worden toegezien dat:

(a) de betrokken actoren volledig met elkaar samenwerken zodat alle vereiste informatie wordt verschaft, en
(b) het duidelijk is wie aan de bijzondere CSM-vereisten moet voldoen (bijvoorbeeld de risicoanalyse uitvoeren of de gevareninventaris beheren).

Als de actoren het niet eens zijn over de na te leven veiligheidsvereisten, mag de nationale veiligheidsinstantie worden geraadpleegd voor advies. De verantwoordelijkheid om een oplossing te vinden blijft echter rusten op de initiatiefnemer en kan niet aan de nationale veiligheidsinstantie worden overgedragen: zie ook punt 0.2.2.

[G 3] Wordt de taak uitbesteed aan een onderaannemer die geen infrastructuurbeheerder of spoorwegonderneming is, dan bestaat geen verplichting tot het hebben van een eigen veiligheidsorganisatie, zeker als de onderaannemer klein in omvang/structuur is of slechts een beperkte rol in het gehele systeem vervult. De verantwoordelijkheid voor het risicobeheer, waaronder begrepen de activiteiten van risicobeoordeling en gevarenbeheer, blijft dan op het bovenliggende organisatieniveau (zijnde de klant van de onderaannemer). De onderaannemer blijft echter de verantwoordelijkheid dragen om de juiste informatie over zijn activiteiten te verschaffen die de bovenliggende organisatie nodig heeft om de risicobeheerdocumentatie samen te stellen.
Samenwerkende organisaties kunnen om redenen van kosteneffectiviteit ook afspreken een gemeenschappelijke veiligheidsorganisatie op te zetten. In dat geval worden de veiligheidsactiviteiten van alle betrokken organisaties door slechts één organisatie beheerd. De organisatie die als taak heeft de met deze veiligheidsmaatregelen verband houdende gevaren te beheersen, blijft verantwoordelijk voor de nauwkeurigheid van de informatie (dat wil zeggen gevaren, risico's en veiligheidsmaatregelen) alsmede voor het beheer van de tenuitvoerlegging van de veiligheidsmaatregelen.

[G 4] De initiatiefnemer bepaalt doorgaans de "veiligheidsniveaus" en "veiligheidsvereisten" die worden toegewezen aan de bij het project betrokken actoren en aan de verschillende subsystemen en installaties van deze actoren:

(a) in de contracten tussen de initiatiefnemer en de respectieve actoren (onderaannemers);

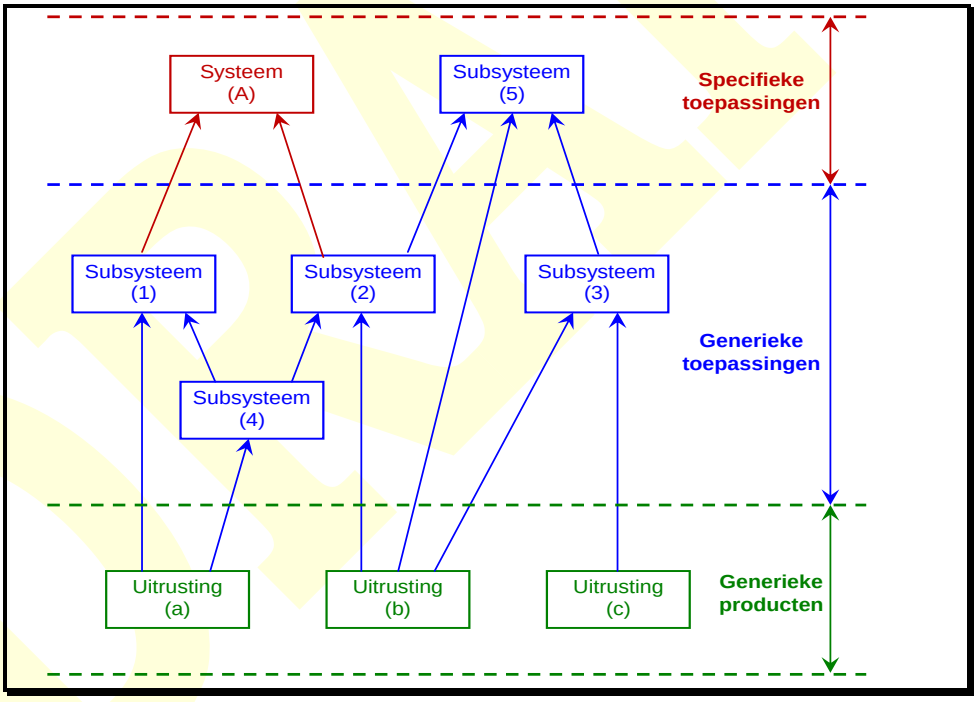
(6) *Dit is in overeenstemming met bijlage A.4 van de CENELEC-norm 50 129 {Ref. 7}.*

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

(b) in een veiligheidsplan, of elk ander relevant document dat hetzelfde doel beoogt, met de beschrijving van de gehele projectorganisatie en verantwoordelijkheden van elke actor, inclusief die van de initiatiefnemer: zie punt 1.1.6;
(c) in de gevareninventaris van de initiatiefnemer: zie punt 4.1.1.

Tijdens de fase “aantonen dat het systeem voldoet aan de veiligheidsvereisten” kan deze toewijzing van systeemspecifieke “veiligheidsniveaus” en “veiligheidsvereisten” tot op het niveau van de onderliggende subsystemen en installaties, en bijgevolg ook aan de respectieve actoren met inbegrip van de initiatiefnemer zelf, worden verfijnd/uitgebreid: zie Figuur 1. Vergeleken met de CENELEC V-cyclus (zie punt 2.1.1 en Figuur 5 op pagina 37) komt deze activiteit overeen met fase 5 "verdeling van de systeemeisen" tot op het niveau van de verschillende subsystemen en onderdelen.

[G 5] Krachtens artikel 5, lid 2, mogen andere actoren dan de spoorwegonderneming en infrastructuurbeheerder de volledige verantwoordelijkheid voor de conformiteit met de CSM op zich nemen, naargelang van hun respectieve behoeften. Wat betreft generieke producten of generieke toepassingen[7] bijvoorbeeld, kan de fabrikant de risicobeoordeling uitvoeren op basis van een "generieke systeemomschrijving" met als doel de veiligheidsniveaus en veiligheidsvereisten te preciseren waaraan generieke producten en generieke toepassingen moeten voldoen.



Figuur 3: Voorbeelden van afhankelijkheidsrelaties tussen veiligheidsbewijzen (overgenomen uit figuur 9 in de norm EN 50 129).

[G 6] CENELEC adviseert dat de fabrikant bewijsstukken afkomstig van de risicobeoordeling overlegt ter onderbouwing van veiligheidsbewijzen en gevareninventarissen voor generieke

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

producten (en/of generieke toepassingen[7]). Deze veiligheidsbewijzen en gevareninventarissen bevatten alle aannames[8] en onderkende "gebruiksbeperkingen" (dat wil zeggen veiligheidsgerelateerde toepassingsvoorwaarden) die voor de desbetreffende generieke producten gelden (en/of generieke toepassingen). Telkens als generieke producten en generieke toepassingen voor exploitatiedoeleinden worden gebruikt in een specifieke toepassing, moet bijgevolg de conformiteit met al deze aannames[8] en "gebruiksbeperkingen" (dat wil zeggen veiligheidsgerelateerde toepassingsvoorwaarden) worden aangetoond in elke specifieke toepassing.

---

(7) *De begrippen "generieke toepassing" en "veiligheidsbewijs generiek product" zijn overgenomen uit CENELEC waar drie verschillende categorieën veiligheidsbewijzen in overweging worden genomen (zie Figuur 3):*

(a) ***Veiligheidsbewijs generiek product*** *(toepassingsonafhankelijk). Een generiek product mag opnieuw worden gebruikt voor verschillende van elkaar losstaande toepassingen;*

(b) ***Veiligheidsbewijs generieke toepassing*** *(voor een toepassingsklasse). Een generieke toepassing mag opnieuw worden gebruikt voor een toepassing van bepaalde klasse of bepaald type met gemeenschappelijke functies;*

(c) ***Toepassingsspecifiek veiligheidsbewijs*** *(voor een specifieke toepassing). Een specifieke toepassing wordt uitsluitend voor één afzonderlijke installatie gebruikt.*

Voor meer informatie over de onderlinge afhankelijkheidsrelaties wordt verwezen naar punt 9.4. en figuur 9.1 van het CENELEC-richtsnoer 50 126-2 {Ref. 9}.

(8) *Deze aannames, onderstellingen en gebruiksbeperkingen bepalen de grenzen en geldigheid van de "veiligheidsbeoordelingen" en "veiligheidsanalyses" die verband houden met de desbetreffende veiligheidsbewijzen van generieke producten en generieke toepassingen. Als de specifieke toepassing in kwestie daar niet aan voldoet, moeten de bijbehorende "veiligheidsbeoordelingen" en "veiligheidsanalyses" (bijvoorbeeld van causale aard, betreffende het verband van oorzaak en gevolg) worden bijgewerkt of vervangen.*

> *Een en ander sluit aan op het volgende algemene veiligheidsbeginsel: "Telkens als generieke toepassingen en generieke producten ten grondslag liggen aan een specifiek (sub)systeemontwerp, moet worden aangetoond dat het specifieke (sub)systeem in kwestie voldoet aan alle aannames, onderstellingen en gebruiksbeperkingen (in CENELEC veiligheidsgerelateerde toepassingsvoorwaarden genoemd) die worden geëxporteerd in de corresponderende veiligheidsbewijzen van de generieke toepassingen en generieke producten (zie Figuur 3)".*

Kan voor een specifieke toepassing niet worden voldaan aan bepaalde aannames, onderstellingen en gebruiksbeperkingen (bijvoorbeeld wat betreft operationele veiligheidsvereisten), dan mogen de bijbehorende aannames, onderstellingen en gebruiksbeperkingen naar een hoger niveau worden overgedragen (zijnde doorgaans het systeemniveau). Deze aannames, onderstellingen en gebruiksbeperkingen worden dan duidelijk omschreven in het "toepassingsspecifieke veiligheidsbewijs" van het desbetreffende subsysteem. Dit is van cruciaal belang om te waarborgen dat de veiligheidsgerelateerde toepassingsvoorwaarden van elk veiligheidsbewijs in zulke afhankelijkheidsrelaties worden nageleefd voor het bovenliggende veiligheidsbewijs, of anders worden overgebracht naar de veiligheidsgerelateerde toepassingsvoorwaarden van het veiligheidsbewijs op het hoogste niveau, meer in het bijzonder dat van het systeem.

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

1.1.6.	*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] Tenzij bij aanvang van het project contractueel anders wordt overeengekomen, bestaat voor elk project doorgaans een document waarin de risicobeheeractiviteiten nader worden omschreven. Dit document wordt telkens bijgewerkt en herzien wanneer belangrijke wijzigingen in het oorspronkelijke systeem worden aangebracht.

[G 2] Dit document bepaalt de organisatiestructuur, de toegewezen personeelsverantwoordelijkheden, de processen, procedures en activiteiten die als geheel waarborgen dat het beoordeelde systeem voldoet aan de opgegeven veiligheidsniveaus en veiligheidsvereisten. Aangezien dit document als hulpmiddel en leidraad dient voor de beoordelingsinstantie, moet het voldoen aan de CSM. In de CENELEC-normen wordt geadviseerd deze informatie op te nemen in een veiligheidsplan of in een ander document waarin deze onderwerpen deels aan bod komen.

[G 3] De gehele projectorganisatie wordt beschreven in het veiligheidsplan van de initiatiefnemer in het bijzonder of in elk ander toepasselijk document. Het beschrijft hoe de functies en verantwoordelijkheden onder de betrokken actoren worden verdeeld. Voor meer informatie kan worden verwezen naar de veiligheidsplannen of veiligheidsorganisaties van de verschillende betrokken actoren. Doorgaans wordt de verantwoordelijkheidsverdeling tussen de verschillende actoren besproken en onderling overeengekomen tijdens de voorafgaande systeemomschrijving (dat wil zeggen bij aanvang van het project), voor zover die bestaat.

[G 4] Het veiligheidsplan is een dynamisch document dat waar nodig tijdens de projectlevensduur wordt bijgewerkt.

[G 5] Meer informatie over de inhoud van een veiligheidsplan is terug te vinden in de norm EN 50 126-1 {Ref. 8} en het daarmee samenhangende richtsnoer 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] Dit behoeft geen verdere uitleg.

1.2. Beheer van 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] Verwacht een spoorwegonderneming bijvoorbeeld om operationele redenen dat een infrastructuurbeheerder bepaalde infrastructurele wijzigingen aanbrengt, dan moet de spoorwegonderneming krachtens het vereiste in bijlage III, punt 2, onder g), van de Spoorwegveiligheidsrichtlijn {Ref. 1} ook toezien op de algemene werkzaamheden om te

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

waarborgen dat de verwachte wijzigingen juist worden uitgevoerd. Deze leidinggevende taak van de spoorwegonderneming ontslaat de infrastructuurbeheerder echter niet van de verantwoordelijkheid om andere spoorwegondernemingen op de hoogte te brengen die door de desbetreffende infrastructurele wijziging kunnen worden beïnvloed. Mogelijk dient de infrastructuurbeheerder zelfs een CSM-conforme risicobeoordeling uit te voeren als het uit zijn oogpunt om een belangrijke wijziging gaat.

[G 2] Overdracht van verantwoordelijkheden tussen de verschillende actoren is mogelijk en onder bepaalde omstandigheden zelfs noodzakelijk. Wanneer echter verschillende actoren bij een systeem betrokken zijn, wordt doorgaans één actor aangewezen die de verantwoordelijkheid voor het systeem als geheel draagt. Er bestaan altijd afhankelijkheidsrelaties tussen subsystemen en de exploitatie die bijzondere inspanningen vergen om in kaart te worden gebracht. Zo dient de instantie die de eindverantwoordelijkheid voor de veiligheidsanalyses op zich neemt ook volledige toegang te krijgen tot alle relevante documentatie. Het spreekt vanzelf dat de initiatiefnemer die voornemens is de belangrijke wijziging in te voeren doorgaans de eindverantwoordelijkheid draagt om te zorgen dat de risicobeoordeling stelselmatig en volledig wordt uitgevoerd.

[G 3] Voor het beheer van een interface tussen de betrokken actoren moet overeenstemming worden bereikt over de volgende hoofdcriteria:

(a) de leiding is doorgaans in handen van de initiatiefnemer die voornemens is de belangrijke wijziging in te voeren;
(b) de vereiste input;
(c) de methoden voor gevareninventarisatie en risicobeoordeling;
(d) de vereiste deelnemers met de verlengde vakbekwaamheid (dat wil zeggen combinatie van kennis, vaardigheden en praktijkervaring – zie ook de definitie van "vakkundigheid van het personeel" onder [G 2], sub b), van artikel 3 in {Ref. 4});
(e) de verwachte output.

Deze criteria worden omschreven in de veiligheidsplannen (of andere relevante documenten) van de ondernemingen die met de desbetreffende interfaces te maken hebben.

[G 4] Onder C.3. in aanhangsel C staan voorbeelden van interfaces, alsmede een voorbeeld van de toepassing van deze hoofdcriteria op het beheer van de interface tussen een treinfabrikant en een infrastructuurbeheerder of spoorwegonderneming.

[G 5] In het interfacebeheer moeten ook de risico's aan bod komen die bij de interfaces kunnen optreden met menselijke operators (die voor exploitatie en onderhoud worden ingezet) met het oog op het ontwerp van deze interfaces.

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

[G 1] Het overdrachtsproces van gevaren en daarmee samenhangende veiligheidsmaatregelen tussen actoren is ook van toepassing op de onderliggende niveaus van de CENELEC V-cyclus in Figuur 5 op pagina 37. Dit proces kan bijvoorbeeld worden toegepast iedere keer dat deze informatie moet worden uitgewisseld tussen een actor en zijn onderaannemers. Het verschil met hetzelfde proces op systeemniveau is dat de initiatiefnemer niet op de hoogte moet worden gesteld van elke overdracht van gevaren en daarmee samenhangende veiligheidsmaatregelen op subsystemniveau. De initiatiefnemer wordt alleen geïnformeerd

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

wanneer de overgedragen gevaren en daarmee samenhangende veiligheidsmaatregelen betrekking hebben op bovenliggende interfaces (voor zover die gevolgen hebben voor een interface met de initiatiefnemer).

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] Het veiligheidsbeheersysteem van de spoorwegonderneming en infrastructuurbeheerder behelst de afspraken en procedures om te waarborgen dat elke non-conformiteit of ontoereikendheid van veiligheidsmaatregelen juist wordt beheerd. Deze afspraken en procedures maken dan ook geen deel uit van de CSM.

[G 2] Op dezelfde wijze worden afspraken en procedures(9) die de andere actoren(10) moeten opzetten om te waarborgen dat elke non-conformiteit of ontoereikendheid van veiligheidsmaatregelen juist wordt beheerd en om de veiligheidsmaatregelen zo nodig aan alle betrokken actoren over te dragen, bij aanvang van het project overeengekomen tussen de betrokken actoren en nader toegelicht in hun veiligheidsplan: zie punt 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] Op die manier kan elke mogelijke non-conformiteit of ontoereikendheid van veiligheidsmaatregelen worden beheerd in het beoordeelde systeem of in soortgelijke systemen waar dezelfde maatregel wordt gebruikt.

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] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

(9) *In beginsel worden deze afspraken en procedures bestreken door het kwaliteitsborgings- en/of veiligheidsbeheerproces van deze actoren dat minstens op projectniveau werd opgesteld (zie ook Figuur 2).*

(10) *Onder "andere actoren" wordt verstaan alle betrokken actoren met uitzondering van infrastructuurbeheerders en spoorwegondernemingen.*

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

1.2.7.	*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] Dit behoeft geen verdere uitleg.

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

2. BESCHRIJVING VAN HET RISICOBEOORDELINGSPROCES

2.1. Algemene beschrijving - Overeenkomst tussen het CSM-conforme risicobeoordelingsproces en de CENELEC V-cyclus

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

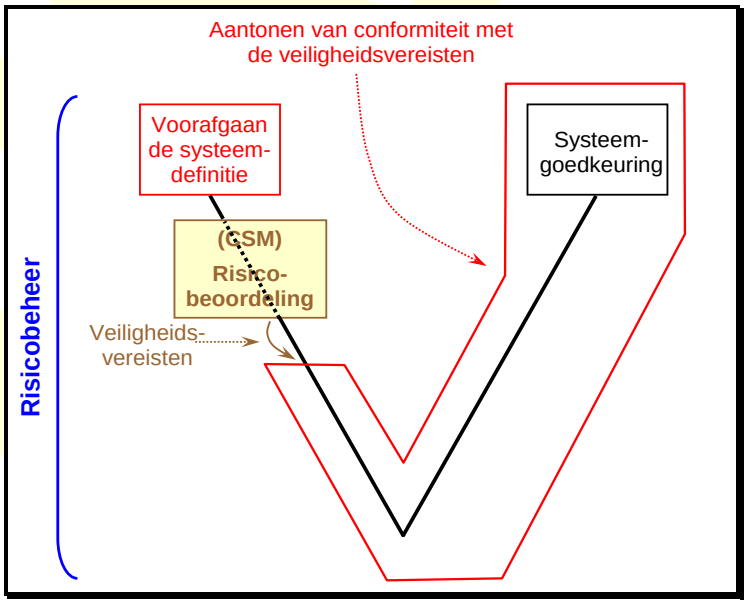
(a) the system definition;
(b) the risk analysis including the hazard identification;
(c) the risk evaluation.

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

[G 1] Het in de CSM behandelde risicobeheerproces kan worden voorgesteld in een V-cyclus die begint met de (voorafgaande) systeemomschrijving en eindigt met de systeemgoedkeuring: zie Figuur 4. Deze vereenvoudigde V-cyclus kan dan worden vertaald in de klassieke V-cyclus in figuur 10 van de norm EN 50 126-1 {Ref. 8}. Om de overeenkomst aan te tonen met het CSM-conforme risicobeheerproces in Figuur 1 wordt de CENELEC V-cyclus in figuur 10 overgenomen in Figuur 5:

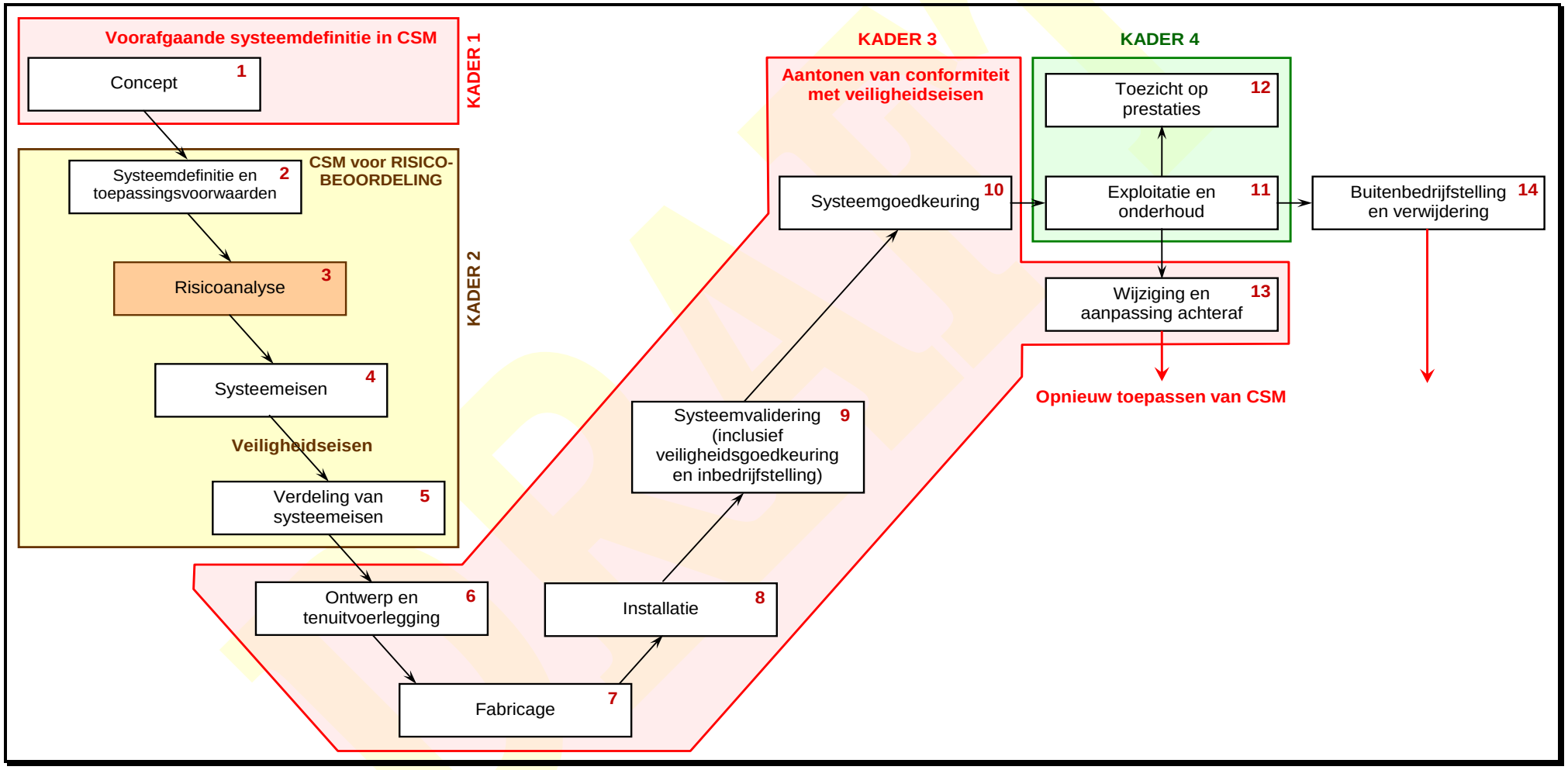
(a) de CSM-conforme "voorafgaande systeemomschrijving" in Figuur 1 komt overeen met fase 1 in de CENELEC V-cyclus, dat wil zeggen met de definitie van het "systeemconcept" (zie KADER 1 in Figuur 5);
(b) de CSM-conforme "risicobeoordeling" in Figuur 1 omvat de volgende fasen van de CENELEC V-cyclus (zie KADER 2 in Figuur 5):

(1) Fase 2 in Figuur 5: "systeemomschrijving en toepassingsvoorwaarden";
(2) Fase 3 in Figuur 5: "risicoanalyse";
(3) Fase 4 in Figuur 5: "systeemeisen";
(4) Fase 5 in Figuur 5: "verdeling van systeemeisen" tot op het niveau van de verschillende subsystemen en onderdelen.



Figuur 4: Vereenvoudigde V-cyclus van figuur 10 in de norm EN 50 126.

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



Figuur 5: Figuur 10 van de V-cyclus in EN 50 126 (CENELEC-systeemlevenscyclus).

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

[G 2] Output van het risicobeoordelingsproces in de CSM (na iteraties - zie Figuur 1):

(a) de "systeemomschrijving" na bijwerking met de "veiligheidsvereisten" resulterend uit de activiteiten "risicoanalyse" en "risico-evaluatie" (zie punt 2.1.6);
(b) de "verdeling van systeemeisen" tot op het niveau van de verschillende subsystemen en onderdelen (fase 5 in Figuur 5);
(c) de "gevareninventaris" waarin de volgende gegevens worden vastgelegd:

(1) alle geïnventariseerde gevaren en daarmee samenhangende veiligheidsmaatregelen;
(2) de resulterende veiligheidsvereisten;
(3) de voor het systeem toegepaste aannames die de grenzen en geldigheid van de risicobeoordeling bepalen (zie onder (g) in punt 2.1.2);

(d) en in het algemeen al het bewijsmateriaal resulterend uit de toepassing van de CSM: zie punt 5.

Deze output van de CSM-conforme risicobeoordeling komt overeen met de veiligheidsgerelateerde output van fase 4 in de CENELEC V-cyclus, dat wil zeggen met de specificatie van de systeemeisen in Figuur 5.

[G 3] De systeemomschrijving na bijwerking met de resultaten van de risicobeoordeling en de gevareninventaris vormt de input voor ontwerp en goedkeuring van het systeem. Het "aantonen dat het systeem het voldoet aan de veiligheidsvereisten" conform de CSM komt overeen met de volgende fasen in de CENELEC V-cyclus (zie KADER 3 in Figuur 5):

(a) Fase 6 in Figuur 5: "ontwerp en tenuitvoerlegging";
(b) Fase 7 in Figuur 5: "fabricage";
(c) Fase 8 in Figuur 5: "installatie";
(d) Fase 9 in Figuur 5: "systeemvalidering (inclusief veiligheidsgoedkeuring en inbedrijfstelling)";
(e) Fase 10 in Figuur 5: "systeemgoedkeuring".

[G 4] De technische, operationele of organisatorische aard van de belangrijke wijziging bepaalt of de conformiteit van het systeem met de veiligheidsvereisten wordt aangetoond. Het kan dus zijn dat niet alle stappen in de CENELEC V-cyclus in Figuur 5 geschikt zijn voor alle belangrijke wijzigingen in kwestie. De V-cyclus in Figuur 5 moet dienovereenkomstig worden bezien en gebruikt met de nodige zaakkundigheid over wat het meest aangewezen is voor elke specifieke toepassing (zo is er bijvoorbeeld voor wijzigingen van operationele en organisatorische aard geen fabricagefase).

[G 5] Anders gezegd, het "aantonen dat het systeem voldoet aan de veiligheidsvereisten" conform de CSM omvat niet alleen de activiteiten van "keuring en validering" door beproevingen of simulatie. In de praktijk behelst dit alle fasen "6 tot 10" (zie bovenstaande lijst en Figuur 5) in de CENELEC V-cyclus. Deze activiteiten omvatten ontwerp, fabricage, installatie, keuring en validering, alsook de daarmee samenhangende activiteiten inzake betrouwbaarheid, beschikbaarheid, onderhoudbaarheid en veiligheid en de systeemgoedkeuring.

[G 6] Bij het "aantonen dat het systeem voldoet aan de veiligheidsvereisten" geldt als stelregel dat de veiligheidsgerelateerde functies en interfaces van het systeem centraal staan in de risicobeoordeling. Met andere woorden: als voor een van de fasen in de CENELEC V-cyclus in Figuur 5 risico- en veiligheidsbeoordelingsactiviteiten nodig zijn, dan worden die gericht op:

(a) de veiligheidsgerelateerde functies en interfaces;

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

(b) de subsystemen en/of onderdelen die van belang zijn ter voltooiing van de veiligheidsgerelateerde functies en/of interfaces die bij de bovenliggende risicobeoordeling worden beoordeeld.

[G 7] Uit de vergelijking met de klassieke CENELEC V-cyclus in Figuur 5 blijkt dan het volgende:

(a) de CSM bestrijkt de fasen "1 tot 10" en "13" van deze V-cyclus. Deze fasen omvatten de gezamenlijke activiteiten die nodig zijn om het beoordeelde systeem goed te keuren;

(b) de CSM bestrijkt niet de fasen "11", "12" en "14" van de systeemlevenscyclus:

(1) de fasen "11" en "12" hebben respectievelijk betrekking op "exploitatie en onderhoud" en "toezicht op de prestaties" van het systeem nadat dit conform de CSM is goedgekeurd. Deze twee fasen komen aan bod in het veiligheidsbeheersysteem van spoorwegondernemingen en infrastructuurbeheerders – (zie KADER 4 in Figuur 5). Blijkt echter tijdens exploitatie, onderhoud of toezicht op de prestaties van het systeem dat dit moet worden gewijzigd en achteraf aangepast (fase 13 in Figuur 5), terwijl het reeds in gebruik is, dan wordt de CSM opnieuw toegepast op de nieuwe vereiste wijzigingen overeenkomstig het bepaalde in Artikel 2. Voor zover het een belangrijke wijziging betreft, betekent dit dat:

(i) de CSM-conforme risicobeheer- en risicobeoordelingsprocessen op deze nieuwe wijzigingen worden toegepast;
(ii) deze nieuwe wijzigingen moeten worden goedgekeurd overeenkomstig het bepaalde in Artikel 6.

(2) de "buitenbedrijfstelling en verwijdering" van een systeem dat reeds in gebruik is (fase 14) kan ook als belangrijke wijziging worden aangemerkt; in dat geval moet de CSM opnieuw worden toegepast overeenkomstig het bepaalde in Artikel 2 voor fase 14 in Figuur 5.

Voor meer informatie over de reikwijdte van elke fase of activiteit in de in Figuur 5 overgenomen CENELEC V-cyclus wordt verwezen naar paragraaf 6 van de norm 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] Dit behoeft geen verdere uitleg.

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

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

[G 1] Dit behoeft geen verdere uitleg.

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] Doorgaans beslist de initiatiefnemer welk risicoaanvaardingsbeginsel het meest geschikt is om de in kaart gebrachte gevaren te beheersen, rekening houdend met de projectspecifieke eisen en de ervaring van de initiatiefnemer met de drie beginselen.

