Europeiska järnvägsbyrån	
Exempelsamling av riskbedömningar och några tänkbara verktyg som stöder förordningen om en gemensam säkerhetsmetod	
Referens hos ERA:	ERA/GUI/02-2008/SAF
Version hos ERA:	1.1
Datum:	6.1.2009

Dokumentet har utarbetats av:	Europeiska järnvägsbyrån Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Frankrike
Typ av dokument:	Vägledning
Dokumentstatus:	Offentlig

	Namn	**Befattning**
Utlagt av	Marcel Verslype	Verkställande direktör
Granskat av	Anders Lundström Thierry Breyne	Chef för enheten Säkerhet Chef för området Säkerhetsbedömning
Skrivet av (författare)	Dragan Jovicic	Enheten Säkerhet – projekthandläggare

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

DOKUMENTINFORMATION

Ändringshistorik

Tabell 1: Dokumentstatus.

Version Datum	Författare	Avsnitts-nummer	Beskrivning av ändringen
Det gamla dokumentets titel och struktur: *”Vägledning för användning av rekommendationen om den första uppsättningen gemensamma säkerhetsmetoder”*			
Vägledning version 0.1 15.2.2007	Dragan Jovicic	Alla	Den första versionen av ”Vägledning för användning” som hör samman med version 1.0 av ”rekommendationen om den första uppsättningen gemensamma säkerhetsmetoder”. Detta är också den första versionen av det dokument som skickades för en formell granskning till arbetsgruppen för gemensamma säkerhetsmetoder.
Vägledning version 0.2 7.6.2007	Dragan Jovicic	Alla	Omorganisation av dokumentet för att matcha strukturen för version 4.0 av rekommendationen om gemensamma säkerhetsmetoder. Uppdatering enligt det formella granskningsförfarande av version 1.0 av rekommendationen som arbetsgruppen för gemensamma säkerhetsmetoder har genomfört.
		Alla	Uppdatering av dokumentet med ytterligare information som samlats in under internmötena på ERA, och enligt begäran från expertgruppen och arbetsgruppen för gemensamma säkerhetsmetoder om att ta fram nya punkter.
		Figur 1	Ändring av figuren som åskådliggör ”ramverket för riskhantering för den första uppsättningen gemensamma säkerhetsmetoder” i enlighet med synpunkterna från granskningen och ISO-terminologin.
Vägledning version 0.3 20.7.2007	Dragan Jovicic	Tillägg	Omorganisation och framtagning av nya tillägg. Nytt tillägg för att samla ihop alla diagram som åskådliggör och underlättar läsningen och förståelsen av vägledningen.
		Alla avsnitt	Dokumentet uppdaterat för att • utveckla befintliga x avsnitt i största möjliga utsträckning, • vidareutveckla vad som menas med ”påvisande av att systemet uppfyller säkerhetskraven”, • koppla samman med Cenelecs V-modell (dvs. figur 8 och figur 10 i EN 50126), • vidareutveckla behovet av samarbete och samordning mellan olika aktörer inom järnvägssektorn vars verksamheter kan påverka järnvägssystemets säkerhet, • göra ett förtydligande om den dokumentation (t.ex. protokoll om faror och säkerhetsbevisning) som förväntas påvisa för bedömningsorganen att riskbedömningsförfarandet för den gemensamma säkerhetsmetoden har tillämpats korrekt. Dokumentet har också uppdaterats i enlighet med byråns första interna granskning.
Vägledning version 0.4 16.11.2007	Dragan Jovicic	Alla avsnitt	Dokumentet har uppdaterats efter det formella granskningsförfarandet i enlighet med de synpunkter som har mottagits om version 0.3 från följande medlemmar av arbetsgruppen för gemensamma säkerhetsmetoder eller organisationer, och som har godkänts i samråd med dem via telefonsamtal: • Den nationella säkerhetsmyndigheten (NSA) i Belgien, Spanien, Finland, Norge, Frankrike och Danmark. • Siemens (medlem i Unife). • Den norska infrastrukturförvaltaren (Jernbaneverket – EIM-medlem).
Vägledning version 0.5 27.2.2008	Dragan Jovicic	Alla avsnitt	Dokumentet har uppdaterats enligt de synpunkter som har mottagits om version 0.3 från följande medlemmar av arbetsgruppen för gemensamma säkerhetsmetoder eller organisationer, och som har

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

Tabell 1: Dokumentstatus.

Version Datum	Författare	Avsnitts-nummer	Beskrivning av ändringen
			godkänts i samråd med dem via telefonsamtal: • CER • Den nationella säkerhetsmyndigheten i Nederländerna
		Alla avsnitt	Dokumentet har uppdaterats i överensstämmelse med den undertecknade versionen av rekommendationen om gemensamma säkerhetsmetoder. Dokumentet har uppdaterats i enlighet med de synpunkter som har framkommit i byråns interna granskning, från Christophe Cassir och Marcus Andersson.
		Alla avsnitt Tillägg	Fullständig omnumrering av avsnitten i dokumentet i enlighet med rekommendationen. Exempel på tillämpning av rekommendationen om gemensamma säkerhetsmetoder har bifogats.
Det nya dokumentets titel och struktur: *”Exempelsamling av riskbedömningar och några tänkbara verktyg som stöder förordningen om en gemensam säkerhetsmetod”*			
Vägledning version 0.1 23.5.2008	Dragan Jovicic	Alla	Första versionen av dokumentet efter uppdelning av ”Vägledning för användning” version 0.5 i två kompletterande dokument.
Vägledning version 0.2 3.9.2008	Dragan Jovicic	Alla	Uppdatering av dokumentet i överensstämmelse med • Europeiska kommissionens förordning om en gemensam säkerhetsmetod {ref. 3}, • synpunkter från workshopen den 1 juli 2008 med medlemmar från RISC (Railway Interoperability and Safety Committee), • synpunkter från medlemmarna i arbetsgruppen för gemensamma säkerhetsmetoder (den nationella säkerhetsmyndigheten i Norge, Finland, Storbritannien respektive Frankrike, CER, EIM, Jens Braband [Unife] och Stéphane Romei [Unife]).
Vägledning version 1.0 10.12.2008	Dragan Jovicic	Alla	Uppdatering av dokumentet i enlighet med Europeiska kommissionens förordning om en gemensam säkerhetsmetod om riskvärdering och riskbedömning {ref. 3} som har antagits av RISC (Railway Interoperability and Safety Committee) under dess plenarmöte den 25 november 2008.
Vägledning version 1.1 6.1.2009	Dragan Jovicic	Alla	Dokumentet har uppdaterats i enlighet med de synpunkter som Europeiska kommissionens jurist- och språktjänster har lämnat om förordningen om en gemensam säkerhetsmetod.

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

Innehåll

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

Förteckning över figurer

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

Förteckning över tabeller

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

0. INLEDNING

0.1. Tillämpningsområde

0.1.1. Syftet med detta dokument är att ytterligare förtydliga ”Kommissionens förordning om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning som avses i artikel 6.3 a i Europaparlamentets och rådets direktiv 2004/49/EG” {ref. 3}. Denna förordning kommer fortsättningsvis att kallas *förordningen om en gemensam säkerhetsmeto*d i detta dokument.

0.1.2. Detta dokument är inte rättsligt bindande och dess innehåll får inte tolkas som det enda sättet att uppfylla kraven enligt den gemensamma säkerhetsmetoden. Detta dokument syftar till att komplettera vägledningen om tillämpningen av förordningen om en gemensam säkerhetsmetod {ref. 4} när det gäller hur processen i förordningen om en gemensam säkerhetsmetod skulle kunna användas och tillämpas. Den ger ytterligare praktisk information utan att på något sätt föreskriva obligatoriska förfaranden som måste följas och utan att upprätta någon rättsligt bindande praxis. Denna information kan vara till nytta för alla aktörer ([1]) vars verksamheter kan ha en inverkan på järnvägssystemens säkerhet och som har ett direkt eller indirekt behov av att tillämpa förordningen om en gemensam säkerhetsmetod. Dokumentet ger exempel på riskbedömningar och några tänkbara verktyg som stöder tillämpningen av den gemensamma säkerhetsmetoden. Dessa exempel utgör enbart råd och stöd. Aktörerna kan använda alternativa metoder eller fortsätta använda sina egen befintliga metoder och verktyg för att uppfylla kraven i den gemensamma säkerhetsmetoden, om de anser att dessa är lämpligare.
Exemplen och den ytterligare information som ges i detta dokument är inte uttömmande och omfattar inte heller alla möjliga situationer för vilka betydande ändringar föreslås, dvs. dokumentet kan endast betraktas som rent informativt.

0.1.3. Detta informativa dokument ska enbart läsas som ett ytterligare stöd vid tillämpningen av förordningen om en gemensam säkerhetsmetod. När det används ska dokumentet läsas tillsammans med förordningen om en gemensam säkerhetsmetod {ref. 3} och den tillhörande vägledningen {ref. 4} för att ytterligare underlätta tillämpningen av förordningen om en gemensam säkerhetsmetod. Dokumentet ersätter inte förordningen.

0.1.4. Dokumentet har tagits fram av Europeiska järnvägsbyrån (ERA) med stöd från experterna från järnvägsorganisationer och nationella säkerhetsmyndigheter i arbetsgruppen för gemensamma säkerhetsmetoder. Den utgör en utexperimenterad samling idéer och information som byrån har samlat in under interna möten och möten med arbetsgruppen och expertgrupperna för gemensamma säkerhetsmetoder. Vid behov kommer ERA att granska och uppdatera dokumentet så att det återspeglar de europeiska standardernas utveckling, ändringarna av den gemensamma säkerhetsmetoden för riskbedömning och erfarenheterna från användningen av förordningen om en gemensam säkerhetsmetod. Eftersom det inte är möjligt att ange en tidsplan för denna revideringsprocess i skrivande stund hänvisas läsaren till Europeiska järnvägsbyrån för information om den senast tillgängliga utgåvan av dokumentet.

([1]) *De berörda aktörerna är de upphandlande enheterna enligt definitionen i artikel 2 r i direktiv 2008/57/EG om driftskompatibiliteten hos järnvägssystemet inom gemenskapen, eller tillverkarna, som alla går under beteckningen ”förslagsställare” i förordningen, eller deras leverantörer och tjänsteleverantörer.*

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

0.2. Utanför tillämpningsområdet

0.2.1. Dokumentet innehåller ingen information om hur ett järnvägssystem eller delar av det ska organiseras, användas eller konstrueras (och tillverkas). Här definieras inte heller några avtalsmässiga överenskommelser eller uppgörelser som kan finnas mellan vissa aktörer för tillämpningen av riskhanteringsprocessen. De projektspecifika avtalsmässiga uppgörelserna faller utanför förordningen om en gemensam säkerhetsmetod samt den tillhörande vägledningen och det aktuella dokumentet.

0.2.2. Även om det ligger utanför dokumentets tillämpningsområde kan överenskommelser mellan de berörda aktörerna skrivas ned i de relevanta avtalen i början av projektet, dock utan att det påverkar bestämmelserna i den gemensamma säkerhetsmetoden. Detta kan till exempel omfatta

(a) kostnader som hör samman med hanteringen av säkerhetsrelaterade risker vid kontaktpunkterna mellan aktörerna,
(b) kostnader som hör samman med överföringen av faror och tillhörande säkerhetsåtgärder mellan aktörerna som inte är kända i början av projektet,
(c) hur konflikter som kan uppstå under projektet ska hanteras,
(d) etc.

Om en tvist eller konflikt skulle uppstå mellan förslagsställaren och dennes underleverantörer under projektets gång, kan hänvisning ske till de relevanta avtalen för att försöka lösa konflikten.

0.3. Principer för detta dokument

0.3.1. Även om detta dokument kan förefalla vara ett dokument som kan läsas fristående ersätter det inte förordningen om en gemensam säkerhetsmetod {ref. 3}. Av praktiska skäl har texten i varje artikel i förordningen om en gemensam säkerhetsmetod kopierats till detta dokument. Vid behov har den relevanta artikeln på förhand förklarats i vägledningen om tillämpningen av förordningen om en gemensam säkerhetsmetod {ref. 4}. Avsnitten som följer innehåller därefter ytterligare information i de fall då det anses nödvändigt för att underlätta förståelsen för förordningen om en gemensam säkerhetsmetod.

0.3.2. Artiklarna respektive avsnitten från förordningen om en gemensam säkerhetsmetod har kopierats in i textrutor i detta dokument och formaterats med kursivt teckensnitt av typen "Bookman Old Style", precis som i denna text. Denna formatering gör det lätt att se skillnad mellan den ursprungliga texten från förordningen om en gemensam säkerhetsmetod {ref. 3} och de ytterligare förklaringarna som ges i detta dokument. Texten från vägledningen om tillämpningen av förordningen om en gemensam säkerhetsmetod {ref. 4} har inte kopierats till detta dokument.

0.3.3. För att underlätta för läsaren motsvarar strukturen i detta dokument strukturen i förordningen om en gemensam säkerhetsmetod och den tillhörande vägledningen.

0.4. Dokumentbeskrivning

0.4.1. Detta dokument är indelat i följande avsnitt:

(a) Kapitel 0. som definierar dokumentets tillämpningsområde och innehåller en förteckning över referensdokument.

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

(b) Bilaga I och bilaga II som ger ytterligare information om motsvarande avsnitt i förordningen om en gemensam säkerhetsmetod {ref. 3} och den tillhörande vägledningen {ref. 4}.
(c) Nya tillägg som ytterligare utvecklar några specifika aspekter och innehåller exempel.

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

0.5. Referensdokument

Tabell 2: Tabell över referensdokument.

{Ref. nr}	Titel	Referens	Version
{ref. 1}	Europaparlamentets och rådets direktiv 2004/49/EG av den 29 april 2004 om säkerhet på gemenskapens järnvägar och om ändring av rådets direktiv 95/18/EG om tillstånd för järnvägsföretag och direktiv 2001/14/EG om tilldelning av infrastrukturkapacitet, uttag av avgifter för utnyttjande av järnvägsinfrastruktur och utfärdande av säkerhetsintyg (järnvägssäkerhetsdirektivet)	2004/49/EG EUT L 164, 30.4.2004 s. 44, rättelse i EUT L 220, 21.6.2004, s. 16.	-
{ref. 2}	Europaparlamentets och rådets direktiv 2008/57/EG av den 17 juni 2008 om driftskompatibiliteten hos järnvägssystemet inom gemenskapen	2008/57/EG EUT L 191, 18.7.2008, s. 1.	-
{ref. 3}	Kommissionens förordning (EG) nr …/… av den […] om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning som avses i artikel 6.3 a i Europaparlamentets och rådets direktiv 2004/49/EG	xxxx/yy/EG	Antagen av RISC 25.11.2008
{ref. 4}	Vägledning om tillämpningen av kommissionens förordning om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning som avses i artikel 6.3 i järnvägssäkerhetsdirektivet	ERA/GUI/01-2008/SAF	1.0
{ref. 5}	Europaparlamentets och rådets direktiv 2008/57/EG av den 17 juni 2008 om driftskompatibiliteten hos järnvägssystemet inom gemenskapen	2008/57/EG EUT L 191, 18.7.2008, s. 1.	-
{ref. 6}	Säkerhetssystem – Bedömningskriterier för järnvägsföretag och infrastrukturförvaltare	Bedömningskriterier för säkerhetsstyrningssystem Del A – Säkerhetsintyg och säkerhetstillstånd	31.5.2007
{ref. 7}	Järnvägsanläggningar – Dataöverföring och järnvägsstyrning – Elektroniska signalsystem av betydelse för säkerheten	EN 50129	Februari 2003
{ref. 8}	Järnvägsanläggningar – Specifikation av tillförlitlighet, funktionssannolikhet, driftsäkerhet, tillgänglighet, underhållsmässighet och säkerhet (RAMS) – Del 1: Själva standarden	EN 50126-1	September 2006
{ref. 9}	Järnvägsanläggningar – Specifikation av tillförlitlighet, funktionssannolikhet, driftsäkerhet, tillgänglighet, underhållsmässighet och säkerhet (RAMS) – Del 2: Vägledning vid tillämpning av EN 50126-1 i frågor som gäller säkerhet	EN 50126-2 (Vägledning)	Slutligt utkast (augusti 2006)
{ref. 10}	Generic Guideline for the Calculation of Risk inherent in the Carriage of Dangerous Goods by Rail (allmänna riktlinjer för att beräkna risker i samband med järnvägstransport av farligt gods)	Otif-riktlinjer godkända av RID:s expertkommitté	24.11.2005
{ref. 11}	Kriterium för riskacceptans för tekniska system	Anmärkning 01/08	1.1 (25.1.2008)
{ref. 12}	ERA:s säkerhetsenhet: Genomförbarhetsstudie – ”Apportionment of safety targets (to TSI sub-systems) and consolidation of TSI from a safety point of view” WP1.1 – Bedömning av möjligheten att tilldela gemensamma säkerhetsmål	WP1.1	1.0
{ref. 13}	”Järnvägar – Klassificeringssystem för järnvägsfordon – Del 4: EN 15380 Del 4: Funktionsgrupper”.	EN 15380 Del 4	

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

0.6. Standarddefinitioner, termer och förkortningar

0.6.1. Allmänna definitioner, termer och förkortningar som används i detta dokument kan slås upp i en normal ordbok.

0.6.2. Nya definitioner, termer och förkortningar som används i denna vägledning finns definierade i avsnitten nedan.

0.7. Specifika definitioner

0.7.1. Se artikel 3

0.8. Specifika termer och förkortningar

0.8.1. I detta avsnitt definieras nya specifika termer och förkortningar som används ofta i detta dokument.

Tabell 3: Tabell över termer.

Term	Definition
byrån	Europeiska järnvägsbyrån (ERA)
vägledning	Den aktuella ”Vägledningen om tillämpningen av kommissionens förordning (EG) nr …/… av den […] om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning som avses i artikel 6.3 a i Europaparlamentets och rådets direktiv 2004/49/EG”
förordningen om en gemensam säkerhetsmetod	”Kommissionens förordning (EG) nr …/… av den […] om antagande av en gemensam säkerhetsmetod för riskvärdering och riskbedömning som avses i artikel 6.3 a i Europaparlamentets och rådets direktiv 2004/49/EG” {ref. 3}

Tabell 4: Tabell över förkortningar.

Förkortning	Innebörd
CCS	Trafikstyrning och signalering
CSM	Gemensam(ma) säkerhetsmetod(er)
CST	Gemensamma säkerhetsmål
EC	Europeiska kommissionen
ERA	Europeiska järnvägsbyrån
IM	Infrastrukturförvaltare
ISA	Oberoende säkerhetsbedömare
Otif	Mellanstatliga organisationen för internationell järnvägstrafik
MS	Medlemsstat
NOBO	Anmält organ
NSA	Nationell säkerhetsmyndighet
QMP	Kvalitetsstyrningsprocess
QMS	Kvalitetsstyrningssystem
RISC	Railway Interoperability and Safety Committee
RU	Järnvägsföretag
SMP	Säkerhetsstyrningsprocess
SMS	Säkerhetsstyrningssystem
SRT	Säkerhet i järnvägstunnlar
TBC	Kommer att kompletteras

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

Tabell 4: Tabell över förkortningar.

Förkortning	Innebörd
TSD	Tekniska specifikationer för driftskompatibilitet

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

FÖRKLARING AV ARTIKLARNA I FÖRORDNINGEN OM EN GEMENSAM SÄKERHETSMETOD

Artikel 1. Syfte

Artikel 1.1

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 1.2

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

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

[G 2] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 2. Tillämpningsområde

Artikel 2.1

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

[G 1] Den gemensamma säkerhetsmetoden gäller hela järnvägssystemet och omfattar bedömning av följande ändringar i järnvägssystem om de bedöms vara betydande vid tillämpningen av artikel 4:

(a) Byggande av nya linjer eller ändringar av befintliga linjer.
(b) Införande av nya och/eller ändrade tekniska system.

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

(c) Driftsrelaterade ändringar (såsom nya eller modifierade driftsregler och underhållsrutiner).
(d) Ändringar i järnvägsföretagens/infrastrukturförvaltarnas organisationer.

Termen ”system” hänför sig i den gemensamma säkerhetsmetoden till alla aspekter av ett system, inklusive bland annat dess utveckling, drift, underhåll etc. fram tills avveckling eller bortskaffande sker.

[G 2] Den gemensamma säkerhetsmetoden omfattar betydande ändringar av både

(a) ”små och enkla” system som kan bestå av några få tekniska delsystem eller element, och
(b) ”stora och mer komplexa” system (som t.ex. kan omfatta stationer och tunnlar).

Artikel 2.2

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

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

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

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

[G 1] Exempelvis måste, i överensstämmelse med järnvägssäkerhetsdirektivet {ref. 1} och direktivet för driftskompatibilitet för järnvägar {ref. 2}, en ny typ av rullande materiel för en höghastighetslinje uppfylla kraven i TSD:n för rullande materiel för höghastighetståg. Även om merparten av det system som är föremål för bedömning omfattas av TSD:n ingår inte den viktiga frågan beträffande den mänskliga faktorn som hänför sig till förarhytten. För att säkerställa att alla rimligen förutsägbara faror som hör samman med den mänskliga faktorn (dvs. kontaktpunkterna mellan föraren, den rullande materielen och resten av järnvägssystemet) identifieras och kontrolleras på ett adekvat sätt ska processen enligt den gemensamma säkerhetsmetoden användas.

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

Artikel 2.3

This Regulation shall not apply to:

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 2.4

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 3. Definitioner

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 Artikel 5.2;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

([2]) *EGT L 235, 17.9.1996, s. 6.*

([3]) *EGT L 110, 20.4.2001, s. 1.*

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 4. Betydande ändringar

Artikel 4.1

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

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

[G 1] Det är förslagsställarens ansvar att fatta beslut om detta, om det inte finns någon anmäld nationell bestämmelse. Betydelsen av ändringen baseras på en expertbedömning. Om till exempel den planerade ändringen av ett befintligt system är komplex kan den bedömas som betydande om risken för att den påverkar befintliga funktioner ([4]) i systemet är hög, även om ändringen i sig inte nödvändigtvis är säkerhetsrelaterad i någon högre grad.

Artikel 4.2

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

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

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

(c) complexity of the change;

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

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

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

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Exempel på små ändringar:** En ökning av den maximala linjehastigheten en gång med 5 km/h, efter att systemet har tagits i bruk, är inte betydande. Om man emellertid fortsätter att öka den maximala linjehastigheten i steg om 5 km/h kan summan av de successiva ändringarna (som individuellt bedöms vara icke betydande ändringar) bli en betydande ändring med avseende på systemets ursprungliga säkerhetskrav.

([4]) *Eftersom funktionerna i ett system inte alltid är oberoende av varandra, kan ändringar av vissa funktioner även påverka andra funktioner i systemet även om det verkar som de inte berörs direkt av ändringarna.*

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

[G 2] För att bedöma om en uppsättning av flera successiva (icke betydande) ändringar är betydande, då de betraktas som helhet, måste alla faror och tillhörande risker som hör samman med alla ändringarna bedömas. Uppsättningen av ändringarna i fråga kan betraktas som icke betydande om den resulterande risken är allmänt godtagbar.

[G 3] I byråns arbete med betydande ändringar har det visat sig att

(a) det inte är möjligt att identifiera harmoniserade gränser eller regler som, för en given förändring, kan användas för att ta beslut om betydelsen av ändringen, och
(b) det inte är möjligt att tillhandahålla en uttömmande lista över betydande ändringar,
(c) beslutet inte kan gälla alla förslagsställare och alla tekniska, driftsrelaterade, organisatoriska och miljömässiga förhållanden.

Det är således viktigt att låta ansvaret att fatta beslut ligga hos förslagsställaren, som i enlighet med artikel 4.3 i järnvägssäkerhetsdirektivet {ref. 1} är ansvarig för en säker drift och riskhanteringen för sin del av systemet.

[G 4] För att hjälpa förslagsställaren finns det ett ”exempel på utvärdering och användning av kriterier” i avsnitt C.2. i tillägg C.

[G 5] Den gemensamma säkerhetsmetoden får inte tillämpas om den säkerhetsrelaterade förändringen inte betraktas som betydande. Trots detta finns det emellertid arbete som måste utföras. För att bestämma om ändringen är betydande har förslagsställaren genomfört någon form av (preliminära) riskanalyser. Dessa riskanalyser, och eventuella motiveringar och synpunkter måste dokumenteras för att göra det möjligt för den nationella säkerhetsmyndigheten att utföra revisioner. Bedömningen av en ändrings betydelse och beslutet om att ändringen inte är betydande behöver inte bedömas av ett oberoende organ.

Artikel 5. Riskhanteringsprocess

Artikel 5.1

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

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 5.2

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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

Artikel 5.3

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 6. Oberoende bedömning

Artikel 6.1

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

[G 1] Vilken grad av oberoende som krävs för bedömningsorganet beror på vilken säkerhetsnivå som krävs för det system som är föremål för bedömning. I väntan på en harmonisering finns den bästa praxisen för detta i IEC 61508-1:2001 punkt 8 eller i avsnitt 5.3.9 i standarden EN 50129 {ref. 7}. Graden av oberoende beror både på allvarlighetsgraden för konsekvensen av den fara som hör samman med utrustningen och nyhetsgraden. I avsnitt 9.7.2 i EN 50126-2 och EN 50129 definieras graden av oberoende för signalsystem. I princip kan detta även användas för andra system.

[G 2] Byrån arbetar fortfarande med definitionen av de olika bedömningsorganens (nationella säkerhetsmyndigheter, anmälda organ och oberoende säkerhetsbedömare) roller och ansvarsområden samt de nödvändiga kontaktpunkterna mellan dem. Arbetet kommer (om det är möjligt) att utmynna i vem bland dessa bedömningsorgan som ska göra vad och på vilket sätt detta ska ske. Detta kommer slutligen att göra det möjligt att definiera

(a) hur man, på grundval av bevisning, ska kontrollera om riskhanterings- och riskbedömningsprocesserna som omfattas av den gemensamma säkerhetsmetoden tillämpas korrekt, och
(b) hur man ska stödja förslagsställaren i dennes beslut att godkänna den betydande ändringen i det system som är föremål för bedömning.

Artikel 6.2

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

[G 1] Ytterligare information kommer att framkomma som ett resultat av byråns arbete med bedömningsorganens roller och användningsområden.

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

Artikel 6.3

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

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

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

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

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

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

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 6.4

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 7. Säkerhetsbedömningsrapporter

Artikel 7.1

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 7.2

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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

Artikel 7.3

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 7.4

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

[G 1] Denna princip om ömsesidigt erkännande är redan godkänd enligt Cenelec-standarderna: se avsnitt 5.5.2 i EN 50129 och avsnitt 5.9 i EN 50126-2. I Cenelec tillämpas principen om korsacceptans eller ömsesidigt erkännande av förslagsställare eller oberoende säkerhetsbedömare på generiska produkter och generiska tillämpningar ([5]) under förutsättning att säkerhetsbedömningen och säkerhetsbevisningen har utförts i enlighet med kraven i Cenelec-standarden.

[G 2] Det ömsesidiga erkännandet måste även tillämpas vid godkännandet av nya eller modifierade system om deras riskbedömning och påvisandet om att systemet uppfyller säkerhetskraven sker i linje med bestämmelserna i förordningen om en gemensam säkerhetsmetod {ref. 3}.

Artikel 8. Styrning av riskhantering/interna och externa revisioner

Artikel 8.1

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

([5]) *Se punkt [G 5] i avsnitt 1.1.5 och fotnoterna ([7]) och ([8]) på sidan 31, och Figur 3 i detta dokument för en närmare förklaring av terminologin ”generisk produkt” och ”generisk tillämpning” och de tillhörande principerna.*

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

Artikel 8.2

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 9. Återkoppling och tekniska framsteg

Artikel 9.1

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 9.2

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 9.3

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 9.4

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

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

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

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 10. Ikraftträdande

Artikel 10.1

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

Artikel 10.2

This Regulation shall apply from 1 July 2012.

However, it shall apply from 19 July 2010:

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

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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

BILAGA I – FÖRKLARING AV PROCESSEN I FÖRORDNINGEN OM EN GEMENSAM SÄKERHETSMETOD

1. ALLMÄNNA PRINCIPER FÖR RISKHANTERINGSPROCESSEN

1.1. Allmänna principer och skyldigheter

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] Ramverket för riskhantering för den gemensamma säkerhetsmetoden och den tillhörande riskbedömningsprocessen åskådliggörs i figur 1. I de fall då det bedöms vara nödvändigt beskrivs varje ruta/aktivitet i denna figur mer ingående i ett särskilt avsnitt i detta dokument.

[G 2] I Cenelec rekommenderas att riskhanterings- och riskbedömningsprocesserna beskrivs i en säkerhetsplan. Om detta inte passar för projektet kan den tillhörande beskrivningen ingå i ett annat relevant dokument. Se avsnitt 1.1.6.

[G 3] Riskbedömningsprocessen utgår från en preliminär systemdefinition. Under projektets gång uppdateras den preliminära systemdefinitionen successivt och ersätts av systemdefinitionen. Om det inte finns någon preliminär systemdefinition används den formella systemdefinitionen för att utföra riskbedömningen. I detta fall är det bra om alla de aktörer som berörs av den betydande ändringen träffas i början av projektet för att

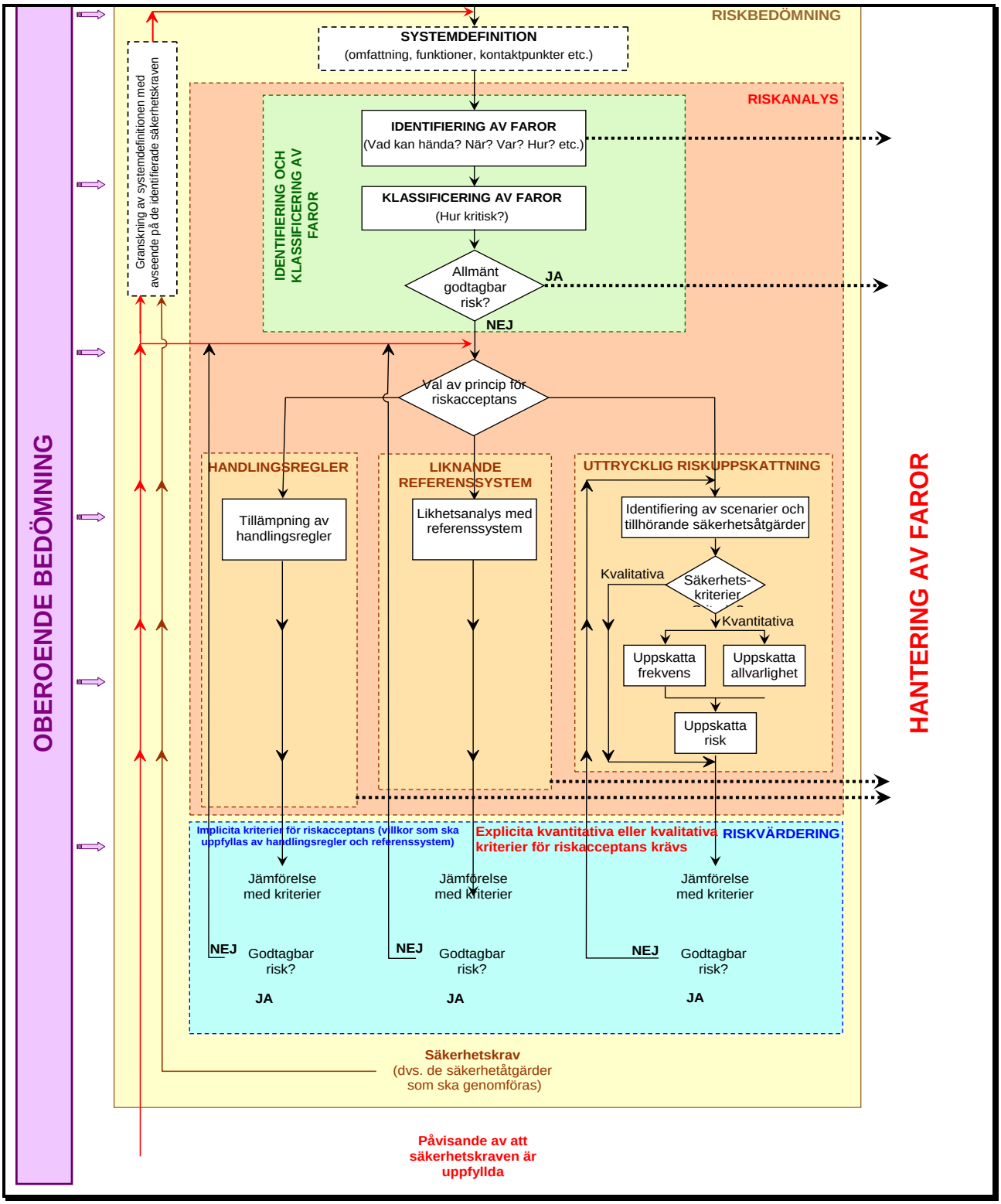
(a) komma överens om de övergripande systemprinciperna, systemfunktionerna etc.; i princip kan detta beskrivas i en preliminär systemdefinition,
(b) komma överens om projektorganisationen,
(c) komma överens om hur rollerna och ansvaret ska fördelas mellan de olika aktörerna som redan är involverade, inklusive de nationella säkerhetsmyndigheterna, de anmälda organen och de oberoende säkerhetsbedömarna där så är relevant.

Sådan samordning under exempelvis den preliminära systemdefinieringen gör det möjligt för förslagsställaren, underleverantörerna, de nationella säkerhetsmyndigheterna, de anmälda

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

organen och de oberoende säkerhetsbedömarna att på ett tidigt stadium, om det behövs, komma överens om handlingsregler eller referenssystem som kan användas inom projektet.

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



Figur 1: Ramverk för riskhantering i förordningen om en gemensam säkerhetsmetod {ref. 3}.

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

1.1.2. This iterative risk management process:

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

[G 1] Järnvägsföretagets och infrastrukturförvaltarens säkerhetsstyrningssystem innehåller den process och de förfaranden som ska

(a) övervaka att systemet fortsätter att vara säkert under hela dess livscykel (dvs. under dess drift och underhåll),
(b) säkerställa en säker demontering eller ersättning av det därtill hörande systemet.