[G 2] Het is niet altijd mogelijk de aanvaardbaarheid van het risico op systeemniveau te evalueren met gebruikmaking van een van de drie risicoaanvaardingsbeginselen. Vaak berust de risicoaanvaarding op een combinatie van deze beginselen. Is het voor een belangrijk gevaar nodig meerdere risicoaanvaardingsbeginselen toe te passen ter beheersing van het daarmee samenhangende risico, dan moet dit in onderliggende gevaren ("deelgevaren") worden onderverdeeld. Zo kan elk afzonderlijk deelgevaar worden beheerst met gebruikmaking van één risicoaanvaardingsbeginsel.

[G 3] Bij de beslissing om een gevaar te beheersen door een risicoaanvaardingsbeginsel toe te passen moet rekening worden gehouden met het gevaar zelf en met de reeds onderkende oorzaken daarvan die in de gevareninventarisatiefase werden aangetoond. Resulteert hetzelfde gevaar uit twee verschillende en van elkaar losstaande oorzaken, dan moet dit worden onderverdeeld in twee verschillende onderliggende gevaren ("deelgevaren"). Elk deelgevaar wordt dan beheerst met gebruikmaking van één risicoaanvaardingsbeginsel. De twee deelgevaren moeten in de gevareninventaris worden geregistreerd en beheerd. Als het gevaar bijvoorbeeld wordt veroorzaakt door een ontwerpfout, kan dit worden beheerd door een praktijkcode toe te passen. Wordt het gevaar echter veroorzaakt door een onderhoudsfout, dan is de praktijkcode alleen mogelijk niet voldoende; in dat geval moet een ander risicoaanvaardingsbeginsel worden toegepast.

[G 4] Om het risico tot een aanvaardbaar niveau terug te brengen, moeten mogelijk meerdere iteraties plaatsvinden tussen de risicoanalyse- en risico-evaluatiefasen totdat de noodzakelijke veiligheidsmaatregelen zijn vastgesteld.

[G 5] Als aanvaardbaar geldt het huidige restrisico dat resulteert uit de operationele ervaring in het veld voor de bestaande systemen en voor de systemen waarop praktijkcodes werden toegepast. Het risico resulterend uit de expliciete risico-inschatting berust op deskundig oordeel en op verschillende tijdens de analyses gemaakte aannames of op databanken met ervaringsgegevens over ongevallen of exploitatievoorvallen. Bijgevolg kan het restrisico van de expliciete risico-inschatting niet rechtstreeks worden bevestigd door retourinformatie afkomstig van veldwerk. Daartoe is tijd nodig om de systemen in kwestie te exploiteren, te bewaken en daarbij relevante ervaring op te doen. Pluspunt van het toepassen van praktijkcodes en het maken van een vergelijking met soortgelijke referentiesystemen is

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

doorgaans dat een overmaat aan onnodig strenge veiligheidsvereisten wordt vermeden als gevolg van te conservatieve aannames op veiligheidsgebied bij expliciete risico-inschattingen. Het kan echter zijn dat wat betreft het beoordeelde systeem niet moet worden voldaan aan bepaalde veiligheidsvereisten uit praktijkcodes of soortgelijke referentiesystemen. In dat geval heeft de toepassing van een expliciete risico-inschatting als voordeel dat een overmaat aan onnodig strenge ontwerpvoorschriften voor het beoordeelde systeem wordt vermeden. Dit maakt een kosteneffectiever ontwerp mogelijk dat nog niet eerder werd uitgeprobeerd.

[G 6] Kunnen de geïnventariseerde gevaren en de daarmee samenhangende risico's van het beoordeelde systeem niet worden beheerst door praktijkcodes of soortgelijke referentiesystemen toe te passen, dan wordt een expliciete risico-inschatting uitgevoerd op basis van kwantitatieve of kwalitatieve analyses van gevaarlijke gebeurtenissen. Dat is het geval wanneer het beoordeelde systeem volledig nieuw is (of een innoverend ontwerp heeft) dan wel afwijkt van een praktijkcode of referentiesysteem. Door de expliciete risico-inschatting uit te voeren, wordt nagegaan of het risico aanvaardbaar is (en dus geen verdere analyse behoeft) dan wel of aanvullende veiligheidsmaatregelen nodig zijn om het risico verder te verminderen.

[G 7] Paragraaf 8 van het richtsnoer EN 50 1262 {Ref. 9} bevat aanwijzingen over risicovermindering en risicoaanvaarding.

[G 8] De beoordelingsinstantie moet het gehanteerde risicoaanvaardingsbeginsel en de toepassing ervan toetsen.

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] Geldt bijvoorbeeld als veiligheidseis voor de software van een onderdeel dat het ontwikkelingsproces van veiligheidsintegriteitsniveau 4 als bedoeld in de norm EN 50 128 moet worden toegepast, dan moet worden aangetoond dat het door de norm aanbevolen proces wordt nageleefd. Daarbij moet onder meer het bewijs worden geleverd dat:

(a) is voldaan aan de onafhankelijkheidseisen wat betreft organisatie van ontwerp, keuring en validering van de software;
(b) de juiste methoden als bedoeld in de norm EN 50 128 voor het veiligheidsintegriteitsniveau 4 worden toegepast;
(c) enzovoort.

[G 2] Moet bijvoorbeeld een specifieke praktijkcode worden gebruikt om elektropneumatische noodremkleppen te fabriceren, dan moet worden aangetoond dat tijdens het fabricageproces aan alle eisen in deze praktijkcode wordt voldaan.

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] Er worden twee soorten veiligheidsmaatregelen onderscheiden:

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

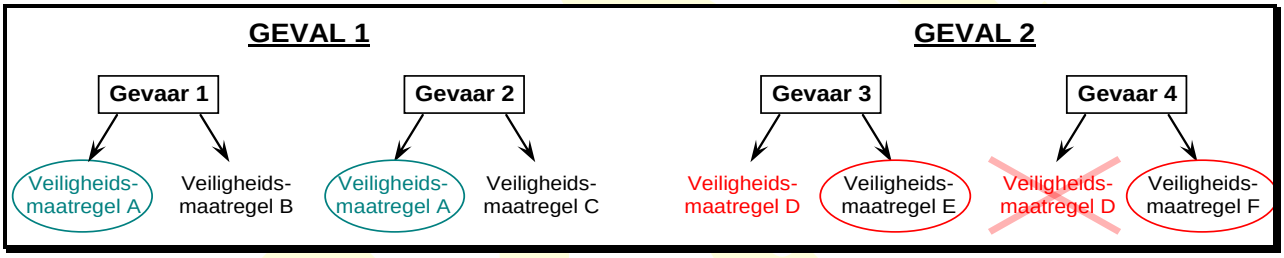
(a) "preventieve veiligheidsmaatregelen" ter voorkoming dat gevaren of de oorzaken daarvan optreden, en
(b) "beperkende veiligheidsmaatregelen" ter voorkoming dat gevaren leiden tot ongevallen of ter beperking van de gevolgen van ongevallen na het optreden (beschermingsmaatregelen)

Met het oog op de operabiliteit is het doorgaans efficiënter om oorzaken te voorkomen.

[G 2] De initiatiefnemer moet de veiligheidsmaatregelen die het juiste midden houden tussen de kosten om het risico te verminderen en het niveau van het restrisico als meest passend beschouwen. De gekozen veiligheidsmaatregelen worden de veiligheidsvereisten voor het beoordeelde systeem.

[G 3] Het is van belang zeker te stellen dat de de veiligheidsmaatregelen die worden gekozen om het ene gevaar te beheersen niet conflicteren met andere gevaren. Zoals weergegeven in Figuur 6 kunnen de volgende twee gevallen zich bijvoorbeeld voordoen(11):

(a) GEVAL 1: als dezelfde veiligheidsmaatregel (maatregel A in Figuur 6) verschillende gevaren kan beheersen zonder die met elkaar in conflict te brengen, en economisch verantwoord is, dan mag die op zichzelf worden gekozen als bijbehorende "veiligheidseis". Globaal beschouwd moet aan minder veiligheidsvereisten worden voldaan dan wanneer zowel maatregel B als maatregel C ten uitvoer worden gelegd;



Figuur 6: Selectie van passende veiligheidsmaatregelen om risico's te beheersen.

(b) GEVAL 2: omgekeerd, als een veiligheidsmaatregel een gevaar kan beheersen, maar conflicteert met een ander gevaar (maatregel D in Figuur 6), dan mag die niet als "veiligheidseis" worden gekozen. In dit geval moeten de andere veiligheidsmaatregelen voor het desbetreffende gevaar worden gebruikt (maatregel E en maatregel F in Figuur 6):

(1) Een typisch voorbeeld voor het besturings- en seingevingssysteem is de plaatsbepaling van de trein op het spoor om de remmen te besturen of toestemming tot het verhogen van de snelheid te geven. Het gebruik van de kop (of de staart) van de trein voor de plaatsbepaling is niet in alle situaties veilig:

(i) wanneer het besturings- en seingevingssysteem met ETCS-functionaliteit (European Train Control System) een veilige noodremming moet uitvoeren, wordt de conditie "MAXIMUM SAFE FRONT END" gebruikt om te waarborgen dat de kop van de trein daadwerkelijk tot stilstand komt alvorens de gevarenzone te bereiken;

(11) *Op te merken valt dat in de leidraad niet alle situaties worden vermeld waarin veiligheidsmaatregelen kunnen conflicteren met andere in kaart gebrachte gevaren. Er worden slechts enkele voorbeelden ter illustratie gegeven.*

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

(ii) omgekeerd, wanneer de trein toestemming tot verhogen van de snelheid heeft, bijvoorbeeld na een snelheidsbegrenzing, gebruikt het besturings- en seingevingssysteem met ETCS-functionaliteit de conditie "MINIMUM SAFE REAR END";

(2) Ander voorbeeld is een veiligheidsmaatregel die geldt om een trein onder vrijwel alle omstandigheden in een faalveilige toestand tot stilstand te brengen, behalve in een tunnel of onder een brug. In dit laatste geval wordt maatregel D in GEVAL 2 van Figuur 6 niet genomen.

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] Afhankelijk van bijvoorbeeld de technische keuzes voor het ontwerp van een systeem, de bijbehorende subsystemen en uitrusting, kunnen nieuwe gevaren in kaart worden gebracht tijdens het "aantonen van de conformiteit met de veiligheidsvereisten" (zo kan het gebruik van bepaalde verfsoorten bij brand leiden tot emissie van giftige gassen). Deze nieuwe gevaren en de daarmee samenhangende risico's moeten dienen als nieuwe input voor een nieuwe cyclus in het iteratieve risicobeoordelingsproces. In aanhangsel A.4.3 van de norm EN 50 129 staan andere voorbeelden waarbij sprake is van nieuwe gevaren die moeten worden beheerst.

2.2. Inventarisatie van de gevaren

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] De gevaren worden in de mate van het mogelijke met hetzelfde detailleringsniveau in kaart gebracht. Tijdens voorafgaande gevarenanalyses kan het zijn dat gevaren met verschillende detailleringsniveaus in kaart worden gebracht (bijvoorbeeld omdat personen met uiteenlopende ervaring deelnemen aan een storingsanalyse of HAZOP - Hazard and Operability Study).
Het detailleringsniveau hangt ook af van het risicoaanvaardingsbeginsel dat wordt geselecteerd om de in kaart gebrachte gevaren te beheersen. Als een gevaar bijvoorbeeld volledig wordt beheerst door gebruik te maken van een praktijkcode of soortgelijk referentiesysteem, is een meer gedetailleerde gevareninventarisatie niet nodig.

[G 2] Alle gevaren die tijdens het risicobeoordelingsproces in kaart werden gebracht (inclusief de gevaren verbonden aan algemeen aanvaardbare risico's) moeten samen met de bijbehorende veiligheidsmaatregelen en risico's worden geregistreerd in de gevareninventaris.

[G 3] Afhankelijk van de aard van het te analyseren systeem kunnen verschillende methoden worden gebruikt om de gevaren te inventariseren:

(a) empirische gevareninventarisatie met gebruikmaking van ervaringsgegevens uit het verleden (bijvoorbeeld controlelijsten of generieke gevarenlijsten);

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

(b) creatieve gevareninventarisatie voor nieuwe aandachtsgebieden (proactieve prognoses, bijvoorbeeld gestructureerde "WHAT-IF"-studies, zoals falingstoestand- en effectenanalyse (FMEA) of storingsanalyses (HAZOP)).

[G 4] De empirische en creatieve methoden voor gevareninventarisatie mogen met elkaar worden gecombineerd om te waarborgen dat alle mogelijke gevaren en veiligheidsmaatregelen in de lijst worden opgenomen.

[G 5] Als inleidende stap kan de gevareninventarisatie beginnen met de samenstelling van een klankbordgroep of brainstormingteam met deskundigen uit verschillende vakgebieden die alle toepasselijke aspecten van de belangrijke wijziging bestrijken. Voor zover het deskundigenpanel dit dienstig acht, mag een specifieke functie of bedrijfswijze worden geanalyseerd met gebruikmaking van empirische methoden.

[G 6] De systeemomschrijving bepaalt welke methoden worden toegepast om de gevaren te inventariseren. In aanhangsel B staan enkele voorbeelden.

[G 7] Meer informatie over de technieken en methoden voor gevareninventarisatie is terug te vinden in bijlage A.2 en E van het richtsnoer EN 50 126-2 {Ref. 9}.

[G 8] Onder C.17. in aanhangsel C is een voorbeeld van een generieke gevarenlijst opgenomen.

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] Als hulp bij het risicobeoordelingsproces kunnen de belangrijke gevaren verder in verschillende categorieën worden gegroepeerd. Zo kunnen de belangrijke gevaren bijvoorbeeld worden geclassificeerd of ingedeeld naargelang van de verwachte ernstgraad van het risico en de frequentie van optreden. De CENELEC-normen bieden een leidraad voor deze classificatie: zie onder A.2. in aanhangsel A.

[G 2] De in punt 2.1.4 beschreven risicoanalyse en -evaluatie worden toegepast door prioriteiten toe te kennen, te beginnen met de hoogst gerangschikte gevaren.

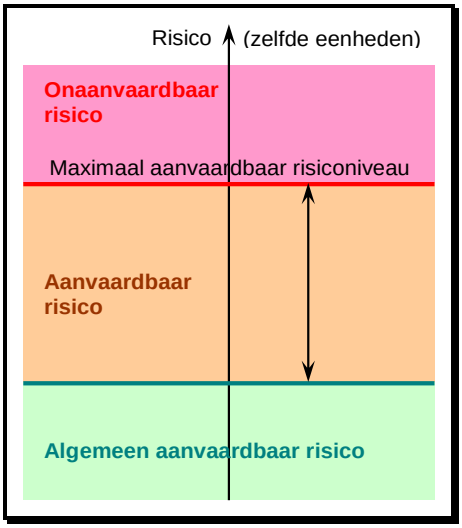
2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed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

[G 1] Zo kan een aan een gevaar gekoppeld risico bijvoorbeeld als algemeen aanvaardbaar worden aangemerkt:

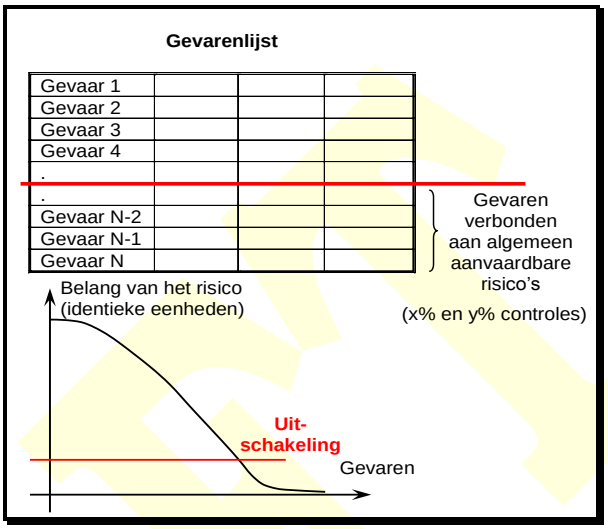
(a) als het risico kleiner is dan een bepaald percentage (bijvoorbeeld x%) van het maximaal aanvaardbare risico voor gevaren van dit type. De waarde van x% kan worden vastgelegd op basis van beste praktijken en de opgedane ervaring met verschillende risicoanalysebenaderingen, bijvoorbeeld het pro rata tussen algemeen aanvaardbare risico's en onaanvaardbare risico's in classificaties van FN-curven of in risicomatrices. Dit wordt geïllustreerd in Figuur 7.

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

(b) of als de aan het risico verbonden schade zodanig klein is dat het onredelijk is daarop te reageren door veiligheidsmaatregelen te nemen.



Figuur 7: Algemeen aanvaardbare risico's



Figuur 8: Uitfilteren van gevaren verbonden aan algemeen aanvaardbare risico's

[G 2] Worden gevaren met verschillende detailleringsniveaus geïnventariseerd (zijnde gevaren op hoog niveau enerzijds en gedetailleerde deelgevaren anderzijds), dan moet bovendien worden vermeden dat die onterecht worden ingedeeld onder gevaren verbonden aan algemeen aanvaardbare risico's. De bijdrage van alle gevaren verbonden aan algemeen aanvaardbare risico's mag niet hoger liggen dan een bepaald pro rata (bijvoorbeeld y%) van het totale risico op systeemniveau. Deze controle is nodig om te voorkomen dat de grondgedachte wordt uitgehold door de gevaren op te delen in een groot aantal onderliggende gevaren ("deelgevaren") op laag niveau. Immers, wanneer een gevaar wordt uitgedrukt als een groot aantal "kleinere" deelgevaren, kan elk deelgevaar afzonderlijk beschouwd eenvoudig worden ingedeeld als verbonden aan algemeen aanvaardbare risico's. Worden alle deelgevaren echter samen geëvalueerd, dan worden ze veeleer geclassificeerd als verbonden aan belangrijke risico's (dat wil zeggen als gevaar op hoog niveau). De waarde van het pro rata (bijvoorbeeld y%) hangt af van de risicoaanvaardingscriteria die op systeemniveau worden toegepast. Operationele ervaring met soortgelijke referentiesystemen kan ten grondslag liggen aan de bepaling en schatting van deze waarde.

[G 3] De twee bovengenoemde controles (ten opzichte van x% en y%) maken het mogelijk de risicobeoordeling te richten op de belangrijkste gevaren en te waarborgen dat elk belangrijk risico wordt beheerst (zie Figuur 8).
Onverminderd de wettelijke voorschriften in een lidstaat draagt de initiatiefnemer de verantwoordelijkheid om op basis van deskundig oordeel de waarden van x% en y% vast te leggen, en die onafhankelijk te laten beoordelen door de beoordelingsinstantie. Deze waarde kan bijvoorbeeld in een orde van grootte liggen van $x = 1\%$ en $y = 10\%$ in zoverre aanvaardbaar geacht op grond van deskundig oordeel

[G 4] Op grond van het bepaalde in punt 2.2.2 moet de classificatie in "algemeen aanvaardbaar geacht risico" onafhankelijk worden beoordeeld door een beoordelingsinstantie.

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

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] Hoofddoel hiervan is het in kaart brengen van de gevaren die in verband staan met de wijziging. Zijn reeds veiligheidsmaatregelen in kaart gebracht, dan moeten die in de gevareninventaris worden geregistreerd. De wijziging bepaalt of de maatregelen van procedurele, technische, operationele of organisatorische aard zijn.

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] Ook al wordt een risico tot een aanvaardbaar niveau teruggebracht, de initiatiefnemer mag oordelen dat een verdergaande gevareninventarisatie noodzakelijk is. Reden hiervoor kan zijn dat een verdergaande gevareninventarisatie kosteneffectievere veiligheidsmaatregelen voor risicobeheersing aan het licht kan brengen.

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] Dit behoeft geen verdere uitleg.

2.3. Gebruik van praktijkcodes en risico-evaluatie

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] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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

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] Dit behoeft geen verdere uitleg.

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

[G 1] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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

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

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

[G 1] Dit behoeft geen verdere uitleg.

2.4. Gebruik van referentiesystemen en risico-evaluatie

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] Meer informatie over deze beginselen is terug te vinden in punt 8 van het richtsnoer EN 50 126-2 {Ref. 9}.

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

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

[G 1] Zo kan een oud besturings- en seingevingssysteem dat tijdens het gebruik een aanvaardbaar veiligheidsniveau bleek te hebben, worden vervangen door een ander systeem met een recentere technologie en betere veiligheidsprestaties. Daarom is het van belang iedere keer dat een referentiesysteem wordt toegepast na te gaan of dit nog in aanmerking komt voor goedkeuring.

[G 2] Aangezien bepaalde aspecten van de veiligheid in spoorwegtunnels of de veiligheid van het vervoer van gevaarlijke goederen mogelijk eigen zijn aan en afhangen van operationele en milieutechnische condities, is het bijvoorbeeld nodig voor elk project zeker te stellen dat het systeem onder dezelfde condities zal worden gebruikt.

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

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

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

[G 1] Dit behoeft geen verdere uitleg.

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] Meer informatie over overeenstemmingsanalyses is terug te vinden in punt 8.1.3. van het richtsnoer EN 50 126-2 {Ref. 9}.

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

[G 1] Dit behoeft geen verdere uitleg.

2.5. Expliciete risico-inschatting en -evaluatie

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] Dit behoeft geen verdere uitleg.

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

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

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

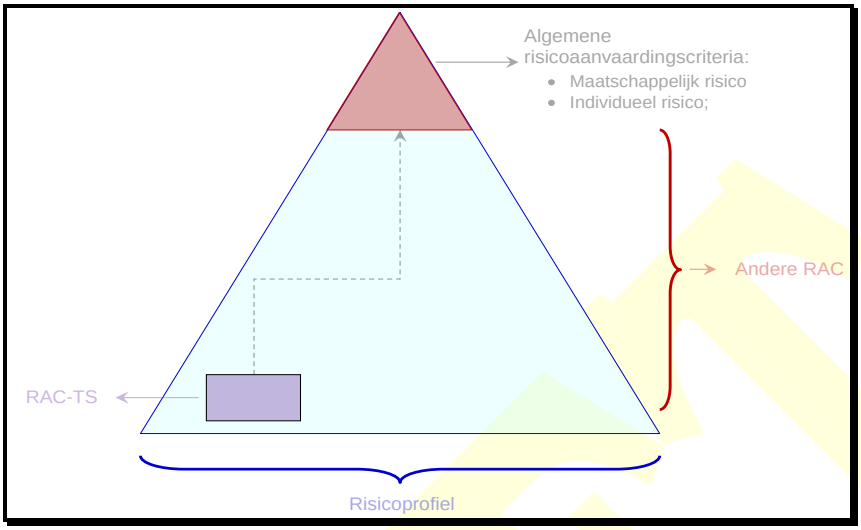
[G 1] Risicoaanvaardingscriteria (zie de kaders “risico-evaluatie” in Figuur 1) dienen om na te gaan of de risico's van het beoordeelde systeem al dan niet aanvaardbaar zijn. Er bestaan impliciete en expliciete risicoaanvaardingscriteria:

(a) impliciete risicoaanvaardingscriteria: volgens het bepaalde in punt 2.3.5 en 2.4.3 worden risico’s waarvoor praktijkcodes worden toegepast of een vergelijking met referentiesystemen wordt gemaakt impliciet als aanvaardbaar aangemerkt mits respectievelijk (zie in stippellijn omcirkelde tekst in Figuur 1):

(1) is voldaan aan de in punt 2.3.2 genoemde toepassingsvoorwaarden van praktijkcodes;
(2) is voldaan aan de in punt 2.4.2 genoemde gebruiksvoorwaarden van een referentiesysteem;

(b) expliciete risicoaanvaardingscriteria: expliciete risicoaanvaardingscriteria dienen om na te gaan of de risico’s die worden beheerst door een expliciete risico-inschatting toe te passen al dan niet aanvaardbaar zijn (zie met doorlopende lijn omcirkelde tekst in Figuur 1 wat betreft het derde beginsel). Risicoaanvaardingscriteria kunnen op verschillende niveaus van een spoorwegsysteem worden gedefinieerd. Deze criteria kunnen grafisch worden voorgesteld in piramidevorm (zie Figuur 9), te beginnen met de risicoaanvaardingscriteria op hoog niveau (bijvoorbeeld uitgedrukt als maatschappelijk risico of individueel risico), gevolgd door subsystemen en onderdelen (om technische systemen aan bod te laten komen) en inclusief de menselijke operators tijdens exploitatie- en onderhoudswerkzaamheden op systeem- en subsysteemniveau. De risicoaanvaardingscriteria dragen bij tot de verwezenlijking van de veiligheidsprestaties van het systeem en staan bijgevolg in verband met gemeenschappelijke veiligheidsdoelen en nationale referentiewaarden. Dit maakt het bijzonder moeilijk een wiskundig model voor deze criteria op te stellen: zie {Ref. 12} voor meer informatie.
De expliciete risicoaanvaardingscriteria moeten worden gedefinieerd op een niveau dat overeenkomt met het belang en de complexiteit van de belangrijke wijziging. Zo is het bijvoorbeeld niet nodig het totale risico voor het spoorwegsysteem te evalueren wanneer een as van een bepaald type in rollend materieel wordt gewijzigd. De veiligheid van het rollend materieel kan centraal staan in de definitie van risicoaanvaardingscriteria. Omgekeerd mogen omvangrijke wijzigingen in of toevoegingen aan een bestaand spoorwegsysteem niet uitsluitend worden geëvalueerd op basis van de veiligheidsfuncties van de afzonderlijke functies of wijzigingen die worden toegevoegd. Ook op het niveau van het spoorwegsysteem moet worden nagegaan of de wijziging als geheel aanvaardbaar is.

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



Figuur 9: Piramide van risicoaanvaardingscriteria (RAC).

[G 2] De huidige werkzaamheden van het Spoorwegbureau wat betreft risicoaanvaardingscriteria beogen de onderlinge afstemming tussen de lidstaten van de expliciete risicoaanvaardingscriteria die nodig zijn om het beginsel van de wederzijdse erkenning toe te passen. Aanvullende informatie wordt, voor zover beschikbaar, in dit document opgenomen.

[G 3] Ondertussen kunnen risico's worden geëvalueerd door bijvoorbeeld de risicomatrix te gebruiken, zoals opgenomen in punt 4.6 van de norm EN 50 126-1 {Ref. 8}. Ook andere passende criteria mogen worden gebruikt, mits die voor het geval in kwestie een aanvaardbaar veiligheidsniveau opleveren.

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] Dit behoeft geen verdere uitleg.

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] Bij voorliggend document is een afzonderlijke nota van het Spoorwegbureau gevoegd met meer informatie over de risicoaanvaardingscriteria voor technische systemen (RAC-TS) en over de aspecten en functies van het technische systeem waarop ze van toepassing zijn: zie onder A.3. in aanhangsel A en het referentiedocument {Ref. 11}.

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

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

[G 1] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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] Dit behoeft geen verdere uitleg.

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

3. AANTONEN DAT WORDT VOLDAAN AAN DE VEILIGHEIDSVEREISTEN

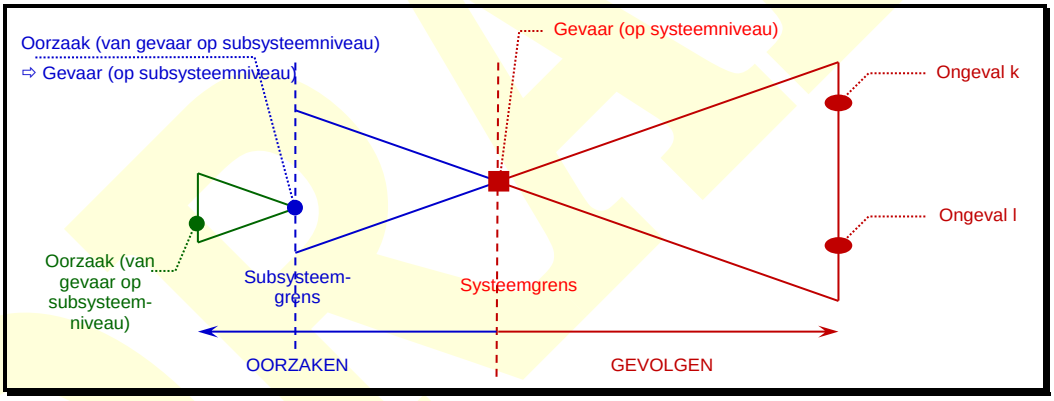
3.1. Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

[G 1] Zoals beschreven onder [G 3] tot [G 6] in punt 2.1.1 omvat het "aantonen dat het systeem voldoet aan de veiligheidsvereisten" de fasen "6 tot 10" van de CENELEC V-cyclus (zie KADER 3 in Figuur 5). Zie onder [G 3] in punt 2.1.1.

[G 2] Zie ook onder [G 4] in punt 2.1.1 van dit 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] Causale analyses zijn een voorbeeld van veiligheidsbeoordelingen en -analyses die op subsysteemniveau kunnen worden uitgevoerd: zie Figuur 10. Elke andere methode mag echter worden gebruikt om aan te tonen dat het subsysteem voldoet aan de als uitgangspunt vastgelegde veiligheidsvereisten.

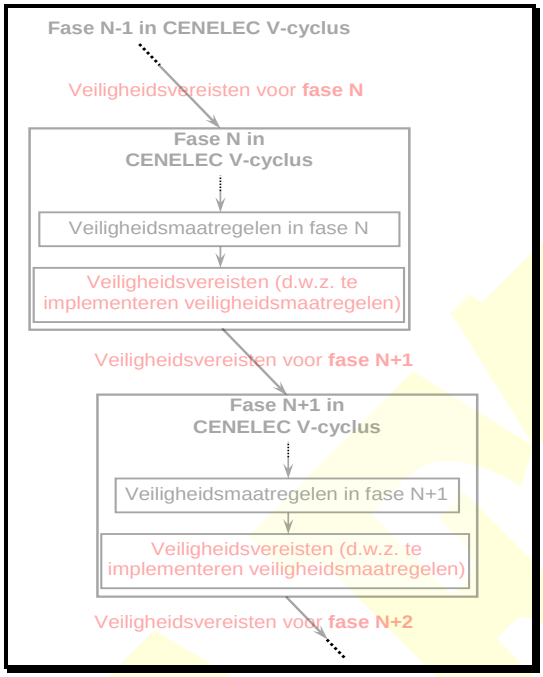


Figuur 10: Figuur A.4 van EN 50 129: Gevarendefinitie rekening houdend met de systeemgrens.

[G 2] De hiërarchische structurering van gevaren en oorzaken wat betreft systemen en subsystemen mag worden herhaald voor elke onderliggende fase van de CENELEC V-cyclus in Figuur 5. De gevareninventarisatie en causale analyse (of elke andere relevante methode) mogen samen met de gebruikte praktijkcodes, soortgelijke referentiesystemen en expliciete analyses en evaluaties, worden herhaald voor elke fase in de systeemontwikkelingscyclus. Doel hiervan is, uitgaande van de op subsysteemniveau onderkende veiligheidsmaatregelen, te bepalen aan welke veiligheidsvereisten in de volgende fase moet worden voldaan. Dit wordt geïllustreerd in Figuur 11.

[G 3] Zie ook onder [G 4] in punt 2.1.1 van dit document.

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



Figuur 11: Afleiden van veiligheidsvereisten voor onderliggende fasen.

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] Bijgevolg worden alle activiteiten in KADER 3[(12)] van de CENELEC V-cyclus in Figuur 5 ook onafhankelijk beoordeeld.