Denna process ingår inte i den gemensamma säkerhetsmetoden om riskbedömning.

[G 2] För att genomföra den gemensamma säkerhetsmetoden måste alla berörda parter vara kompetenta (dvs. ha rätt kompetens, färdigheter och erfarenhet). Det finns ett ständigt behov inom järnvägssektorn av kompetensstyrning i aktörernas organisationer:

(a) För infrastrukturförvaltarna och järnvägsföretagen uppfylls detta krav av deras säkerhetsstyrningssystem i enlighet med bilaga III.2 e i järnvägssäkerhetsdirektivet {ref. 1}.
(b) De andra aktörerna, vars verksamhet kan påverka järnvägssystemets säkerhet, har i allmänhet, även om säkerhetsstyrningssystemet inte är obligatoriskt, åtminstone på projektnivå (se punkt [G 1] i avsnitt 5.1) en kvalitetsstyrningsprocess (QMP) och/eller en säkerhetsstyrningsprocess (SMP) som uppfyller detta krav.

[G 3] I följande avsnitt av Cenelec-standarden EN 50126-1 {ref. 8} finns vägledning om kompetens:

(a) I avsnitt 5.3.5.(b) anges att *all personal med ansvar inom riskhanteringsprocessen måste ha kompetens att fullgöra detta ansvar*.
(b) I avsnitt 5.3.5.(d) anges att kraven gällande riskhanteringen och riskbedömningen måste *genomföras inom affärsprocesser som stöds av ett kvalitetsstyrningssystem (QMS) som uppfyller kraven enligt EN ISO 9001, EN ISO 9002 eller EN ISO 9003 beroende på det system som är föremål för bedömning*. Ett exempel på de aspekter som styrs av kvalitetsstyrningssystemet finns i avsnitt 5.2 i standarden EN 50129 {ref. 7}.

Dessa avsnitt omfattar de kvalitetssäkringsaktiviteter och personalens/personernas kompetens respektive den utbildning som krävs för att stödja processen enligt den gemensamma säkerhetsmetoden.

[G 4] Mycket ofta följs riskbedömningsprocessen upp av ett bedömningsorgan redan från början av projektet, men om detta inte krävs enligt någon nationell lag i medlemsstaten är en sådan tidig inblandning av bedömningsorganet inte obligatorisk, även om det rekommenderas. Synpunkter från det oberoende bedömningsorganet kan vara till nytta innan man går vidare från ett steg i riskbedömningen till ett annat. Närmare information om den oberoende bedömningen finns i artikel 6.

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.

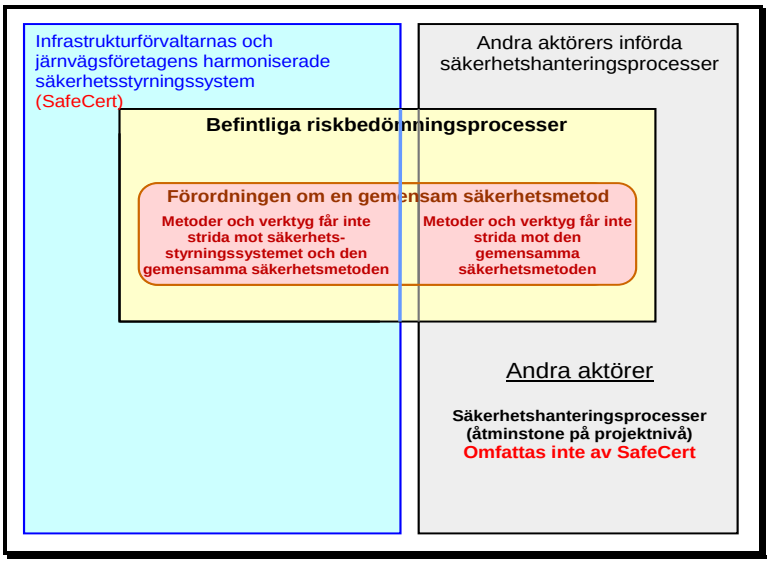
[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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

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

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

[G 1] Figur 2 åskådliggör sambandet mellan den gemensamma säkerhetsmetoden och ”säkerhetsstyrningssystemen och riskbedömningsprocesserna”.



Figur 2: Harmoniserat säkerhetsstyrningssystem och den gemensamma säkerhetsmetoden.

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] Om förslagsställaren är en infrastrukturförvaltare eller ett järnvägsföretag kan det ibland vara nödvändigt att involvera andra aktörer i processen ([6]) (se avsnitt 1.2.1). I vissa fall kan infrastrukturförvaltaren eller järnvägsföretaget lägga ut riskbedömningsaktiviteterna helt eller delvis på entreprenad. De berörda aktörerna kommer normalt på ett tidigt stadium av projekt överens om vilka roller och ansvarsområde som respektive aktör ska ha.

([6]) *Detta överensstämmer med tillägg A.4 i Cenelec-standarden 50129 {ref. 7}.*

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

[G 2] Det är viktigt att notera att förslagsställaren alltid behåller ansvaret för tillämpningen av den gemensamma säkerhetsmetoden, för godkännandet av risken och därför för systemets säkerhet. Hit hör att säkerställa att

(a) de berörda aktörerna samarbetar till fullo så att all information som behövs tillhandahålls, och
(b) det är fullständigt klart vem som måste uppfylla bestämda krav enligt den gemensamma säkerhetsmetoden (t.ex. att utföra riskanalysen eller sköta protokollet om faror).

Vid oenighet mellan aktörerna om vilka säkerhetskrav de måste uppfylla kan den nationella säkerhetsmyndigheten rådfrågas. Men ansvaret för att hitta en lösning kvarstår hos förslagsställaren och kan inte överföras till den nationella säkerhetsmyndigheten: se även avsnitt 0.2.2.

[G 3] Om uppgiften läggs ut på entreprenad är inte underleverantören skyldig att ha en egen säkerhetsorganisation, såvida denne inte är infrastrukturförvaltare eller ett järnvägsföretag. Detta gäller särskilt om underleverantörens organisation/storlek är liten eller om dennes bidrag till det övergripande systemet är litet. Ansvaret för riskhanteringen, inklusive riskbedömningen och hanteringen av faror kan kvarstå hos organisationen på den högre nivån (dvs. hos underleverantörens kund). Underleverantören är dock alltid skyldig att tillhandahålla rätt information om sina aktiviteter och den information som organisationen på den högre nivån behöver för att ta fram riskhanteringsdokumentationen.
Samarbetande organisationer kan också komma överens om att instifta en gemensam säkerhetsorganisation för att exempelvis optimera kostnaderna. I detta fall kommer endast en organisation att sköta säkerhetsaktiviteterna för alla de berörda organisationerna. Ansvaret för korrektheten hos informationen (dvs. faror, risker och säkerhetsåtgärder) liksom hanteringen av genomförandet av säkerhetsåtgärderna, kvarstår hos den organisation som har hand om kontrollen av de faror som dessa säkerhetsåtgärder hör samman med.

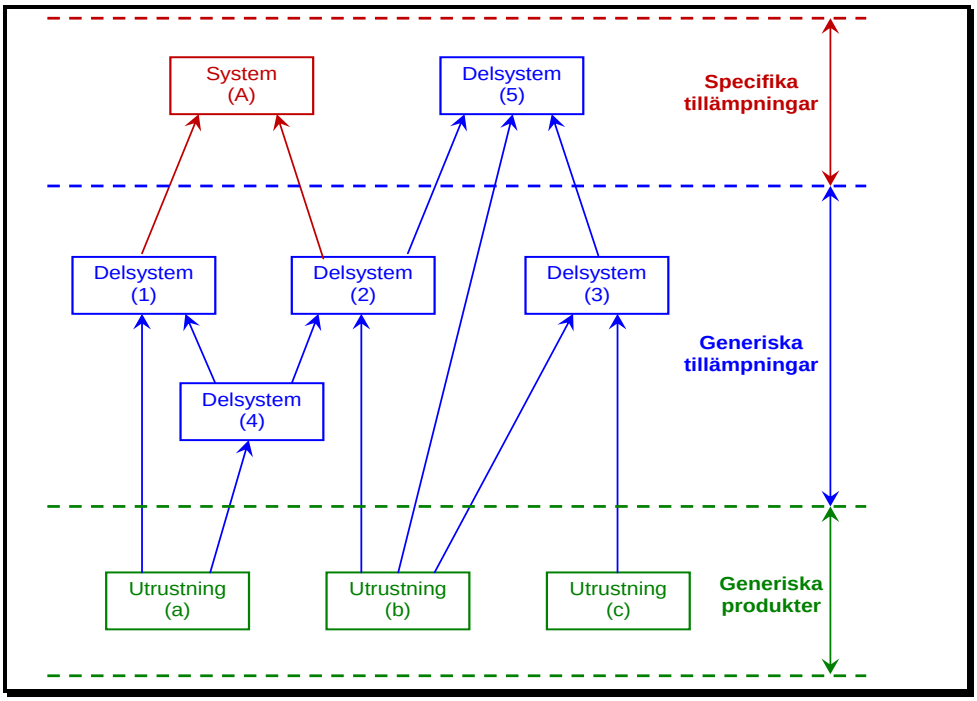
[G 4] Förslagsställaren kommer normalt att ange de ”säkerhetsnivåer” och ”säkerhetskrav” som har tilldelats aktörerna som deltar i projektet och som gäller deras olika delsystem och utrustning

(a) i avtal mellan förslagsställaren och respektive aktörer (underleverantörer),
(b) i en säkerhetsplan, eller något annat relevant dokument med samma syfte, tillsammans med en beskrivning av hela projektorganisationen och varje aktörs ansvar, inklusive förslagsställarens ansvar, se avsnitt 1.1.6,
(c) i förslagsställarens protokoll om faror, se avsnitt 4.1.1.

Denna tilldelning av systemets ”säkerhetsnivåer” och ”säkerhetskrav” till de bakomliggande delsystemen och utrustning, och därför respektive aktörer inklusive förslagsställaren själv, kan förfinas/utökas under ”påvisandet om att systemet uppfyller säkerhetskraven”: se avsnitt 2.1.1 och figur 1. I jämförelse med Cenelecs V-modell (se avsnitten 2.1.1 och figur 5 på sidan 36), motsvarar denna aktivitet fas 5 som handlar om ”fördelning av systemkrav” ned till de olika delsystemen och komponenterna.

[G 5] Enligt artikel 5.2 kan andra aktörer än järnvägsföretaget och infrastrukturförvaltaren överta hela ansvaret för att kraven i den gemensamma säkerhetsmetoden uppfylls, beroende på deras respektive behov. För exempelvis generiska produkter eller generiska tillämpningar (7) kan tillverkaren utföra riskbedömningen på grundval av en ”generisk systemdefinition” för att specificera de säkerhetsnivåer och säkerhetskrav som de generiska produkterna och de generiska tillämpningarna måste uppfylla.

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



Figur 3: Exempel på beroende mellan säkerhetsbevisningar (härledda från figur 9 i standarden EN 50129).

[G 6] I Cenelec rekommenderas att tillverkaren tillhandahåller dokumentation från riskbedömningen i säkerhetsbevisningar och protokoll om faror för den generiska produkten (respektive den generiska tillämpningen ([7])). Dessa säkerhetsbevisningar och protokoll om faror innehåller alla de antaganden ([8]) och identifierade ”begränsningar av användningen”

([7]) *Terminologin ”säkerhetsbevisningar för generisk tillämpning” respektive ”generisk produkt” är en återanvändning från Cenelec, där tre olika kategorier av säkerhetsbevisningar kan övervägas (se Figur 3):*

(a) ***Säkerhetsbevisning för generisk produkt*** *(oberoende av tillämpning). En generisk produkt kan återanvändas för olika oberoende tillämpningar.*

(b) ***Säkerhetsbevisning för generisk tillämpning*** *(för en tillämpningsklass). En generisk tillämpning kan återanvändas för en klass/typ av tillämpning med gemensamma funktioner.*

(c) ***Säkerhetsbevisning för specifik tillämpning*** *(för en specifik tillämpning). En specifik tillämpning används endast för en bestämd installation.*

Mer information om deras ömsesidiga beroende finns i avsnitt 9.4 och figur 9.1 i Cenelecs vägledning 50126-2 {ref. 9}.

([8]) *Dessa antaganden och begränsningar av användningen bestämmer gränserna och validiteten för de ”säkerhetsbedömningar” och de ”säkerhetsanalyser” som hör samman med de därtill hörande säkerhetsbevisningarna för en generisk produkt och en generisk tillämpning. Om de inte uppfylls av den betraktade specifika tillämpningen måste motsvarande ”säkerhetsbedömningar” och ”säkerhetsanalyser” (t.ex. orsaksanalyser) uppdateras eller ersättas.*

> *Detta ligger i linje med följande allmänna säkerhetsprincip: ”Då en specifik (del-) systemdesign är baserad på generiska tillämpningar och generiska produkter måste det påvisas att det specifika (del-)systemet överensstämmer med alla antaganden och*

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

(dvs. säkerhetsrelaterade tillämpningsvillkor) som gäller de därtill hörande generiska produkterna (respektive generiska tillämpningen). Därför måste, då en generisk produkt och en generisk tillämpning används i drift i en specifik tillämpning, överensstämmelse med dessa antaganden ([8]) och ”begränsningar av användningen” (eller säkerhetsrelaterade tillämpningsvillkor) påvisas i varje specifik tillämpning.

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] Mycket ofta, om man inte har kommit överens om något annat i avtalen i början av projektet, finns det ett dokument till varje projekt med en beskrivning av riskhanteringsaktiviteterna. Det relevanta dokumentet uppdateras och granskas då betydande ändringar görs i det ursprungliga systemet.

[G 2] I ett sådant dokument anges den organisatoriska strukturen, personalens tilldelade ansvarsområden, processerna, förfarandena och aktiviteterna som tillsammans säkerställer att det system som är föremål för bedömning uppfyller de specificerade säkerhetsnivåerna och säkerhetskraven. Dokumentet måste uppfylla kraven i den gemensamma säkerhetsmetoden eftersom det stöder och ger vägledning till bedömningsorganet. I Cenelec-standarderna rekommenderas att denna typ av information ingår i en säkerhetsplan, eller i ett annat dokument med ett avsnitt som är reserverat för dessa områden.

[G 3] I synnerhet i förslagsställarens säkerhetsplan, eller något annat relevant dokument, presenteras den övergripande projektorganisationen. Den beskriver hur rollerna och ansvarsområdena är fördelade mellan de berörda aktörerna. Om mer detaljerad information önskas hänvisas till de olika berörda aktörernas säkerhetsplaner eller säkerhetsorganisationer. Normalt diskuteras fördelningen av de olika ansvarsområdena mellan de olika aktörerna och görs överenskommelser under den preliminära systemdefinieringen (dvs. i början av projektet), om det finns någon.

[G 4] Säkerhetsplanen är ett levande dokument som uppdateras när så behövs under projektets gång.

Fortsättning på fotnoten

> *begränsningar av användningen (som kallas säkerhetsrelaterade tillämpningsvillkor i Cenelec) som har exporterats till motsvarande säkerhetsbevisningar för en generisk tillämpning och en generisk produkt (se Figur 3).”*

Om vissa antaganden och begränsningar av användningen inte kan uppfyllas för en specifik tillämpning på delsystemnivå (t.ex. när det gäller driftsrelaterade säkerhetskrav) kan motsvarande antaganden och begränsningar av användningen överföras till en högre nivå (dvs. normalt systemnivån). Dessa antaganden och begränsningar av användningen identifieras därefter tydligt i ”säkerhetsbevisningen för den specifika tillämpningen” i det därtill hörande delsystemet. Det är viktigt att i sådana exempel på beroenden säkerställa att de säkerhetsrelaterade tillämpningsvillkoren för varje säkerhetsbevisning uppfylls i säkerhetsbevisningen på den högre nivån, eller i annat fall överförs till de säkerhetsrelaterade tillämpningsvillkoren i säkerhetsbevisningen på högsta nivån (dvs. säkerhetsbevisningen för systemet).

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

[G 5] Närmare information om innehållet i en säkerhetsplan finns i standarden EN 50126-1 {ref. 8} och den tillhörande vägledningen 50126-2 {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] Ytterligare förklaring bedöms inte vara nödvändig.

1.2. Förvaltning av kontaktpunkter

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] Om ett järnvägsföretag av driftsmässiga skäl har behov av att en infrastrukturförvaltare utför definierade ändringar i infrastrukturen, enligt kraven i bilaga III.2 g i järnvägssäkerhetsdirektivet {ref. 1}, övervakar även järnvägsföretaget hela arbetet för att säkerställa att de förväntade ändringarna utförs korrekt. Trots att järnvägsföretaget innehar ledningen ansvarar infrastrukturförvaltaren fortfarande för att de andra järnvägsföretagen informeras, om de också påverkas av den därtill hörande ändringen av infrastrukturen. Infrastrukturförvaltaren måste till och med utföra en riskbedömning i enlighet med den gemensamma säkerhetsmetoden om den därtill hörande ändringen är betydande ur infrastrukturförvaltarens synvinkel.

[G 2] Det är möjligt att överföra ansvar mellan olika aktörer, och i vissa fall till och med nödvändigt. När flera aktörer är involverade i ett system utses dock ofta en aktör som ansvarig för hela systemet. Det finns alltid beroenden mellan delsystem och driftoperationer som kräver att särskilda insatser görs för att identifiera dem. Det är således nödvändigt att någon tar över hela ansvaret för säkerhetsanalyserna och också får fullständig tillgång till alla relevant dokumentation. Uppenbarligen har förslagsställaren som har för avsikt att införa den betydande ändringen i allmänhet det övergripande ansvaret för att riskbedömningen är systematisk och fullständig.

[G 3] De huvudkriterier om hanteringen av en kontaktpunkt mellan de berörda aktörerna som man måste komma överens om är följande:

(a) Ledningen, som normalt innehas av den förslagsställare som har för avsikt att införa den betydande ändringen.
(b) De indata som krävs.
(c) Metoderna för identifiering av faror och riskbedömning.
(d) De deltagare som krävs och som har den kompetens som krävs (dvs. en kombination av kunskap, färdigheter och praktisk erfarenhet – se även definitionen av ”personalens kompetens” i punkt [G 2](b) i artikel 3 i {ref. 4}).
(e) De förväntade resultaten.

Dessa kriterier beskrivs i säkerhetsplanerna (eller i andra relevanta dokument) hos de företag som har hand om de berörda kontaktpunkterna.

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

[G 4] Exempel på kontaktpunkter finns i avsnitt C.3. i tillägg C, liksom ett exempel på tillämpning av dessa huvudkriterier för hanteringen av kontaktpunkten mellan en tågtillverkare och en infrastrukturförvaltare eller ett järnvägsföretag.

[G 5] I hanteringen av kontaktpunkter ingår även att ta hänsyn till de risker som skulle kunna uppstå vid kontaktpunkterna med operatörerna (som används under drift och underhåll) under utformningen av dessa kontaktpunkter.

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] Processen för att överföra faror och tillhörande säkerhetsåtgärder mellan aktörer kan också tillämpas på de lägre nivåerna i Cenelecs V-modell i figur 5 på sidan 36. Den kan tillämpas när det finns behov av att utbyta sådan information, till exempel mellan en aktör och dennes underleverantörer. Skillnaden mot när samma process används på systemnivå är att förslagsställaren inte behöver informeras om alla överföringar av faror och tillhörande säkerhetsåtgärder på delsystemnivå. Förslagsställaren informeras endast då överföringen av faror och tillhörande säkerhetsåtgärder hör samman med kontaktpunkter på högre nivå (dvs. som påverkar en av förslagsställarens kontaktpunkter).

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] Järnvägsföretagets och infrastrukturförvaltarens säkerhetsstyrningssystem innefattar åtgärder och förfaranden för att säkerställa att icke-överensstämmelser och brister hos säkerhetsåtgärder hanteras korrekt. Därför ingår inte dessa åtgärder och förfaranden i den gemensamma säkerhetsmetoden.

[G 2] På samma sätt kommer de berörda aktörerna i början av projektet överens om vilka åtgärder och förfaranden ([9]) som ska införas av de andra aktörerna ([10]) för att säkerställa att icke-överensstämmelse eller brister hos säkerhetsåtgärderna hanteras korrekt och, om det behövs, att säkerhetsåtgärderna överförs till alla berörda aktörer. Detta specificeras i deras säkerhetsplan: se avsnitt 0.2.

([9]) *I princip innefattas dessa åtgärder och förfaranden i dessa aktörers kvalitetsstyrnings- och/eller säkerhetsstyrningsprocess som fastställts åtminstone på projektnivå (se även Figur 2).*

([10]) *Terminologin ”andra aktörer” avser alla berörda aktörer utöver infrastrukturförvaltarna och järnvägsföretagen.*

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

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] Detta gör det möjligt att hantera eventuell icke-överensstämmelse eller brister hos säkerhetsåtgärden i det system som är föremål för bedömning eller i liknande system i vilka samma åtgärd används.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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

2. BESKRIVNING AV RISKBEDÖMNINGSPROCESSEN

2.1. Allmän beskrivning – Överensstämmelse mellan riskbedömningsprocessen i den gemensamma säkerhetsmetoden och Cenelecs V-modell

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

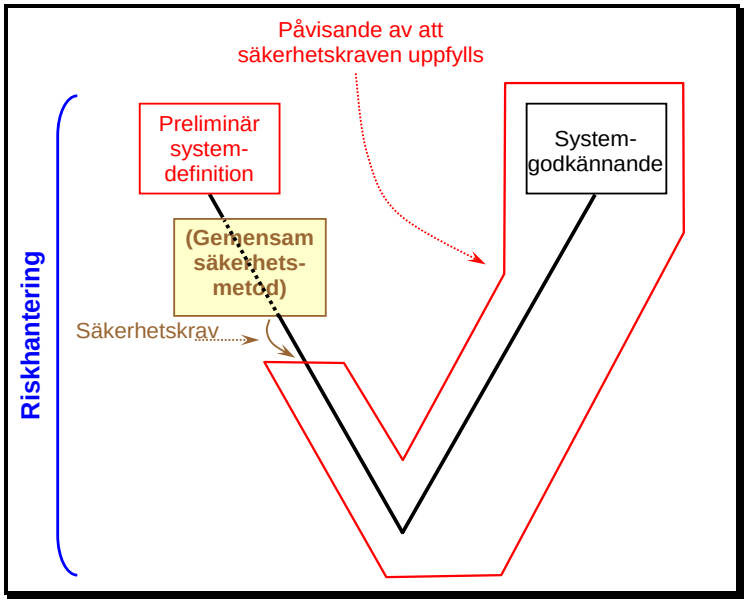
(a) the system definition;
(b) the risk analysis including the hazard identification;
(c) the risk evaluation.

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

[G 1] Riskhanteringsprocessen som ingår i den gemensamma säkerhetsmetoden kan åskådliggöras i en V-modell som börjar med den (preliminära) systemdefinitionen och slutar med godkännandet av systemet: se figur 4. Denna förenklade V-modell kan därefter passas in i den klassiska V-modellen i figur 10 enligt standarden EN 50126-1 {ref. 8}. För att visa överensstämmelsen med riskhanteringsprocessen enligt den gemensamma säkerhetsmetoden i figur 1, återges Cenelecs V-modell enligt figur 10 i figur 5:

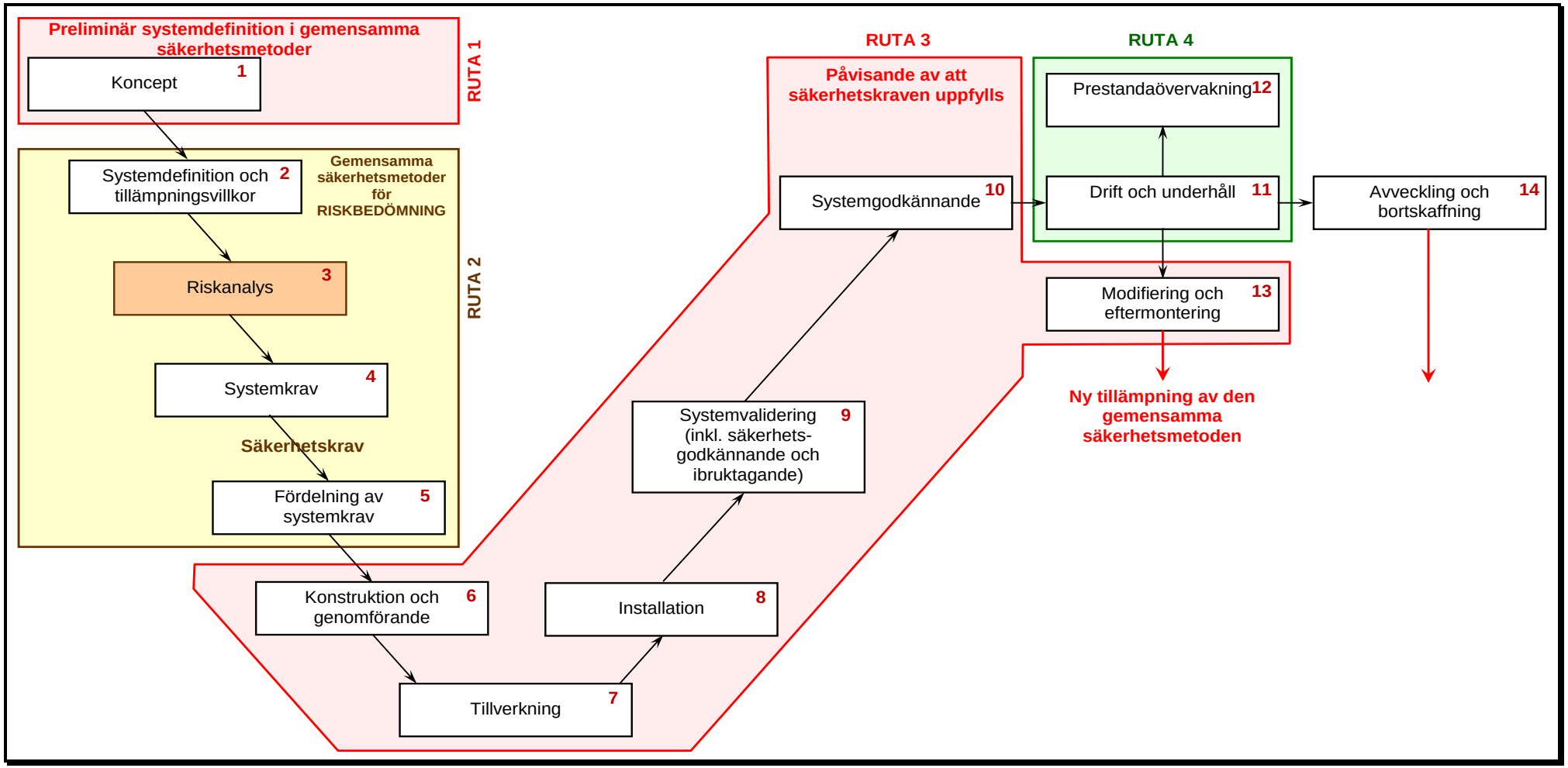
(a) Den ”preliminära systemdefinitionen” enligt den gemensamma säkerhetsmetoden i figur 1 motsvarar fas 1 i Cenelecs V-modell, dvs. definitionen av systemets ”koncept” (se RUTA 1 i figur 5).
(b) I ”riskbedömningen” enligt den gemensamma säkerhetsmetoden i figur 1 ingår följande faser från Cenelecs V-modell (se RUTA 2 i figur 5):

(1) Fas 2 i figur 5: ”systemdefinition och tillämpningsvillkor”.
(2) Fas 3 i figur 5: ”riskanalys”.
(3) Fas 4 i figur 5: ”systemkrav”.
(4) Fas 5 i figur 5: ”fördelning av systemkrav” ned till de olika delsystemen och komponenterna.



Figur 4: Förenklad V-modell enligt figur 10 i standarden EN 50126 .

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



Figur 5: V-modellen enligt figur 10 i EN 50126 (Cenelecs systemlivscykel).

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

[G 2] Resultaten från riskbedömningsprocessen i den gemensamma säkerhetsmetoden är (efter iterationer – se figur 1) följande:

(a) ”Systemdefinitionen” uppdaterad med ”säkerhetskraven” från ”riskanalysen” och ”riskvärderingen” (se avsnitt 2.1.6).
(b) ”Fördelningen av systemkrav” ned till de olika delsystemen och komponenterna (fas 5 i figur 5).
(c) ”Protokollet om faror” i vilket följande registreras:

(1) Alla identifierade faror och tillhörande säkerhetsåtgärder.
(2) De resulterande säkerhetskraven.
(3) De antaganden som har beaktats för systemet och som fastställer gränserna och validiteten för riskbedömningen (se punkt (g) i avsnitt 2.1.2).

(d) I allmänhet alla bevis från tillämpningen av den gemensamma säkerhetsmetoden: se avsnitt 5.

Resultaten från riskbedömningen enligt den gemensamma säkerhetsmetoden motsvarar de säkerhetsrelaterade resultaten från fas 4 i Cenelecs V-modell, dvs. specifikationen av systemkrav i figur 5.

[G 3] Systemdefinitionen som har uppdaterats med resultaten från riskbedömningen och protokollet om faror utgör de indata enligt vilket systemet utformas och godkänns. ”Påvisandet av att systemet uppfyller säkerhetskraven” enligt den gemensamma säkerhetsmetoden motsvarar följande faser i Cenelecs V-modell (se RUTA 3 i figur 5):

(a) Fas 6 i figur 5: ”konstruktion och genomförande”.
(b) Fas 7 i figur 5: ”tillverkning”.
(c) Fas 8 i figur 5: ”installation”.
(d) Fas 9 i figur 5: ”systemvalidering (inklusive säkerhetsgodkännande och ibruktagande)”.
(e) Fas 10 i figur 5: ”systemgodkännande”.

[G 4] Påvisandet av att systemet uppfyller säkerhetskraven är beroende av om den betydande ändringen är teknisk, driftsrelaterad eller organisatorisk. Detta innebär att de olika stegen i Cenelecs V-modell i figur 5 kanske inte passar för alla betydande ändringar av en viss typ. V-modellen i figur 5 måste betraktas i enlighet med detta och användas med lämplig bedömning om vad som passar varje specifik tillämpning (exempelvis finns det inte någon tillverkningsfas för driftsrelaterade och organisatoriska ändringar).

[G 5] Detta innebär att ”påvisandet av att systemet uppfyller säkerhetskraven” i den gemensamma säkerhetsmetoden inte enbart omfattar ”verifiering och validering” genom tester eller simulering. I praktiken omfattar det alla faserna ”6 till 10” (se listan ovan och figur 5) i Cenelecs V-modell. Faserna omfattar konstruktion, tillverkning, installation, verifiering och validering, liksom tillhörande RAMS-aktiviteter och systemgodkännande.

[G 6] Under ”påvisandet av att systemet uppfyller säkerhetskraven”, gäller den allmänna principen om att riskbedömningen ska koncentreras enbart till systemets säkerhetsrelaterade funktioner och kontaktpunkter. Detta innebär att varje gång som risk- och säkerhetsbedömningsaktiviteter krävs inom ramen för någon fas i Cenelecs V-modell i figur 5 ska dessa inriktas på

(a) de säkerhetsrelaterade funktionerna och kontaktpunkterna,
(b) de delsystem och/eller komponenter som ingår i de säkerhetsrelaterade funktionerna och/eller kontaktpunkterna som har bedömts under riskbedömningen på högre nivå.

[G 7] Följande framgår av jämförelsen med den klassiska V-modellen enligt Cenelec i figur 5:

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

(a) Den gemensamma säkerhetsmetoden omfattar faserna ”1 till 10” och ”13” av denna V-modell. De innefattar den uppsättning aktiviteter som krävs för att det system som är föremål för bedömning ska godkännas.

(b) Den gemensamma säkerhetsmetoden omfattar inte faserna ”11”, ”12” och ”14” i systemlivscykeln:

(1) Faserna ”11” och ”12” hänför sig till ”drift och underhåll” respektive ”prestandaövervakning” av systemet efter att det har godkänts baserat på den gemensamma säkerhetsmetoden. Dessa två faser ingår i järnvägsföretaget och infrastrukturförvaltarens säkerhetsstyrningssystem – (se RUTA 4 i figur 5). Om det emellertid under drift, underhåll eller prestandaövervakningen av systemet verkar nödvändigt att modifiera och utföra eftermonteringar i systemet (fas 13 i figur 5), då det redan har tagits i drift, tillämpas den gemensamma säkerhetsmetoden igen på de nya ändringarna som krävs i enlighet med artikel 2. Om ändringen är betydande

(i) tillämpas riskhanterings- och riskbedömningsprocesserna enligt den gemensamma säkerhetsmetoden på dessa nya ändringar,
(ii) krävs ett godkännande för dessa nya ändringar i enlighet med artikel 6.

(2) ”Avveckling och bortskaffande” av ett system som redan är i drift (fas 14) kan också betraktas som en betydande ändring och därför skulle den gemensamma säkerhetsmetoden kunna tillämpas igen i enlighet med artikel 2 för fas 14 i figur 5.

Mer information om tillämpningsområdet för varje fas eller aktivitet i Cenelecs V-modell som återges i figur 5 finns i avsnitt 6 i standarden EN 50126-1 {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] Ytterligare förklaring bedöms inte vara nödvändig.

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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);

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

(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] I allmänhet kommer förslagsställaren att besluta om vilken princip för riskacceptans som är mest lämplig för att kontrollera de identifierade farorna på grundval av de specifika kraven för projektet liksom förslagsställarens erfarenhet av de tre principerna.

[G 2] Det är inte alltid möjligt att bedöma om riskerna är godtagbara på systemnivå genom användning av enbart en av de tre principerna för riskacceptans. Riskacceptansen kommer därför ofta att grundas på en kombination av dessa principer. Om mer än en princip för riskacceptans måste tillämpas för en betydande fara för att kontrollera den tillhörande risken måste den därtill hörande faran delas in i delfaror, så att varje enskild delfara kontrolleras på ett adekvat sätt med hjälp av enbart en princip för riskacceptans.