[G 2] De aard en het detailleringsniveau van de onafhankelijke beoordeling die wordt uitgevoerd door de beoordelingsinstanties (dat wil zeggen gedetailleerde of macroscopische beoordeling) komen ter sprake in de verduidelijking van Artikel 6.

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

[G 1] Zo kan de manier waarop een brand wordt geblust een nieuw gevaar (verstikking) veroorzaken waarvoor nieuwe veiligheidsmaatregelen geboden zijn (bijvoorbeeld een specifieke ontruimingsprocedure voor reizigers). Een ander voorbeeld is het gebruik van hardglas om te voorkomen dat vensters bij een botsing breken en dat reizigers gewond

(12) *De overeenkomst van de activiteiten tussen de gemeenschappelijke veiligheidsmethoden en Figuur 5 (zijnde figuur 10 van CENELEC 50 126 V-cyclus) wordt nader toegelicht in punt 2.1.1. Onder [G 3] in punt 2.1.1 staat meer in het bijzonder welke CENELEC-activiteiten deel uitmaken van de CSM-fase "aantonen dat het systeem voldoet aan de veiligheidsvereisten".*

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

raken door glassplinters of uit het rijtuig worden geslingerd. In dit geval ontstaat een nieuw gevaar, namelijk dat het veel moeilijker is de reizigersrijtuigen in noodgevallen via de vensters te ontruimen. Dat kan resulteren in veiligheidsmaatregelen doordat voor bepaalde vensters een bijzonder ontwerp noodzakelijk is om ontruiming mogelijk te maken.

[G 2] Voorbeeld van een operationele wijziging: er moet een verbod worden uitgevaardigd op het vervoer van gevaarlijke goederen in dichtbevolkte gebieden. In plaats daarvan moet een alternatieve route via tunnels worden gevolgd. Daarbij ontstaan verschillende andere gevaren.

[G 3] In aanhangsel A.4.3 van de norm EN 50 129 staan andere voorbeelden van nieuwe gevaren die in kaart kunnen worden gebracht tijdens het aantonen dat het systeem voldoet aan de veiligheidsvereisten.

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

4. GEVARENBEHEER

4.1. Gevarenbeheerproces

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] Het gebruik van een gevareninventaris voor het registreren, beheren en controleren van veiligheidsrelevante informatie wordt ook aanbevolen in de CENELEC-normen 50 126-1 {Ref. 8} en 50 129 {Ref. 7}.

[G 2] Zo kan een actor bijvoorbeeld een of meer gevareninventarissen hebben naargelang van de complexiteit van het systeem. In beide gevallen moet iedere gevareninventaris worden onderworpen aan een onafhankelijke beoordeling door de beoordelingsinstantie. In dit geval is een mogelijke oplossing bijvoorbeeld:

(a) een "interne gevareninventaris" om alle interne veiligheidsvereisten te beheren die gelden voor het subsysteem dat onder de verantwoordelijkheid van de actor valt. De omvang van de gevareninventaris en het daarmee gepaard gaande beheerswerk worden bepaald door de structuur van de gevareninventaris en uiteraard door de complexiteit van het subsysteem. Aangezien de gevareninventaris voor doeleinden van intern beheer wordt gebruikt, is het echter niet nodig dit aan andere actoren over te leggen. In de interne gevareninventaris staan alle geïnventariseerde gevaren die worden beheerst, alsook de daarmee samenhangende veiligheidsmaatregelen die werden gevalideerd;
(b) een "externe gevareninventaris" om gevaren en de daarmee samenhangende veiligheidsmaatregelen (die de actor niet volledig zelf ten uitvoer kan leggen) over te dragen aan andere actoren overeenkomstig het bepaalde in punt 1.2.2. Doorgaans is deze tweede gevareninventaris beperkter in opzet en vergt het minder beheerswerk (zie bijvoorbeeld onder C.16.4. in aanhangsel C).

[G 3] Blijkt het praktisch niet haalbaar verschillende gevareninventarissen te beheren, dan bestaat een andere oplossing erin alle gevaren en de daarmee samenhangende veiligheidsmaatregelen als bedoeld onder a) en b) hierboven te beheren in één gevareninventaris, zij het dan met de mogelijkheid van twee gevareninformatierapporten (zie het voorbeeld onder C.16.3. in aanhangsel C):

(a) een intern gevareninformatierapport dat eventueel achterwege mag blijven voor zover de gevareninventaris voldoende is gestructureerd om een onafhankelijke beoordeling mogelijk te maken;
(b) een extern gevareninformatierapport om gevaren en de daarmee samenhangende veiligheidsmaatregelen aan andere actoren over te dragen.

[G 4] Zoals uitgelegd in punt 4.2, worden na afloop van het project wanneer het systeem werd goedgekeurd:

(a) alle aan andere actoren overgedragen gevaren gecontroleerd in de externe gevareninventaris van de actor die deze gevaren overdraagt. Aangezien deze gevaren in de gevareninventarissen van de andere actoren worden geïmporteerd en beheerd,

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

behoeft de betrokken actor ze niet verder te beheren tijdens de levenscyclus van het (sub)systeem;

(b) alle bijbehorende veiligheidsmaatregelen mogen echter niet in de gevareninventaris worden gevalideerd om de onder [G 9] in punt 4.2 vermelde redenen. Het is immers nuttig dat de organisatie die de gebruiksbeperkingen exporteert duidelijk in de gevareninventaris vermeldt dat de daarmee samenhangende veiligheidsmaatregelen niet werden gevalideerd.

[G 5] Omgekeerd worden alle interne gevareninventarissen bijgehouden tijdens de volledige levenscyclus van het (sub)systeem. Dat maakt een voortgangscontrole mogelijk van de risicobewaking wat betreft de gevaren die in kaart werden gebracht, niet alleen tijdens exploitatie en onderhoud van het (sub)systeem, maar ook nadat dit buiten bedrijf werd gesteld: zie KADER 4 in de CENELEC V-cyclus in Figuur 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] De informatie over de van andere actoren ontvangen gevaren en de daarmee samenhangende veiligheidsmaatregelen (zie punt 1.2.2) omvat alle aannames(13) en gebruiksbeperkingen(13) (ook veiligheidsgerelateerde toepassingsvoorwaarden genoemd) die gelden voor de verschillende subsystemen alsmede in voorkomend geval de door de fabrikant overgelegde veiligheidsbewijzen voor generieke toepassingen en generieke producten.

[G 2] Een mogelijk voorbeeld voor de structuur van de gevareninventaris wordt beschreven onder C.16. in aanhangsel C.

4.2. Informatie-uitwisseling

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] Zo kan de fabrikant bijvoorbeeld voor het subsysteem "Odometrie" van de ETCS-treinapparatuur in het laboratorium de algoritmen valideren door theoretische signalen te simuleren die door de bijbehorende kilometertellers worden gegenereerd. Om het subsysteem "Odometrie" echter volledig te valideren, is de hulp van de spoorwegonderneming en infrastructuurbeheerder nodig aangezien daarvoor een echte trein nodig is met een echt contact tussen wiel en rail.

(13) *Zie onder [G 5] in punt 1.1.5 en de voetnoten (7) en (8) op pagina 31 van voorliggend document voor meer uitleg over de gehanteerde terminologie betreffende veiligheidsbewijzen "generiek product en generieke toepassing", "aannames, onderstellingen en gebruiksbeperkingen".*

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

[G 2] Een ander voorbeeld is de overdracht door fabrikanten aan spoorwegondernemingen en infrastructuurbeheerders van veiligheidsmaatregelen inzake exploitatie of onderhoud voor technische uitrusting. Deze veiligheidsmaatregelen moeten door de spoorwegonderneming ten uitvoer worden gelegd.

[G 3] Om deze gevaren, de bijbehorende veiligheidsmaatregelen en risico's opnieuw gezamenlijk te laten beoordelen door de betrokken instanties, is het handig dat de organisatie die ze in kaart heeft gebracht alle nodige toelichtingen geeft om het probleem inzichtelijk te maken. Het kan zijn dat de aanvankelijke omschrijving van de gevaren, veiligheidsmaatregelen en risico's moet worden aangepast zodat alle betrokken partijen die beter begrijpen zonder ze opnieuw met elkaar te bespreken. Op het moment dat de gevaren gezamenlijk opnieuw worden beoordeeld, kunnen nieuwe veiligheidsmaatregelen in kaart worden gebracht.

[G 4] De ontvangende actor die verantwoordelijk is voor de tenuitvoerlegging, keuring en validering van de ontvangen of nieuwe veiligheidsmaatregelen registreert in zijn gevareninventaris alle daarmee samenhangende gevaren alsmede de bijbehorende veiligheidsmaatregelen (zowel de geïmporteerde als de gezamenlijk in kaart gebrachte veiligheidsmaatregelen).

[G 5] Wanneer een veiligheidsmaatregel niet onverkort werd gevalideerd, moet een duidelijke gebruiksbeperking (bijvoorbeeld beperkende maatregelen van operationele aard) worden uitgewerkt en vastgelegd in de gevareninventaris. Het is inderdaad mogelijk dat (ontwerp)technische veiligheidsmaatregelen:

(a) onjuist ten uitvoer werden gelegd, of
(b) onvolledig ten uitvoer werden gelegd, of
(c) met opzet niet ten uitvoer werden gelegd, bijvoorbeeld omdat andere veiligheidsmaatregelen worden uitgevoerd dan in de gevareninventaris zijn vermeld (bijvoorbeeld uit kostenoverwegingen). Aangezien deze veiligheidsmaatregelen nog niet werden gevalideerd, moeten ze duidelijk in de gevareninventaris in kaart worden gebracht. Verder moet worden bewezen/verantwoord waarom de in plaats daarvan uitgevoerde veiligheidsmaatregelen[(14)] geschikter zijn. Ook moet worden aangetoond dat het systeem met de vervangende veiligheidsmaatregelen aan de veiligheidsvereisten voldoet;
(d) enzovoort.

In deze gevallen is het niet mogelijk de bijbehorende (ontwerp)technische veiligheidsmaatregelen te keuren en te valideren tijdens het gevarenbeheer. De gevaren en veiligheidsmaatregelen in kwestie moeten dan als open punten worden aangemerkt in de gevareninventaris. Doel hiervan is te vermijden dat de veiligheidsmaatregelen onbedoeld voor andere systemen worden gebruikt met toepassing van het risicoaanvaardingsbeginsel "soortgelijk referentiesysteem".

[G 6] Doorgaans worden "onjuist" en/of "onvolledig" ten uitvoer gelegde veiligheidsmaatregelen vroegtijdig in de systeemlevenscyclus ontdekt en rechtgezet alvorens het systeem goed te keuren. Worden ze echter te laat vastgesteld voor een juiste en volledige tenuitvoerlegging van de technische veiligheidsmaatregel, dan moet de voor de tenuitvoerlegging en het beheer verantwoordelijke organisatie duidelijke gebruiksbeperkingen voor het beoordeelde systeem in kaart brengen en registreren in de gevareninventaris. Deze gebruiksbeperkingen zijn vaak operationele toepassingseisen voor het beoordeelde systeem.

(14) *Worden andere veiligheidsmaatregelen uitgevoerd dan die welke aanvankelijk waren vastgesteld, dan moeten die ook in het gevareninformatieblad worden geregistreerd.*

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

[G 7] Het kan ook nuttig zijn in de gevareninventaris te vermelden of de veiligheidsmaatregelen in kwestie in een later stadium van de systeemlevenscyclus juist ten uitvoer zullen worden gelegd dan wel of het systeem verder zal worden gebruikt met de onderkende gebruiksbeperkingen. Verder kan het handig zijn in de gevareninventaris te rechtvaardigen waarom de desbetreffende technische veiligheidsmaatregelen onjuist of onvolledig ten uitvoer werden gelegd.

[G 8] De actor die de gebruiksbeperkingen ontvangt:

(a) importeert die allemaal in zijn gevareninventaris;
(b) ziet erop toe dat de gebruiksvoorwaarden van het beoordeelde systeem overeenstemmen met alle ontvangen gebruiksbeperkingen;
(c) gaat na of het beoordeelde systeem voldoet aan de gebruiksbeperkingen, en valideert dit.

[G 9] Naargelang van de beslissingen die door de betrokken organisaties werden overeengekomen:

(a) worden de desbetreffende technische veiligheidsmaatregelen in een later stadium juist ten uitvoer gelegd in het ontwerp.
De organisatie die de gebruiksbeperkingen exporteert, houdt verder bij of de daarmee samenhangende veiligheidsmaatregelen technisch gezien juist ten uitvoer worden gelegd. Dit betekent dat de bijbehorende veiligheidsmaatregelen pas kunnen worden gevalideerd en dat de daaraan verbonden gevaren pas in de gevareninventaris kunnen worden gecontroleerd nadat de corresponderende technische maatregelen volledig ten uitvoer werden gelegd. Dat moet worden gewaarborgd, zelfs wanneer de geëxporteerde gebruiksbeperkingen in de tussentijd werden geoperationaliseerd.

(b) of worden de desbetreffende technische veiligheidsmaatregelen niet in een later stadium ten uitvoer gelegd in het ontwerp. Het systeem blijft dan tijdens de volledige levenscyclus in gebruik met de bijbehorende gebruiksbeperkingen. In dit geval is het volgende mogelijk:

(1) de organisatie die de gebruiksbeperkingen exporteert, registreert de bijbehorende veiligheidsmaatregelen niet als “gevalideerd” in de gevareninventaris. Op die manier worden de daarmee samenhangende veiligheidskwesties niet uit het oog verloren wanneer het desbetreffende systeem als referentiesysteem voor andere projecten wordt gebruikt. Ook al is een andere actor bereid de desbetreffende risico’s anders te beheren, is het nuttig dat de organisatie die de gebruiksbeperkingen exporteert duidelijk in de gevareninventaris vermeldt dat de bijbehorende veiligheidsmaatregelen niet werden gevalideerd; of

(2) de systeembeschrijving kan worden gewijzigd door de gebruiksbeperkingen op te nemen in het toepassingsgebied van het systeem (dat wil zeggen de systeemspecifieke aannames) en in de veiligheidsmaatregelen. Zo wordt het mogelijk de gevaren te beheersen. Fungeert het systeem als referentiesysteem voor een andere toepassing, dan:

(i) moet het nieuwe systeem onder dezelfde omstandigheden worden gebruikt (dat wil zeggen voldoen aan de gebruiksbeperkingen die verbonden zijn aan deze aannames), of
(ii) dan moet de initiatiefnemer een aanvullende risicobeoordeling uitvoeren om na te gaan of van deze aannames werd afgeweken.

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

5. BEWIJS VAN DE TOEPASSING VAN HET RISICOBEHEERPROCES

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.

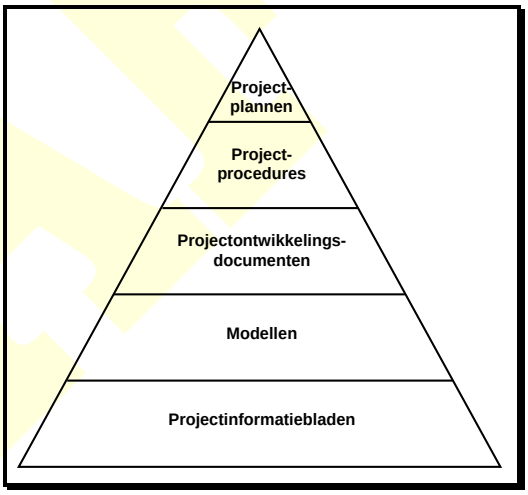
[G 1] Deze eisen komen reeds aan bod in het veiligheidsbeheersysteem van de infrastructuurbeheerder en spoorwegonderneming. Doorgaans moeten de andere actoren van de spoorwegsector die bij de belangrijke wijziging betrokken zijn minstens op projectniveau beschikken over een kwaliteitsborgingssysteem en/of veiligheidsbeheerproces, ook al is het veiligheidsbeheersysteem niet verplicht. Voor beide processen wordt een hiërarchische documentatiestructuur gebruikt binnen de onderneming of minstens in projectverband. Zij voorzien ook in de behoeften aan documentatie over het beheer van de bruikbaarheid, beschikbaarheid, onderhoudbaarheid en veiligheid. Deze gestructureerde documentatie kan in wezen als volgt samengesteld zijn (zie ook Figuur 12):

(a) **Projectplannen** waarin wordt beschreven welke organisatie wordt opgezet om een activiteit in projectverband te beheren.

(b) **Projectprocedures** met een uitvoerige beschrijving van de manier waarop een specifieke taak wordt voltooid. Doorgaans bestaan in de onderneming procedures en instructies die als zodanig worden gebruikt. Nieuwe projectprocedures worden alleen uitgewerkt voor zover het nodig is een specifieke taak voor het desbetreffende project te beschrijven.

(c) **Projectontwikkelingsdocumenten** die worden uitgewerkt tijdens de systeemlevenscyclus, zoals weergegeven in Figuur 5.

(d) **Modellen op ondernemings- of minstens op projectniveau** voor de verschillende soorten over te leggen documenten.



Figuur 12: Hiërarchische documentatiestructuur.

(e) **Projectinformatiebladen** die tijdens het project worden uitgewerkt om de conformiteit aan te tonen met het kwaliteitsborgings- en veiligheidsbeheerproces van de onderneming.

Deze werkwijze is een mogelijkheid om de vereiste bewijsstukken beschikbaar te stellen. Er zijn ook andere manieren mogelijk mits de CSM-criteria worden nageleefd.

[G 2] De CENELEC-normen adviseren om in een veiligheidsbewijs (of veiligheidsrapport) aan te tonen dat het systeem voldoet aan de functionele en veiligheidsvereisten. Ook al is dit niet verplicht, het veiligheidsbewijs is een gestructureerd bewijsstuk ter staving van:

(a) de kwaliteitsborging;

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

(b) het veiligheidsbeheer;
(c) de functionele en technische veiligheid.

Tegelijk heeft dit document als voordeel dat het de beoordelingsinstanties helpt en assisteert met de onafhankelijke beoordeling van de juiste toepassing van de CSM.

[G 3] In het veiligheidsbewijs wordt het onderlinge verband beschreven en samengevat tussen de productdocumenten die resulteren uit de toepassing van het kwaliteitsborgings- en/of veiligheidsbeheerproces van de onderneming of het project in het systeemontwikkelingsproces met als doel aan te tonen dat het systeem veilig is. Het veiligheidsbewijs bevat doorgaans geen groot aantal gedetailleerde bewijsstukken, maar wel nauwkeurige verwijzingen naar deze documenten.

[G 4] **Veiligheidsbewijs voor technische systemen:** de CENELEC-normen kunnen dienen als leidraad om veiligheidsbewijzen te schrijven en/of samen te stellen:

(a) zie de norm EN 50 129 {Ref. 7} “Spoorwegtoepassingen – Communicatie, signalering en processystemen - elektronische signaleringssystemen met betrekking tot veiligheid”; in aanhangsel H.2 van het richtsnoer EN 50 126-2 {Ref. 9} wordt ook een structuur voorgesteld van het veiligheidsbewijs voor seingevingssystemen;
(b) zie aanhangsel H.1 van het richtsnoer EN 50 126-2 {Ref. 9} voor de structuur van het veiligheidsbewijs voor rollend materieel;
(c) zie aanhangsel H.3 van het richtsnoer EN 50 126-2 {Ref. 9} voor de structuur van het veiligheidsbewijs voor infrastructuur.

Zoals blijkt uit deze referenties, hangt niet alleen de structuur, maar ook de inhoud van het veiligheidsbewijs af van het systeem waarvoor de conformiteit met de veiligheid moet worden aangetoond.

Het veiligheidsbewijs in aanhangsel H van het richtsnoer EN 50 126-2 {Ref. 9} reikt alleen voorbeelden aan en is mogelijk niet geschikt voor alle soortgelijke systemen. Bijgevolg moet dit overzicht worden gebruikt met de nodige zaakkennis over wat zich precies leent voor elke specifieke toepassing.

[G 5] **Veiligheidsbewijs voor organisatorische en operationele aspecten in spoorwegsystemen:**

Op dit moment bestaat geen specifieke norm waarin structuur, inhoud en nadere instructies zijn vastgelegd om het veiligheidsbewijs op te stellen voor organisatorische en operationele aspecten van een spoorwegsysteem. Aangezien het veiligheidsbewijs beoogt op gestructureerde wijze aan te tonen dat het systeem voldoet aan de veiligheidsvereisten, mag echter dezelfde indeling worden gebruikt als voor technische systemen. De referenties onder [G 4] in punt 5.1 dienen inderdaad als advies en geven een controlelijst van onderwerpen die aan bod moeten komen, ongeacht het type systeem dat wordt beoordeeld. Om organisatorische en operationele wijzigingen te beheren, moet een soortgelijk kwaliteitsborgings- en veiligheidsbeheerproces worden toegepast als voor technische wijzigingen. Daarbij moet worden aangetoond dat het systeem voldoet aan de opgegeven veiligheidsvereisten. Eisen in CENELEC-normen die niet gelden voor organisatorische en operationele aspecten houden louter verband met ontwerpvoorzieningen voor technische systemen, zoals bijvoorbeeld beginselen inzake “intrinsieke faalveiligheid van apparatuur”, elektromagnetische compatibiliteit (EMC), enz.

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

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

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] Naargelang van de complexiteit van het systeem kan dit bewijsmateriaal in een of meer veiligheidsbewijzen worden verzameld. Zie respectievelijk onder [G 4] en onder [G 5] in punt 5.1 voor de structuur van het veiligheidsbewijs wat betreft technische systemen, en voor operationele en organisatorische aspecten.

[G 2] Zie ook onder A.4. in aanhangsel A voor mogelijke voorbeelden van bewijsmateriaal.

[G 3] De levensduur van technische systemen en subsystemen in de spoorwegsector wordt doorgaans geschat op een dertigtal jaar. Tijdens een dergelijke lange periode is de kans groot dat een aantal belangrijke wijzigingen in deze systemen worden aangebracht. Er moeten dan ook aanvullende risicobeoordelingen plaatsvinden voor deze systemen en de interfaces ervan. Daarbij moet de begeleidende documentatie worden herzien, aangevuld en doorgegeven aan de verschillende actoren en organisaties die gevareninventarissen gebruiken. Een en ander betekent dat hoge eisen worden gesteld inzake documentenadministratie en configuratiebeheer.

[G 4] Daarom is het handig dat de onderneming die alle informatie over risicobeoordeling en -beheer archiveert, zorgt dat de resultaten/gegevens worden opgeslagen op een informatiedrager die tijdens de volledige levensduur en levenscyclus van het systeem (dat wil zeggen 30 jaar lang) kan worden gelezen en geraadpleegd.

[G 5] De belangrijkste redenen voor deze vereiste zijn onder meer:

(a) waarborgen dat alle veiligheidsanalyses en veiligheidsaantekeningen van het beoordeelde systeem toegankelijk blijven tijdens de volledige levensduur van het systeem. Op die manier:

(1) is de recentste systeemdocumentatie beschikbaar voor het geval aanvullende belangrijke wijzigingen in hetzelfde systeem worden aangebracht;
(2) kunnen de toepasselijke veiligheidsanalyses en veiligheidsaantekeningen worden geraadpleegd als tijdens de levensduur van het systeem een probleem optreedt;

(b) waarborgen dat de veiligheidsanalyses en veiligheidsaantekeningen van het beoordeelde systeem beschikbaar zijn wanneer het systeem als soortgelijk referentiesysteem in andere toepassingen wordt gebruikt.

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

BIJLAGE II BIJ DE CSM-VERORDENING

Criteria waaraan de beoordelingsinstanties moeten voldoen

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] Dit behoeft geen verdere uitleg.

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

AANHANGSEL A: EXTRA TOELICHTINGEN

A.1. Inleiding

A.1.1. Dit aanhangsel beoogt voorliggend document beter leesbaar te maken. Complexere onderwerpen worden verder uitgewerkt in dit aanhangsel om de lezer niet te overstelpen met informatie in het hoofddocument.

A.2. Gevareninventarisatie

A.2.1. In punt 4.6.3. van de norm EN 50 126-1 {Ref. 8} alsmede in aanhangsel B.2 van het richtsnoer EN 50 126-2 {Ref. 9} staan aanwijzingen over gevarenclassificatie/-indeling.

A.3. Risicoaanvaardingscriterium voor technische systemen (RAC-TS)

A.3.1. Bovengrens van risicoaanvaardbaarheid voor technische systemen

A.3.1.1. Het RAC-TS wordt omschreven in punt 2.5.4. van {Ref. 4}.

A.3.1.2. Het RAC-TS beoogt een bovengrens af te bakenen van de risicoaanvaardbaarheid voor technische systemen waarvoor veiligheidsvereisten niet kunnen worden afgeleid door praktijkcodes toe te passen of door een vergelijking met soortgelijke referentiesystemen te maken. Bijgevolg fungeert dit criterium als ijkpunt voor kalibrering van risicoanalysemethoden voor technische systemen. Zoals beschreven onder A.3.6. in aanhangsel A van dit document, kan dit ijkpunt of deze bovengrens van de risicoaanvaardbaarheid ook worden gebruikt om de risicoaanvaardingscriteria te bepalen voor andere functionele storingen van technische systemen waarvan niet aannemelijk is dat ze rampzalige gevolgen zullen hebben (zijnde voor andere ernstgraden). Het RAC-TS is echter geen methode voor risicoanalyse.

A.3.1.3. Het RAC-TS is een semikwantitatief criterium. Het is zowel van toepassing op willekeurige als op systematische apparatuurstoringen/-fouten van het technische systeem. Bijgevolg bestrijkt dit criterium ook systematische storingen/fouten van het technische systeem die worden veroorzaakt door menselijke fouten tijdens het ontwikkelingsproces van het technische systeem (dat wil zeggen specificatie, ontwerp, tenuitvoerlegging en validering). Menselijke fouten tijdens bediening en onderhoud van de technische systemen komen echter niet aan bod in het RAC-TS.

A.3.1.4. Volgens bijlage A.3 en bijlage A.4 van de CENELEC-norm 50 129 zijn systematische storingen/fouten niet kwantificeerbaar. Bijgevolg moet de kwantitatieve doelstelling alleen voor willekeurige apparatuurfouten worden aangetoond. Systematische storingen/fouten worden behandeld door kwalitatieve methoden(15). *"De systematische storingsintegriteit kan niet worden beoordeeld door kwantitatieve methoden. Daarom worden*

(15) *Volgens de CENELEC-normen 50 126, 50 128 en 50 129 moet het kwantitatieve waardecijfer voor willekeurige apparatuurstoringen altijd worden gerelateerd aan een veiligheidsintegriteitsniveau om de systematische storingen/fouten te beheren. Daarom moet voor het waardecijfer $10^{-9}\,h^{-1}$ van het RAC-TS ook een passend proces worden opgezet om de systematische storingen/fouten juist te beheren. Ter wille van de leesbaarheid wordt in de nota echter vaak alleen verwezen naar de willekeurige apparatuurstoringen van het technische systeem.*

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

veiligheidsintegriteitsniveaus gebruikt om methoden, hulpmiddelen en technieken te groeperen die, wanneer ze effectief worden toegepast, een geschikte mate van betrouwbaarheid bieden om een systeem met een bepaald integriteitsniveau te realiseren."

A.3.1.5. Ook is het volgens de CENELEC-normen niet mogelijk de integriteit van de software van technische systemen te kwantificeren. De CENELEC-norm 50 128 biedt een leidraad voor het ontwikkelingsproces van veiligheidsgerelateerde software naargelang van het vereiste veiligheidsintegriteitsniveau. Dat omvat het proces van ontwerp, keuring, validering en kwaliteitsborging voor de software.
Volgens de CENELEC-norm 50 128 is voor een programmeerbaar elektronisch besturingssysteem waarin veiligheidsfuncties ten uitvoer worden gelegd niveau 4 het hoogst mogelijke veiligheidsintegriteitsniveau wat betreft het softwareontwikkelingsproces, wat overeenkomt met een kwantitatieve aanvaardbare risicofactor van 10^{-9} h^{-1}.

A.3.1.6. Voor zover systematische storingen/fouten niet kwantificeerbaar zijn, moeten ze in de plaats daarvan kwalitatief worden beheerd door een kwaliteitsborgings- en veiligheidsbeheerproces op te zetten dat compatibel is met het voor het beoordeelde systeem vereiste veiligheidsintegriteitsniveau.

(a) dit kwaliteitsborgingsproces beoogt *"de frequentie van optreden van menselijke fouten in elk stadium van de levenscyclus minimaal te houden en zodoende het risico van systematische fouten in het systeem te beperken"*;
(b) het veiligheidsbeheerproces beoogt *"de frequentie van optreden van veiligheidsgerelateerde menselijke fouten in de gehele levenscyclus verder te reduceren en zodoende het restrisico van veiligheidsgerelateerde systematische fouten minimaal te houden."*

A.3.1.7. De volgende normen bieden een leidraad voor het beheren van de frequentie van optreden van systematische storingen/fouten, alsmede voor mogelijke ontwerpmaatregelen ter bescherming tegen gemeenschappelijk/meervoudig falen (Common Cause Failure/Common Mode Failure of CCF/CMF) en ter waarborging dat het technische systeem bij dergelijke storingen/fouten in een faalveilige toestand overgaat:

(a) de CENELEC-norm 50 126-1 {Ref. 8} en het bijbehorende richtsnoer 50 126-2 {Ref. 9} geeft een overzicht van de bepalingen uit CENELEC 50 129 en de toepasbaarheid daarvan wat betreft bewijsstukken voor andere dan seingevingssystemen: zie tabel 9.1 in richtsnoer 50 126-2 {Ref. 9}. Dit overzicht biedt een leidraad voor de wijze waarop niet alleen fouten die hun oorsprong vinden in het systeem zelf, maar ook de gevolgen daarvan op de omgeving van het beoordeelde systeem, moeten worden aangepakt;

Zo worden bijvoorbeeld technieken/maatregelen voor ontwerpeigenschappen gegeven in *"Tabel E.5: Ontwerpeigenschappen (als bedoeld in 5.4)"* van de CENELEC-norm 50 129 {Ref. 7}, *"ter vermijding en beheersing van fouten veroorzaakt door:*

(1) *"residuele ontwerpfouten";*
(2) *"milieutechnische condities";*
(3) *"verkeerd gebruik of bedieningsfouten";*
(4) *"residuele fouten in de software";*
(5) *"menselijke factoren";*

Bijlage D en bijlage E van de CENELEC-norm 50 129 {Ref. 7} bevatten technieken en maatregelen ter vermijding van systematische fouten en ter beheersing van willekeurige apparatuurstoringen en systematische storingen/fouten voor veiligheidsgerelateerde elektronische seingevingssystemen. Tal van deze technieken en maatregelen kunnen ook worden toegepast op andere dan seingevingssystemen door te refereren aan deze aanwijzingen in tabel 9.1 van het richtsnoer 50 126-2 {Ref. 9}.

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

(b) de CENELEC-norm 50 128 biedt een leidraad voor het ontwikkelingsproces van veiligheidsgerelateerde software naargelang het veiligheidsintegriteitsniveau (niveau 0 tot niveau 4) dat wordt vereist voor de software van het beoordeelde systeem.