[G 3] I beslutet om att kontrollera en fara med en princip för riskacceptans måste hänsyn tas till faran och orsakerna till faran som redan har definierats under identifieringen av faran. Om två olika och oberoende orsaker hör samman med samma fara måste faran delas in i två olika delfaror. Varje delfara kommer därefter att kontrolleras av en enda princip för riskacceptans. De två delfarorna måste registreras och förvaltas i protokollet om faror. Om exempelvis faran orsakas av ett konstruktionsfel kan detta hanteras genom tillämpning av en handlingsregel. Om å andra sidan orsaken till faran är ett underhållsfel är det inte säkert att enbart handlingsregeln är tillräcklig. Då krävs tillämpning av ytterligare en princip för riskacceptans.

[G 4] Minskningen av risken till en godtagbar nivå kan leda till flera iterationer mellan riskanalys- och riskvärderingsfaserna tills lämpliga säkerhetsåtgärder har identifierats.

[G 5] Den nuvarande kvarvarande risken som kommer från erfarenhet från fältet av befintliga system och system som baseras på tillämpningen av handlingsregler betraktas som godtagbar. Den risk som är resultatet av en uttrycklig riskuppskattning grundar sig på en expertbedömning och olika antaganden som experten har gjort under analyserna eller på databaser som hör samman med olycks- eller drifterfarenhet. Den kvarvarande risken från en uttrycklig riskuppskattning kan därför inte bekräftas omedelbart genom erfarenheter från fältet. Ett sådant påvisande kräver tid för drift, övervakning och att få en representativ erfarenhet för det därtill hörande systemet. I allmänhet har tillämpningen av handlingsregler och jämförelse med liknande referenssystem fördelen att man kan undvika en överspecificering av onödigt strikta säkerhetskrav som kan härröra från överdrivet konservativa (säkra) antaganden i uttryckliga riskuppskattningar. Det kan dock hända att vissa säkerhetskrav i handlingsreglerna eller liknande referenssystem inte behöver uppfyllas av det system som är föremål för bedömning. I ett sådant fall skulle tillämpningen av en uttrycklig riskuppskattning ha den fördelen att man undviker en överkonstruktion av det system som är föremål för bedömning och möjliggör en mer kostnadseffektiv konstruktion som inte har provats tidigare.

[G 6] Om de identifierade farorna och de tillhörande riskerna för det system som är föremål för bedömning inte kan kontrolleras genom tillämpning av handlingsregler eller liknande referenssystem kan en uttrycklig riskuppskattning utföras, baserad på kvantitativa eller kvalitativa analyser av farliga händelser. Denna situation uppkommer då det system som är föremål för bedömning är helt nytt (eller konstruktionen är innovativ) eller då systemet avviker från en handlingsregel eller ett referenssystem. Med den uttryckliga riskuppskattningen kommer en bedömning att göras om risken är godtagbar (dvs. att

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

ytterligare analys inte behövs) eller om ytterligare säkerhetsåtgärder krävs för att minska risken ytterligare.

[G 7] Vägledning om riskminskning och riskacceptans finns även i avsnitt 8 i vägledningen EN 50126-2 {ref. 9}.

[G 8] Den princip för riskacceptans som används och dess tillämpning måste bedömas av bedömningsorganet.

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] Om exempelvis tillämpningen av en SIL 4-utvecklingsprocess enligt standarden EN 50128 är specificerad som ett säkerhetskrav för programvaran till en komponent, måste det bevisas att den process som rekommenderas i standarden uppfylls. Detta innefattar exempelvis påvisande av att

(a) kraven på oberoende i organisationen för konstruktion, verifiering och validering av programvaran uppfylls,
(b) de korrekta metoderna enligt standarden EN 50128 och tillförlitlighetsnivån SIL 4 tillämpas,
(c) etc.

[G 2] Om exempelvis en särskild handlingsregel ska användas för att tillverka elektromagnetiska ventiler till nödbromsarna, måste det bevisas att alla krav i handlingsregeln uppfylls under tillverkningsprocessen.

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] Två typer av säkerhetsåtgärder kan identifieras:

(a) ”Förebyggande säkerhetsåtgärder” som förebygger förekomsten av faror eller deras orsaker.
(b) ”Mildrande säkerhetsåtgärder” som förhindrar att faror leder till olyckor eller minskar konsekvenserna för olyckorna efter att de har uppkommit (skyddsåtgärder).

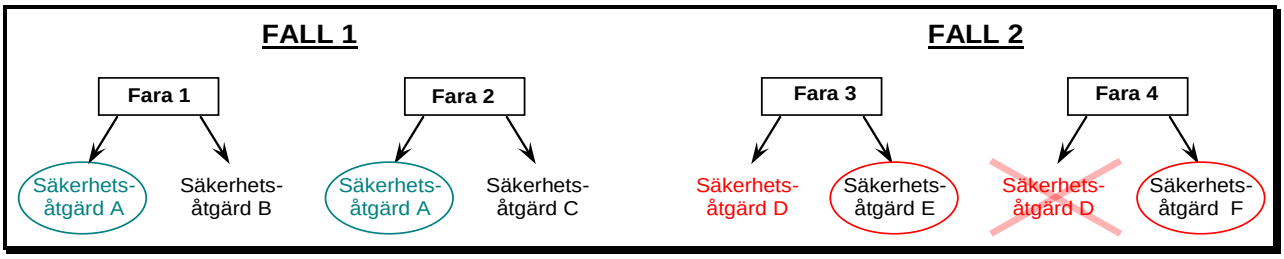
Ur ett driftsperspektiv är det i allmänhet effektivare att förebygga orsakerna.

[G 2] Den lämpligaste säkerhetsåtgärden enligt förslagsställaren är den säkerhetsåtgärd som utgör den bästa kompromissen mellan kostnaden för att uppnå riskminskningen och den kvarvarande risknivån. De valda säkerhetsåtgärderna blir säkerhetskraven för det system som är föremål för bedömning.

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

[G 3] Det är viktigt att kontrollera att de säkerhetsåtgärder som har valts för att kontrollera en fara inte står i konflikt med andra faror. Så som framgår av figur 6 kan följande två fall exempelvis inträffa ([11]):

(a) FALL 1: Om samma säkerhetsåtgärd (åtgärd A i figur 6) kan kontrollera olika faror utan att det uppstår några konflikter mellan dem, och om det är ekonomiskt försvarbart, kan den därtill hörande säkerhetsåtgärden väljas som det enda tillhörande ”säkerhetskravet”. Det totala antalet säkerhetskrav som ska uppfyllas är lägre än om man genomför både åtgärd B och C.



Figur 6: Val av lämpliga säkerhetsåtgärder för att kontrollera risker.

(b) FALL 2: Omvänt, om en säkerhetsåtgärd kan kontrollera en fara men detta leder till en konflikt med en annan fara (åtgärd D i figur 6) kan den inte väljas som ”säkerhetskrav”. De andra säkerhetsåtgärderna för den berörda faran måste användas (åtgärderna E och F i figur 6):

(1) Ett typiskt exempel i trafikstyrningssystemet är användningen av tågets placering på spåret, antingen för att kontrollera bromsningen eller för att godkänna att tåget accelererar. Att använda tågets front (respektive tågets bakände) som tågets placering är inte säkert i alla situationer:

(i) Då ETCS-trafikstyrningssystemet måste använda nödbromsarna på ett säkert sätt, använder det kommandot MAXIMUM SAFE FRONT END, dvs. minimigräns för säker front, för att säkerställa att tågets front verkligen stannar innan den når riskpunkten.

(ii) Omvänt, då tåget tillåts accelerera efter exempelvis en hastighetsbegränsning använder ETCS-trafikstyrningssystemet kommandot, MINIMUM SAFE REAR END, dvs. minimigräns för säker bakände.

(2) Ett annat exempel är en säkerhetsåtgärd som skulle kunna användas för att stanna ett tåg under nästan alla omständigheter och anta ett felsäkert tillstånd, förutom i en tunnel eller på en bro. I detta senare fall ska åtgärd D i FALL 2 i figur 6 inte användas.

([11]) *Det måste noteras att denna vägledning inte tar upp alla de situationer i vilka säkerhetsåtgärder skulle kunna komma i konflikt med andra identifierade faror. Endast ett fåtal illustrativa exempel ingår.*

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

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

[G 1] Beroende på exempelvis tekniska val för konstruktionen av ett system, dess delsystem och utrustning, kan nya faror identifieras under ”påvisandet av att systemet uppfyller säkerhetskraven” (t.ex. skulle användning av viss lackering kunna leda till toxiska gaser vid brand). Dessa nya faror och tillhörande risker måste betraktas som nya indata i en ny loop i den löpande riskbedömningsprocessen. I tillägg A.4.3 till standarden EN 50129 finns andra exempel på när nya faror skulle kunna införas som måste kontrolleras.

2.2. Identifiering av faror

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] Farorna ska så långt det är möjligt uttryckas med samma detaljnivå. Det kan hända under de preliminära riskanalyserna att faror med olika detaljnivå identifieras (t.ex. på grund av att människor med olika erfarenhet samlas under HAZOP-analysen).
Detaljnivån beror också på vilken princip för riskacceptans som väljs för att kontrollera de identifierade farorna. Om exempelvis en fara kontrolleras fullständigt genom en handlingsregel eller ett liknande referenssystem kommer en mer detaljerad identifiering av faran inte att behövas.

[G 2] Alla faror som identifieras under riskbedömningsprocessen (inklusive de som hör samman med allmänt godtagbara risker), de tillhörande säkerhetsåtgärderna och de tillhörande riskerna måste registreras i protokollet om faror.

[G 3] Olika metoder kan användas för identifieringen av faror, beroende på karaktären hos det system som ska analyseras:

(a) Empirisk identifiering av faror kan användas för att utnyttja tidigare erfarenheter (t.ex. användning av checklistor eller generiska förteckningar över faror).
(b) Kreativ identifiering av faror kan användas för nya angelägna områden (proaktiv prognostisering, t.ex. strukturerade ”Vad-händer-om”-studier såsom FMEA eller HAZOP).

[G 4] De empiriska och kreativa metoderna för identifiering av faror kan användas tillsammans för att komplettera varandra och därmed säkerställa att listan över potentiella faror och säkerhetsåtgärder, i förekommande fall, är fullständig.

[G 5] Som ett preliminärt steg kan identifieringen av faror starta med ett brainstormingmöte, där experter med olika kompetens som täcker alla relevanta aspekter för en betydande ändring träffas. Om expertpanelen anser det vara nödvändigt kan empiriska metoder användas för att analysera en specifik funktion eller ett specifikt driftläge.

[G 6] Vilka metoder som används för identifieringen av faror beror på systemdefinitionen. Några exempel ges i tillägg B.

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

[G 7] Mer information om tekniker och metoder för identifiering av faror finns i bilagorna A.2 och E i vägledningen EN 50126-2 {ref. 9}.

[G 8] Ett exempel på en generisk förteckning över faror finns i avsnitt C.17. i tillägg C.

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

[G 1] För att underlätta riskbedömningsprocessen kan betydande faror grupperas i olika kategorier. Exempelvis kan betydande faror klassificeras eller rankas efter deras förväntade allvarlighetsgrad och förekomstfrekvens. Vägledning för en sådan övning finns i Cenelec-standarden: se avsnitt A.2. i tillägg A.

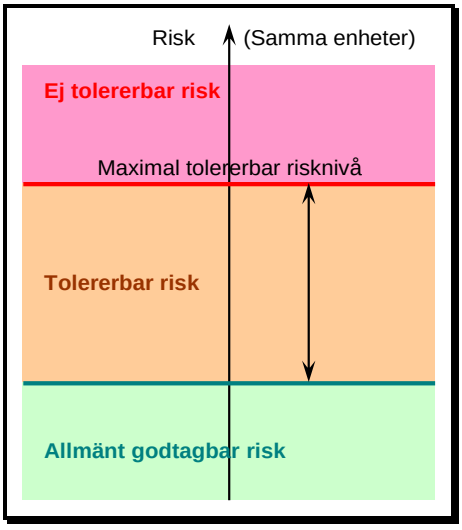
[G 2] Riskanalysen och riskvärderingen som beskrivs i avsnitt 2.1.4 tillämpas enligt en prioriteringsordning, och börjar med de högst rankade farorna.

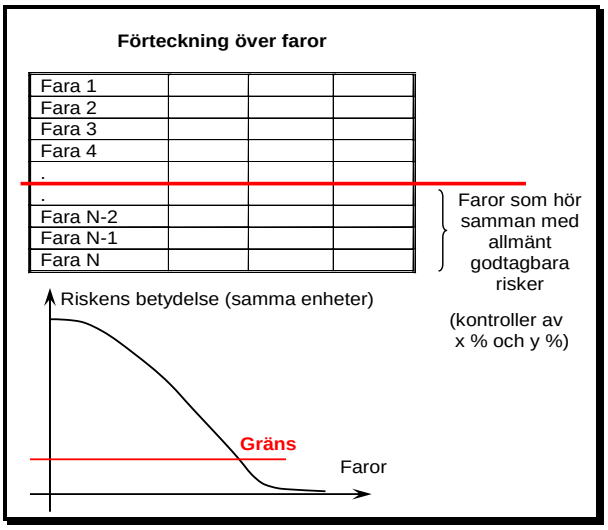
2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed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

[G 1] En risk som hör samman med en fara kan betraktas som allmänt godtagbar om

(a) risken är mindre än en given procentandel (t.ex. x %) av den maximalt tolererbara risken för denna typ av fara. Värdet för x % kan vara baserat på bästa praxis och erfarenhet med flera riskanalysmetoder, t.ex. kvoten mellan en allmänt godtagbar risk- och ej tolererbar riskklassificering i FN-kurvor eller riskmatriser. Detta kan åskådliggöras så som visas i figur 7.

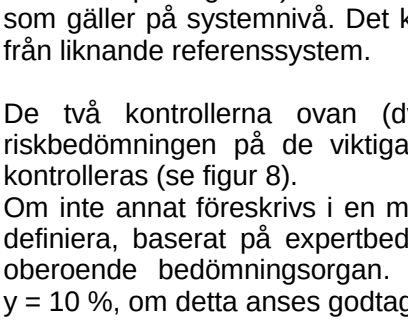
(b) förlusten som hör samman med risken är så liten att det inte är rimligt att införa någon säkerhetsåtgärd för att motverka denna.





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

Figur 7: Allmänt godtagbara risker



Figur 8: Utfiltrering av faror som hör samman med allmänt godtagbara risker.

[G 2] Utöver detta kan, om faror med olika detaljnivå identifieras (dvs. å ena sidan faror på hög nivå och å andra sidan detaljerade delfaror), försiktighetsåtgärder behöva vidtas för att undvika att de klassificeras felaktigt som faror som hör samman med allmänt godtagbara risker. Bidraget av alla faror som hör samman med allmänt godtagbara risker får inte överskrida en given andel (t.ex. y %) av den totala risken på systemnivå. Denna kontroll är nödvändig för att undvika att helhetsbilden urholkas av en underindelning av faror i många delfaror på låg nivå. Om en fara uttrycks som många olika ”mindre” delfaror, kan var och en av dem lätt klassificeras som tillhörande allmänt godtagbara risker om de utvärderas separat, men tillhörande en betydande risk om man utvärderar dem tillsammans (dvs. som enda fara på hög nivå). Värdet för andelen (t.ex. y %) beror på de kriterier för riskacceptans som gäller på systemnivå. Det kan baseras på och uppskattas med hjälp av drifterfarenhet från liknande referenssystem.

[G 3] De två kontrollerna ovan (dvs. mot x % och y %) gör det möjligt att fokusera riskbedömningen på de viktigaste farorna och att säkerställa att alla betydande risker kontrolleras (se figur 8).
Om inte annat föreskrivs i en medlemsstats lagstiftning är förslagsställaren ansvarig för att definiera, baserat på expertbedömning, värdena x % och y % och att de bedöms av ett oberoende bedömningsorgan. Ett exempel på storleksordning kan vara x = 1 % och y = 10 %, om detta anses godtagbart enligt expertbedömningen.

[G 4] I avsnitt 2.2.2 krävs att klassificering i ”allmänt godtagbara risker” bedöms av ett oberoende bedömningsorgan.

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] Huvudsyftet för denna aktivitet är att identifiera faror som hör samman med ändringen. Om säkerhetsåtgärder redan har identifierats måste de registreras i protokollet om faror. Typen av åtgärder beror på ändringen: de kan vara förfarandemässiga, tekniska, driftsrelaterade eller organisatoriska.

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] Även om en risk är kontrollerad på en godtagbar nivå kan förslagsställaren fortfarande besluta sig för att en mer detaljerad identifiering av faror behövs. Ett skäl till detta skulle kunna vara att det är mer sannolikt att man hittar mer kostnadseffektiva säkerhetsåtgärder för att kontrollera risker om man utför en mer detaljerad identifiering av farorna.

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

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] Ytterligare förklaring bedöms inte vara nödvändig.

2.3. Användning av handlingsregler och riskvärdering

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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

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

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

[G 1] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

2.4. Användning av referenssystem och riskvärdering

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] Mer information om dessa principer finns i avsnitt 8 i vägledningen EN 50126-2 {ref. 9}.

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

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

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

[G 1] Ett gammalt trafikstyrningssystem som i drift har visat sig ha en godtagbar säkerhetsnivå kan ersättas av ett annat system, med nyare teknik och bättre säkerhetsprestanda. Det är alltså relevant att varje gång ett referenssystem tillämpas kontrollera om det fortfarande uppfyller kraven för godkännande.

[G 2] Eftersom vissa aspekter gällande tunnelsäkerhet eller säkerhet vid transport av farligt gods kan vara specifika och beroende av driftsrelaterade och miljömässiga förhållanden, måste man före varje projekt kontrollera att systemet kommer att användas under samma förhållanden.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Mer information om likhetsanalyser finns i avsnitt 8.1.3 i vägledningen EN 50126-2 {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] Ytterligare förklaring bedöms inte vara nödvändig.

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

2.5. Uttrycklig riskuppskattning och riskvärdering

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] Ytterligare förklaring bedöms inte vara nödvändig.

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.

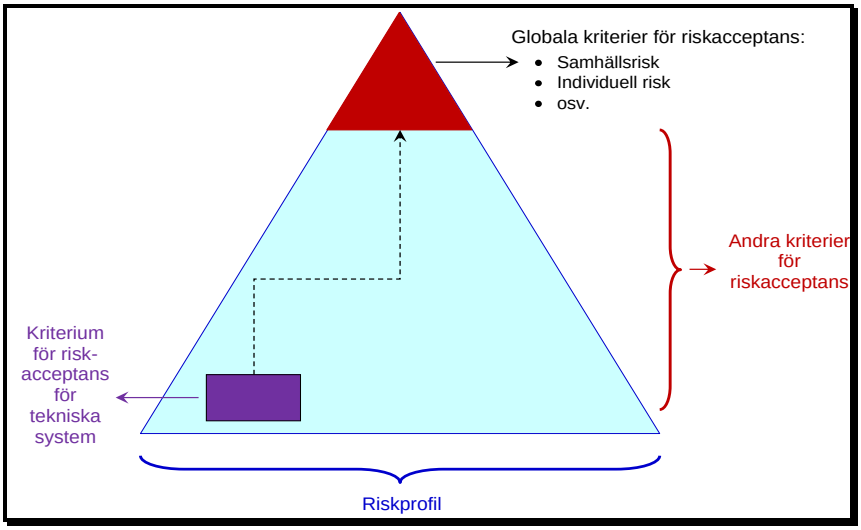
[G 1] För att kunna utvärdera om riskerna i det system som är föremål för bedömning är godtagbara eller inte krävs det kriterier för riskacceptans (se ”riskvärderingsrutorna” i figur 1). Kriterierna för riskacceptans kan antingen vara implicita eller explicita:

(a) Implicita kriterier för riskacceptans: Enligt avsnitten 2.3.5 och 2.4.3 betraktas riskerna som omfattas av tillämpningen av handlingsregler och jämförelse med referenssystem implicit som godtagbara under förutsättning att (se prickad cirkel i figur 1)

(1) förhållandena för att tillämpa handlingsregler enligt avsnitt 2.3.2 är uppfyllda,
(2) förhållandena för att använda ett referenssystem enligt avsnitt 2.4.2 är uppfyllda.

(b) Explicita kriterier för riskacceptans: För att kunna utvärdera om en risk som kontrolleras genom tillämpning av uttrycklig riskuppskattning är godtagbar eller inte krävs explicita kriterier för riskacceptans (se heldragen cirkel i figur 1 för den tredje principen). Dessa kan definieras på olika nivåer i ett järnvägssystem. De kan ses som en ”pyramid av kriterier” (se figur 9) som startar med kriterier för riskacceptans för höga nivåer (uttryckt exempelvis som en samhällsrisk eller en individuell risk) och fortsätter ned till delsystem och komponenter (för att täcka tekniska system) omfattande operatörerna under drift av och underhållsarbeten på systemet och delsystemen. Även om kriterierna för riskacceptans bidrar till att uppnå systemets säkerhetsprestanda, och därmed är sammankopplade med gemensamma säkerhetsmål och nationella referensvärden, är det mycket svårt att skapa en matematisk modell mellan dem: se {ref. 12} för mer information om detta.
Den nivå på vilken de explicita kriterierna för riskacceptans definieras måste matcha den betydande ändringens betydelse och komplexitet. Exempelvis är det inte nödvändigt att utvärdera den totala risken för järnvägssystemet då en typ av axel i den rullande materielen ändras. Definitionen av kriterierna för riskacceptans kan koncentreras till den rullande materielens säkerhet. Omvänt bör stora ändringar eller tillägg till ett befintligt järnvägssystem inte utvärderas enbart på grundval av säkerhetsprestanda för de enskilda funktionerna eller ändringarna som läggs till. Det måste också verifieras på järnvägssystemsnivå att ändringen är godtagbar i sin helhet.

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



Figur 9: Pyramid av kriterier för riskacceptans.

[G 2] De explicita kriterierna för riskacceptans som krävs för att stödja det ömsesidiga erkännandet kommer att harmoniseras mellan medlemsstaterna genom det arbete med kriterierna för riskacceptans som pågår på byrån. Ytterligare information kommer att inkluderas i detta dokument då sådan finns tillgänglig.

[G 3] Under tiden kan riskerna utvärderas med hjälp av exempelvis den riskmatris som finns i avsnitt 4.6 i standarden EN 50126-1 {ref. 8}. Andra typer av lämpliga kriterier kan också användas under förutsättning att dessa kriterier anses kunna ge en godtagbar säkerhetsnivå i det aktuella fallet.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare information om kriteriet för riskacceptans för tekniska system och vilka aspekter och funktioner för det tekniska systemet som kriteriet gäller för finns i ett separat meddelande från byrån som hör samman med det aktuella dokumentet: se avsnitt A.3. i tillägg A och referensdokument {ref. 11}.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Frankrike ● Tfn +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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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] Ytterligare förklaring bedöms inte vara nödvändig.

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

3. PÅVISANDE AV ATT SÄKERHETSKRAVEN ÄR UPPFYLLDA

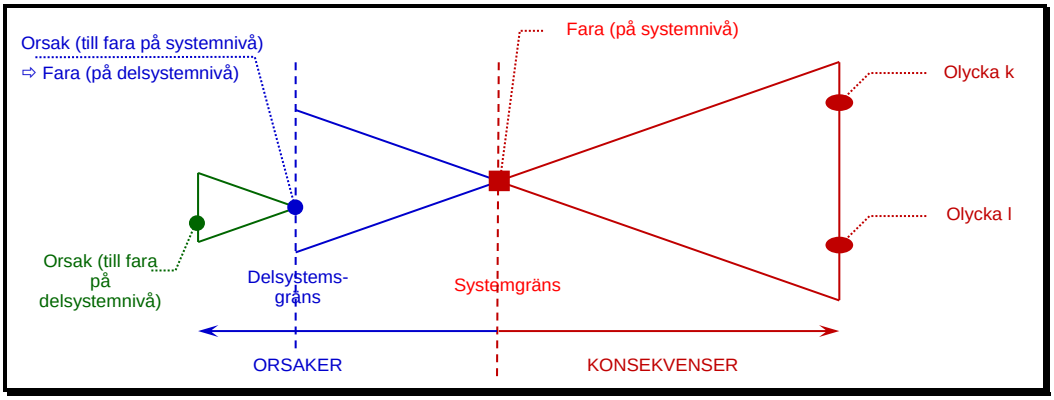
3.1. Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

[G 1] Så som förklarades i punkterna [G 3] till [G 6] i avsnitt 2.1.1, omfattar ”påvisandet av att säkerhetskraven för systemet är uppfyllda” faserna ”6 till 10” i Cenelecs V-modell (se RUTA 3 i figur 5). Se punkt [G 3] i avsnitt 2.1.1.

[G 2] Se även punkt [G 4] i avsnitt 2.1.1 i detta dokument.

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] Ett exempel på säkerhetsbedömningar och säkerhetsanalyser som kan utföras på delsystemnivå är orsaksanalyser: se figur 10. Men andra metoder kan också användas för att påvisa att delsystemet uppfyller de ingående säkerhetskraven.

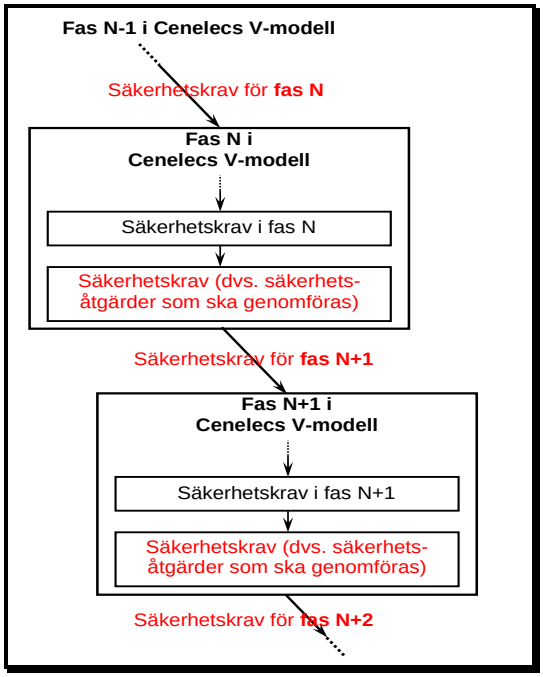


Figur 10: Figur A.4 i EN 50129: Definition av faror med hänsyn till systemgränsen.

[G 2] Den hierarkiska strukturering av faror och orsaker, med hänsyn till system och delsystem, kan upprepas för varje fas på lägre nivå i Cenelecs V-modell i figur 5. Identifieringen av faror och orsaksanalyser (eller någon annan relevant metod) liksom användning av handlingsregler, liknande referenssystem och explicita analyser och utvärderingar kan också upprepas för varje fas i systemets utvecklingscykel för att, utgående från de säkerhetsåtgärder som har identifierats på delsystemnivå, härleda de säkerhetskrav som måste uppfyllas av nästa fas. Detta åskådliggörs i figur 11.

[G 3] Se även punkt [G 4] i avsnitt 2.1.1 i detta dokument.

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



Figur 11: Härledning av säkerhetskrav för faser på lägre nivå.

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] Alla aktiviteter som finns i RUTA 3 ([12]) i Cenelecs V-modell i figur 5 kommer därmed också att genomgå en oberoende bedömning.

[G 2] Vilken typ av och detaljnivån för den oberoende bedömning som utförs av bedömningsorganen (dvs. detaljerad eller makroskopisk bedömning) diskuteras i förklaringarna till 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] Exempelvis kan den metod som används för att släcka bränder leda till en ny fara (kvävning) som innebär nya säkerhetskrav (t.ex. ett specifikt förfarande för att evakuera passagerare). Ett annat exempel är användningen av härdat glas för att undvika att fönster går sönder vid krascher och att passagerare skadas av glas eller till och med kastas ut. Den nya faran som

([12]) *Överensstämmelsen mellan aktiviteterna i den gemensamma säkerhetsmetoden och Figur 5 (dvs. figur 10 i Cenelecs V-modell i 50126) beskrivs i avsnitt 2.1.1. I punkt [G 3] i avsnitt 2.1.1 anges särskilt vilka Cenelec-aktiviteter som ingår i fasen "påvisande av att systemet uppfyller säkerhetskraven" i den gemensamma säkerhetsmetoden.*

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

detta leder till är att en nödevakuering från vagnarna genom fönstren försvåras, vilket kan leda till säkerhetskrav på att vissa fönster måste vara specialutformade för att möjliggöra en evakuering.

[G 2] Exempel på en driftsrelaterad ändring: Ett förbud mot alla transporter av farligt gods på en linje som går genom tätbefolkade områden. Transporterna ska i stället ske via en alternativ rutt med tunnlar, vilket ger upphov till andra typer av faror.

[G 3] Andra exempel på nya faror som skulle kunna identifieras under påvisandet av att systemet uppfyller säkerhetskraven finns i tillägg A.4.3 i standarden EN 50129.

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

4. HANTERING AV FAROR

4.1. Process för hantering av faror

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] Användning av ett protokoll om faror för registrering, hantering och kontroll av säkerhetsrelevant information rekommenderas också i Cenelecs standarder 50126-1 {ref. 8} och 50129 {ref. 7}.

[G 2] En aktör kan exempelvis, beroende på systemets komplexitet ha ett eller flera protokoll om faror. I båda fallen ska protokollet eller protokollen bedömas av ett eller flera oberoende bedömningsorgan. En möjlig lösning skulle exempelvis kunna vara att ha

(a) ett ”internt protokoll om faror” för hantering av alla interna säkerhetskrav som gäller det delsystem som aktören ansvarar för; dess storlek och hanteringsarbetets omfattning beror på dess struktur och naturligtvis på delsystemets komplexitet; eftersom protokollet används för interna hanteringsändamål behöver inte de andra aktörerna informeras om det; det interna protokollet om faror innehåller alla identifierade faror som kontrolleras och de tillhörande säkerhetsåtgärder som har validerats,
(b) ett ”externt protokoll om faror” för att överföra faror och tillhörande säkerhetsåtgärder (som den berörda aktören inte kan genomföra på egen hand) till andra aktörer i enlighet med avsnitt 1.2.2. Normalt är detta protokoll om faror mindre och kräver mindre hanteringsarbete (se exempel i avsnitt C.16.4. i tillägg C).

[G 3] En annan möjlig lösning, om det verkar komplicerat att hantera flera protokoll om faror, är att hantera alla faror och de tillhörande säkerhetsåtgärderna som ingår i punkterna a och b ovan i ett enda protokoll om faror men med möjlighet till två protokollrapporter om faror (se exempel i avsnitt C.16.3. i tillägg C):

(a) En intern protokollrapport om faror, som eventuellt inte behövs om protokollet om faror är så välstrukturerat att det möjliggör en oberoende bedömning.
(b) En extern protokollrapport om faror för att överföra faror och tillhörande säkerhetsåtgärder till andra aktörer.

[G 4] Så som förklaras i avsnitt 4.2 gäller följande i slutet av projektet då systemet är godkänt:

(a) Alla faror som har överförts till andra aktörer kommer att kontrolleras i det externa protokollet om faror av den aktör som överför dem. Eftersom de importeras och hanteras i de interna protokollen om faror av de andra aktörerna måste de inte hanteras vidare av den berörda aktören under (del-)systemets livscykel.
(b) Alla tillhörande säkerhetsåtgärder ska inte valideras i protokollet om faror av de skäl som förklaras i punkt [G 9] i avsnitt 4.2. Det är i själva verket lämpligt att den organisation som exporterar begränsningar av användningen tydligt påpekar i sitt protokoll om faror att de tillhörande säkerhetsåtgärderna inte har validerats.

[G 5] Omvänt förvaltas alla interna protokoll om faror under hela (del-)systemets livscykel. På så sätt kan arbetet med övervakningen av de risker som hör samman med de identifierade

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

farorna under driften och underhållet av (del-)systemet spåras, dvs. även efter dess ibruktagande: se RUTA 4 i Cenelecs V-modell i figur 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] Information om faror och tillhörande säkerhetsåtgärder som fås från andra aktörer (se avsnitt 1.2.2) omfattar även alla de antaganden ([13]) och begränsningar av användning ([13]) (även kallat säkerhetsrelaterade tillämpningsvillkor) som gäller de olika delsystemen, säkerhetsbevisningar för generiska tillämpningar och generiska produkter som har tagits fram av tillverkarna, där så är relevant.

[G 2] Ett exempel på en möjlig struktur för ett protokoll om faror finns beskriven i avsnitt C.16. i tillägg C.

4.2. Utbyte av information

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

[G 1] För exempelvis delsystemet för distansmätning i den fordonsbaserade ETCS-utrustningen kan tillverkaren validera algoritmerna i laboratoriet genom att simulera de teoretiska signalerna som skulle kunna genereras av tillhörande sensorer för distansmätning. Den fullständiga valideringen av delsystemet för distansmätning kräver hjälp av järnvägsföretaget och infrastrukturförvaltaren för att utföra valideringen med hjälp av ett riktigt tåg och riktig kontakt mellan tågets hjul och rälsen.

[G 2] Andra exempel skulle kunna vara överföring av driftsrelaterade eller underhållsmässiga säkerhetsåtgärder för teknisk utrustning från tillverkare till järnvägsföretag. Dessa säkerhetsåtgärder måste genomföras av järnvägsföretaget.

[G 3] För att göra det möjligt för de berörda organisationerna att göra en ny gemensam bedömning av dessa faror, tillhörande säkerhetsåtgärder och risker underlättar det om organisationen, som har identifierat dem, tillhandahåller all information som krävs för att tydligt förstå problemet. Eventuellt måste de ursprungliga formuleringarna av farorna, säkerhetsåtgärderna och riskerna ändras för att göra dem begripliga utan att de behöver diskuteras gemensamt igen. Den gemensamma nya bedömningen av farorna kan leda till att nya säkerhetsåtgärder identifieras.

([13]) *Se punkt [G 5] i avsnitt 1.1.5 och fotnoterna ([7]) och ([8]) på sidan 31 i detta dokument om en närmare förklaring av terminologin "säkerhetsbevisning för generisk produkt och generisk tillämpning", "antaganden och begränsningar av användning".*

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

[G 4] Den mottagande aktören som ansvarar för genomförande, verifiering och validering av de mottagna eller nya säkerhetsåtgärderna registrerar alla därtill hörande faror med de tillhörande säkerhetsåtgärderna (både de importerade och de gemensamt identifierade) i sitt eget protokoll om faror.