A.3.1.8. Het RAC-TS stelt het hoogste veiligheidsintegriteitsniveau voor dat overeenkomstig de CENELEC- en IEC-normen kan worden vereist. Duidelijkheidshalve worden de in IEC 61508-1 en CENELEC 50 129 genoemde eisen overgenomen:

(a) IEC 61508-1: *"Deze norm bepaalt een ondergrens voor de doelmaatstaf van storingen die bij een gevaarlijke faalwijze kan worden toegepast. Deze doelmaatstaf kan worden gespecificeerd als ondergrens voor veiligheidsintegriteitsniveau 4. Mogelijk kunnen veiligheidsgerelateerde systemen met een lagere doelmaatstaf worden ontworpen voor zover het niet-complexe systemen betreft. Aangenomen wordt echter dat de cijfers in de tabel de grenswaarde voorstellen die op dit moment voor relatief complexe systemen kan worden bereikt (bijvoorbeeld veiligheidsgerelateerde programmeerbare elektronische systemen)."*

(b) EN 50129: *"Een functie met kwantitatieve eisen van meer dan 10^{-9} h^{-1} moet op een van de volgende manieren worden behandeld:*

(1) *als de functie kan worden onderverdeeld in functioneel onafhankelijke subfuncties, kan de aanvaardbare risicofactor (THR of Tolerable Hazard Rate) worden opgesplitst tussen deze subfuncties en kan aan elke subfunctie een veiligheidsintegriteitsniveau worden toegekend;*

(2) *kan de functie niet worden onderverdeeld, dan moet minstens worden voldaan aan de voor het veiligheidsintegriteitsniveau 4 vereiste maatregelen en methoden, en moet de functie worden gebruikt in combinatie met andere technische of operationele maatregelen om de vereiste aanvaardbare risicofactor te bereiken."*

A.3.1.9. De kwantitatieve veiligheidseis moet dan in alle technische systemen tot dit cijfer worden beperkt. Wordt een hoger beschermingsniveau vereist, dan kan dit niet met één systeem worden bereikt. In dit geval moet de systeemarchitectuur worden gewijzigd, bijvoorbeeld door twee onafhankelijke systemen naast elkaar te gebruiken en kruiselings te controleren om veilige resultaten te krijgen. Dit leidt echter onvermijdelijk tot een kostenstijging voor de ontwikkeling van het technische systeem.

Opmerking: zijn er bestaande functies, bijvoorbeeld zuiver mechanische systemen waarvoor op basis van operationele ervaring een hoger integriteitsniveau werd bereikt, dan kan hetzelfde veiligheidsniveau worden beschreven door een specifieke praktijkcode of kunnen veiligheidsvereisten worden vastgelegd door de overeenstemming met het bestaande systeem te analyseren. In de werkingssfeer van de CSM mag het RAC-TS alleen worden toegepast als geen praktijkcode en geen referentiesysteem bestaan.

A.3.1.10. Dit kan als volgt worden samengevat:

(a) volgens de CENELEC-normen 50 126, 50 128 en 50 129 zijn systematische storingen/fouten niet kwantificeerbaar in de ontwikkelingsfase;

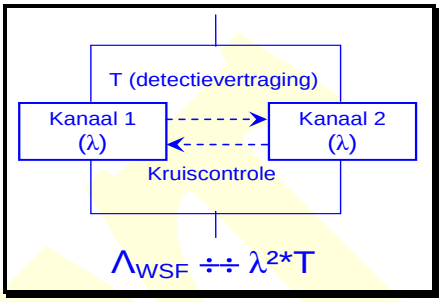
(b) de frequentie van optreden van systematische storingen/fouten moet samen met het daaraan verbonden restrisico worden beheerst en beheerd door passende kwaliteitsborgings- en veiligheidsbeheerprocessen toe te passen die verenigbaar zijn met het veiligheidsintegriteitsniveau dat van het beoordeelde systeem wordt vereist;

(c) het hoogste veiligheidsintegriteitsniveau dat kan worden bereikt is niveau 4, zowel voor willekeurige apparatuurstoringen als voor systematische storingen/fouten van technische systemen;

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

(d) deze begrenzing tot veiligheidsintegriteitsniveau 4 houdt in dat de maximaal aanvaardbare risicofactor, dat wil zeggen het maximale storings- of faaltempo, voor technische systemen ook tot 10^{-9} h^{-1} moet worden beperkt.

A.3.1.11. Een aanvaardbare risicofactor van 10^{-9} h^{-1} kan worden bereikt voor het technische systeem met een "faalveilige architectuur" (die per definitie voldoet aan zulke veiligheidsprestaties) of een "redundante architectuur" (dat wil zeggen twee onafhankelijke verwerkingskanalen die elkaar kruiselings controleren).



Figuur 13: Redundante architectuur voor een technisch systeem.

Wat betreft een redundante architectuur blijkt dat de foutieve seingeving (Λ_{WSF}) van het technische systeem algemeen beschouwd evenredig is met λ^2*T, waarbij:

(a) λ^2 het kwadraat is van het storingstempo van foutieve seingevingen in een kanaal;

(b) T de tijd is die het ene kanaal nodig heeft om een foutieve seingeving van het andere kanaal op te sporen. Doorgaans is dit een veelvoud van de verwerkingstijd/-cyclus van een kanaal. T bedraagt gewoonlijk minder dan 1 seconde.

A.3.1.12. Volgens deze formule (λ^2*T) kan in theorie worden aangetoond (door alleen de willekeurige apparatuurstoringen van het technische systeem te beschouwen – zie ook onder A.3.1.13. in aanhangsel A) dat een kwantitatieve eis van 10^{-9} h^{-1} voor het RAC-TS haalbaar is. De systematische storingen/fouten moeten procesmatig worden beheerd: zie onder A.3.1.6. in aanhangsel A. Bijvoorbeeld:

(a) met een gemiddeld storingsvrij interval van 10.000 uur als betrouwbaarheidsgraad van een kanaal, en de conservatieve aanname dat elke kanaalstoring onveilig is, komt de foutieve seingeving van het kanaal uit op 10^{-4} h^{-1};

(b) zelfs als het 10 minuten (dat wil zeggen $\approx 2*10^{-3}$ uur) duurt om de foutieve seingeving(en) van het andere kanaal op te sporen, wat eveneens een conservatieve aanname is;

bedraagt de totale foutieve seingeving $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}

A.3.1.13. In de praktijk moet voor een dergelijke redundante architectuur bij de evaluatie van de kwantitatieve totale foutieve seingevingen rekening worden gehouden met in het ontwerpstadium genomen maatregelen ter bescherming tegen gemeenschappelijk/meervoudig falen (Common Cause Failure/Common Mode Failure of CCF/CMF), en ter waarborging dat het technische systeem in een faalveilige toestand overgaat in geval van gemeenschappelijk/meervoudig falen. Bijgevolg moet de totale foutieve seingeving (Λ_{WSF}) worden geëvalueerd rekening houdend met:

(a) de voor alle kanalen gemeenschappelijke onderdelen, bijvoorbeeld enkelvoudige of gemeenschappelijke ingangen naar alle kanalen, gemeenschappelijke stroomvoorziening, vergelijkers, kiezers, enz.;

(b) de benodigde tijd om verborgen of latente storingen op te sporen. Voor complexe technische systemen kan die tijd in verschillende orden van grootte boven 1 seconde liggen;

(c) het effect van gemeenschappelijk/meervoudig falen (CCF/CMF).

De normen onder A.3.1.7. in aanhangsel A van voorliggend document vormen een leidraad over deze onderwerpen.

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

A.3.2. Stroomschema voor de toepasbaarheidstest van het RAC-TS

A.3.2.1. In Figuur 14 wordt geïllustreerd hoe het RAC-TS wordt toegepast op gevaren die ontstaan door het falen van technische systemen.

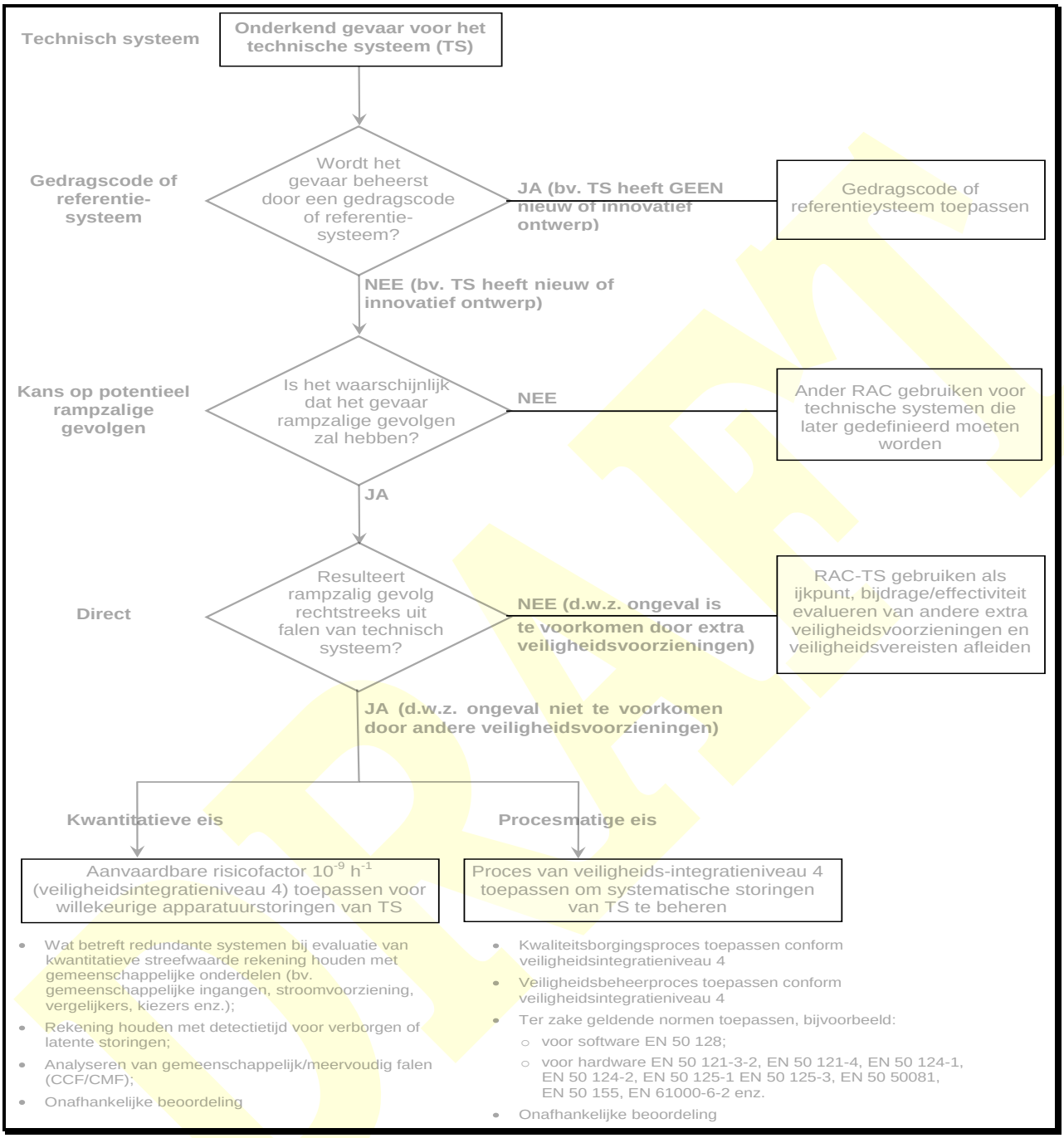
A.3.2.2. Onder C.15. in aanhangsel C wordt dit stroomschema op een voorbeeld toegepast.

A.3.3. Definitie van een technisch systeem in de CSM

A.3.3.1. Het RAC-TS is alleen van toepassing op technische systemen. In Artikel 3(22), van de CSM-verordening wordt "technisch systeem" als volgt gedefinieerd:

'technisch systeem' is te verstaan als een product of samenstel van producten met inbegrip van ontwerp, implementatie en documenten ter staving. De ontwikkeling van een technisch systeem begint met de specificatie van de eisen ervan, en eindigt met de goedkeuring ervan. Ook al komt het ontwerp van toepasselijke interfaces met het menselijke gedrag daarbij aan bod, menselijke operators en de door hen uitgevoerde handelingen maken geen deel uit van een technisch systeem. Het onderhoudsproces wordt nader toegelicht in de onderhoudshandleidingen, maar maakt geen deel uit van het technische systeem.

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



Figuur 14: Stroomschema voor de toepasbaarheidstest van het RAC-TS.

A.3.4. Verduidelijking van de definitie “technisch systeem”

A.3.4.1. In deze definitie van een technisch systeem wordt het toepassingsgebied van een technisch systeem beschreven: *"technisch systeem is een product of een geheel van producten met inbegrip van het ontwerp, de invoering en de begeleidende documenten."* Bijgevolg behelst en omvat dit:

(a) de fysieke delen waaruit het technische systeem is samengesteld;

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

(b) eventueel daarmee samenhangende software;
(c) het ontwerp en de implementatie van het technische systeem, indien van toepassing met inbegrip van de configuratie of parameterbepaling van een generiek product volgens toepassingsspecifieke eisen;
(d) de documenten ter staving die nodig zijn voor:

(1) de ontwikkeling van het technische systeem;
(2) de bediening (exploitatie) en het onderhoud van het technische systeem.

A.3.4.2. De toelichtingen bij deze definitie geven nauwkeurig het toepassingsgebied van het technische systeem aan:

(a) *"De ontwikkeling van een technisch systeem begint met de vaststelling van de eisen en eindigt met de goedkeuring van het systeem."* Dit omvat de fasen 1 tot 10 van de V-cyclus in figuur 10 van de CENELEC-norm 50 126-1 {Ref. 8};

(b) *"Hoewel rekening wordt gehouden met het ontwerp van interfaces met menselijk gedrag, maken personeel en bediening door de mens geen deel uit van een technisch systeem."* Fouten te wijten aan menselijke factoren tijdens bediening en onderhoud van het technische systeem maken geen deel uit van het technische systeem zelf. Toch moet daarmee rekening worden gehouden bij het ontwerp van de interfaces met de menselijke operators. Doel hiervan is het minimaliseren van de kans op menselijke fouten te wijten aan een gebrekkig ontwerp van de desbetreffende interfaces met de menselijke operators;

(c) *"Het onderhoudsproces wordt beschreven in de onderhoudshandleidingen, maar maakt zelf geen deel uit van het technisch systeem."* Dit betekent dat het RAC-TS niet moet worden toegepast op de bediening en het onderhoud van de technische systemen; deze zijn in hoge mate afhankelijk van de door menselijk personeel uitgevoerde processen en handelingen.
Nochtans moeten alle relevante eisen (bijvoorbeeld periodiek preventief onderhoud of correctief onderhoud in geval van storingen) met voldoende detailleringsniveau in de technische systeemomschrijving worden opgenomen ter ondersteuning van het onderhoud van technische systemen. De manier waarop het onderhoud wordt georganiseerd en uitgevoerd op het desbetreffende technische systeem moet echter niet in de technische systeemomschrijving, maar in de bijbehorende onderhoudshandleidingen worden opgenomen.

A.3.4.3. Zie ook onder A.3.1. in aanhangsel A.

A.3.5. Functies van technische systemen waarop het RAC-TS van toepassing is

A.3.5.1. Volgens de definitie van het RAC-TS is dit van toepassing op foutieve seingevingen van de functies die het technische systeem moet vervullen, voor zover die *"aannemelijk"* en ***"direct"*** kunnen leiden tot *"rampzalige gevolgen kan leiden"*: zie punt 2.5.4. in {Ref. 4}.

A.3.5.2. Het RAC-TS mag ook worden toegepast op functies waarbij technische systemen zijn betrokken, maar die bij falen **niet** ***"direct"*** kunnen leiden tot *"rampzalige gevolgen"*. In dit geval moet het RAC-TS worden toegepast als totale streefwaarde voor de reeks gebeurtenissen die rampzalige gevolgen heeft. Op basis van deze totale streefwaarde moet de werkelijke bijdrage van elke gebeurtenis en dus ook van het niet-functioneren van het technische systeem waarop het faalscenario in kwestie betrekking heeft, worden afgeleid zoals bepaald onder A.3.6. in aanhangsel A.

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

De CSM-werkgroep moet dit gebruik van het RAC-TS nog bespreken en het daarover eens worden.

A.3.5.3. Op welke functies van het technische systeem is het RAC-TS van toepassing? In de IEC-norm 61226:2005 staat het volgende:

(a) een functie is in deze context te verstaan als een *"te bereiken specifiek doel dat of een te verwezenlijken specifieke doelstelling die moet worden gespecificeerd of omschreven zonder te refereren aan de fysieke middelen om daarin te slagen"*;
(b) een functie (als zwarte doos beschouwd) zet inputparameters (bijvoorbeeld materiaal, energie, informatie) om in doelgerelateerde outputparameters (bijvoorbeeld materiaal, energie, informatie);
(c) de functie wordt geanalyseerd onafhankelijk van de technische realisatie ervan.

A.3.5.4. Het RAC-TS is van toepassing op functies van de volgende typen:

(a) voorbeelden voor het subsysteem "ETCS-treinapparatuur" (European Train Control System):

(1) "de bestuurder de nodige informatie verschaffen om de trein veilig te besturen en een dwangremming in te zetten wanneer met te hoge snelheid wordt gereden". De bestuurder en de ETCS-treinapparatuur kunnen erop toezien dat de trein de maximaal toegestane snelheid niet overschrijdt op basis van informatie afkomstig van de baanapparatuur (toegestane snelheid) en de door de ETCS-treinapparatuur berekende snelheid van de trein. Het RAC-TS is van toepassing op de beoordeling van de snelheid van de trein door de treinapparatuur aangezien:

(i) er geen (directe) aanvullende veiligheidsvoorziening is doordat de aan de treinbestuurder doorgegeven informatie ook te laag wordt ingeschat;
(ii) snelheidsoverschrijding de trein kan doen ontsporen, wat een ongeval met potentieel rampzalige gevolgen is;

(2) "de bestuurder de nodige informatie verschaffen om de trein veilig te besturen en een dwangremming in te zetten in geval van niet-naleving van een rittoestemming".

(b) voorbeeld voor een spoorstroomloop: "treindetectie (baanvak bezet)". Het RAC-TS is van toepassing op deze functie omdat geen "volgordecontrole" in de baanvakbeveiligingsfunctie is geïmplementeerd;
(c) voorbeeld voor een wissel: "controle van de wisselstand";

A.3.5.5. In bepaalde normen zijn functies gedefinieerd waarop het RAC-TS van toepassing kan zijn. Bijvoorbeeld:

(a) in het normatieve gedeelte van de norm prEN 0015380-4 {Ref. 13} (MODTRAIN-project) worden drie hiërarchische functieniveaus gedefinieerd (uitgebreid tot vijf niveaus in informatieve bijlagen). In totaal worden honderden treingerelateerde functies gedefinieerd in prEN 0015380-4;
(b) doorgaans wordt aanbevolen de functies op de eerste drie niveaus van prEN 0015380-4 te selecteren (maar niet op de lager gelegen niveaus) en daarbij tevens rekening te houden met de onderverdeling naar product;
(c) voor functies die niet behoren tot de werkingssfeer van prEN 0015380-4, moet het passende functionele niveau vergelijkenderwijs worden bepaald op basis van deskundig oordeel.

Het Spoorwegbureau moet deze voorbeelden van functies uit prEN 0015380-4 verder uitwerken in het kader van de werkzaamheden inzake algemeen aanvaardbare risico's en risicoaanvaardingscriteria.

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

A.3.5.6. Het RAC-TS is bijvoorbeeld ook van toepassing op volgende in prEN 0015380-4 genoemde functie: *"controle kantelbaktechniek"* (code = CLB). Deze functie kan als volgt op systeemniveau worden gebruikt:

(a) eerste geval: de trein moet in bochten naar binnen hellen met het oog op het reizigerscomfort; daarbij moet worden gecontroleerd of het constructieprofiel van de trein overeenkomt met de baaninfrastructuur;
(b) tweede geval: de trein moet in bochten naar binnen hellen uitsluitend met het oog op het reizigerscomfort zonder te controleren of het constructieprofiel van de trein overeenkomt met de baaninfrastructuur;

Het RAC-TS wordt toegepast in het eerste geval, maar niet in het tweede omdat het falen van de kantelbakfunctie geen rampzalige gevolgen heeft.

A.3.5.7. Uit voorbeeld (b) onder A.3.5.4. en de voorbeelden onder A.3.5.6. in aanhangsel A blijkt duidelijk dat het niet haalbaar is een voorgedefinieerde lijst van functies samen te stellen waarop het RAC-TS te allen tijde van toepassing is. Dit hangt altijd af van de manier waarop het systeem deze subsysteemfuncties gebruikt.

A.3.5.8. Onder C.15. in aanhangsel C staat een toepassingsvoorbeeld van het RAC-TS.

A.3.6. Toepassingsvoorbeelden van het RAC-TS

A.3.6.1. Inleiding

(a) De voorbeelden in dit hoofdstuk geven aan hoe het storings- of faaltempo voor de andere ernstgraden van gevaren wordt bepaald en hoe veiligheidsvereisten kleiner dan $10^{-9}\,h^{-1}$ kunnen worden afgeleid. In voorliggend document wordt geen specifieke methode geprefereerd of opgelegd. Er wordt alleen uitgelegd hoe bepaalde gangbare methoden met behulp van het RAC-TS kunnen worden gekalibreerd. Een en ander moet verder worden uitgediept in het kader van de werkzaamheden van het Spoorwegbureau inzake algemeen aanvaardbare risico's en risicoaanvaardingscriteria.

(b) Het RAC-TS kan inderdaad slechts op een klein aantal gevallen direct worden toegepast, want in de praktijk gebeurt het zelden dat het falen van technische systemen rechtstreeks ongevallen met potentieel rampzalige gevolgen veroorzaakt. Om het criterium toe te passen op gevaren met niet-rampzalige gevolgen en de streefwaarde qua storings-of faaltempo te bepalen, kunnen bijgevolg afwegingen worden gemaakt (bijvoorbeeld door een risicomatrix op basis van dit criterium te kalibreren) tussen verschillende parameters, bijvoorbeeld ernst versus frequentie.

A.3.6.2. Voorbeeld 1: Directe risicoafweging

(a) Het RAC-TS kan eenvoudig worden toegepast op scenario's die, enkele onafhankelijke parameters buiten beschouwing gelaten, overeenkomen met de referentietoestand zoals gedefinieerd in het RAC-TS in lid 2.5.4. van de CSM-verordening {Ref. 3};

(b) Stel dat voor een specifieke parameter p een multiplicatieve relatie met het risico bestaat. Stel dat p* aanwezig is in de referentietoestand, terwijl p‘ van toepassing is in het alternatieve scenario. In dit geval is alleen de parameterverhouding p*/p’ relevant en mag de frequentie van optreden worden gereduceerd. Deze procedure mag worden herhaald als de parameters onafhankelijk zijn.

(c) Voorbeeld:

(1) Stel dat de werkelijke waarschijnlijkheid van rampzalige gevolgen op grond van deskundig oordeel tien keer kleiner werd bevonden dan in de referentietoestand

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

zoals bedoeld in lid 2.5.4 van de CSM-verordening {Ref. 3}. In dit geval wordt de eis $10^{-8}\,h^{-1}$ in plaats van $10^{-9}\,h^{-1}$.

(2) Stel dat een extra veiligheidsvoorziening van een ander technisch systeem (ongeacht de gevolgen), die in 50% van de gevallen effectief is, wordt onderkend;

(3) dan wordt de veiligheidseis $5*10^{-7}\,h^{-1}$ (dat wil zeggen $0{,}5*10^{-8}\,h^{-1}$) in plaats van $10^{-9}\,h^{-1}$.

A.3.6.3. Voorbeeld 2: Kalibrering risicomatrix

(a) Om het RAC-TS juist te gebruiken in een risicomatrix, moet de matrix betrekking hebben op het juiste systeemniveau (vergelijkbaar met het niveau genoemd onder A.3.5. in aanhangsel A).

(b) Het RAC-TS definieert een veld in de risicomatrix als aanvaardbaar, zijnde de coördinaat (rampzalige ernstgraad; frequentie van optreden $10^{-9}\,h^{-1}$): zie het rode veld in Tabel 5. Alle velden die betrekking hebben op een hogere frequentie moeten als "onaanvaardbaar" worden aangemerkt. Op te merken valt dat de frequentie van optreden van ongevallen alleen identiek is aan de frequentie van niet-functioneren wanneer het waarschijnlijk is dat het gevaar direct potentieel rampzalige gevolgen zal hebben.

(c) Nu kan de volledige matrix worden ingevuld, zij het dan rekening houdend met andere effecten, zoals het risicomijdende karakter (risicoaversie) of de extrapolatie naar categorieën. In het eenvoudigste geval van een lineaire decimale extrapolatie (aangegeven door de pijl in Tabel 5) wordt het veld dat volgens het RAC-TC als "aanvaardbaar" werd aangemerkt, lineair geëxtrapoleerd in de rest van de matrix. Dit betekent dat alle velden op (of onder) dezelfde schuine streep ook als "aanvaardbaar" worden aangemerkt. De velden daaronder kunnen ook als "aanvaardbaar" worden aangemerkt.

Tabel 5: Typevoorbeeld van een gekalibreerde risicomatrix.

Ongevalsfrequentie (veroorzaakt door gevaar)	**Risiconiveau**			
Frequent (10^{-4} per uur)	**Onaanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**
Waarschijnlijk (10^{-5} per uur)	**Onaanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**
Incidenteel (10^{-6} per uur)	**Aanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**
Gering (10^{-7} per uur)	**Aanvaardbaar**	**Aanvaardbaar**	**Onaanvaardbaar**	**Onaanvaardbaar**
Onwaarschijnlijk (10^{-8} per uur)	**Aanvaardbaar**	**Aanvaardbaar**	**Aanvaardbaar**	**Onaanvaardbaar**
Onaannemelijk (10^{-9} per uur)	**Aanvaardbaar**	**Aanvaardbaar**	**Aanvaardbaar**	**Aanvaardbaar**
	Verwaarloosbaar	Onbeduidend	Kritiek	Catastrofaal
	Ernstgraad van gevolgen van gevaren (bv. ongeval)			

Risico-evaluatie	**Risicovermindering/-beheersing**
Onaanvaardbaar	Het risico moet worden geëlimineerd.
Aanvaardbaar	Het risico is aanvaardbaar. Onafhankelijke beoordeling noodzakelijk.

(d) Als de matrix is ingevuld, kan die ook op niet-rampzalige gevaren worden toegepast. Heeft een andere functionele storing bijvoorbeeld de ernstgraad "kritiek", dan mag de aanvaardbare frequentie van optreden van ongevallen volgens de gekalibreerde risicomatrix hoogstens "onwaarschijnlijk" (of nog minder) zijn.

(e) Op te merken valt dat het gebruik van de risicomatrix overmatig conservatieve resultaten kan opleveren wat betreft de frequentie van optreden van functionele storingen (dat wil zeggen voor elk falen dat niet rechtstreeks ongevallen veroorzaakt).

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

A.3.6.4. Grondslag voor kalibrering van andere risicoanalysemethoden

Om andere risicoanalysemethoden te kalibreren, bijvoorbeeld het voorgestelde schema voor numerieke risicoprioritering of de risicografiek uit VDV 331 of IEC 61508, mag een soortgelijke procedure worden toegepast als voor de risicomatrix:

(a) Stap 1: het ijkpunt uit het RAC-TS classificeren als aanvaardbaar, en punten met een hogere frequentie of ernstgraad als onaanvaardbaar RAC-TS.
(b) Stap 2: de specifieke methode afwegen om de risicoaanvaardbaarheid te extrapoleren naar niet-rampzalige gevaren (met de lineaire risicoafweging als uitgangspunt).
(c) Stap 3: wat betreft niet-rampzalige gevaren het RAC-TS afleiden van de gekalibreerde risicoanalysemethode door de coördinaat (frequentie; ernstgraad) te extrapoleren naar de aldus verkregen FN-curve.

A.3.7. Conclusies voor het RAC-TS

A.3.7.1. In het algemene raamwerk voor risicobeoordeling zoals dit door de CSM wordt voorgesteld, zijn risicoaanvaardingscriteria nodig om te bepalen wanneer het restrisico tot een aanvaardbaar niveau wordt teruggebracht en dus ook wanneer de expliciete risico-inschatting mag worden stopgezet.

A.3.7.2. Het RAC-TS is een streefwaarde ($10^{-9}\,h^{-1}$) voor het ontwerp van technische systemen.

A.3.7.3. Hier volgen de belangrijkste doelstellingen van het RAC-TS:

(a) een bovengrens voor risicoaanvaardbaarheid vastleggen en zodoende fungeren als ijkpunt voor kalibrering van risicoanalysemethoden voor technische systemen;
(b) waarborgen van de wederzijdse erkenning wat betreft technische systemen aangezien de bijbehorende risico- en veiligheidsbeoordelingen in alle lidstaten aan hetzelfde risicoaanvaardingscriterium worden getoetst;
(c) kosten besparen door geen onnodig hoge kwantitatieve veiligheidsvereisten op te leggen;
(d) de concurrentie tussen fabrikanten bevorderen. Het gebruik van risicoaanvaardingscriteria die verschillen naargelang van de initiatiefnemer of lidstaat zou het bedrijfsleven verplichten telkens opnieuw aan te tonen dat dezelfde technische systemen aan de gestelde eisen voldoen. Dat zou de concurrentiepositie van fabrikanten in gevaar brengen en producten nodeloos duur maken.

A.3.7.4. Het is niet altijd nodig aan te tonen dat technische systemen voldoen aan de semikwantitatieve eis in het RAC-TS. Krachtens de CSM is het RAC-TS inderdaad alleen van toepassing op technische systemen waarvoor het niet mogelijk is de geïnventariseerde gevaren naar behoren te beheersen door praktijkcodes te gebruiken of een vergelijking te maken met soortgelijke referentiesystemen. Op die manier kunnen lagere veiligheidsvereisten worden gesteld mits het totale veiligheidsniveau gewaarborgd blijft.

A.3.7.5. Een geharmoniseerd semikwantitatief risicoaanvaardingscriterium voor technische systemen is alleen nodig wanneer geen praktijkcode noch referentiesysteem bestaat.

A.3.7.6. Het veiligheidsintegriteitsniveau voor systematische storingen/fouten is beperkt tot niveau 4. Bijgevolg moet het veiligheidsintegriteitsniveau voor willekeurige apparatuurstoringen van technische systemen ook tot niveau 4 worden beperkt. Dat komt overeen met een aanvaardbare risicofactor van $10^{-9}\,h^{-1}$ (zijnde het maximale storings- of faaltempo). Als strengere veiligheidsvereisten nodig zijn, kunnen die volgens de CENELEC-norm 50 129 niet met één systeem worden bereikt. In dat geval moet de systeemarchitectuur worden gewijzigd, bijvoorbeeld door twee systemen te gebruiken. Dat kan de kosten van het

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

technische systeem fors doen oplopen. Zie onder A.3.1. in aanhangsel A voor meer bijzonderheden.

A.3.7.7. Tot slot wordt onder A.3.6. in aanhangsel A samengevat hoe het RAC-TS kan fungeren als ijkpunt voor kalibrering van bijzondere risicoanalysemethoden wanneer technische systemen tot minder ernstige gevolgen kunnen leiden dan rampzalige gevolgen.

A.4. Bewijsmateriaal resulterend uit de veiligheidsbeoordeling

A.4.1. In dit punt wordt uitgelegd welk bewijsmateriaal doorgaans aan een beoordelingsinstantie wordt bezorgd om een onafhankelijke beoordeling mogelijk te maken en de veiligheidsgoedkeuring te krijgen zonder afbreuk te doen aan de nationale voorschriften in een lidstaat. Deze informatie kan dienen als controlelijst om na te gaan of alle relevante aspecten aan bod komen en zo nodig worden gedocumenteerd tijdens de toepassing van de CSM.

A.4.2. Veiligheidsplan: CENELEC adviseert bij aanvang van het project een veiligheidsplan over te leggen of, als dat praktisch niet haalbaar is, de desbetreffende beschrijving op te nemen in een ander relevant document. Worden beoordelingsinstanties aangesteld bij aanvang van het project, dan mag het veiligheidsplan ook ter beoordeling aan hen worden voorgelegd. Principieel moet het veiligheidsplan een beschrijving geven van:

(a) de opgezette organisatie en de vakkundigheid van iedereen die betrokken is bij de ontwikkeling en risicobeoordeling;
(b) alle veiligheidsgerelateerde activiteiten die in de verschillende projectfasen worden gepland, samen met de verwachte resultaten/uitkomsten (output);

A.4.3. In de systeemomschrijvingfase wordt het volgende bewijsmateriaal vereist:

(a) systeembeschrijving:
    (1) definitie van de reikwijdte/begrenzing van het systeem;
    (2) functionele beschrijving;
    (3) beschrijving van de systeemstructuur:
    (4) beschrijving van de milieutechnische en bedrijfscondities;
(b) beschrijving van de externe interfaces;
(c) beschrijving van de interne interfaces;
(d) beschrijving van de verschillende fasen in de levenscyclus;
(e) beschrijving van de veiligheidsbeginselen;
(f) beschrijving van de aannames die de grenzen voor risicobeoordeling afbakenen.

A.4.4. Om de risicobeoordeling mogelijk te maken, moet in de systeemomschrijving rekening worden gehouden met de context waarin de voorgenomen wijziging plaatsvindt:

(a) behelst de voorgenomen wijziging een wijziging van een bestaand systeem, dan dient de systeemomschrijving niet alleen het systeem in de toestand van vóór de wijziging, maar ook de voorgenomen wijziging zelf te beschrijven;
(b) bestaat de voorgenomen wijziging uit de bouw van een nieuw systeem, dan blijft de beschrijving beperkt tot de systeemomschrijving aangezien geen beschrijving van een bestaand systeem voorhanden is.

A.4.5. In de gevareninventarisatiefase wordt het volgende bewijsmateriaal vereist:

(a) beschrijving en verantwoording (inclusief beperkingen) van methoden en hulpmiddelen voor gevareninventarisatie (top-down- en bottom-up-methode, storingsanalyse of HAZOP, enz.);

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

(b) resultaten:

(1) gevarenlijsten;
(2) systeemspecifieke gevaren(grenzen);
(3) subsysteemgevaren;
(4) interfacegevaren;
(5) de veiligheidsmaatregelen die in deze fase in kaart kunnen worden gebracht;

A.4.6. Ook het volgende bewijsmateriaal wordt vereist in de risicoanalysefase:

(a) wanneer gevaren worden beheerst met gebruikmaking van praktijkcodes, moet worden aangetoond dat het beoordeelde systeem voldoet aan alle relevante eisen in de praktijkcode. Daarbij moet eveneens worden aangetoond dat de desbetreffende praktijkcodes juist worden toegepast;

(b) wanneer soortgelijke referentiesystemen worden gebruikt om gevaren te beheersen:

(1) definitie voor het beoordeelde systeem van de veiligheidsvereisten uit de desbetreffende referentiesystemen;
(2) het bewijs dat het beoordeelde systeem wordt gebruikt onder soortgelijke operationele en milieutechnische condities als het desbetreffende referentiesysteem. Als dat niet mogelijk is, moet worden aangetoond dat de afwijkingen van het referentiesysteem juist worden beoordeeld;
(3) het bewijs dat de veiligheidsvereisten uit referentiesystemen juist ten uitvoer worden gelegd in het beoordeelde systeem;

(c) wanneer een expliciete risico-inschatting wordt gebruikt om gevaren te beheersen:

(1) beschrijving en verantwoording (inclusief beperkingen) van methoden en hulpmiddelen voor risicoanalyse (kwalitatief, kwantitatief, semikwantitatief, niet-regressieanalyse...);
(2) inventarisatie van bestaande veiligheidsmaatregelen en risicobeperkende factoren voor elk gevaar (met inbegrip van aspecten die verband houden met menselijke factoren);
(3) risico-evaluatie en -rangschikking voor elk gevaar:

(i) inschatting van gevolgen van gevaren, met verantwoording (inclusief aannames, onderstellingen en randvoorwaarden);
(ii) inschatting van de frequentie van optreden van gevaren, met verantwoording (inclusief aannames, onderstellingen en randvoorwaarden);
(iii) gevarenrangschikking naar mate van kritiek-zijn en frequentie van optreden;

(4) inventarisatie van aanvullende adequate veiligheidsmaatregelen die de risico's voor elk gevaar tot een aanvaardbaar niveau terugbrengen (iteratief proces na de risico-evaluatiefase);

A.4.7. Van de risico-evaluatie vereist bewijsmateriaal:

(a) wanneer een expliciete risico-inschatting wordt uitgevoerd:

(1) definitie en verantwoording van risico-evaluatiecriteria voor elk gevaar;
(2) bewijs/verantwoording dat de veiligheidsmaatregelen en veiligheidsvereisten elk gevaar tot een aanvaardbaar niveau terugbrengen (gemeten naar het bovenvermelde risico-evaluatiecriterium);

(b) volgens het bepaalde in punt 2.3.5 en 2.4.3 van de CSM-verordening worden risico's waarvoor praktijkcodes worden toegepast en een vergelijking met referentiesystemen wordt gemaakt impliciet als aanvaardbaar aangemerkt mits respectievelijk (zie in stippellijn omcirkelde tekst in Figuur 1):

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

(1) is voldaan aan de in punt 2.3.2 genoemde toepassingsvoorwaarden van praktijkcodes;
(2) is voldaan aan de in punt 2.4.2 genoemde gebruiksvoorwaarden van een referentiesysteem;

Voor deze twee risicoaanvaardingsbeginselen zijn de risicoaanvaardingscriteria impliciet.

A.4.8. Bewijsmateriaal resulterend uit het gevarenbeheer:

(a) registratie van alle gevaren in een gevareninventaris met de volgende gegevens:
(1) het in kaart gebrachte gevaar;
(2) veiligheidsmaatregelen ter voorkoming dat het gevaar optreedt of ter beperking van de gevolgen;
(3) veiligheidsvereisten wat betreft de maatregelen;
(4) het desbetreffende deel van het systeem;
(5) de voor de veiligheidsmaatregelen verantwoordelijke actor;
(6) status van het gevaar (bijvoorbeeld openstaand, opgelost, verwijderd, overgedragen, beheerst enz.);
(7) datum waarop elk gevaar werd geregistreerd, herzien en beheerst;

(b) beschrijving van de manier waarop gevaren effectief zullen worden beheerst tijdens de gehele levenscyclus;
(c) beschrijving van de informatie-uitwisseling tussen de partijen wat betreft gevaren bij de interfaces, en verantwoordelijkheidsverdeling.

A.4.9. Bewijsmateriaal over de kwaliteit van het risico-evaluatie- en risicobeoordelingsproces:

(a) beschrijving van de bij het proces betrokken personen en hun vakkundigheid;
(b) wat betreft expliciete risico-inschattingen, beschrijving van informatie, gegevens en andere statistieken die in het proces worden gebruikt, en verantwoording van de mate waarin die geschikt zijn (bijvoorbeeld gevoeligheidsonderzoek van de gebruikte gegevens).

A.4.10. Bewijsmateriaal over conformiteit met veiligheidsvereisten:

(a) lijst van de gebruikte normen;
(b) beschrijving van ontwerp en operationele beginselen;
(c) bewijs dat een degelijk kwaliteitsborgings- en veiligheidsbeheersysteem voor het project wordt toegepast: zie onder [G 3] in punt 1.1.2;
(d) overzicht van de gevarenanalyserapporten (bijvoorbeeld analyse van de gevaarsoorzaak) waarin wordt aangetoond dat aan de veiligheidsvereisten is voldaan;
(e) beschrijving en verantwoording van methoden en hulpmiddelen (Failure Mode Effect and Criticality Analysis of FMECA, foutenboomanalyse…) die worden gebruikt om de gevaarsoorzaak te analyseren;
(f) overzicht van de tests voor veiligheidskeuring en -validering.

A.4.11. Veiligheidsbewijs: CENELEC adviseert elk hierboven genoemde bewijsmateriaal te groeperen en samen te vatten in één document dat aan de beoordelingsinstantie wordt overgelegd: zie onder [G 4] en [G 5] in punt 5.1.

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

AANHANGSEL B: VOORBEELDEN VAN TECHNIEKEN EN HULPMIDDELEN TER ONDERBOUWING VAN HET RISICOBEOORDELINGSPROCES

B.1. In bijlage E van het richtsnoer EN 50126-2 {Ref. 9} staan voorbeelden van technieken en hulpmiddelen om de in de CSM genoemde risicobeoordelingsactiviteiten uit te voeren. Deze technieken en hulpmiddelen worden samengevat in tabel E.1. Elke techniek wordt nader toegelicht. Waar nodig wordt voor meer informatie naar andere normen verwezen.

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

AANHANGSEL C: VOORBEELDEN

C.1. Inleiding

C.1.1. Dit aanhangsel beoogt voorliggend document beter leesbaar te maken. Het geeft een overzicht van alle verzamelde voorbeelden die tot doel hebben de CSM eenvoudiger toe te passen.

C.1.2. De voorbeelden van risico- of veiligheidsbeoordelingen in dit aanhangsel werden niet afgeleid van de toepassing van het CSM-proces. Reden hiervoor is dat ze werden uitgevoerd toen de CSM-verordening nog niet bestond. De voorbeelden kunnen als volgt worden ingedeeld:

(a) voorbeelden met herkomstaanduiding, zoals die van deskundigen in de CSM-werkgroep werden ontvangen
(b) voorbeelden opzettelijk zonder herkomstaanduiding, eveneens ontvangen van deskundigen in de CSM-werkgroep De herkomst moest op verzoek van de betrokken deskundigen vertrouwelijk blijven;
(c) voorbeelden zonder herkomstaanduiding, die werden opgesteld door personeelsleden van het Spoorwegbureau op basis van hun persoonlijke beroepservaring uit het verleden.

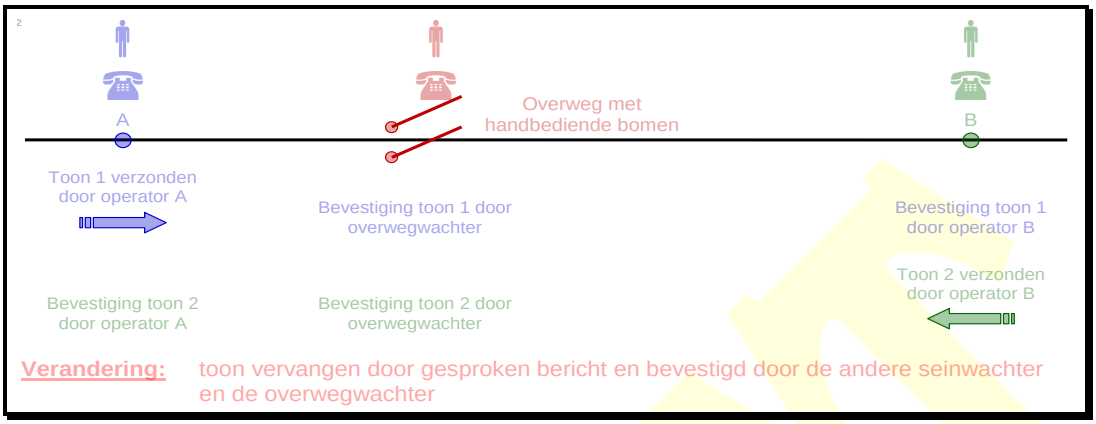
Voor zulke voorbeelden wordt de traceerbaarheid aangegeven tussen het toegepaste proces en het door de CSM voorgeschreven proces, alsmede de argumentatie en toegevoegde waarde om de eventueel in de CSM vereiste extra maatregelen te nemen.

C.2. Toepassingsvoorbeelden van criteria voor een belangrijke wijziging, zoals bepaald in artikel 4, lid 2

C.2.1. Het Spoorwegbureau werkt op dit ogenblik aan een begripsomschrijving van wat als "belangrijke wijziging" kan worden aangemerkt. In dit deel staat een daarmee samenhangend voorbeeld van de manier waarop de in artikel 4, lid 2, genoemde criteria kunnen worden toegepast.

C.2.2. De wijziging bestaat erin bij een overweg met handbediende bomen de manier te wijzigen waarop de seinwachter informatie over de richting van een naderende trein aan de overwegwachter doorgeeft. De wijziging wordt voorgesteld in Figuur 15.

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



Figuur 15: Voorbeeld van niet-belangrijke wijziging Telefonische melding voor overwegbewaking.

C.2.3. Bestaand systeem: vóór de geplande wijziging werd de informatie over de richting van een naderende trein automatisch aan de overwegwachter gemeld door de beltoon van de telefoon. De beltoon verschilde naargelang van de oorsprong van de oproep.

C.2.4. Voorgenomen wijziging: het bestaande telefoonsysteem is verouderd en moet worden vervangen door een nieuwe digitale telefooninstallatie; bijgevolg kan de desbetreffende informatie niet meer via de beltoon worden doorgegeven. De beltoon is precies dezelfde, ongeacht de seinwachter die de oproep maakt. Besloten werd deze functie te laten uitvoeren door een operationele procedure:

(a) bij het vertrek van de trein deelt de seinwachter de overwegwachter mondeling mee uit welke richting de trein komt;
(b) de informatie wordt vergeleken met de dienstregeling en bevestigd door zowel de overwegwachter als de andere seinwachter om zeker te zijn dat die goed wordt begrepen door de operator.

De voorgenomen wijziging en bijbehorende operationele procedure worden geïllustreerd in Figuur 15.

C.2.5. Ook al heeft de wijziging kennelijk gevolgen voor de veiligheid (risico dat de overwegboom niet tijdig wordt gesloten), uit andere criteria in artikel 4, lid 2 zoals:

(a) weinig complex;
(b) niet-innoverend, en
(c) eenvoudig te monitoren,

valt op te maken dat de voorgenomen wijziging geen belangrijke wijziging is.

C.2.6. In dit voorbeeld is een veiligheidsanalyse of op zijn minst een veiligheidsargumentatie nodig om aan te tonen dat, wat betreft deze voor de veiligheid kritieke taak, het vervangen van een verouderd technisch systeem door een operationele procedure (met personeel dat elkaar kruiselings controleert) hetzelfde veiligheidsniveau oplevert. Vraag is of het nodig is hierop het volledige CSM-proces toe te passen, compleet met gevareninventaris, onafhankelijke beoordeling door een beoordelingsinstantie, enz. In dat geval valt te betwijfelen of dit meerwaarde zal opleveren, wat meteen zou inhouden dat een dergelijke wijziging niet als belangrijk kan worden aangemerkt.

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

C.3. Voorbeelden van interfaces tussen actoren in de spoorwegsector

C.3.1. Hier volgen enkele voorbeelden van interfaces en redenen waarom actoren in de spoorwegsector moeten samenwerken:

(a) Infrastructuurbeheerder – infrastructuurbeheerder: in beide spoorweginfrastructuren moeten bijvoorbeeld veiligheidsmaatregelen worden geïntegreerd om een veilige overgang van treinen tussen beide infrastructuren te waarborgen;

(b) Infrastructuurbeheerder – spoorwegonderneming: er kunnen bijvoorbeeld specifieke infrastructuurafhankelijke bedrijfsvoorschriften bestaan die de treinbestuurder moet naleven;

(c) Infrastructuurbeheerder – fabrikant: voor de subsystemen van de fabrikant kunnen bijvoorbeeld gebruiksbeperkingen gelden die de infrastructuurbeheerder moet naleven;

(d) IM – dienstverlener: er kunnen bijvoorbeeld infrastructuurspecifieke onderhoudsbeperkingen bestaan die de onderaannemer van onderhoudswerkzaamheden moet naleven;

(e) Spoorwegonderneming – fabrikant: voor de subsystemen van de fabrikant kunnen bijvoorbeeld gebruiksbeperkingen gelden die de spoorwegonderneming moet naleven;

(f) Spoorwegonderneming – dienstverlener: er kunnen bijvoorbeeld infrastructuurspecifieke onderhoudsbeperkingen bestaan die de onderaannemer van onderhoudswerkzaamheden moet naleven;

(g) Spoorwegonderneming – houders: er kunnen bijvoorbeeld voertuigspecifieke gebruiksbeperkingen bestaan die moeten worden nageleefd door de spoorwegonderneming die deze voertuigen exploiteert;

(h) Fabrikant – fabrikant: bijvoorbeeld het beheer van veiligheidsgerelateerde technische interfaces tussen subsystemen van twee verschillende fabrikanten;

(i) Fabrikant – dienstverlener: bijvoorbeeld dat de fabrikant de gevareninventaris moet beheren wanneer werk wordt uitbesteed aan een onderneming die te klein is om een veiligheidsorganisatie te hebben voor het project in kwestie;

(j) Dienstverlener – dienstverlener: soortgelijk voorbeeld als onder j) hierboven;

C.3.2. Dienstverleners staan in voor alle activiteiten die worden uitbesteed door de infrastructuurbeheerder, spoorwegonderneming of fabrikant, zoals onderhoud, beheer van vervoerbewijzen (ticketing of reisbiljettenverkoop), constructietechnische diensten, enz.

C.3.3. Het volgende voorbeeld illustreert het interfacebeheer en de daaraan verbonden gevareninventarisatie. Het betreft een interface tussen een treinfabrikant en een initiatiefnemer (spoorwegonderneming). Vervolgens wordt uitgelegd hoe kan worden voldaan aan de belangrijkste criteria onder [G 3] in punt 1.2.1:

(a) Leiding: de initiatiefnemer (spoorwegonderneming);

(b) Input:

(1) lijst(en) van toepasselijke gevaren resulterend uit soortgelijke projecten;
(2) beschrijving van elke input en output (I/O) voor de interface, inclusief de prestatie-eigenschappen;

(c) Methoden: zie aanhangsel A.2 van het richtsnoer EN 50 126-2 {Ref. 9};

(d) Vereiste deelnemers:

(1) manager veiligheidszorg van de initiatiefnemer (spoorwegonderneming);
(1) manager veiligheidszorg van de treinfabrikant;

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

(2) met het treinontwerp belaste instantie van de initiatiefnemer;
(3) met het ontwerp belaste instantie van de treinfabrikant;
(4) met het treinonderhoud belaste personeel van de initiatiefnemer (hangt deels af van geanalyseerde I/O);
(5) treinbestuurders (hangt deels af van geanalyseerde I/O);

(e) Output:

(1) in onderlinge overeenstemming opgesteld gevareninventarisatierapport;
(2) veiligheidsmaatregelen voor de gevareninventaris met een duidelijke verantwoordelijkheidsomschrijving.

C.4. Voorbeelden van methoden ter bepaling van algemeen aanvaardbare risico's

C.4.1. Inleiding

C.4.1.1. Algemeen aanvaardbare risico's worden in de CSM-verordening omschreven als risico's die *"dat het risico dermate klein is dat extra veiligheidsmaatregelen niet redelijkerwijs kunnen worden verantwoord (om het risico verder te verminderen)"*. Worden bepaalde gevaren in de gevareninventarisatie ingedeeld als verbonden aan algemeen aanvaardbare risico's, dan is het niet mogelijk deze gevaren verder te analyseren in het risicobeoordelingsproces. De bovengenoemde definitie van algemeen aanvaardbare risico's laat echter nog ruimte voor interpretatie. Daarom wordt in de verordening aangegeven dat de beslissing om gevaren onder de noemer algemeen aanvaardbare risico's te brengen aan deskundig oordeel wordt overgelaten.

C.4.1.2. Het is inderdaad moeilijk voor algemeen aanvaardbare risico's een algemeen geldend, explicieter criterium vast te leggen dat van toepassing is op alle mogelijke systeemniveaus waar zulke gevaren in kaart worden gebracht, en dat tevens de verschillende risicomijdende factoren verklaart die het overwicht kunnen hebben in bepaalde toepassingen. Belangrijk is dat het oordeel van deskundigen bevattelijk en traceerbaar is. Daarom zijn bepaalde aanwijzingen van nut om te bepalen wanneer sprake is van algemeen aanvaardbare risico's. Kwantitatieve, kwalitatieve of semikwalitatieve criteria bepalen welke risico's als algemeen aanvaardbaar worden aangemerkt. Hier volgen enkele voorbeelden om criteria af te leiden waarmee algemeen aanvaardbare risico's kwantitatief of semikwantitatief kunnen worden geëvalueerd.

C.4.1.3. Dit beginsel wordt geïllustreerd in de volgende voorbeelden die werden overgenomen uit: *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Afleiding van kwantitatief criterium

C.4.2.1. Algemeen aanvaardbare risico's zijn te omschrijven als risico's die kleiner zijn dan het aanvaardbare risico voor een bepaalde gevarenklasse. Het huidige risiconiveau voor spoorwegsystemen kan worden bepaald met gebruikmaking van statistische gegevens. Het berekende niveau kan vervolgens als aanvaardbaar worden aangemerkt. Het aanvaardbare risiconiveau per gevarencategorie wordt berekend door dit risiconiveau te delen door het aantal (N) gevaren (als willekeurig uitgangspunt mag worden aangenomen dat er ongeveer N = 100 hoofdcategorieën gevaren in het spoorwegsysteem bestaan). Vervolgens mag worden gesteld dat een gevaar met een risico dat twee orden van grootte kleiner is dan het aanvaardbare risiconiveau per gevaar (zijnde parameter x% onder [G1] in punt 2.2.3) als algemeen aanvaardbaar risico mag worden aangemerkt.

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

C.4.2.2. Er moet echter worden gewaarborgd dat de bijdrage van alle gevaren verbonden aan algemeen aanvaardbare risico's niet hoger ligt dan een bepaald pro rata (bijvoorbeeld y%) van het totale risico op systeemniveau. Zie punt 2.2.3 en de uitleg onder [G 2] in punt 2.2.3.

C.4.3. Evaluatie van algemeen aanvaardbare risico's

C.4.3.1. De grenswaarden voor algemeen aanvaardbare risico's zoals die in de bovenstaande voorbeelden werden afgeleid, kunnen worden gebruikt om kwalitatieve hulpmiddelen te kalibreren, zoals een risicomatrix, een risicografiek of numerieke risicoprioritering. Deze hulpmiddelen helpen de deskundige beslissen of het risico als algemeen aanvaardbaar moet worden aangemerkt. Daarbij is het van belang op te merken dat, ook al werden kwantitatieve waarden als criteria voor algemeen aanvaardbare risico's vastgelegd, dit niet inhoudt dat een nauwkeurige risicoschatting of -analyse moet worden uitgevoerd om te oordelen over de algemene aanvaardbaarheid van het risico. Deze ruwe schatting wordt in de gevareninventarisatiefase gemaakt op basis van het oordeel van de deskundige.

C.4.3.2. Er moet tevens worden gewaarborgd dat de bijdrage van alle gevaren verbonden aan algemeen aanvaardbare risico's niet hoger ligt dan een bepaald pro rata (bijvoorbeeld y%) van het totale risico op systeemniveau. zie punt 2.2.3 en de uitleg onder [G 2] in punt 2.2.3.

C.5. Voorbeeld van risicobeoordeling voor een belangrijke wijziging van organisatorische aard

C.5.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.5.2. Dit voorbeeld betreft een wijziging van organisatorische aard. Deze wijziging werd door de betrokken initiatiefnemer als belangrijk aangemerkt. De wijziging werd geëvalueerd volgens een op risicobeoordeling gebaseerde benadering.

C.5.3. Een bijkantoor van de infrastructuurbeheerder, dat tot het ogenblik van de wijziging bepaalde onderhoudswerkzaamheden uitvoerde (uitgezonderd seingevings- en telematicasystemen), moest in concurrentie worden gebracht met andere ondernemingen die op hetzelfde gebied actief waren. Direct gevolg daarvan was de behoefte aan personeelsinkrimping en herverdeling van taken in het gedetacheerde bijkantoor van de infrastructuurbeheerder dat aan de mededinging deelnam.

C.5.4. Aandachtspunten voor de betrokken infrastructuurbeheerder:

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

(a) het personeel van de infrastructuurbeheerder dat door de wijziging werd beïnvloed, stond in voor spoedeisende onderhouds- en reparatiewerkzaamheden als gevolg van plotselinge storingen in de infrastructuur. Het personeel voerde ook plan- of projectmatige onderhoudswerkzaamheden uit, zoals aanbrengen en reinigen van ballast, beheersen van de vegetatie;
(b) deze taken waren van cruciaal belang voor een veilige en stipte verkeersregeling. Bijgevolg moesten deze taken worden geanalyseerd met als doel de juiste maatregelen in kaart te brengen om te vermijden dat de toestand verslechtert doordat talloze veiligheidsverantwoordelijken de organisatie van de infrastructuurbeheerder gingen verlaten.
(c) de veiligheid en stiptheid van de treinenloop moest op hetzelfde niveau worden gehandhaafd tijdens en na de organisatorische wijziging.

C.5.5. Vergeleken met het CSM-proces werden de volgende stappen ondernomen (zie ook Figuur 1):

(a) systeembeschrijving [punt 2.1.2]:

(1) beschrijving van de taken die worden uitgevoerd door de bestaande organisatie (dat wil zeggen de organisatie van de infrastructuurbeheerder vóór de wijziging);
(2) beschrijving van de geplande organisatorische wijzigingen bij de infrastructuurbeheerder.
(3) van de interfaces tussen het "te detacheren bijkantoor" en andere branchegenoten of de fysieke omgeving kon slechts een summiere beschrijving worden gegeven. De grenzen konden niet voor honderd procent worden afgebakend;

(b) gevareninventarisatie [punt 2.2]:

(1) brainstorming door een deskundigengroep met als doel:

(i) alle gevaren in kaart te brengen die relevante gevolgen hebben voor het risico dat door de geplande organisatorische wijziging wordt teweeggebracht;
(ii) mogelijke maatregelen in kaart te brengen om het risico te beheersen;

(2) gevareninventarisatie:

(i) naargelang van de ernst van het verbonden risico: hoog, middelhoog, laag risico;
(ii) naargelang van de gevolgen van de wijziging: verhoogd, ongewijzigd, verminderd risico;

(c) gebruik van een referentiesysteem [punt 2.4]:

Het veiligheidsniveau van het systeem vóór de wijziging werd als aanvaardbaar aangemerkt. Het werd bijgevolg gebruikt als "referentiesysteem" om de risicoaanvaardingscriteria voor de organisatorische wijziging af te leiden;

(d) expliciete risicoschatting en -evaluatie [punt 2.5]:

Voor elk gevaar met een verhoogd risico als gevolg van de organisatorische wijziging werden risicobeperkende maatregelen in kaart gebracht. Het restrisico wordt vergeleken met de risicoaanvaardingscriteria van het referentiesysteem om na te gaan of aanvullende maatregelen nodig zijn;

(e) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

(1) de risicoanalyse en de gevareninventaris hebben aangetoond dat gevaren pas kunnen worden beheerst nadat ze werden getoetst en nadat is aangetoond dat de veiligheidsvereisten (dat wil zeggen de geselecteerde veiligheidsmaatregelen) ten uitvoer werden gelegd;
(2) de risicoanalyse en de gevareninventaris waren dynamische documenten. De effectiviteit van de ingevoerde maatregelen werd periodiek getoetst om na te gaan

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

of de randvoorwaarden waren veranderd en of de risicoanalyse en -beoordeling dienden te worden bijgewerkt;

(3) bleken de geïmplementeerde maatregelen ontoereikend, dan werden de gevareninventaris en de risicoanalyse en -beoordeling opnieuw bijgewerkt en getoetst;

(f) gevarenbeheer [punt 4.1]:

De in kaart gebrachte gevaren en veiligheidsmaatregelen werden geregistreerd en in een gevareninventaris bijgehouden. Uit dit voorbeeld werd onder meer geconcludeerd dat de risicoanalyse en de gevareninventaris voortdurend moesten worden bijgewerkt aangezien tijdens de organisatorische wijziging beslissingen en maatregelen werden genomen. Ook het interfacerisico, bijvoorbeeld wat betreft onder(aan)nemers, kwam aan bod in de risicoanalyse.

De structuur en velden voor de gevareninventaris zijn samen met een uittreksel uit bepaalde regels terug te vinden onder C.16.2. in aanhangsel C.

(g) onafhankelijke beoordeling [Artikel 6]:

Er werd een onafhankelijke beoordeling door een derde uitgevoerd teneinde:

(1) na te gaan of het risicobeheer en de risicobeoordeling naar behoren werden uitgevoerd;
(2) zeker te stellen dat de organisatorische wijziging geschikt is en het mogelijk maakt de veiligheid op hetzelfde niveau te handhaven als vóór de wijziging.

C.5.6. Uit dit voorbeeld blijkt dat de door de gemeenschappelijke veiligheidsmethode voorgeschreven beginselen overeenkomen met bestaande methoden in de spoorwegsector die reeds worden toegepast om de risico's van organisatorische wijzigingen te beoordelen. De risicobeoordeling in dit voorbeeld voldoet aan alle eisen in de CSM. Daarbij worden twee van de drie risicoaanvaardingsbeginselen gebruikt die toegestaan zijn volgens de geharmoniseerde benaderingswijze als bedoeld in de CSM:

(a) er wordt een "referentiesysteem" toegepast om te bepalen welke risicoaanvaardingscriteria nodig zijn om de organisatorische wijziging te toetsen op risicoaanvaardbaarheid;
(b) "expliciete risicoschatting en -evaluatie" met als doel:

(1) na te gaan in hoeverre de wijziging afwijkt van het referentiesysteem;
(2) risicobeperkende maatregelen in kaart te brengen gelet op het verhoogde risico dat de wijziging meebrengt;
(3) te evalueren of een aanvaardbaar risiconiveau wordt bereikt.

C.6. Voorbeeld van risicobeoordeling van een operationele wijziging – andere rijtijden

C.6.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

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

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.6.2. Dit voorbeeld betreft een operationele wijziging waarbij de spoorwegonderneming nieuwe rijwegen en mogelijk nieuwe arbeidstijden (inclusief roulering en ploegendiensten) aan de treinbestuurders wilde toekennen.

C.6.3. Vergeleken met het CSM-proces werden de volgende stappen ondernomen (zie ook Figuur 1):

(a) significantieniveau van de wijziging [Artikel 4]:

De spoorwegonderneming heeft een voorafgaande risicobeoordeling uitgevoerd waaruit bleek dat het ging om een belangrijke wijziging van operationele aard. Aangezien de treinbestuurders nieuwe rijwegen moesten volgen, mogelijk buiten hun gebruikelijke werktijden, bestond een niet te verwaarlozen kans op het voorbijrijden van een onveilig (gesloten of stoptonend) sein, het rijden met te hoge snelheid (snelheidsoverschrijding) of het negeren van tijdelijke snelheidsbeperkingen.