[G 5] Då en säkerhetsåtgärd inte kan valideras fullständigt måste en klar begränsning av användningen (t.ex. driftsrelaterade mildrande åtgärder) utarbetas och registreras i protokollet om faror. Det är möjligt att tekniska/konstruktionsmässiga säkerhetsåtgärder

(a) inte är korrekt genomförda, eller
(b) inte är fullständigt genomförda, eller
(c) avsiktligt inte är genomförda, exempelvis eftersom flera säkerhetsåtgärder är genomförda i stället för de som är registrerade i protokollet om faror (t.ex. av kostnadsskäl); eftersom de inte är validerade måste sådana säkerhetsåtgärder tydligt identifieras i protokollet om faror; bevisning/motivering måste tillhandahållas varför dessa säkerhetsåtgärder som har genomförts i stället ([14]) är lämpliga, liksom ett påvisande av att systemet uppfyller säkerhetskraven med dessa nya säkerhetsåtgärder,
(d) etc.

I dessa fall kan de därtill hörande tekniska/konstruktionsmässiga säkerhetsåtgärderna inte verifieras och valideras under hanteringen av faror. De därtill hörande farorna och säkerhetsåtgärderna måste då förbli öppna i protokollet om faror för att undvika felaktig användning av säkerhetsåtgärderna i andra system genom tillämpning av principen för riskacceptans för ”liknande referenssystem”.

[G 6] Normalt upptäcks de ”inte korrekt” och/eller ”inte fullständigt” genomförda säkerhetsåtgärderna tidigt i systemets livscykel och korrigeras innan systemet har godkänts. Om detta upptäcks för sent för att en teknisk säkerhetsåtgärd ska kunna genomföras korrekt och fullständigt, måste den organisation som är ansvarig för genomförandet och hanteringen identifiera och registrera tydliga begränsningar av användningen för det system som är föremål för bedömning i protokollet om faror. Dessa begränsningar av användningen utgörs ofta av driftsrelaterade tillämpningsbegränsningar för det system som är föremål för bedömning.

[G 7] Det kan också vara praktiskt att registrera i protokollet om faror om de tillhörande säkerhetsåtgärderna kommer att genomföras på ett korrekt sätt under ett senare skede i systemets livscykel eller om systemet kommer att fortsätta användas med de identifierade begränsningarna av användningen. Det kan också vara praktiskt att registrera motiveringen till varför de tillhörande tekniska säkerhetsåtgärderna inte genomfördes korrekt/fullständigt i protokollet om faror.

[G 8] Aktören som tar emot begränsningarna av användning

(a) ska importera alla dessa i sitt eget protokoll om faror,
(b) säkerställa att användningsförhållandena för det system som är föremål för bedömning överensstämmer med de mottagna begränsningarna av användning,
(c) verifiera och validera att det system som är föremål för bedömning överensstämmer med dessa begränsningar av användning.

[G 9] Beroende på de beslut som de berörda organisationerna har kommit överens om gäller följande:

([14]) *Om andra säkerhetsåtgärder genomförs i stället för dem som ursprungligen identifierades måste detta också registreras i protokollet om faror.*

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

(a) Antingen ska de därtill hörande tekniska säkerhetsåtgärderna genomföras korrekt i konstruktionen i ett senare skede.
Den organisation som exporterar begränsningar av användning fortsätter att spåra korrekt tekniskt genomförande av de tillhörande säkerhetsåtgärderna. Följaktligen kan de därtill hörande säkerhetsåtgärderna inte valideras och de faror som hör samman med dem inte kontrolleras i denna organisations protokoll om faror så länge motsvarande tekniska säkerhetsåtgärder inte har genomförts fullständigt. Detta måste säkerställas även om de exporterade begränsningarna av användning införs under tiden.

(b) Eller så kommer de därtill hörande tekniska säkerhetsåtgärderna inte att genomföras i konstruktionen i ett senare skede. Systemet kommer därmed under hela sin livscykel att fortsätta användas med de tillhörande begränsningarna av användning. I detta fall kan följande göras:

(1) Den organisation som exporterar begränsningarna av användning registrerar inte de tillhörande säkerhetsåtgärderna som ”validerade” i sitt protokoll om faror. På detta sätt kommer inte de motsvarande säkerhetsproblemen att förbises om systemet används som ett referenssystem i andra projekt. Även om en annan aktör går med på att hantera de tillhörande riskerna på ett annat sätt, är det praktiskt om den organisation som exporterar begränsningarna av användning tydligt markerar i sitt protokoll om faror att de tillhörande säkerhetsåtgärderna inte har validerats.

(2) Systembeskrivningen kan ändras så att den innefattar begränsningarna av användning i systemets tillämpningsområde (dvs. antagandena för systemet) och i säkerhetskraven. Detta gör det möjligt att kontrollera farorna. Om systemet används som referenssystem i en annan tillämpning

(i) måste det nya systemet användas under samma förhållanden (dvs. för att uppfylla de begränsningar av användning som hör samman med dessa antaganden) eller
(ii) ska en ytterligare riskbedömning utföras av förslagsställaren för avvikelserna gentemot dessa antaganden.

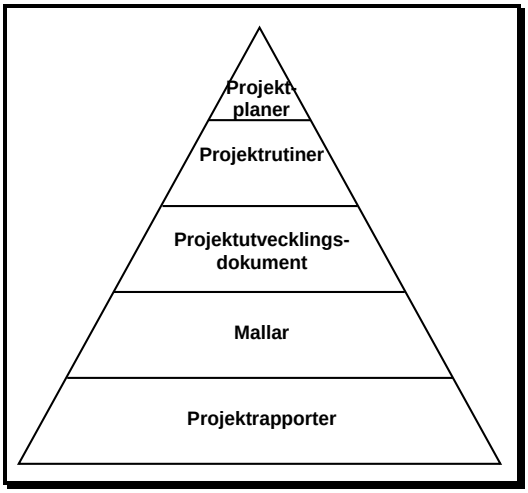
European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Frankrike ● Tfn +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

5. BEVISNINGAR FRÅN TILLÄMPNINGEN AV RISKHANTERINGSPROCESSEN

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] Dessa krav beaktas redan i infrastrukturförvaltarens och järnvägsföretagets säkerhetsstyrningssystem. Även om säkerhetsstyrningssystemet inte är obligatoriskt för de andra aktörerna inom järnvägssektorn som berörs av den betydande ändringen har de i allmänhet, åtminstone på projektnivå, en kvalitetsstyrningsprocess och/eller en säkerhetsstyrningsprocess. Båda dessa processer är beroende av en strukturerad dokumentationshierarki, antingen inom företaget eller åtminstone inom projektet. De tar även hänsyn till dokumentationsbehoven som hör samman med RAMS-hanteringen. En sådan strukturerad dokumentation kan i princip bestå av följande (se även figur 12):

(a) **Projektplaner** som har tagits fram för att beskriva den organisation som ska inrättas för att hantera en aktivitet inom ett projekt.
(b) **Projektrutiner** som har tagits fram för att i detalj beskriva hur en särskild uppgift ska genomföras. Normalt finns det redan rutiner och anvisningar inom företaget som kan användas. Nya projektrutiner tas endast fram om det finns ett behov att beskriva en specifik uppgift inom projektet i fråga.
(c) **Projektutvecklingsdokument** som har tagits fram under systemets livscykel enligt figur 5.
(d) **Företagsmallar eller åtminstone projektmallar** för olika typer av dokument som ska tas fram.



Figur 12: Strukturerad dokumentationshierarki.

(e) **Projektrapporter** som har tagits fram under projektets gång och som krävs för att påvisa att kraven i företagets kvalitets- och säkerhetsstyrningsprocesser uppfylls.

Detta är ett sätt att uppfylla dokumentationskraven. Det kan finnas andra sätt som också uppfyller kriterierna enligt den gemensamma säkerhetsmetoden.

[G 2] I Cenelec-standarderna rekommenderas påvisandet av att systemet uppfyller funktions- och säkerhetskraven i ett säkerhetsbevisningsdokument (eller i en säkerhetsrapport). Även om detta inte är obligatoriskt tillhandahåller säkerhetsbevisningen följande i ett strukturerat dokument som bestyrker säkerheten:

(a) Bevis på kvalitetsstyrning.
(b) Bevis på säkerhetsstyrning.
(c) Bevis på funktionell och teknisk säkerhet.

Den innebär samtidigt den fördelen att den stöder och vägleder bedömningsorganen i sin oberoende bedömning av om den gemensamma säkerhetsmetoden har tillämpats korrekt.

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

[G 3] I säkerhetsbevisningen beskrivs och sammanfattas hur projektdokumenten från tillämpningen av företagets eller projektets kvalitets- och/eller säkerhetsstyrningsprocesser hänger ihop med systemutvecklingsprocessen för att påvisa systemets säkerhet. Normalt omfattar säkerhetsbevisningen inte stora mängder detaljerade bevis eller stödjande dokumentation utan tillhandahåller i stället noggranna hänvisningar till sådana dokument.

[G 4] **Säkerhetsbevisning för tekniska system:** Cenelec-standarderna kan användas som riktlinjer för att skriva säkerhetsbevisningar och/eller strukturera dem:

(a) Se standarden EN 50129 {ref. 7} ”Järnvägsanläggningar – Dataöverföring och järnvägsstyrning – Elektroniska signalsystem av betydelse för säkerheten”. I tillägg H.2 i vägledningen EN 50126-2 {ref. 9} föreslås också en struktur för säkerhetsbevisningen för signalsystem.
(b) Se tillägg H.1 i vägledningen EN 50126-2 {ref. 9} om strukturen för säkerhetsbevisningen för rullande materiel.
(c) Se tillägg H.3 i vägledningen EN 50126-2 {ref. 9} om strukturen för säkerhetsbevisningen för infrastrukturer.

Så som framgår av dessa referenser beror säkerhetsbevisningens struktur för tekniska system, liksom dess innehåll, på det system för vilket uppfyllandet av säkerhetskraven ska påvisas.

Den säkerhetsbevisning som beskrivs i tillägg H i vägledningen EN 50126-2 {ref. 9} utgör endast exempel och kan kanske inte tillämpas på alla system av den angivna typen. Därför bör de allmänna principerna användas med lämplig bedömning av vad som passar i varje specifik tillämpning.

[G 5] **Säkerhetsbevisning för organisatoriska och driftsrelaterade aspekter för järnvägssystem:**

För närvarande finns det inte någon särskild standard som anger strukturen, innehållet och en vägledning för hur man skriver säkerhetsbevisning för organisatoriska och driftsrelaterade aspekter för ett järnvägssystem. Men eftersom säkerhetsbevisningen strävar efter att på ett strukturerat sätt påvisa att systemet uppfyller sina säkerhetskrav kan samma typ av säkerhetsbevisningsstruktur användas som för tekniska system. Referenserna i punkt [G 4] i avsnitt 5.1 tillhandahåller råd och en checklista med punkter som bör behandlas oberoende av vilken typ av system som är föremål för bedömning. Hanteringen av organisatoriska och driftsrelaterade ändringar kräver samma typ av kvalitets- och säkerhetsstyrningsprocesser som tekniska ändringar, med ett påvisande av att systemet uppfyller de specificerade säkerhetskraven. De krav i Cenelec-standarderna som inte kan tillämpas på organisatoriska och driftsrelaterade aspekter är de som uteslutande hänför sig till konstruktionsmöjligheter för tekniska system, såsom principer för ”inneboende felsäkerhet hos maskinvara”, elektromagnetisk kompatibilitet (EMC) etc.

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

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

[G 1] Beroende på systemets komplexitet kan dessa bevis samlas i en eller flera säkerhetsbevisningar. Se punkterna [G 4] och [G 5] i avsnitt 5.1 för strukturerna för säkerhetsbevisningen för tekniska system samt driftsrelaterade och organisatoriska aspekter.

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

[G 2] Se exemplen på bevisningar i avsnitt A.4. i tillägg A.

[G 3] Livstiden för tekniska system och delsystem inom järnvägssektorn beräknas i allmänhet till omkring 30 år. Under en sådan lång tidsperiod är det rimligt att även anta att en rad betydande ändringar av systemet kommer att göras. Ytterligare riskbedömningar ska därför utföras för dessa system och deras kontaktpunkter med tillhörande dokumentation som kommer att behöva granskas, kompletteras och överföras mellan olika aktörer och organisationer med hjälp av protokoll om faror. Detta innebär tämligen strikta krav på dokumentationskontroll och konfigurationsstyrning.

[G 4] Det är då praktiskt att företaget som arkiverar all riskbedömnings- och riskhanteringsinformation säkerställer att resultaten/informationen lagras på ett fysiskt medium som kan läsas/är åtkomligt under systemets hela livscykel (t.ex. under 30 år).

[G 5] De viktigaste skälen till detta krav är bland annat

(a) att säkerställa att alla säkerhetsanalyser och all säkerhetsdokumentation för det system som är föremål för bedömning är åtkomliga under hela systemlivslängden; således

(1) vid ytterligare betydande ändringar av samma system finns den senaste systemdokumentationen tillgänglig,
(2) vid några problem under systemets livslängd är det praktiskt att kunna gå tillbaka till de tillhörande säkerhetsanalyserna och säkerhetsdokumentationen,

(b) att säkerställa att säkerhetsanalyserna och säkerhetsdokumentationen för det system som är föremål för bedömning är åtkomliga i det fall det används i en annan tillämpning som ett liknande referenssystem.

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

BILAGA II TILL FÖRORDNINGEN OM EN GEMENSAM SÄKERHETSMETOD

Kriterier som måste uppfyllas av bedömningsorganen

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] Ytterligare förklaring bedöms inte vara nödvändig.

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

TILLÄGG A: YTTERLIGARE FÖRTYDLIGANDEN

A.1. Inledning

A.1.1. Syftet med detta tillägg är att underlätta läsningen av det aktuella dokumentet. I stället för att tillhandahålla en stor mängd information i dokumentet, förklaras komplicerade ämnen mer ingående i detta tillägg.

A.2. Klassificering av faror

A.2.1. Det finns en vägledning i avsnitt 4.6.3 i standarden EN 50126-1 {ref. 8}, liksom i tillägg B.2 i vägledningen EN 50126-2 {ref. 9}, för klassificeringen/rankningen av faror.

A.3. Kriterium för riskacceptans för tekniska system

A.3.1. Övre gräns för riskacceptans för tekniska system

A.3.1.1. Kriteriet för riskacceptans för tekniska system beskrivs i avsnitt 2.5.4. i {ref. 4}.

A.3.1.2. Syftet med kriteriet för riskacceptans för tekniska system är att specificera en övre gräns för riskacceptans för tekniska system för vilka säkerhetskrav varken kan härledas genom tillämpning av handlingsregler eller genom jämförelse med liknande referenssystem. Följaktligen definieras en referenspunkt, som kan användas för kalibreringen av riskanalysmetoderna för tekniska system. Så som beskrivs i avsnitt A.3.6. i tillägg A till detta dokument kan denna referenspunkt eller den övre gränsen för godtagbara risker också användas för att bestämma kriterier för riskacceptans för andra funktionsfel för tekniska system som inte har någon trolig direkt potential för en katastrofal konsekvens (dvs. för andra allvarliga följder). Kriteriet för riskacceptans för tekniska system är dock inte någon riskanalysmetod.

A.3.1.3. Kriteriet för riskacceptans för tekniska system är ett semikvantitativt kriterium. Det gäller både slumpmässiga maskinvarufel och systematiska felyttringar/fel i tekniska system. De systematiska felyttringarna/felen i tekniska system som skulle kunna orsakas av mänskliga fel under det tekniska systemets utvecklingsprocess (dvs. specifikation, konstruktion, genomförande och validering) täcks således. Men mänskliga fel under drift och underhåll av tekniska system ingår inte i kriteriet för riskacceptans för tekniska system.

A.3.1.4. Enligt tilläggen A.3 och A.4 i Cenelec-standarden 50129 är systematiska felyttringar/fel inte kvantifierbara och därför måste det kvantitativa målet endast visas för slumpmässiga maskinvarufel, eftersom de systematiska felyttringarna/felen hanteras av de kvalitativa metoderna ([15]). *Eftersom det inte är möjligt att bedöma tillförlitligheten mot systematiska fel med hjälp av kvantitativa metoder används tillförlitlighetsnivåer för att gruppera metoder, verktyg och tekniker som, då de används på ett effektivt sätt, anses*

([15]) *Enligt Cenelec-standarderna 50126, 50128 och 50129 måste den kvantitativa uppgiften för slumpmässiga maskinvarufel alltid kopplas till en tillförlitlighetsnivå för att de systematiska felyttringarna/felen ska kunna hanteras. Därför innebär värdet $10^{-9}\,h^{-1}$ i kriteriet för riskacceptans för tekniska system att en lämplig process måste införas för att även de systematiska felyttringarna/felen ska kunna hanteras på ett korrekt sätt. För att underlätta läsningen av denna anmärkning hänför sig värdet normalt enbart till slumpmässiga maskinvarufel för tekniska system.*

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

tillhandahålla en lämplig konfidensnivå vid genomförandet av ett system med en angiven tillförlitlighetsnivå.