Werd deze voorafgaande risicobeoordeling vergeleken met de in artikel 4, lid 2, van de CSM-verordening genoemde criteria, dan kon de wijziging ook als belangrijk worden aangemerkt op basis van de volgende criteria:

(1) veiligheidsrelevantie: de wijziging houdt verband met de veiligheid aangezien het wijzigen van de werkwijze van de treinbestuurders rampzalige gevolgen kan hebben;
(2) storingsgevolg: de bovengenoemde bestuurdersfouten kunnen potentieel rampzalige gevolgen hebben;
(3) nieuwheidsfactor: de spoorwegonderneming zou mogelijk nieuwe werkmethoden voor de treinbestuurders kunnen invoeren;
(4) complexiteit van de wijziging: de rijtijden wijzigen kan complex zijn aangezien de bestaande arbeidsomstandigheden volledig opnieuw moeten worden beoordeeld en waar nodig aangepast;

(b) systeemomschrijving [punt 2.1.2]:

De systeemomschrijving behelsde aanvankelijk een beschrijving van:

(1) de bestaande arbeidsomstandigheden: arbeidstijden, ploegendiensten, enz.;
(2) arbeidstijdwijzigingen;
(3) interfacekwesties (bijvoorbeeld met de infrastructuurbeheerder);

Tijdens de verschillende iteraties werd de systeemomschrijving bijgewerkt met de veiligheidsvereisten resulterend uit het risicobeoordelingsproces. Bij dit iteratieve proces werd personeel op sleutelposities betrokken om de gevaren in kaart te brengen en de systeemomschrijving bij te werken.

(c) gevareninventarisatie [punt 2.2]:

De gevaren en mogelijke veiligheidsmaatregelen werden in kaart gebracht door een brainstorming van een deskundigengroep, inclusief vertegenwoordigers van treinbestuurders, wat betreft de nieuwe rijwegen en ploegendiensten. De taken van de treinbestuurders werden in het licht van de nieuwe omstandigheden besproken om te bepalen welke gevolgen die hadden voor de treinbestuurders en hun werkdruk, het geografische toepassingsgebied en de duur van het ploegenstelsel.

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

De spoorwegonderneming heeft ook werknemersorganisaties voor eventuele aanvullende informatie geraadpleegd en heeft nagegaan welke gevolgen een eventuele toename van overwerk als gevolg van langdurige trajecten op onbekende rijwegen zou kunnen hebben wat betreft vermoeidheids- en ziekterisico's.
Aan elk gevaar werd een ernstgraad toegekend, gemeten naar risico en gevolgen (hoog, middelhoog, laag). Het effect van de geplande wijziging werd daaraan getoetst om het (verhoogde, ongewijzigde, verminderde) risico te bepalen.

(d) gebruik van praktijkcodes [punt 2.3]:

Praktijkcodes inzake arbeidstijden en risico's van vermoeidheid werden gebruikt met als doel de bestaande arbeidsomstandigheden te onderzoeken en de nieuwe veiligheidsvereisten vast te leggen. Overeenkomstig de praktijkcodes werden de nodige bedrijfsvoorschriften uitgewerkt voor het nieuwe ploegenstelsel. Alle nodige partijen werden betrokken bij de herziene operationele procedures bij de beslissing om de wijziging door te voeren.

(e) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

De herziene operationele procedures werden ingevoerd in het veiligheidsbeheersysteem van de spoorwegonderneming. De procedures werden gecontroleerd en er werd een herzieningsproces opgezet om te waarborgen dat de in kaart gebrachte gevaren verder naar behoren worden beheerst tijdens de exploitatie van het spoorwegsysteem.

(f) gevarenbeheer [punt 4.1]:

In dat verband wordt naar het bovenstaande punt verwezen aangezien het gevarenbeheerproces wat betreft spoorwegondernemingen deel kan uitmaken van hun veiligheidsbeheersysteem voor risicoregistratie en -beheer. De in kaart gebrachte gevaren werden samen met de veiligheidsvereisten (dat wil zeggen onder verwijzing naar de herziene operationele procedures) in een gevareninventaris geregistreerd ter beheersing van het daarmee samenhangende risico.
De herziene procedures werden gecontroleerd en waar nodig aangepast om te waarborgen dat de in kaart gebrachte gevaren verder naar behoren worden beheerst tijdens de exploitatie van het spoorwegsysteem.

(g) onafhankelijke beoordeling [Artikel 6]:

Het risicobeoordelings- en risicobeheerproces werd beoordeeld door een vakkundig persoon bij de spoorwegonderneming die niet eerder bij het beoordelingsproces betrokken was. Deze persoon heeft het proces beoordeeld alsmede de resultaten, dat wil zeggen de in kaart gebrachte veiligheidsvereisten.

De spoorwegonderneming heeft het onafhankelijke beoordelingsrapport van de vakkundige persoon gebruikt ter verantwoording van haar beslissing om het nieuwe systeem te operationaliseren.

C.6.4. Uit dit voorbeeld blijkt dat de beginselen en processen die de spoorwegonderneming toepast, overeenstemmen met de gemeenschappelijke veiligheidsmethode. Het risicobeheer- en risicobeoordelingsproces voldoet aan alle in de CSM voorgeschreven eisen.

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

C.7. Voorbeeld van risicobeoordeling van een belangrijke wijziging van technische aard (besturing en seingeving)

C.7.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

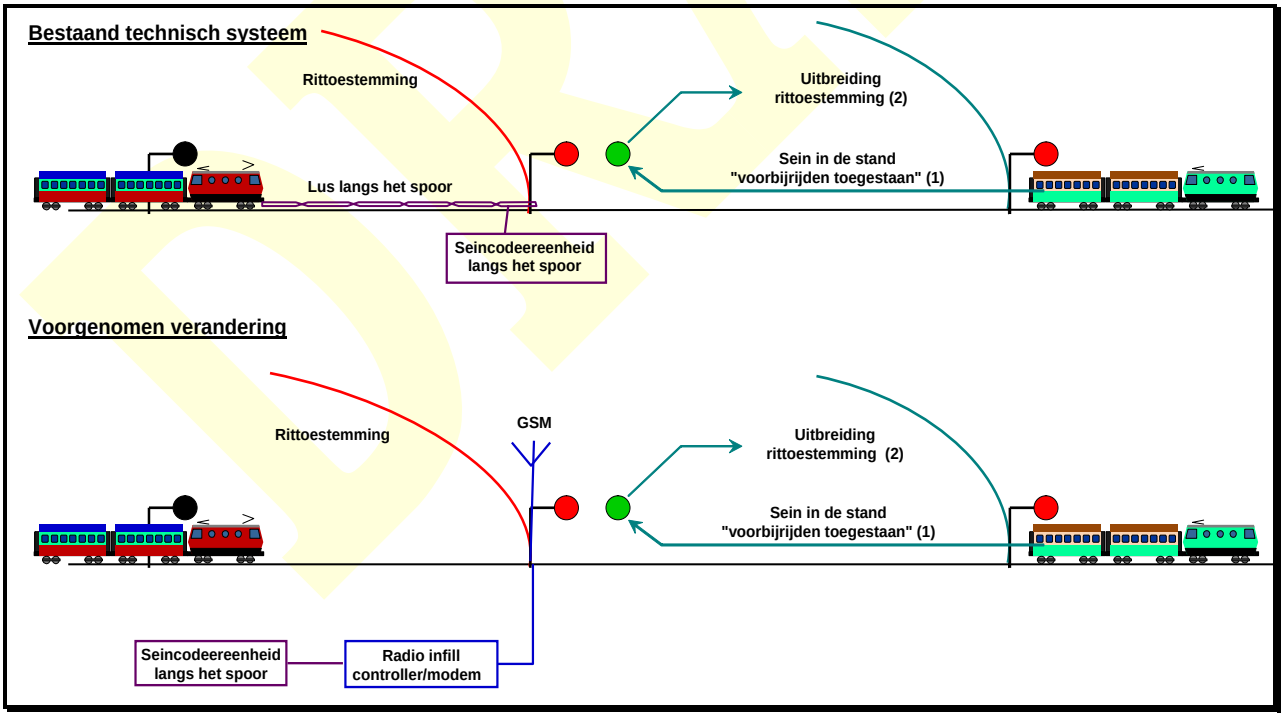
(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.7.2. Dit voorbeeld betreft een technische wijziging van het besturings- en seingevingssysteem. Deze wijziging werd door de betrokken fabrikant als belangrijk aangemerkt. De wijziging werd geëvalueerd volgens een op risicobeoordeling gebaseerde benadering.

C.7.3. Beschrijving van de wijziging: de wijziging bestaat erin een lus langs het spoor vóór een sein te vervangen door een subsysteem "Radio infill + GSM" (zie Figuur 16).

C.7.4. Aandachtspunt: het veiligheidsniveau van het systeem handhaven na de wijziging.



Figuur 16: Vervanging van lus langs het spoor door een subsysteem "Radio infill".

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

C.7.5. Vergeleken met het CSM-proces worden de volgende stappen ondernomen (zie ook Figuur 1):

(a) beoordeling van de mate van belangrijkheid van de wijziging [Artikel 4]

De in artikel 4, lid 2, genoemde criteria worden toegepast om de mate van belangrijkheid van een wijziging te beoordelen. In het bijzonder de complexiteit en de nieuwheidsfactor werden als criteria gehanteerd om te bepalen of het om een belangrijke wijziging gaat.

(b) systeembeschrijving [punt 2.1.2]:

(1) beschrijving van het bestaande systeem: lus langs het spoor en de bijbehorende functies in het besturings- en seingevingssysteem;
(2) beschrijving van de door de initiatiefnemer en fabrikant geplande wijziging;
(3) beschrijving van de functionele en fysieke interfaces van de lus met de rest van het systeem;

In het bestaande systeem heeft de “lus+seincodeereenheid” als functie het sein bij het naderen van een trein in de stand “voorbijrijden toegestaan” te brengen wanneer het baanvak achter het sein (dat wil zeggen vóór de naderende trein) niet langer bezet is ("spoor vrij"): zie Figuur 16.

(c) gevareninventarisatie [punt 2.2]:

Het iteratieve risicobeoordelingsproces en de gevareninventarisatie (zie punt 2.1.1) worden toegepast op basis van een brainstorming door een deskundigengroep met als doel:

(1) de gevaren in kaart te brengen die een relevante invloed hebben op het risico dat door de voorgenomen wijziging wordt teweeggebracht;
(2) mogelijke maatregelen in kaart te brengen om het risico te beheersen;

Aangezien de lus en dus ook het subsysteem “Radio infill” het sein in de stand "voorbijrijden toegestaan" brengt, bestaat het risico dat een onveilige rittoestemming aan de naderende trein wordt gegeven aangezien het baanvak vóór het sein nog bezet is door de voorliggende trein. Dat risico moet tot een aanvaardbaar niveau worden teruggebracht.

(d) gebruik van een referentiesysteem [punt 2.4]:

Het veiligheidsniveau van het systeem vóór de wijziging (lus) wordt als aanvaardbaar aangemerkt. Dit geldt dus als “referentiesysteem” om de veiligheidsvereisten af te leiden voor het subsysteem “Radio infill”.

(e) expliciete risicoinschatting en -evaluatie [punt 2.5]:

(1) de verschillen tussen de subsystemen "Lus" en "Radio infill+GSM" worden geanalyseerd door een expliciete risicoschatting en -evaluatie. De volgende nieuwe gevaren worden in kaart gebracht voor het subsysteem "Radio infill + GSM":

(i) doorgifte van onveilige informatie in de airgap door hackers aangezien "Radio infill+GSM" een open transmissiesubsysteem is;
(ii) vertraagde doorgifte of transmissie van gememoriseerde datapakketten in de airgap;

(2) expliciete risico-inschatting en gebruik van RAC-TS voor het gedeelte "Radio infill controller";

(f) gebruik van praktijkcodes [punt 2.3]:

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

(1) de norm EN 50159-2 (*"Spoorwegtoepassingen: Deel 2: Veiligheidsvereisten voor communicatie in open transmissiesystemen"*) bepaalt de veiligheidsvereisten om nieuwe gevaren tot een aanvaardbaar niveau terug te brengen, bijvoorbeeld:

(i) gegevensversleuteling en -beveiliging;
(ii) controleren van de volgorde van berichten en digitale tijdstempel;

(2) gebruik bijvoorbeeld van de norm EN 50 128 voor de softwareontwikkeling van de Radio infill controller;

(g) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

(1) vervolgcontrole van de tenuitvoerlegging van veiligheidsvereisten in het ontwikkelingsproces van het subsysteem "Radio infill + GSM";
(2) controle of het systeem, zoals dit is ontworpen en geïnstalleerd, voldoet aan de veiligheidsvereisten;

(h) gevarenbeheer [punt 4.1]:

De in kaart gebrachte gevaren, de veiligheidsmaatregelen en resulterende veiligheidsvereisten zoals die werden bepaald bij de risicobeoordeling en de toepassing van de drie risicoaanvaardingsbeginselen worden geregistreerd en bijgehouden in een gevareninventaris.

(i) onafhankelijke beoordeling [Artikel 6]:

Er wordt ook een onafhankelijke beoordeling door een derde uitgevoerd teneinde:

(1) na te gaan of het risicobeheer en de risicobeoordeling naar behoren werden uitgevoerd;
(2) zeker te stellen dat de technische wijziging geschikt is en het mogelijk maakt de veiligheid op hetzelfde niveau te handhaven als vóór de wijziging.

C.7.6. Uit dit voorbeeld blijkt dat de drie risicoaanvaardingsbeginselen die door de gemeenschappelijke veiligheidsmethode worden opgelegd elkaar elkaar aanvullen bij het vastleggen van de veiligheidsvereisten voor het beoordeelde systeem. De risicobeoordeling in dit voorbeeld beantwoordt aan alle CSM-eisen die in Figuur 1 worden samengevat, inclusief het beheer van de gevareninventaris en de onafhankelijke veiligheidsbeoordeling door een derde.

C.8. Voorbeeld van het Zweedse richtsnoer BVH 585.30 voor de risicobeoordeling van spoorwegtunnels

C.8.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke

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

belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.8.2. Dit voorbeeld beoogt het CSM-proces te vergelijken met het richtsnoer BVH 585.30 dat door de Zweedse infrastructuurbeheerder Banverket wordt gebruikt voor het ontwerp van, en de controle of een toereikend veiligheidsniveau wordt bereikt in de planning en bouw van nieuwe spoorwegtunnels. De raakpunten en verschillen met de CSM worden hierna opgesomd. De gedetailleerde eisen inzake risicobeoordeling zijn terug te vinden in het richtsnoer BVH 585.30.

C.8.3. Vergeleken met het CSM-proces in Figuur 1:

(a) vertoont het richtsnoer BVH 585.30 de volgende raakpunten:

(1) systeembeschrijving [punt 2.1.2]:

In het richtsnoer vraagt een gedetailleerde systeembeschrijving met:

(i) een beschrijving van de tunnel;
(ii) een beschrijving van het spoor;
(iii) een typebeschrijving van het rollend materieel (inclusief treinpersoneel);
(iv) een beschrijving van het verkeer en de geplande exploitatie;
(v) een beschrijving van de externe bijstand (inclusief reddings- en hulpverleningsdiensten);

(2) gevareninventarisatie [punt 2.2]:

In het richtsnoer wordt niet uitdrukkelijk een gevareninventarisatie gevraagd. Het richtsnoer vraagt een risico-inventarisatie en een "ongevallenlijst" met de types in kaart gebrachte mogelijke ongevallen die een aanzienlijke invloed hebben op het risiconiveau van de tunnel en die in de aansluitende beoordeling aan bod moeten komen. Voorbeelden van ongevallen:

(i) "ontsporing van een passagierstrein";
(ii) "ontsporing van een goederentrein";
(iii) "ongeval met gevaarlijke goederen";
(iv) "brand in het voertuig";
(v) "botsing tussen passagierstrein en licht/zwaar voorwerp";
(vi) enzovoort.

(3) er wordt niets gezegd over de toepassing van praktijkcodes of soortgelijke referentiesystemen. Aangenomen wordt dat in elk geval een risicoanalyse moet worden uitgevoerd;

(4) expliciete risicoschatting en -evaluatie [punt 2.5]:

(i) doorgaans wordt in het richtsnoer aanbevolen voor elk ongevalstype een volledige gebeurtenissenboom uit te werken op basis van een kwantitatieve risicoanalyse. De risicoanalyse heeft echter ten doel het algemene veiligheidsniveau van de tunnel te analyseren, en niet zozeer de individuele veiligheid op meer gedetailleerde niveaus. Daarom worden de gevolgen van alle scenario's samen in beschouwing genomen om het totale risiconiveau voor de tunnel te bepalen;
(ii) de aanvaardbaarheid van dit totale risiconiveau voor de tunnel moet worden vergeleken met het volgende expliciete kwantitatieve risicoaanvaardingscriterium. *"het spoorwegverkeer per kilometer in tunnels moet even veilig zijn als het spoorwegverkeer per kilometer op sporen in de openlucht, met uitzondering van overwegen"*. Dit criterium wordt omgezet in een FN-curve op basis van gegevens uit het verleden over

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

spoorwegongevallen in Zweden, en wordt geëxtrapoleerd om ook gevolgen te behandelen die niet in de statistieken zijn opgenomen;

(iii) naast dit criterium wat betreft het totale risiconiveau van de tunnel, moet ook aan extra eisen worden voldaan, meer in het bijzonder voor de evacuatie in tunnels en inzetmogelijkheden van de reddings- en hulpverleningsdiensten:

- controleren of zelfredding mogelijk is bij brand in een trein voor een aannemelijk worstcasescenario (er worden ook criteria voor deze beoordeling opgegeven);
- de tunnel moet zodanig worden gepland dat reddingswerkzaamheden en noodhulpverlening mogelijk zijn voor bepaalde scenario's;

(5) output van de risicobeoordeling [punt 2.1.6]:

Hier volgt de output van de risicobeoordeling:

(i) een lijst van veiligheidsmaatregelen resulterend uit de minimumnorm die berust op technische specificatie voor interoperabiliteit en de veiligheid in spoorwegtunnels alsmede nationale voorschriften die voor het ontwerp van de tunnel moeten worden gebruikt, en

(ii) alle aanvullende veiligheidsmaatregelen die noodzakelijk worden geacht op grond van de risicoanalyse, met vermelding van het doel daarvan. Er moet over de maatregelen worden beslist met inachtneming van de onderstaande prioriteitsvolgorde:

- ongevallen voorkomen;
- gevolgen van ongevallen verminderen;
- evacuatie vergemakkelijken;
- reddingswerkzaamheden en noodhulpverlening vergemakkelijken;

(6) gevarenbeheer [punt 4.1]:

In het richtsnoer wordt niet uitdrukkelijk gevraagd een gevareninventaris bij te houden. Reden hiervoor is dat het gaat om een algemene beoordeling waarbij de gevaren niet afzonderlijk worden geëvalueerd en beheerst. De aanvaardbaarheid van het totale risico van de tunnel wordt geëvalueerd, zonder het totale risicoaanvaardingscriterium te verdelen tot op het niveau van de verschillende ongevalstypen of onderliggende gevaren.

Wel is er een lijst van alle veiligheidsmaatregelen, zowel de maatregelen die voortvloeien uit de "minimumnorm" als die welke noodzakelijk worden geacht op grond van de risicoanalyse: zie onder (a)(5)(ii) hierboven. In de lijst van veiligheidsmaatregelen moet worden aangegeven of die verband houden met de tunnelinfrastructuur, het spoor, de exploitatie of het rollend materieel. Verder moet het beoogde effect worden toegelicht volgens de nummerlijst onder (a)(5)(ii). In het richtsnoer wordt echter niet gevraagd expliciet aan te geven welke gevaren door de veiligheidsmaatregelen worden beheerst en wie verantwoordelijk is voor welke maatregelen.

(7) onafhankelijke beoordeling [Artikel 6]:

Een onafhankelijke beoordeling door een derde is verplicht teneinde:

(i) na te gaan of het in het richtsnoer BVH 585.30 aanbevolen risicobeoordelingsproces naar behoren wordt uitgevoerd;

(ii) te bepalen of de risicoanalyse aanvaardbaar is;

(iii) te controleren of duidelijk is aangegeven hoe het veiligheidsbeheer in de toekomst moet worden uitgevoerd voor het project;

Het einddocument van de risicoanalyse wordt ondertekend door de onafhankelijke veiligheidsbeoordelaar alsook door de veiligheidscoördinator van het project.

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

(b) het richtsnoer BVH 585.30 verschilt in de volgende opzichten:

(1) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

In het richtsnoer BVH 585.30 wordt niet gevraagd de tenuitvoerlegging van de in kaart gebrachte veiligheidsvereisten traceerbaar te maken, noch te controleren of het eindontwerp van de tunnel voldoet aan de opgegeven veiligheidsvereisten. Het richtsnoer beschrijft alleen hoe deze eisen moeten worden overgedragen om zeker te stellen dat ze in de bouwfase ten uitvoer worden gelegd.

Het richtsnoer geeft aan welke veiligheidsvereisten moeten worden gebruikt om zeker te stellen dat de risicoanalyse naar behoren en op transparante wijze wordt uitgevoerd, en als aanvaardbaar kan worden aangemerkt voor het project.

C.8.4. Concluderend valt uit de vergelijking met de CSM op te maken dat:

(a) het richtsnoer BVH 585.30 voldoet aan de desbetreffende delen van de CSM, ook al zijn toepassingsgebied en doel niet geheel identiek;
(b) het richtsnoer BVH 585.30 het totale risiconiveau van de spoorwegtunnel beoordeelt;
(c) de gevaren niet afzonderlijk worden beheerst, wat betekent dat minder nadruk op gevarenbeheer wordt gelegd;
(d) er geen uitdrukkelijke bepalingen bestaan inzake het aantonen van de conformiteit en het controleren of alle veiligheidsmaatregelen naar behoren ten uitvoer worden gelegd. Wel bepaalt het richtsnoer dat de veiligheidscoördinator in projectverband als functie heeft (welke functie en vakkundigheid worden voorgeschreven in het richtsnoer BVH 585.30) na te gaan of de conclusies van de risicoanalyse ten uitvoer worden gelegd in de ontwerpdocumenten en -tekeningen, alsmede erop toe te zien dat die naar behoren in de bouwfase ten uitvoer worden gelegd;

C.8.5. De CSM is algemener van opzet dan het richtsnoer BVH 585.30 in die zin dat die ruimte biedt voor de toepassing van drie verschillende risicoaanvaardingsbeginselen. De toepassing van het richtsnoer BVH 585.30 in het kader van de CSM vormt echter geen enkel probleem vermits dit verenigbaar is met het derde beginsel van de expliciete risico-inschatting.

C.9. Voorbeeld van risicobeoordeling op systeemniveau voor de metro van Kopenhagen

C.9.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.9.2. Dit voorbeeld betreft een compleet en complex bestuurderloos metrosysteem, inclusief onderliggende technische subsystemen (bijvoorbeeld automatische treinbeveiliging en

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

rollend materieel), exploitatie en onderhoud van het systeem. Een op risicobeoordeling gebaseerde benadering werd toegepast om het systeem en de onderliggende subsystemen te beoordelen. Het project behelsde tevens de certificering van het veiligheidsbeheersysteem van de exploitant. Dit heeft te maken met het vermogen van de spoorwegonderneming en infrastructuurbeheerder om het gehele systeem veilig te exploiteren en te onderhouden tijdens de volledige systeemlevenscyclus.

C.9.3. Vergeleken met het CSM-proces werden de volgende stappen ondernomen (zie ook Figuur 1):

(a) systeembeschrijving [punt 2.1.2]:

(1) beschrijving van de systeemspecifieke prestatie-eisen;
(2) beschrijving van de bedrijfsvoorschriften;
(3) duidelijke beschrijving van de interfaces en de verantwoordelijkheden van de verschillende actoren, meer in het bijzonder tussen de technische subsystemen;
(4) definitie van systeemeisen op hoog niveau (wat betreft aanvaardbare ongevallenfrequentie en definitie van een ALARP-zone (As Low As Reasonably Practicable) waar het veiligheidsrisico zo laag moet zijn als redelijkerwijs praktisch haalbaar is);

(b) gevareninventarisatie [punt 2.2]:

(1) voorafgaande gevarenanalyse op systeemniveau;
(2) functionele analyse op systeemniveau met de nadruk op alle subsystemen, niet alleen die welke klaarblijkelijk cruciaal voor de veiligheid zijn (bijvoorbeeld automatische treinbeveiliging en rollend materieel), die van belang zijn voor veiligheidsfuncties en een actieve rol spelen om de veiligheid van passagiers en personeel te waarborgen;
(3) intensieve coördinatie tussen de actoren (aannemers, leveranciers van technische subsystemen en civieltechnische werken) met als doel:

(i) alle redelijkerwijs voorzienbare gevaren stelselmatig in kaart te brengen;
(ii) mogelijke acties in kaart te brengen om alle risico's verbonden aan de onderkende gevaren tot een aanvaardbaar niveau terug te brengen;

(c) gebruik van praktijkcodes [punt 2.3]:

Verschillende praktijkcodes, normen en voorschriften werden gebruikt, bijvoorbeeld:

(1) BOStrab-regelgeving inzake de bouw en exploitatie van trams (Duitse voorschriften die van toepassing zijn op stedelijke railvervoerssystemen) en de bestuurderloze exploitatie;
(2) VDV-beleidsdocumenten (Duitse praktijkcodes) met eisen voor uitrusting ter waarborging van de veiligheid van passagiers in stations voor bestuurderloze exploitatie;
(3) CENELEC-normen voor spoorwegsystemen (EN 50 126, 50 128 en 50 129). Deze normen behandelen technische spoorwegsystemen in het bijzonder. Aangezien in deze normen ook een algemeen geldende methodologische benaderingswijze is vastgelegd, werden die veelvuldig toegepast voor de metro van Kopenhagen:

(i) EN 50 126 werd toegepast voor alles wat te maken heeft met veiligheidsbeheer en risicobeoordeling van het volledige spoorwegsysteem;
(ii) EN 50 129 werd toegepast voor het volledige seinstelsel;
(iii) EN 50 128 werd toegepast voor softwareontwikkeling (inclusief keuring en validering) wat betreft technische subsystemen;

(4) brandveiligheidsnormen voor tunnels (NEPA 130);
(5) normen voor civiele techniek en civieltechnische werken (Eurocodes);

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

(d) gebruik van een referentiesysteem [punt 2.4]:

De metro moest het veiligheidsniveau bereiken van corresponderende moderne installaties in Duitsland, Frankrijk of Groot-Brittannië. Deze bestaande systemen werden als soortgelijke referentiesystemen gebruikt om de risicoaanvaardingscriteria af te leiden qua ongevallenfrequentie in de metro van Kopenhagen;

(e) expliciete risicoschatting en -evaluatie [punt 2.5] met als doel:

(1) aan specifieke gevaren verbonden risico's in te schatten;
(2) de tunnelventilatie in noodgevallen te controleren (inclusief menselijke factoren bij het optreden van de brandweer);
(3) risicobeperkende maatregelen in kaart te brengen;
(4) na te gaan of een aanvaardbaar risiconiveau wordt bereikt voor het volledige systeem;

(f) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

(1) beheersmatige en technische inspanningen die verenigbaar zijn met de complexiteit van het systeem om aan te tonen dat het systeem veilig is;
(2) verdeling van systeemspecifieke veiligheidsvereisten tot op het niveau van technische subsystemen en civieltechnische werken, alsook van alle veiligheidsgerelateerde metrofuncties;
(3) aantonen dat elk subsysteem, zoals dit is gebouwd, voldoet aan de desbetreffende veiligheidsvereisten;
(4) wat betreft veiligheidsfuncties die door meerdere subsystemen worden vervuld, kon de conformiteit met de veiligheidsvereisten niet op subsysteemniveau worden aangetoond. Dit werd op systeemniveau aangetoond door de verschillende subsystemen, hulpmiddelen en procedures te integreren;
(5) aantonen dat het volledige systeem voldoet aan de veiligheidsvereisten op hoog niveau;

(g) gevarenbeheer [punt 4.1]:

De in kaart gebrachte gevaren, de daarmee samenhangende veiligheidsmaatregelen en de resulterende veiligheidsvereisten werden geregistreerd en bijgehouden in een centraal gevareninventaris. De projectoverkoepelende veiligheidsmanager droeg de verantwoordelijkheid voor deze gevareninventaris. In de gevareninventaris werd melding gemaakt van de operationele gevaren die bij ontwerp en installatie in kaart werden gebracht, alsmede van gevaren verbonden aan exploitatie en onderhoud;

(h) bewijsmateriaal resulterend uit risicobeheer en risicobeoordeling [punt 5]:

De resultaten van de risicobeoordeling werden formeel gedocumenteerd en onderbouwd door een veiligheidsbewijs overeenkomstig de eisen in de CENELEC-normen:

(1) veiligheidsbewijs voor het volledige systeem;
(2) veiligheidsbewijs voor elk technisch subsysteem (inclusief seingevingssubsystemen en civieltechnische werken);
(3) veiligheidsbewijs voor civieltechnische werken (stations, tunnels, viaducten, spoorbermen);
(4) veiligheidsbewijs voor installatie;
(5) veiligheidsbewijs voor voertuigen;
(6) veiligheidsbewijs voor de operator (ter staving van de certificering van het veiligheidsbeheersysteem van de spoorwegonderneming en infrastructuurbeheerder, dat wil zeggen het bewijs dat de initiatiefnemer in staat is het systeem veilig te exploiteren en te onderhouden);

(i) onafhankelijke beoordeling [Artikel 6]:

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

Het totale proces werd opgevolgd en beoordeeld door een onafhankelijke veiligheidsbeoordelaar in opdracht van de technisch bevoegde instantie (dat wil zeggen het Deense ministerie van vervoer). De functies van deze onafhankelijke veiligheidsbeoordelaar zijn vastgelegd in een relevante praktijkcode en omvatten onder meer het volgende:

(1) controleren of risicobeheer en risicobeoordeling naar behoren worden uitgevoerd;
(2) controleren of het systeem geschikt is voor het beoogde doel, en tijdens de volledige levenscyclus veilig zal worden geëxploiteerd en onderhouden;
(3) aanbevelen van goedkeuring aan de technisch bevoegde instantie.

C.9.4. Het volledige project werd ondersteund door een passend kwaliteitsborgingsproces.

C.9.5. In het project werd het bewijsmateriaal van de leveranciers (dat wil zeggen veiligheidsbewijzen en uitvoerige documenten ter staving voor de technische subsystemen en civieltechnische werken) overgelegd aan de veiligheidsbeheerder van de initiatiefnemer. Vervolgens werd dit bewijsmateriaal nagezien door de veiligheidsbeheerorganisatie alsook door de onafhankelijke veiligheidsbeoordelaar wiens conclusies in het beoordelingsrapport werden opgetekend.
Het onafhankelijke veiligheidsbeoordelingsrapport werd nagezien door de veiligheidsbeheerder van de initiatiefnemer. Daarna werd het overgelegd aan de initiatiefnemer die alle dossiers ter definitieve goedkeuring doorstuurde naar de technisch bevoegde instantie (dat wil zeggen het Deense ministerie van vervoer).

C.9.6. Uit dit voorbeeld blijkt dat de beginselen die in de gemeenschappelijke veiligheidsmethode worden voorgeschreven, overeenkomen met bestaande methoden in de spoorwegsector. De risicobeoordeling in dit voorbeeld voldoet aan alle eisen in de CSM. Daarbij worden meer in het bijzonder alle drie de risicoaanvaardingsbeginselen gebruikt die zijn toegestaan volgens de geharmoniseerde benaderingswijze, als bedoeld in de CSM.

C.10. Voorbeeld van het OTIF-richtsnoer ter berekening van het risico verbonden aan het spoorwegvervoer van gevaarlijke goederen

C.10.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.10.2. De kerngedachte van het OTIF-richtsnoer beantwoordt aan het door de CSM beoogde doel, zij het dan dat dit richtsnoer een beperkt toepassingsgebied heeft. Het OTIF-*"richtsnoer beoogt meer uniformiteit in de benadering te brengen wat betreft de risicobeoordeling voor het vervoer van gevaarlijke goederen in de lidstaten die zijn toegetreden tot het verdrag*

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

betreffende het internationale spoorwegvervoer (COTIF), en zodoende de afzonderlijke risicobeoordelingen beter vergelijkbaar te maken". Het richtsnoer onderbouwt derhalve de wederzijdse erkenning tussen de COTIF-lidstaten van risicobeoordelingen betreffende het spoorwegvervoer van gevaarlijke goederen.

C.10.3. Vergeleken met de CSM en het stroomschema in Figuur 1:

(a) vertoont het OTIF-richtsnoer de volgende raakpunten:

(1) het is een gemeenschappelijke benaderingswijze voor risicobeoordeling, maar berust desalniettemin uitsluitend op een expliciete risico-inschatting (dat wil zeggen het derde risicoaanvaardingsbeginsel in de CSM);
(2) de OTIF-risicobeoordeling bestaat uit:

(i) een risicoanalysefase die uit de volgende fasen is samengesteld:

- gevareninventarisatie;
- risico-inschatting;

(ii) risico-evaluatie op basis van nog niet geharmoniseerde risico(acceptatie)criteria. Deze criteria kunnen inderdaad worden beïnvloed door tal van nationale bijzonderheden;

(b) het OTIF-richtsnoer verschilt in de volgende opzichten:

(1) het heeft een ander toepassingsgebied. Terwijl de CSM-verordening uitsluitend mag worden toegepast voor belangrijke wijzigingen van het spoorwegsysteem, moet het OTIF-richtsnoer worden toegepast ter beoordeling van de risico's verbonden aan het spoorwegvervoer van gevaarlijke goederen, ongeacht of het daarbij gaat om een al dan niet belangrijke wijziging van het spoorwegsysteem;
(2) het is niet mogelijk een keuze te maken uit drie risicoaanvaardingsbeginselen ter beheersing van risico's. Alleen het derde beginsel, dat wil zeggen de expliciete risico-inschatting, is toegestaan. Bovendien moet die niet zozeer op een kwalitatieve als wel uitsluitend op een kwantitatieve schatting berusten. De kwalitatieve risicoanalyse is alleen aangewezen om keuzemogelijkheden qua risicobeperkende (veiligheids)maatregelen met elkaar te vergelijken;
(3) het ALARP-beginsel (As Low As Reasonably Practicable) moet worden toegepast om te bepalen of extra veiligheidsmaatregelen het beoordeelde risico verder kunnen verminderen tegen een redelijke prijs;
(4) er bestaat geen concept "gevaren verbonden aan algemeen aanvaardbare risico's" dat het mogelijk maakt de risicobeoordeling te richten op de gevaren die de grootste risicobijdrage leveren. Desalniettemin wordt aanbevolen het aantal mogelijke ongevalsscenario's terug te brengen tot een redelijk aantal basisscenario's (zie punt 3.2 in {Ref. 10});
(5) risicobeoordeling staat centraal in het proces; de volgende processen blijven dus achterwege:

(i) selectie en tenuitvoerlegging van (veiligheids)maatregelen om het risico te wijzigen;
(ii) risicoaanvaardings;
(iii) aantonen dat het systeem voldoet aan de veiligheidsvereisten;
(iv) kennisgeving van het risico aan de andere betrokken actoren (zie het onderstaande punt);

(6) er is niets bepaald over het bewijsmateriaal dat het risicobeoordelingsproces moet opleveren;
(7) er wordt geen gevarenbeheer gevraagd;

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

(8) er wordt niet gevraagd de juiste toepassing van de gemeenschappelijke benaderingswijze te onderwerpen aan een onafhankelijke beoordeling door een derde.

C.10.4. Uit de vergelijking van het OTIF-richtsnoer en de CSM blijkt dat beide verenigbaar met elkaar zijn, ook al zijn toepassingsgebied en doel niet geheel identiek. De CSM is algemener in opzet dan het OTIF-richtsnoer en biedt dan ook meer ruimte voor flexibiliteit. Daartegenover staat dat in de CSM ook meer risicobeheeractiviteiten aan bod komen:

(a) er mogen drie risicoaanvaardingsbeginselen worden toegepast die berusten op bestaande handelwijzen in de spoorwegsector: zie punt 2.1.4;
(b) er wordt alleen gevraagd de CSM toe te passen voor belangrijke wijzigingen; aanvullende risicoanalyses worden alleen vereist voor gevaren die losstaan van een algemeen aanvaardbaar risico;
(c) de CSM behandelt de selectie en tenuitvoerlegging van veiligheidsmaatregelen die beogen de onderkende gevaren en daaraan verbonden risico's te beheersen;
(d) de CSM harmoniseert het risicobeheerproces, waaronder begrepen:

(1) de harmonisatie van risicoaanvaardingscriteria die kadert in de werkzaamheden van het Spoorwegbureau betreffende algemeen aanvaardbare risico's en risicoaanvaardingscriteria,
(2) het aantonen dat het systeem voldoet aan de veiligheidsvereisten;
(3) de resultaten en het bewijsmateriaal voortvloeiend uit het risicobeoordelingsproces;
(4) de uitwisseling van veiligheidsgerelateerde informatie tussen de betrokken actoren bij interfaces;
(5) het bijhouden in een gevareninventaris van alle in kaart gebrachte gevaren en daarmee samenhangende veiligheidsmaatregelen;
(6) de onafhankelijke beoordeling door een derde van de correcte toepassing van de CSM.

C.10.5. De toepassing van het OTIF-richtsnoer in het kader van de CSM (voor zover het vervoer van gevaarlijke goederen strekt tot belangrijke wijziging wat betreft een infrastructuurbeheerder of spoorwegonderneming) doet echter geen problemen rijzen vermits dit verenigbaar is met het gebruik van het derde beginsel van de expliciete risico-inschatting.

C.11. Voorbeeld van risicobeoordeling van een goedkeuringsaanvraag voor een nieuw type rollend materieel

C.11.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

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

C.11.2. Dit voorbeeld van risicobeoordeling betreft een goedkeuringsaanvraag voor een nieuw type rollend materieel. Er werd een risicoanalyse uitgevoerd om de risico's te evalueren die ontstaan door de invoering van een nieuwe goederenwagen.

C.11.3. De wijziging had ten doel de effectiviteit, capaciteit, prestaties en betrouwbaarheid te verhogen voor het vervoer van stortgoed op een specifieke goederenvervoerslijn. Aangezien de goederenwagens bestemd waren voor grensoverschrijdend goederenverkeer, was de goedkeuring van twee verschillende nationale veiligheidsinstanties nodig. De initiatiefnemer was een leverancier van goederenvervoer per spoor ("vervoersexploitant") die op zijn beurt in handen was van de fabrikant van de te transporteren goederen.

C.11.4. De projectontwikkeling behelsde de bouw, fabricage, montage, indienststelling en keuring van het nieuwe rollend materieel. Er werd een risicoanalyse uitgevoerd om na te gaan of het nieuwe ontwerp voldeed aan de veiligheidsvereisten voor alle afzonderlijke subsystemen alsook voor het systeem als geheel.

C.11.5. In de risicoanalyse wordt verwezen naar de procedures en definities in CENELEC EN 50126. De risico-evaluatie wordt overeenkomstig deze norm uitgevoerd.

C.11.6. Vergeleken met het CSM-proces werden de volgende stappen ondernomen:

(a) systeembeschrijving [punt 2.1.2]:

Voor elke ontwerpfase werden eisen gesteld inzake de documentatie over de veiligheidskeuring en de beschrijving van het systeemontwerp:

(1) conceptuele fase: voorafgaande beschrijving van de exploitatie-eisen van de vervoersexploitant;

(2) specificatiefase: functionele specificatie, toepasselijke technische normen, plan voor beproeving en keuring. Door de vervoersexploitant gestelde eisen qua gebruik en onderhoud van de goederenwagen werden ook opgenomen;

(3) fabricagefase: technische documentatie van de fabrikant, waaronder begrepen tekeningen, normen, berekeningen, analyses enz. Grondige risicoanalyse voor nieuwe of innoverende ontwerpen of nieuwe toepassingsgebieden;

(4) keuringsfase:

(i) keuring door de fabrikant van de technische prestaties van de goederenwagen (beproevingsverslagen/testrapporten, berekeningen, keuringen overeenkomstig normen en functionele eisen);
(ii) documentatie over risicobeperkende maatregelen en beproevingsverslagen/testrapporten ter staving van de compatibiliteit van de goederenwagons met de spoorweginfrastructuur;
(iii) onderhouds- en opleidingsdocumenten, gebruiksaanwijzingen, handleidingen enz.

(5) goedkeuringsfase:

(i) de veiligheidsverklaring en het veiligheidsbewijs van de fabrikant;
(ii) de goedkeuring door de vervoersexploitant van de goederenwagen en bijbehorende documentatie;

(b) gevareninventarisatie [punt 2.2]:

werd doorlopend in alle ontwerpfasen uitgevoerd. Eerst wordt een “bottom-up”-benadering toegepast, waarbij de verschillende fabrikanten de sequentiële risico's evalueerden van het falen van onderdelen in hun subsysteem. De verdeling in subsystemen ziet er als volgt uit:

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

(1) frame (onderstel);
(2) remsysteem;
(3) centrale koppeling;
(4) enzovoort.

Aanvullend werd een “top-down”-benadering toegepast om te controleren op hiaten of ontbrekende informatie. Niet direct aanvaardbare risico's werden overgebracht in de gevareninventaris voor verdere verwerking en classificatie.

(c) gebruik van risicoaanvaardingsbeginselen [punt 2.1.4]:

Het systeem als geheel werd onderworpen aan een expliciete risico-inschatting. Afzonderlijke gevaren mochten echter worden beoordeeld met gebruikmaking van praktijkcodes of soortgelijke referentiesystemen. Uitgangspunt is dat elk nieuw subsysteem minstens even veilig moet zijn als het subsysteem dat het vervangt. Op die manier ontstaat een nieuw compleet systeem met een hoger veiligheidsniveau dan het vorige. De in kaart gebrachte gevaren werden voorgesteld in de risicomatrix conform EN50126. Voorts werden verschillende aanvullende risicoaanvaardingscriteria toegepast, waaronder:

(1) enkelvoudig falen mocht niet leiden tot een toestand waarin personen, materieel of milieu/omgeving ernstige schade werd toegebracht;
(2) is dat niet te vermijden door constructietechnische voorzieningen, dan moet het worden voorkomen door bedrijfsvoorschriften of onderhoudseisen. Dat was alleen van toepassing op gevaren waarvoor het niet mogelijk was de opgetreden storing te identificeren voordat die een gevaarlijke situatie deed ontstaan;
(3) voor onderdelen met een hoge kans op falen (storingskans), of waarvoor het niet mogelijk is storingen op voorhand op te sporen of te voorkomen door onderhoud of bedrijfsvoorschriften, moeten aanvullende veiligheidsfuncties en -voorzieningen in overweging worden genomen;
(4) redundante systemen met onderdelen die tijdens exploitatie op ondetecteerbare wijze kunnen falen, moeten worden beschermd door onderhoudsmaatregelen om verminderde redundantie te voorkomen;
(5) over het resulterende uiteindelijke veiligheidsniveau werd op managementniveau beslist op basis van een kwantitatieve en kwalitatieve risicoanalyse;

(d) aantonen dat het systeem voldoet aan de veiligheidsvereisten [punt 3]:

Alle in kaart gebrachte risico's en gevaren werden geregistreerd. De lijst werd doorlopend geraadpleegd en bijgewerkt. Residuele gevaren werden opgetekend in de gevareninventaris met de corresponderende lijst van de te treffen risicobeperkende maatregelen qua bouw, exploitatie en onderhoud. Op basis hiervan werd een definitief veiligheidsrapport opgesteld ter staving dat de veiligheidsvereisten ten uitvoer werden gelegd;

(e) gevarenbeheer [punt 4.1]:

Zoals hierboven uiteengezet, werden de gevaren en daarmee samenhangende veiligheidsmaatregelen geregistreerd in een gevareninventaris, waarin alle in kaart gebrachte gevaren en veiligheidsmaatregelen werden bijgehouden. Gevaren verbonden aan risico's die aanvaardbaar waren zonder maatregelen te treffen, werden echter niet in de gevareninventaris vermeld;

(f) onafhankelijke beoordeling [Artikel 6]:

In de over deze belangrijke wijziging ontvangen documenten werd geen melding gemaakt van een onafhankelijke beoordeling.

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

C.11.7. Dit voorbeeld van risicobeoordeling berust op de CENELEC-norm EN 50126 en komt derhalve goed overeen met het CSM-proces. De risicobeoordeling in dit voorbeeld voldoet aan alle in de CSM genoemde eisen, uitgezonderd de eis inzake onafhankelijke beoordeling die niet uitdrukkelijk werd opgehelderd in de ontvangen documenten. Er werden expliciete risicoaanvaardingscriteria gebruikt en duidelijk aangegeven.

C.12. Voorbeeld van risicobeoordeling van een belangrijke wijziging van operationele aard – DOO-treinbesturing

C.12.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.12.2. Dit voorbeeld betreft een operationele wijziging waarbij de spoorwegonderneming besliste dat de trein uitsluitend door de bestuurder mocht worden bestuurd (Driver Only Operated – DOO) op een rijweg waar vroeger een conducteur op het voertuig was die de bestuurder mocht bijstaan met de treindienstleiding.

C.12.3. Vergeleken met het CSM-proces werden de volgende stappen ondernomen (zie ook Figuur 1):

(a) significantieniveau van de wijziging [Artikel 4]:

De spoorwegonderneming heeft een voorafgaande risicobeoordeling uitgevoerd waaruit bleek dat het ging om een belangrijke wijziging van operationele aard. Aangezien de bestuurder de trein alleen moest besturen zonder hulp of bijstand, bestond een niet te verwaarlozen kans dat passagiers bekneld raakten tussen de deuren of ten val kwamen op het spoor (bijvoorbeeld wanneer de deuren aan de verkeerde zijde worden geopend).

Werd deze voorafgaande risicobeoordeling vergeleken met de in Artikel 4, van de CSM-verordening genoemde criteria, dan kon de wijziging ook als belangrijk worden aangemerkt op basis van de volgende criteria:

(1) veiligheidsrelevantie: de wijziging houdt verband met de veiligheid aangezien het opleggen van een volledig andere manier om de treindienst te regelen catastrofale gevolgen kan hebben;
(2) gevolg bij faling: de mogelijke invloed op de prestaties van de bestuurder kan rampzalige gevolgen hebben als de treinbesturing niet effectief wordt gecontroleerd;
(3) nieuwigheid: de DOO-treinbesturing kan innovatieve manieren van treindienstleiding vereisen waarvan de risico's moeten worden beoordeeld;

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

(b) systeemomschrijving [punt 2.1.2]:

De systeemomschrijving behelsde een beschrijving van:

(1) het bestaande systeem, waarbij duidelijk werd aangegeven welke taken door de bestuurder werden uitgevoerd en welke andere taken door het treinpersoneel (of de conducteur) werden uitgevoerd ter ondersteuning van de bestuurder;
(2) de gewijzigde verantwoordelijkheden van de treinbestuurder als gevolg van het wegvallen van begeleidend boordpersoneel;
(3) de technische eisen van het systeem om rekening te houden met de wijzigingen in treindienstleiding;
(4) de bestaande interfaces tussen het begeleidende boordpersoneel, de treinbestuurder en het niet-rijdende personeel van de infrastructuurbeheerder;

Tijdens de verschillende iteraties werd de systeemomschrijving bijgewerkt met de veiligheidsvereisten resulterend uit het risicobeoordelingsproces. Bij dit iteratieve proces werd personeel op sleutelposities (onder wie treinbestuurders, personeelsvertegenwoordigers en de infrastructuurbeheerder) betrokken om de gevaren in kaart te brengen en de systeemomschrijving bij te werken.

(c) gevareninventarisatie [punt 2.2]:

De gevaren en mogelijke veiligheidsmaatregelen werden in kaart gebracht via een brainstorming van een deskundigengroep met onder meer:

(1) treinbestuurders en personeelsvertegenwoordigers in verband met hun operationele ervaring;
(2) vertegenwoordigers van de infrastructuurbeheerder aangezien deze laatste ook kan worden beïnvloed door de wijziging, in zoverre bijvoorbeeld aanpassingen in stations moeten worden doorgevoerd (bijvoorbeeld installeren van spiegels/gesloten televisiecircuit [CCTV] op perrons);

De aanvullende taken die de treinbestuurder moest uitvoeren, werden doorgelicht om alle voorzienbare gevaren in kaart te brengen die konden ontstaan door het wegvallen van het begeleidende boordpersoneel. Bij de gevareninventarisatie werd meer in het bijzonder nagegaan wat de voornaamste operationele gevaren waren die zich konden voordoen in stations, op de bestaande rijwegen waar vroeger bijstand werd geleverd door treinpersoneel of niet-rijdend personeel, met inbegrip van de veilige treindienstleiding, specifieke aandachtspunten wat betreft treinbestuurder, rollend materieel (bijvoorbeeld controle op openen/sluiten van de deuren), onderhoudseisen enz.

Aan elk onderkend gevaar werd een ernstgraad toegekend, gemeten naar risico en gevolgen (hoog, middelhoog, laag). Het effect van de geplande wijziging werd daaraan getoetst om het (verhoogde, ongewijzigde, verminderde) risico te bepalen.

(d) gebruik van praktijkcodes [punt 2.3] en van soortgelijke referentiesystemen [punt 2.4]:

Beide praktijkcodes (dat wil zeggen de normenreeks voor DOO-treinbesturing) en soortgelijke referentiesystemen werden gebruikt om de veiligheidsvereisten voor de onderkende gevaren vast te leggen. Daarbij ging het onder meer om de volgende veiligheidsvereisten:

(1) de herziene operationele procedures voor de bestuurder die nodig zijn om treinen veilig te besturen zonder hulp of bijstand aan boord;
(2) eventueel benodigde aanvullende trein- of baanapparatuur ter waarborging van een veilige en betrouwbare treindienstleiding;

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

(3) een controlelijst om te waarborgen dat de stuurcabine geschikt was, rekening houdend met de interface tussen het spoorwegsysteem (zowel aan boord als naast het spoor) en de treinbestuurder;

De vereiste bedrijfsvoorschriften werden herzien overeenkomstig de eisen in de toepasselijke praktijkcodes en referentiesystemen. Alle nodige partijen werden betrokken bij de herziene operationele procedures en de goedkeuring om de wijziging door te voeren.

(e) aantonen dat wordt voldaan aan de veiligheidsvereisten [punt 3]:

Het systeem werd geïmplementeerd met inachtneming van de onderkende veiligheidsvereisten (extra uitrusting en herziene procedures). Deze werden adequaat bevonden om een toereikend veiligheidsniveau voor het beoordeelde systeem te waarborgen.

De herziene operationele procedures werden ingevoerd in het veiligheidsbeheersysteem van de spoorwegonderneming. De herziene procedures werden gecontroleerd en waar nodig aangepast om te waarborgen dat de in kaart gebrachte gevaren verder naar behoren worden beheerst tijdens de exploitatie van het spoorwegsysteem.

(f) gevarenbeheer [punt 4.1]:

In dat verband wordt naar het bovenstaande punt verwezen aangezien het gevarenbeheerproces wat betreft spoorwegondernemingen deel kan uitmaken van hun veiligheidsbeheersysteem voor risicoregistratie en -beheer. De onderkende gevaren werden in een gevareninventaris geregistreerd samen met de veiligheidsvereisten ter beheersing van het daarmee samenhangende risico, dat wil zeggen onder verwijzing naar de extra trein- en baanapparatuur alsook naar de herziene operationele procedures.
De herziene procedures werden gecontroleerd en waar nodig aangepast om te waarborgen dat de in kaart gebrachte gevaren verder naar behoren worden beheerst tijdens de exploitatie van het spoorwegsysteem.

(g) onafhankelijke beoordeling [Artikel 6]:

Het risicobeoordelings- en risicobeheerproces werd beoordeeld door een vakkundig persoon bij de spoorwegonderneming die niet eerder bij het beoordelingsproces betrokken was. Deze persoon heeft het proces beoordeeld alsmede de resultaten, dat wil zeggen de in kaart gebrachte veiligheidsvereisten.

De spoorwegonderneming heeft het onafhankelijke beoordelingsrapport van de vakkundige persoon gebruikt ter verantwoording van haar beslissing om het nieuwe systeem te operationaliseren.

C.12.4. Uit dit voorbeeld blijkt dat de beginselen en processen die de spoorwegonderneming toepast overeenstemmen met de gemeenschappelijke veiligheidsmethode. Het risicobeheer- en risicobeoordelingsproces voldoet aan alle in de CSM voorgeschreven eisen.

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

C.13. Voorbeeld van het gebruik van een referentiesysteem om veiligheidsvereisten af te leiden voor nieuwe elektronische baanvakbeveiligingssystemen in Duitsland

C.13.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.13.2. Met als doel standaardveiligheidsvereisten af te leiden voor toekomstige elektronische baanvakbeveiligingssystemen heeft Deutsche Bahn een risicoanalyse uitgevoerd op een reeds goedgekeurd elektronisch systeem. Dit systeem werd goedgekeurd overeenkomstig de Duitse praktijkcodes (Mü 8004).

C.13.3. De risicoanalyse werd uitgevoerd overeenkomstig de CENELEC-normen (EN 50126 en EN 50129) en bestond uit de volgende stappen:

(a) systeemomschrijving;
(b) gevareninventarisatie;
(c) gevarenanalyse en -kwantificering.

C.13.4. Wat betreft de systeemomschrijving werden de grenzen van het systeem samen met de bijbehorende functies en interfaces duidelijk afgebakend. Belangrijkste uitdaging was het systeem zodanig te definiëren dat het onafhankelijk is van de interne architectuur van een baanvakbeveiligingssysteem, maar tegelijk compatibel bleef met bestaande baanvakbeveiligingssystemen. Bijzondere aandacht werd besteed aan het eenduidig definiëren van de interfaces buiten systemen die in interactie staan met de baanvakbeveiliging zonder de intrinsieke baanvakbeveiligingsfuncties te detailleren.

C.13.5. Vervolgens werden de gevaren in kaart gebracht, zij het dan alleen bij de interfaces om zo algemeen mogelijk te blijven (dat wil zeggen eventuele afhankelijkheid van specifieke architecturen te vermijden). Daarbij kwamen alleen gevaren aan bod die door technische fouten werden veroorzaakt. Voor elke interface werden op die manier twee algemene gevaren in kaart gebracht:

(a) doorgifte van onjuiste outputparameters van de baanvakbeveiliging aan de interface
(b) beschadiging van (correcte) inputparameters bij de interface

C.13.6. Aan deze algemene gevaren bij elke interface werden specifiekere eigenschappen toegekend.

C.13.7. In de volgende fase werd nagegaan welke bijdrage de bestaande systeemonderdelen aan elk onderkend gevaar leverden. Deze gegevens werden in een foutenboom verwerkt. Op die

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

manier werd het mogelijk op basis van het geschatte storings- of faaltempo van de onderdelen de frequentie van optreden van elk gevaar te berekenen, en dit gegeven te gebruiken als aanvaardbare risicofactor voor toekomstige generaties van elektronische baanvakbeveiligingssystemen.

C.13.8. De risicoanalyse werd opgevolgd en beoordeeld door de nationale veiligheidsinstantie (EBA).

C.13.9. Als onderdeel van de risicoanalyse werden ook de bedienings- en weergavefuncties in het elektronische systeem onderzocht. Ook hier werd een bestaand goedgekeurd elektronisch baanvakbeveiligingssysteem als referentie genomen om veiligheidsvereisten af te leiden voor de functies van de mens-machine-interface (MMI) ter beheersing van willekeurige storingen en fouten alsmede van systematische fouten. Op basis hiervan werden de veiligheidsintegriteitsniveaus voor de verschillende functies vastgelegd: voor MMI-functies in standaardbedrijf, voor MMI-functies in storingsbedrijf (besturing-opheffen), en voor de weergavefunctionaliteit.

C.13.10. Ook deze risicoanalyse werd opgevolgd en beoordeeld door de nationale veiligheidsinstantie (EBA).

C.13.11. Deze voorbeelden van risicobeoordeling tonen aan hoe het tweede risicoaanvaardingsbeginsel (referentiesysteem) in de CSM kan worden gebruikt om veiligheidsvereisten voor nieuwe systemen af te leiden. Bovendien berusten deze voorbeelden op de CENELEC-normen zodat ze goed overeenkomen met het CSM-proces. De risicobeoordeling in deze voorbeelden voldoet aan de CSM-eisen voor elke daarmee samenhangende fase. Aangezien ontwerpactiviteiten buiten beschouwing blijven, wordt niet verwezen naar het beheer van het veiligheidsinformatieblad en evenmin naar het aantonen dat het beoordeelde systeem voldoet aan de onderkende veiligheidsvereisten.

C.13.12. Meer informatie over deze risicoanalyses is terug te vinden in:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15, en

(b) Bock, H., Braband, J., and Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

C.14. Voorbeeld van een expliciet risicoaanvaardingscriterium voor op FFB-radiocommunicatie gebaseerde treinbesturing in Duitsland

C.14.1. **Opmerking:** dit voorbeeld van risicobeoordeling resulteert niet uit de toepassing van het CSM-proces, maar werd uitgewerkt toen de CSM-verordening nog niet bestond. Dit voorbeeld heeft ten doel:

(a) de raakpunten in kaart te brengen tussen de bestaande risicobeoordelingsmethoden en het CSM-proces;
(b) het bestaande proces traceerbaar te maken ten opzichte van het in de CSM-verordening voorgeschreven proces;
(c) de meerwaarde te verantwoorden die wordt gecreëerd door eventuele in de CSM-verordening voorgeschreven extra maatregelen te nemen.

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

Op te merken valt dat dit voorbeeld alleen ter informatie is bedoeld. Het beoogt het CSM-proces inzichtelijk te maken voor de lezer. Op zichzelf mag het voorbeeld niet worden omgezet in of gebruikt als referentiesysteem voor andere belangrijke wijzigingen. Voor elke belangrijke wijziging moet de risicobeoordeling worden uitgevoerd overeenkomstig de CSM-verordening.

C.14.2. Er werd een risicoanalyse overeenkomstig de CENELEC-normen uitgevoerd voor een volledig nieuwe exploitatieprocedure die in overweging was genomen (maar nooit in de praktijk gebracht) voor conventionele spoorlijnen in Duitsland. Het concept bestond erin treinen veilig te besturen door uitsluitend gebruikt te maken van op radiocommunicatie gebaseerde verkeersleiding (rijweg- en treinloopsturing). Aangezien voor een dergelijk nieuw systeem geen praktijkcodes (erkende constructietechnische voorschriften) noch referentiesystemen bestonden, werd een expliciete risico-inschatting uitgevoerd om de veiligheid van de nieuwe procedure aan te tonen. Daarbij moest worden aangetoond dat het risiconiveau voor een passagier als gevolg van het nieuwe systeem niet hoger lag dan een aanvaardbare risicograad (expliciet risicoaanvaardingscriterium).

C.14.3. Dit expliciete risicoaanvaardingscriterium werd geschat op basis van statistieken in Duitsland over door besturings- en seingevingssystemen veroorzaakte ongevallen. De aannemelijkheid daarvan werd getoetst aan het MEM-criterium. Dergelijk veiligheidsbewijs beantwoordt aan het vereiste van de Duitse EBO dat bij afwijkingen van de constructietechnische voorschriften "hetzelfde veiligheidsniveau" moet worden gehandhaafd. De risicoanalyse werd eveneens opgevolgd en beoordeeld door de nationale veiligheidsinstantie (EBA).

C.14.4. Dit voorbeeld van risicobeoordeling toont aan hoe een algemeen expliciet criterium (wat betreft het derde risicoaanvaardingsbeginsel in de CSM) voor nieuwe systemen kan worden afgeleid zonder bestaande praktijkcodes of referentiesystemen. De risicoanalyse die aansluitend daarop werd uitgevoerd voor het nieuwe systeem berust op de CENELEC-normen en beantwoordt derhalve goeddeels aan het CSM-proces. De risicobeoordeling in dit voorbeeld voldoet aan de CSM-eisen. Er wordt echter niet verwezen naar het beheer van de gevareninventaris, noch naar het aantonen dat het beoordeelde systeem voldoet aan de onderkende veiligheidsvereisten.

C.14.5. Meer informatie over deze risicoanalyse is terug te vinden in: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, 10-15.

C.15. Voorbeeld van toepasbaarheidstest van het RAC-TS

C.15.1. Dit aanhangsel beoogt aan de hand van een functievoorbeeld van het subsysteem "ETCS-treinapparatuur" aan te tonen hoe het in punt 2.5.4 genoemde criterium kan worden gebruikt en hoe kan worden nagegaan of het RAC-TS toepasbaar is.

C.15.2. Het subsysteem "ETCS-treinapparatuur" is een technisch systeem. De volgende functie wordt in overweging genomen: *"de bestuurder de nodige informatie verschaffen om de trein veilig te besturen en een dwangremming in te zetten wanneer met te hoge snelheid wordt gereden"*.

Beschrijving van de functie: op basis van informatie die van de apparatuur naast het spoor wordt ontvangen (toegestane snelheid) en de door het subsysteem "ETCS-treinapparatuur" berekende snelheid van de trein:

(a) bestuurt de treinbestuurder de trein zonder de toegestane snelheid te overschrijden;

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

(b) ziet het subsysteem "ETCS-treinapparatuur" erop toe dat de trein de maximaal toegestane snelheid nooit overschrijdt. Bij snelheidsoverschrijding worden de remmen automatisch in werking gesteld.

Zowel de treinbestuurder als het subsysteem "ETCS-treinapparatuur" gebruiken de snelheid zoals die wordt berekend door het subsysteem "ETCS-treinapparatuur".

C.15.3. Vraag: "Is het RAC-TS van toepassing op de door het subsysteem "ETCS-treinapparatuur" berekende snelheid van de trein?"

C.15.4. Toepassing van het stroomschema in Figuur 14 en antwoorden op de verschillende vragen:

(a) In aanmerking genomen gevaar wat betreft het technische systeem:

"Overschrijding van de veilige snelheid zoals gemeld aan ETCS" (zie UNISIG SUBSET 091).

(b) Kan het gevaar worden beheerst met gebruikmaking van een praktijkcode of referentiesysteem?

NEE. Aangenomen wordt dat het ETCS-systeem een nieuw en innovatief ontwerp heeft. Bijgevolg bestaan geen praktijkcodes of referentiesystemen om het gevaar tot een aanvaardbaar risiconiveau terug te brengen.

(c) Is het waarschijnlijk dat het gevaar rampzalige gevolgen zal hebben?

JA, want een *"overschrijding van de veilige snelheid zoals gemeld aan ETCS"* kan een trein doen ontsporen met mogelijk *"doden en/of meerdere zwaargewonden en/of ernstige milieuschade"* tot gevolg.

(d) Resulteren de rampzalige gevolgen direct uit het falen van het technische systeem?

JA, voor zover er geen aanvullende veiligheidsvoorzieningen zijn. De snelheid van de trein die door het subsysteem "ETCS-treinapparatuur" wordt berekend, wordt gemeld aan de treinbestuurder en de remcontrolefunctie van het het subsysteem "ETCS-treinapparatuur". Dit betekent dat wanneer de bestuurder de trein (om prestatieredenen) tegen de door de baanapparatuur toegestane maximumsnelheid laat rijden, noch de bestuurder, noch het subsysteem "ETCS-treinapparatuur" kunnen vaststellen dat de trein met te hoge snelheid rijdt als de snelheid te laag wordt ingeschat. Dat kan de trein doen ontsporen met rampzalige gevolgen.

(e) Conclusies:

(1) wat betreft de kwantitatieve eisen: een aanvaardbare risicofactor van 10^{-9} h^{-1} toepassen voor de willekeurige apparatuurstoringen van het subsysteem "ETCS-treinapparatuur" om te waarborgen dat:

(i) in redundante systemen bij de evaluatie van deze kwantitatieve streefwaarde rekening wordt gehouden met de gemeenschappelijke onderdelen (bijvoorbeeld enkelvoudige of gemeenschappelijke ingangen naar alle kanalen, gemeenschappelijke stroomvoorziening, vergelijkers, kiezers enz.);
(ii) de detectietijden van verborgen of latente storingen worden gecompenseerd;
(iii) een analyse van gemeenschappelijk/meervoudig falen (CCF/CMF) wordt uitgevoerd;
(iv) een onafhankelijke beoordeling wordt uitgevoerd;

(2) wat betreft de procesmatige eisen: een proces van veiligheidsintegriteitsniveau 4 toepassen voor het beheer van systematische storingen/fouten van het subsysteem "ETCS-treinapparatuur". Dat vereist de toepassing van:

(i) een kwaliteitsborgingsproces conform veiligheidsintegriteitsniveau 4;

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

(ii) een veiligheidsbeheerproces conform veiligheidsintegriteitsniveau 4;
(iii) de toepasselijke normen, bijvoorbeeld:

- de norm EN 50 128 wat betreft softwareontwikkeling;
- de normen 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 enz. wat betreft hardwareontwikkeling;

(3) een onafhankelijke beoordeling van de processen.

C.16. Voorbeelden van mogelijke structuren voor de gevareninventaris

C.16.1. Inleiding

C.16.1.1. In punt 4.1.2 van de CSM-verordening staan de minimumeisen wat betreft de inhoud van de gevareninventaris. In de volgende voorbeelden van gevareninventarissen zijn deze eisen gearceerd.

C.16.1.2. Een gevareninventaris kan op velerlei manieren worden gestructureerd. Dat geldt ook voor aanvullende informatie die kan worden gebruikt om de gevaren en daarmee samenhangende veiligheidsmaatregelen te karakteriseren. Zo kan één veld worden gebruikt voor elk gegeven dat betrekking heeft op de gevaren en daarmee samenhangende veiligheidsmaatregelen. Welke structuur ook wordt gebruikt, het is van belang dat in de gevareninventaris duidelijke kruisverwijzingen staan tussen de gevaren en daarmee samenhangende veiligheidsmaatregelen. Een mogelijke oplossing bestaat erin voor elk gevaar en elke veiligheidsmaatregel in de gevareninventaris minstens een veld te vermelden met:

(a) een duidelijke beschrijving inclusief herkomstaanduidingen en verwijzingen naar het risicoaanvaardingsbeginsel dat werd geselecteerd om het bijbehorende gevaar te beheersen. Dit veld verschaft inzicht in het gevaar en de daarmee samenhangende veiligheidsmaatregelen en geeft aan in welke veiligheidsanalyses ze in kaart werden gebracht.

De gevareninventaris wordt tijdens de volledige levenscyclus (dat wil zeggen exploitatie en onderhoud) van het systeem gebruikt en bijgehouden. Vandaar het nut van een goede traceerbaarheid, of duidelijke koppeling, tussen elk gevaar en:

(1) het daaraan verbonden risico;
(2) de gevaarsoorzaken in zoverre die reeds in kaart werden gebracht;
(3) de daarmee samenhangende veiligheidsmaatregelen alsook de aannames die de grenzen van het beoordeelde systeem afbakenen;
(4) de daarmee samenhangende veiligheidsanalyses waarin het gevaar wordt onderkend.

Bovendien moeten niet alleen de veiligheidsmaatregelen (inzonderheid met het oog op de overdracht aan andere actoren, zoals de initiatiefnemer), maar ook de daarmee samenhangende gevaren en risico's duidelijk en in voldoende mate worden omschreven. Met “duidelijk en in voldoende mate” wordt bedoeld dat uit de veiligheidsmaatregelen en daarmee samenhangende gevaren moet kunnen worden opgemaakt welke risico’s zij beogen te beheersen, zonder de bijbehorende veiligheidsanalyses erop na te slaan.

(b) het risicoaanvaardingsbeginsel dat werd gebruikt om het gevaar te beheersen met als doel het beginsel van de wederzijdse erkenning te eerbiedigen en de beoordelingsinstantie te helpen een oordeel uit te spreken over de juiste toepassing van de CSM;

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

(c) duidelijke informatie over de status ervan: in dit veld wordt aangegeven of de desbetreffende gevaren/veiligheidsmaatregelen nog openstaan dan wel werden beheerst, respectievelijk gevalideerd.

(1) openstaande gevaren/veiligheidsmaatregelen worden nagespoord tot ze worden beheerst, respectievelijk gevalideerd;

(2) omgekeerd worden de beheerste gevaren/gevalideerde veiligheidsmaatregelen niet langer nagespoord tenzij belangrijke wijzigingen wat betreft exploitatie of onderhoud van het systeem plaatsvinden: zie onder [G 6](b) in punt 2.1.1. In dit geval:

(i) moet de CSM opnieuw op de desbetreffende wijzigingen worden toegepast overeenkomstig het bepaalde in Artikel 2. Zie ook onder [G 6](b)(1) in punt 2.1.1;

(ii) moeten alle beheerste gevaren en gevalideerde veiligheidsmaatregelen opnieuw worden bezien om zeker te stellen dat ze niet door de wijzigingen worden beïnvloed. Worden ze beïnvloed, dan moeten de bijbehorende gevaren en daarmee samenhangende veiligheidsmaatregelen opnieuw in behandeling worden genomen en beheerd in de gevareninventaris;

Het kan zijn dat andere veiligheidsmaatregelen ten uitvoer worden gelegd dan die welke in de gevareninventaris zijn vermeld (bijvoorbeeld uit kostenoverwegingen). De ten uitvoer gelegde veiligheidsmaatregelen worden dan in de gevareninventaris opgetekend met het bewijsmateriaal en de verantwoording van de geschiktheid ervan alsmede het bewijs dat het systeem met deze maatregelen voldoet aan de veiligheidsvereisten.

(d) de verwijzing naar het bijbehorende bewijsmateriaal ter beheersing van een gevaar of ter validering van een veiligheidsmaatregel. Via dit veld kan achteraf het bewijsmateriaal worden teruggevonden dat het mogelijk heeft gemaakt het gevaar te beheersen en de bijbehorende veiligheidsmaatregelen te valideren;

Een gevaar mag als beheerst in de gevareninventaris worden aangemerkt wanneer alle aan dit gevaar verbonden veiligheidsmaatregelen op voorhand werden gevalideerd;

(e) de met het beheer ervan belaste organisatie(s) of instantie(s).

C.16.1.3. Aanhangsel A.3. van het richtsnoer EN 50126-2 {Ref. 9} geeft nog een voorbeeld van de mogelijke inhoud van een gevareninventaris.

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

C.16.2. Voorbeeld van de gevareninventaris voor de onder C.5. in aanhangsel C genoemde organisatorische wijziging

Tabel 6: Voorbeeld van de gevareninventaris voor de onder C.5. in aanhangsel C genoemde organisatorische wijziging.

Gevaaromschrijving	Veiligheidsmaatregelen	Prioriteit/veiligheid stiptheid	Tenuitvoerlegging(16)	Toelichtingen	Verantwoordelijkheid(16)	Oorsprong	Gebruikt risicoaanvaardingsbegin sel	Keurings-verantwoordelijkheid	Keurings-methode	Status xx.xx.xx
Gebrek aan motivatie bij het overblijvende personeel van de onderneming. Als gevolg daarvan onafgebroken uitstroom van personeel. Gedemotiveerde/ uitgebluste managers	Nieuwe motiveringsslag voor het personeel, uit te voeren in kleinere groepen Herverdeling van financiële middelen zodat de onderneming betekenisvolle taken krijgt toebedeeld Frequentere inspectiebeurten door baanvakbeheerder. Financiële middelen toewijzen om te waarborgen dat personeel op sleutelposities tijdens het proces in dienst blijft. In het bijzonder erop toezien dat informatie en kennis wordt overgedragen tussen uittredende werknemers en hun plaatsvervangers. enzovoort.	Hoog/hoog	Gecoördineerd door XYZ. Regio's moeten maatregelen in beschouwing nemen om baanvakken beter te controleren, meer raakvlakken te creëren op personeelsniveau en een betere opvolging door de lijnmanager te garanderen	Aangescherpte inspecties moeten contractueel worden vastgelegd etc.	Bedrijfsdirecteur	Brainstorming HAZID-rapport R_X	N.v.t.			Dit risico is fors verminderd door gewijzigde randvoorwaarden of omstandigheden Arbeidsmilieu werd geanalyseerd en personeel enigermate opgeleid.
Gebrekkige kwaliteitsbeheersing en tekort aan vaardigheden en competenties bij onderaannemers	Verhoogde vraag naar competentiebewijzen. Stelselmatig toezicht op uitgevoerde taken	Hoog/ middelhoog	Infrastructuur beheerder heeft coördinerende taak. Regio's	Uitgevoerd via contractuele follow-up. Input voor herzienings-planning.	Infrastructuurbeheerder	Brainstorming HAZID-rapport R_X	N.v.t.	Veiligheidsbeheerder		Accentuering van routines bij controle (twee operationele controles per

(16) *Deze twee kolommen hebben betrekking op de informatie/het veld over de actoren die belast zijn met de beheersing van de in kaart gebrachte gevaren.*

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

Tabel 6: Voorbeeld van de gevareninventaris voor de onder C.5. in aanhangsel C genoemde organisatorische wijziging.

Gevaaromschrijving	Veiligheidsmaatregelen	Prioriteit/veiligheid stiptheid	Tenuitvoerlegging[16]	Toelichtingen	Verantwoordelijkheid[16]	Oorsprong	Gebruikt risicoaanvaardingsbeginsel	Keuringsverantwoordelijkheid	Keuringsmethode	Status xx.xx.xx
			moeten maatregelen ten uitvoer leggen om competentie verplicht te stellen en het werk te controleren							maand en per werkingsgebied)
Onzekerheid over functies en verantwoordelijken in de interface tussen onderneming en infrastructuurbeheerder (baanvakbeheerder).	Functies en verantwoordelijkheden definiëren. Alle interfaces in kaart brengen en aangeven wie de verantwoordelijkheid daarvoor draagt.	Middelhoog/ middelhoog	In elke regio afzonderlijk	Uitgevoerd door onderhoudscontract en beleidsplan voor reorganisatie	Regiomanagers	Brainstorming HAZID-rapport R_X	N.v.t.	Veiligheidsbeheerder		Regio's hebben hun strategie uiteengezet.

C.16.3. Voorbeeld van een volledige gevareninventaris voor een besturings- en seingevingssubsysteem aan boord

C.16.3.1. Het voorbeeld in dit punt toont aan hoe één gevareninventaris (zie onder [G 3] in punt 4.1.1) kan worden gebruikt voor het beheren van:

(a) alle interne veiligheidsvereisten die gelden voor het subsysteem dat onder de verantwoordelijkheid van de actor valt; en
(b) alle onderkende gevaren en daarmee samenhangende veiligheidsmaatregelen die de actor niet ten uitvoer kan leggen en die aan andere actoren moeten worden overgedragen.

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

Tabel 7: Voorbeeld van een gevareninventaris van de fabrikant voor een besturings- en seingevingssubsysteem aan boord.

Nr. gevaar	Oor-sprong	Gevaaromschrijving	Extra informatie	Verantwoor-delijke actor	Veiligheidsmaatregel	Gebruikt risicoaanvaardingsbegin-sel	Geëxpor-teerd	Status
1	HAZOP-rapport R_X	Maximumsnelheid van de trein te hoog ingesteld (Vmax)	Onjuiste configuratie van het specifieke subsysteem aan boord (onderhoudspersoneel) Onjuiste gegevensinvoer aan boord (treinbestuurder)	Spoorwegon-derneming	• Procedure definiëren om de configuratiegegevens van het subsysteem aan boord goed te keuren • Operationele procedure definiëren voor gegevensinvoer door de treinbestuurder	Expliciete risico-inschatting	Ja	Beheerst (geëxporteerd naar spoorwegonderne-ming) Zie ook onder C.16.4.2. in aanhangsel C
2	HAZOP-rapport R_X	Remcurven (dat wil zeggen rittoestemming) in configuratiegegevens van subsysteem aan boord te permissief	De configuratieprocedure voor het specifieke subsysteem aan boord hangt af van: • de gehanteerde veiligheidsmarges voor het remsysteem van de trein • de aanspreekvertraging van het remsysteem van de trein (hangt rechtstreeks af van de treinlengte, met name voor goederentreinen)	Spoorwegon-derneming	• De systeemeisen juist specificeren in de systeemomschrijving • Voldoende veiligheidsmarges incalculeren voor het remsysteem van de trein in kwestie	Expliciete risico-inschatting	Ja	Beheerst (geëxporteerd naar spoorwegonderne-ming) Zie ook onder C.16.4.2. in aanhangsel C
3	HAZOP-rapport R_X	• Maximumsnelheid van de trein te hoog ingesteld (Vmax) • Remcurven (dat wil zeggen rittoestemming) in configuratiegegevens van subsysteem aan boord te permissief	Het bijwerken van de wieldiameter van de trein in de configuratie van het specifieke subsysteem aan boord is mislukt (onderhoudspersoneel)	Spoorwegon-derneming	• Procedure definiëren om de wieldiameter van de trein te laten meten door het onderhoudspersoneel • Procedure definiëren om de wieldiameter van de trein periodiek bij te werken in het subsysteem aan boord	Expliciete risico-inschatting	Ja	Beheerst (geëxporteerd naar spoorwegonderne-ming) Zie ook onder C.16.4.2. in aanhangsel C
			Fout in procedure van fabrikant voor het voorbereiden en uploaden van de configuratiegegevens in het subsysteem aan boord	Fabrikant	Procedure definiëren om de wieldiameter van de trein bij te werken in de configuratiegegevens aan boord	Expliciete risico-inschatting	Ja	Beheerst via procedure P_X
4	HAZOP-rapport R_X	Trein rijdt op hoge snelheid (160 km/h met baansein "spoor vrij") in het baanvak zonder actief subsysteem aan boord en zonder seinen langs het spoor	Kan alleen worden beheerst door de waakzaamheid van de treinbestuurder. Het binnenrijden van baakvakken die zijn uitgerust met een ATB-systeem langs het spoor hangt af van de bevestigingsprocedure van de treinbestuurder vóór de overgangslocatie. Bevestigt de treinbestuurder niet, dan worden de remmen automatisch in werking gesteld door het besturings- en seingevingssubsysteem aan boord.	Infrastructuur-beheerder	De infrastructuurbeheerder moet zorgen dat treinen die niet beschikken over een actief besturings- en seingevingssubsysteem aan boord het baanvak in kwestie niet binnenrijden. Procedure definiëren voor verkeersleiding	Expliciete risico-inschatting	Ja	Beheerst (geëxporteerd naar infrastructuurbeheer-der) Zie ook onder C.16.4.2. in aanhangsel C

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

Tabel 7: Voorbeeld van een gevareninventaris van de fabrikant voor een besturings- en seingevingssubsysteem aan boord.

Nr. gevaar	Oor-sprong	Gevaaromschrijving	Extra informatie	Verantwoor-delijke actor	Veiligheidsmaatregel	Gebruikt risicoaanvaardingsbegin-sel	Geëxpor-teerd	Status
				Spoorwegonderneming	Treinbestuurder opleiden in procedure om baanvakken binnen te rijden die zijn uitgerust met een ATB-systeem langs het spoor	Expliciete risico-inschatting	Ja	Beheerst (geëxporteerd naar spoorwegonderne-ming) Zie ook onder C.16.4.2. in aanhangsel C
5	HAZOP-rapport R_X	Maximumsnelheid van de trein op het beeldscherm van de treinbestuurder te hoog (Vmax)	De informatie die op de bestuurdersinterface verschijnt wordt gecontroleerd door het besturings- en seingevingssubsysteem aan boord van veiligheidsintegriteitsniveau 4 dat een noodremming inzet wanneer de weergegeven waarde verschilt van de verwachte waarde. Wordt de rittoestemming niet nageleefd, dan zet het besturings- en seingevingssysteem aan boord een noodremming in	Fabrikant	Besturings- en seingevingssubsysteem aan boord van veiligheidsintegriteitsniveau 4 ontwikkelen	Expliciete risico-inschatting	Ja	Veiligheidsbewijs ter staving dat een subsysteem van veiligheidsintegriteits-niveau 4 werd beoordeeld door een onafhankelijke veiligheidsbeoorde-laar
6	HAZOP-rapport R_X	Trein vertrekt zonder bestuurdersinterface	Verlies van redundante architectuur van het subsysteem aan boord	Fabrikant	Besturings- en seingevingssubsysteem aan boord van veiligheidsintegriteitsniveau 4 ontwikkelen	Expliciete risico-inschatting	Ja	Veiligheidsbewijs ter staving dat een subsysteem van veiligheidsintegriteits-niveau 4 werd beoordeeld door een onafhankelijke veiligheidsbeoorde-laar
enzovoort.								

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

C.16.4. Voorbeeld van gevareninventaris doorgifte van informatie aan andere actoren

C.16.4.1 Het voorbeeld in dit punt toont aan hoe de onderkende gevaren en daarmee samenhangende veiligheidsmaatregelen die de betrokken actor niet ten uitvoer kan leggen via een gevareninventaris aan andere actoren worden doorgegeven. Zie onder 4.1 in punt 4.1.1.
Dit voorbeeld komt overeen met het voorbeeld onder C.16.3. in aanhangsel C. Het enige verschil is dat hier alle interne gevaren en veiligheidsmaatregelen zijn weggelaten die de betrokken actor wel heeft kunnen beheersen.

C.16.4.2. De laatste kolom in Tabel 8 is bedoeld om te voldoen aan het vereiste in punt 4.2, van de CSM-verordening. Hiervoor zijn verschillende oplossingen mogelijk. Zo kan worden verwezen naar het bewijsmateriaal dat wordt gebruikt door de actor die de geëxporteerde veiligheidsinformatie ontvangt. Andere mogelijkheid is een vergadering tussen beide actoren om in onderling overleg de passende oplossing te vinden ter beheersing van de bijbehorende risico's. De uitkomsten van deze vergaderingen kunnen worden opgenomen in een overeengekomen document (bijvoorbeeld de notulen). De actor die de veiligheidsgerelateerde informatie exporteert kan aan dit document refereren om de desbetreffende gevaren in zijn gevareninventaris als afgehandeld aan te merken.

Tabel 8: Voorbeeld van gevareninventaris voor doorgifte van veiligheidsgerelateerde informatie aan andere actoren.

Nr. gevaar	Oorsprong gevaar		Gevaaromschrijving	Extra informatie	Verantwoordelijke actor	Veiligheidsmaatregel	Opmerkingen ontvanger
	Nr. in Tabel 7	Overige					
1	Nr.1	HAZOP-rapport R_X	Maximumsnelheid van de trein te hoog ingesteld (Vmax)	Onjuiste configuratie van het specifieke subsysteem aan boord (onderhoudspersoneel) Onjuiste gegevensinvoer aan boord (treinbestuurder)	Spoorwegonderneming	• Procedure definiëren om de configuratiegegevens van het subsysteem aan boord goed te keuren • Operationele procedure definiëren voor gegevensinvoer door de treinbestuurder	• De configuratiegegevens van het besturings- en seingevingssubsysteem aan boord hangen af van de fysieke eigenschappen van het rollend materieel • Vervolgens worden veiligheidsmarges op deze gegevens toegepast in onderling overleg tussen de infrastructuurbeheerder en de spoorwegonderneming • Deze gegevens worden dan geüpload in het subsysteem aan boord overeenkomstig de adequate procedure van de fabrikant tijdens de installatie, integratie in het rollend materieel en goedkeuring van het besturings- en seingevingssubsysteem • De treinbestuurders worden opgeleid en geëvalueerd volgens procedure D_P • Treinbestuurders worden ook door de infrastructuurbeheerder geëvalueerd op basis van de voorschriften die voor diens infrastructuur gelden
2	Nr.2	HAZOP-rapport R_X	Remcurven (dat wil zeggen rittoestemming) in configuratiegege-	De configuratieprocedure voor het specifieke subsysteem aan boord hangt af van: • de gehanteerde	Spoorwegonderneming	• De systeemeisen juist specificeren in de systeemomschrijving • Voldoende	Zie opmerking bij regel 1 hierboven.

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

Tabel 8: Voorbeeld van gevareninventaris voor doorgifte van veiligheidsgerelateerde informatie aan andere actoren.

Nr. gevaar	Oorsprong gevaar		Gevaaromschrijving	Extra informatie	Verantwoordelijke actor	Veiligheidsmaatregel	Opmerkingen ontvanger
	Nr. in Tabel 7	Overige					
			vens van subsysteem aan boord te permissief	veiligheidsmarges voor het remsysteem van de trein • de aanspreekvertraging van het remsysteem van de trein (hangt rechtstreeks af van de treinlengte, met name voor goederentreinen)		veiligheidsmarges incalculeren voor het remsysteem van de trein in kwestie	
3	Nr.3	HAZOP-rapport R_X	• Maximumsnelheid van de trein te hoog ingesteld (Vmax) • Remcurven (dat wil zeggen rittoestemming) in configuratiege-gevens van subsysteem aan boord te permissief	Het bijwerken van de wieldiameter van de trein in de configuratie van het specifieke subsysteem aan boord is mislukt (onderhoudspersoneel)	Spoorwegon-derneming	• Procedure definiëren om de wieldiameter van de trein te laten meten door het onderhoudspersoneel • Procedure definiëren om de wieldiameter van de trein periodiek bij te werken in het subsysteem aan boord	• Het besturings- en seingevingssubsysteem aan boord moet worden onderhouden overeenkomstig de "Onderhoudsprocedure MP_Z" • De wieldiameter van de trein wordt met vaste tussentijden bijgewerkt volgens procedure P_W • Wat betreft de gegevensinvoer worden de treinbestuurders opgeleid en geëvalueerd volgens "Procedure P_{DE}"
4	Nr.4	HAZOP-rapport R_X	Trein rijdt op hoge snelheid (160 km/h met baansein "spoor vrij") in het baanvak zonder actief subsysteem aan boord en zonder seinen langs het spoor	Kan alleen worden beheerst door de waakzaamheid van de treinbestuurder. Het binnenrijden van baanvakken die zijn uitgerust met een ATB-systeem langs het spoor hangt af van de bevestigingsprocedure van de treinbestuurder vóór de overgangslocatie. Bevestigt de treinbestuurder niet, dan worden de treinremmen automatisch in werking gesteld door het besturings- en seingevingssysteem aan boord.	Infrastructuur-beheerder	De infrastructuurbeheerder moet zorgen dat treinen die niet beschikken over een actief besturings- en seingevingssubsysteem aan boord het baanvak in kwestie niet binnenrijden. Procedure definiëren voor verkeersleiding	De verkeersleiding op de infrastructuur van de infrastructuurbeheerder wordt bepaald door het geheel van regels R_{TM}
					Spoorwegon-derneming	Treinbestuurder opleiden in procedure om baanvakken binnen te rijden die zijn uitgerust met een ATB-	• De treinbestuurders worden periodiek opgeleid in de procedure van de infrastructuurbeheerder P_{IM_DP} • Treinbestuurders worden ook door de infrastructuurbeheerder geëvalueerd op basis van het geheel van regels (S_R) dat voor diens

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

Tabel 8: Voorbeeld van gevareninventaris voor doorgifte van veiligheidsgerelateerde informatie aan andere actoren.

Nr. gevaar	Oorsprong gevaar		Gevaaromschrijving	Extra informatie	Verantwoordelijke actor	Veiligheidsmaatregel	Opmerkingen ontvanger
	Nr. in Tabel 7	Overige					
						systeem langs het spoor	infrastructuur geldt
enzo voort.							

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

C.17. Voorbeeld van een algemene gevarenlijst voor spoorwegactiviteiten

C.17.1. ROSA (Rail Optimisation Safety Analysis) is een project dat kadert in DEUFRAKO (Frans-Duitse samenwerking) en beoogt een algemene en alomvattende gevarenlijst samen te stellen voor standaardspoorwegactiviteiten. Doel en uitdaging van dit project bestond erin deze gevaren met een zo groot mogelijk detailleringsniveau te definiëren zonder de bijzonderheden van het Franse en Duits spoor daarbij tot uitdrukking te laten komen. De lijst werd opgesteld met gebruikmaking van bestaande gevarenlijsten uit beide landen (SNCF en DB), en werd kruiselings gecontroleerd met gevarenlijsten uit andere landen. Ook al was het doel een alomvattende en algemene gevarenlijst samen te stellen, de onderstaande lijst geldt uitsluitend als indicatief voorbeeld ter ondersteuning van de actoren die gevaren voor een specifiek project in kaart moeten brengen. De in deze lijst genoemde gevaren zullen naar alle waarschijnlijkheid moeten worden verfijnd of aangevuld om projectmatige bijzonderheden tot uitdrukking te laten komen.

C.17.2. De gevaren in de onderstaande ontwerplijst zijn zogenoemde “Starting Point Hazards” (SPH), wat betekent dat de gevolgen en causaliteit voor deze gevaren nog moeten worden geanalyseerd met als doel de veiligheidsmaatregelen/-voorzieningen en veiligheidsvereisten vast te leggen ter beheersing van de gevaren.

C.17.3. Gevarenlijst van het ROSA-project:

SPH 01	Initiële onjuiste bepaling van maximumsnelheid (infrastructuurgebonden)
SPH 02	Onjuiste bepaling van maximumsnelheid (treingebonden)
SPH 03	Onjuiste remafstand/remweg bepaald/onjuist snelheidsprofiel/onjuiste remcurven
SPH 04	Ontoereikende vertraging/snelheidsvermindering (fysieke oorzaken)
SPH 05	Onjuiste/onaangepaste snelheid/beremming (remopdracht)
SPH 06	Onjuiste snelheidsregistratie (onjuiste snelheid van de trein)
SPH 07	Communicatiestoring maximumsnelheid
SPH 08	Trein komt ongewild in beweging (wegloopbeveiliging)
SPH 09	Onjuiste rijrichting/opzettelijk achteruitrijden - (combinatie van SPH 08 en SPH 14)
SPH 10	Onjuiste absolute/relatieve plaatsbepaling geregistreerd
SPH 11	Fout in treindetectie
SPH 12	Verlies van treinintegriteit
SPH 13	Mogelijk onjuiste rijweg voor trein (afwijking van de route)
SPH 14	Fout in transmissie/communicatie van dienstregeling/rittoestemming
SPH 15	Gebreken in geleidingsconstructie (leibaan)
SPH 16	Defect onderdeel wissel
SPH 17	Onjuiste wisselbediening
SPH 18	Onjuiste wisselstand
SPH 19	Systeemeigen voorwerp op leibaan/in vrijeruimteprofiel (uitgezonderd ballast)
SPH 20	Vreemd voorwerp op leibaan/in vrijeruimteprofiel
SPH 21	Weggebruiker op overweg
SPH 22	Slipstreameffect (zuigeffect) op ballast
SPH 23	Inwerking van aerodynamische krachten op trein
SPH 24	Indringing van treinapparatuur/element/lading in vrijeruimteprofiel van trein
SPH 25	Onaangepaste afmeting van vrijeruimteprofiel voor trein (langs het spoor)
SPH 26	Onjuiste lastverdeling
SPH 27	Wielbreuk, asbreuk
SPH 28	Oververhitting as/wiel/lager
SPH 29	Defect draaistel/ophanging, dempinrichting

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

SPH 30	Defect voertuigonderstel/wagenbak
SPH 31	Toegang tot verboden terrein door onbevoegden (veiligheidsaspect)
SPH 32	Bevoegde persoon steekt het spoor over
SPH 33	Personeel aan het werk op het spoor
SPH 34	Onbevoegde dringt het spoor binnen (onachtzaamheid)
SPH 35	Persoon valt van perronrand op het spoor
SPH 36	Slipstream (zuigeffect)/persoon staat te dicht bij perronrand
SPH 37	Personeel aan het werk bij het spoor, bijvoorbeeld naastliggend spoor (nevenspoor)
SPH 38	Persoon verlaat opzettelijk de trein (uitgezonderd overstap van passagiers)
SPH 39	Persoon valt uit (zij)deur
SPH 40	Persoon valt uit kopwanddeur
SPH 41	Trein vertrekt/komt in beweging met geopende deuren (zonder indringing vrijeruimteprofiel)
SPH 42	Persoon valt in doorgang tussen twee rijtuigen met overloop-/overgangsbruggen
SPH 43	Passagier leunt uit de deur
SPH 44	Passagier leunt uit het venster
SPH 45	Treinbediende/conducteur leunt uit de deur
SPH 46	Treinbediende/conducteur leunt uit het venster
SPH 47	Rangeerder leunt naar buiten vanaf opstaptrede
SPH 48	Persoon valt/klimt van perron in ruimte tussen voertuig en perron (instapspleet)
SPH 49	Persoon valt uit/verlaat trein zonder aanwezigheid van perron
SPH 50	Persoon valt in deuropening tijdens overstap van passagiers
SPH 51	Treindeuren gaan dicht terwijl iemand in deuropening staat
SPH 52	Trein komt in beweging tijdens overstap van passagiers
SPH 53	Mogelijke gewonde in trein
SPH 54	Brand-/explosiegevaar (in/bij trein) - ongevalscategorie, gevolg van SPH 55, SPH 56)
SPH 55	Onaangepaste temperatuur (in trein)
SPH 56	Vergiftiging/verstikking (in/bij trein)
SPH 57	Elektrocutie (in/bij trein)
SPH 58	Persoon komt ten val op het perron (uitgezonderd overstap van passagiers)
SPH 59	Onaangepaste temperatuur (op perron)
SPH 60	Vergiftiging/verstikking (op perron)
SPH 61	Elektrocutie (op perron)

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