A.3.1.5. Likaledes är enligt Cenelec-standarderna tillförlitligheten för programvara till tekniska system inte kvantifierbar. I Cenelec-standarden 50128 finns vägledning för utvecklingsprocessen för säkerhetsrelaterad programvara med avseende på den tillförlitlighetsnivå som krävs. Den omfattar processer för utformning, verifiering, validering och kvalitetssäkring av programvaran.
Enligt Cenelec-standarden 50128 är SIL 4 den högsta möjliga tillförlitlighetsnivån för programvaruutvecklingsprocessen för ett programmerbart elektroniskt styrsystem vid genomförandet av säkerhetsfunktioner, vilket motsvarar en kvantitativ tolererbar risknivå på $10^{-9}\ h^{-1}$.

A.3.1.6. Eftersom de systematiska felyttringarna/felen inte kan kvantifieras behöver de i stället hanteras kvalitativt genom införandet av en kvalitets- och säkerhetsprocess som är förenlig med den tillförlitlighetsnivå som krävs för det system som är föremål för bedömning.

(a) Syftet med kvalitetsprocessen är *att minimera förekomsten av mänskliga fel i varje steg i livscykeln och på så sätt minska risken för systematiska fel i systemet.*
(b) Syftet med säkerhetsprocessen är *att minska ytterligare förekomsten av säkerhetsrelaterade mänskliga fel under hela livscykeln och på så sätt minska den kvarvarande risken för säkerhetsrelaterade systematiska fel.*

A.3.1.7. Vägledning för att hantera förekomsten av systematiska felyttringar/fel samt vägledning för eventuella konstruktionsrelaterade åtgärder för att skydda mot gemensamma felorsaker (CCF)/gemensamma felyttringar (CMF) och säkerställa att det tekniska systemet övergår till ett felsäkert tillstånd vid sådana felyttringar/fel finns i följande standarder:

(a) I Cenelec-standarden 50126-1 {ref. 8} och dess vägledning 50126-2 {ref. 9} anges bestämmelserna enligt Cenelec 50129 och deras tillämpbarhet på dokumenterad bevisning för andra system än signalsystem: se tabell 9.1 i vägledningen 50126-2 {ref. 9}. Denna förteckning innehåller hänvisningar till vägledningen om hur man ska hantera både fel som kommer från själva systemet och dess påverkan på miljön för det system som är föremål för bedömning.

Tekniker/åtgärder för konstruktionsegenskaper anges exempelvis i *tabell E.5: Konstruktionsegenskaper (som hänvisas till i 5.4)* i Cenelec-standarden 50129 {ref. 7}, *för att undvika och kontrollera fel som orsakas av*

(1) *eventuella kvarvarande konstruktionsfel,*
(2) *miljöbetingelser,*
(3) *felaktig användning eller driftsrelaterade misstag,*
(4) *eventuella kvarvarande fel i programvaran,*
(5) *mänskliga faktorer.*

Tilläggen D och E till Cenelec-standarden 50129 {ref. 7} innehåller tekniker och åtgärder för att undvika systematiska fel och för att kontrollera slumpmässiga felyttringar/fel för maskinvaran och systematiska felyttringar/fel för säkerhetsrelaterade elektroniska signalsystem. Många av dem kan utökas till andra system än signalsystem genom en hänvisning till dessa riktlinjer i tabell 9.1 i vägledningen 50126-2 {ref. 9}.

(b) Cenelec-standarden 50128 innehåller vägledning för utvecklingsprocessen för säkerhetsrelaterad programvara med avseende på den tillförlitlighetsnivå (SIL 0 till SIL 4) som krävs för programvaran för det system som är föremål för bedömning.

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

A.3.1.8. Kriteriet för riskacceptans för tekniska system utgör även den högsta tillförlitlighetsnivån som kan krävas enligt både Cenelec- och IEC-standarderna. Av praktiska skäl återges här kraven från IEC 61508-1 och Cenelec 50129:

(a) IEC 61508-1: *I denna standard fastställs en lägre gräns för de eftersträvade felyttringsvärdena för en farlig felmod som kan åberopas. Dessa definieras som de lägre gränserna för tillförlitlighetsnivå 4. Det kan vara möjligt att åstadkomma säkerhetsrelaterade system vars utformning leder till lägre värden för de eftersträvade felyttringsvärdena för icke-komplexa system, men det anses att siffrorna i tabellen utgör den gräns som för närvarande kan uppnås för relativt komplexa system (t.ex. programmerbara elektroniska säkerhetsrelaterade system).*

(b) EN 50129: *En funktion vars kvantitativa krav är strängare än 10^{-9} h^{-1} ska behandlas på ett av följande sätt:*

(1) *Om det är möjligt att dela upp funktionen i funktionellt oberoende delfunktioner, kan den tolererbara risknivån delas upp mellan dessa delfunktioner och ett SIL-värde tilldelas till var och en av delfunktionerna.*

(2) *Om funktionen inte kan delas upp ska minst de åtgärder och metoder som krävs för SIL 4 uppfyllas och funktionen ska användas i kombination med andra tekniska eller driftsrelaterade åtgärder för att uppnå den tolererbara risknivå som krävs.*

A.3.1.9. Alla tekniska system måste därefter begränsa det kvantitativa säkerhetskravet till detta värde. Om det finns behov för en högre grad av skydd kan detta inte uppnås med endast ett system. Systemets arkitektur måste ändras, exempelvis genom parallell användning av två oberoende system som utför en dubbelkontroll mellan varandra för att generera säkra resultat. Men detta ökar definitivt utvecklingskostnaderna för det tekniska systemet.

Anmärkning: Om det finns befintliga funktioner, t.ex. rent mekaniska system med vilka man, baserat på drifterfarenhet, kan uppnå en högre tillförlitlighetsnivå, kan säkerhetsnivån beskrivas med hjälp av en särskild handlingsregel eller så kan säkerhetskraven anges genom likhetsanalys med befintliga system. Inom ramen för den gemensamma säkerhetsmetoden behöver kriteriet för riskacceptans för tekniska system endast tillämpas om det inte finns någon handlingsregel eller något referenssystem.

A.3.1.10. Följande slutsatser kan dras:

(a) Enligt Cenelec-standarderna 50126, 50128 och 50129 är systematiska felyttringar/fel inom utvecklingen inte kvantifierbara.

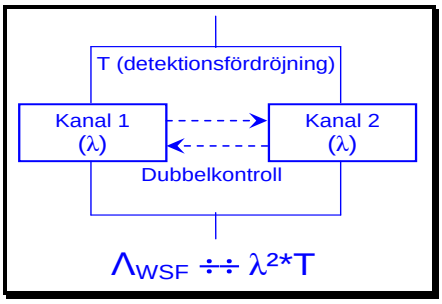
(b) Förekomsten av systematiska felyttringar/fel liksom deras kvarvarande risk, måste kontrolleras och hanteras genom tillämpning av lämplig kvalitets- och säkerhetsprocess som är förenlig med den tillförlitlighetsnivå som krävs för det system som är föremål för bedömning.

(c) Den högsta uppnåbara tillförlitlighetsnivån är SIL 4 för både slumpmässiga maskinvarufel och systematiska felyttringar/fel i tekniska system.

(d) Denna gräns för tillförlitlighetsnivån SIL 4 innebär att den maximalt tolererbara risknivån (dvs. den maximala felintensiteten) för tekniska system också måste begränsas till 10^{-9} h^{-1}.

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

A.3.1.11. En tolererbar risknivå på 10^{-9} h^{-1} kan uppnås för tekniska system med antingen en "felsäker arkitektur" (som per definition uppfyller ett sådant säkerhetskrav) eller "en redundant arkitektur" (t.ex. två oberoende bearbetningskanaler som dubbelkontrollerar varandra).



Figur 13: Redundant arkitektur för ett tekniskt system.

För en redundant arkitektur kan det visas att det totala säkerhetsfarliga felet (Λ_{WSF}) för tekniska system är proportionellt mot λ^2*T där

(a) λ^2 utgör kvadraten på intensiteten för säkerhetsfarliga fel för en av kanalerna,

(b) T utgör den tid som krävs för att en kanal ska upptäcka ett eller flera säkerhetsfarliga fel för den andra kanalen. Detta är normalt en multipel av bearbetningstiden/-cykeln för en kanal. Normalt är T mycket mindre än 1 sekund.

A.3.1.12. Baserat på denna formel (λ^2*T) kan det teoretiskt visas (då endast hänsyn tas till de slumpmässiga maskinvarufelen i det tekniska systemet – se även punkt A.3.1.13. i tillägg A) – att ett kvantitativt krav på 10^{-9} h^{-1} för kriteriet för riskacceptans för tekniska system kan uppnås. De systematiska felyttringarna/felen måste hanteras med hjälp av en process: se punkt A.3.1.6. i tillägg A. Exempel:

(a) Med en medeltid mellan fel (MTBF) på 10 000 h för tillförlitlighetsnivån per kanal och ett konservativt antagande om att alla kanalfel är farliga är det säkerhetsfarliga felet för kanalen 10^{-4} h^{-1}.

(b) Även med en tid på 10 min (dvs. $\approx 2*10^{-3}$ h) för att upptäcka det säkerhetsfarliga felet för den andra kanalen, som också är ett konservativt antagande,

är det totala säkerhetsfarliga felet $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}.

A.3.1.13. För en sådan redundant arkitektur måste i praktiken hänsyn tas, vid utvärderingen av de kvantitativa totala säkerhetsfarliga maskinvarufelen, till de åtgärder som har vidtagits vid konstruktionen för att skydda mot de gemensamma felorsakerna och de gemensamma felyttringarna (CCF/CMF) och för att säkerställa att det tekniska systemet övergår till ett felsäkert läge vid CCF/CMF-felyttring/fel. Denna utvärdering av det totala säkerhetsfarliga felet (Λ_{WSF}) behöver således också beakta

(a) de komponenter som är gemensamma för alla kanalerna, t.ex. enskilda eller gemensamma indata till alla kanaler, gemensam strömförsörjning, komparatorer, väljare etc.,

(b) den tid som krävs för att upptäcka vilande eller latenta fel; för komplexa tekniska system kan denna tid vara flera storleksordningar längre än 1 sekund,

(c) inverkan av den gemensamma felorsaken/felyttringen (CCF/CMF).

Vägledning om dessa ämnen finns i de standarder som anges i punkt A.3.1.7. i tillägg A till detta dokument.

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

A.3.2. Flödesschema för tillämplighetstestet för kriteriet för riskacceptans för tekniska system

A.3.2.1. Det sätt som kriteriet för riskacceptans för tekniska system ska tillämpas på för de faror som uppkommer på grund av felyttringar i tekniska system kan åskådliggöras så som visas i figur 14.

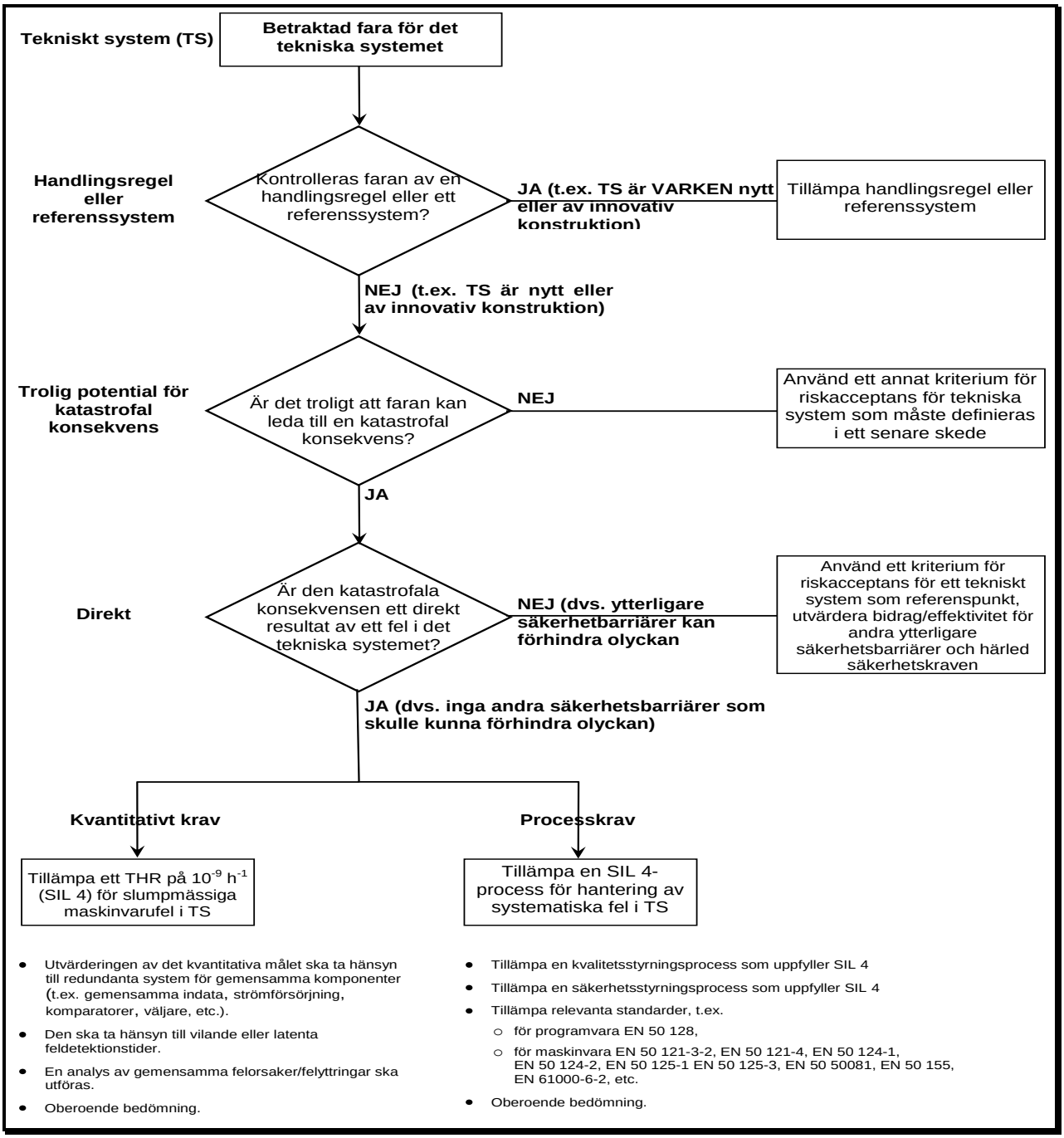
A.3.2.2. Tillämpningen av detta flödesschema på ett exempel ges i avsnitt C.15. i tillägg C.

A.3.3. Definition av ett tekniskt system enligt den gemensamma säkerhetsmetoden

A.3.3.1. Kriteriet för riskacceptans för tekniska system gäller endast tekniska system. Följande definition för ”tekniska system” finns i artikel 3(22) i förordningen om en gemensam säkerhetsmetod:

"tekniskt system: en produkt eller sammansättning av produkter inklusive utformning, förverkligande och dokumentation. Utvecklingen av ett tekniskt system påbörjas med dess kravspecifikation och slutförs med att systemet godkänns. Även om utformningen av relevanta kontaktpunkter med människor beaktas, innefattas människor och deras åtgärder inte i ett tekniskt system. Underhållsprocessen beskrivs i underhållsmanualer men ingår inte i sig i det tekniska systemet."

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



Figur 14: Flödesschema för tillämplighetstesten enligt kriteriet för riskacceptans för tekniska system.

A.3.4. Förklaring av definitionen av ”tekniskt system”

A.3.4.1. Denna definition av ett tekniskt system beskriver vad som menas med ett tekniskt system: ”*tekniskt system: en produkt eller sammansättning av produkter inklusive utformning, förverkligande och dokumentation.*” Följaktligen består det av och omfattar följande:

(a) De fysiska delarna som utgör det tekniska systemet.

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

(b) Den tillhörande programvaran (om det finns någon).
(c) Konstruktionen och genomförandet av det tekniska systemet, inklusive i tillämpliga fall konfigureringen eller parametriseringen av en generisk produkt enligt specifika krav för den specifika tillämpningen.
(d) Stödjande dokumentation som krävs för

(1) utvecklingen av det tekniska systemet,
(2) drift och underhåll av det tekniska systemet.

A.3.4.2. De kommentarer som hör samman med denna definition specificerar ytterligare det tekniska systemets omfång:

(a) *”Utvecklingen av ett tekniskt system påbörjas med dess kravspecifikation och slutförs med att systemet godkänns.”* Detta omfattar faserna 1 till 10 i den V-modell som visas i figur 10 i Cenelec-standarden 50126-1 {ref. 8}.

(b) *”Även om utformningen av relevanta kontaktpunkter med människor beaktas, innefattas människor och deras åtgärder inte i ett tekniskt system.”* Även om fel under drift och underhåll av ett tekniskt system som beror på den mänskliga faktorn inte utgör en del av det tekniska systemet i sig, måste hänsyn tas till utformningen av kontaktpunkter med operatörer. Syftet är att minimera sannolikheten för mänskliga fel på grund av dålig utformning av de relevanta kontaktpunkterna med operatörerna.

(c) *”Underhållsprocessen beskrivs i underhållsmanualer men ingår inte i sig i det tekniska systemet.”* Detta innebär att kriteriet för riskacceptans för tekniska system inte behöver tillämpas på driften och underhållet av ett tekniskt system. Detta är starkt beroende av de processer och handlingar som utförs av personalen.
För att stödja underhållet av tekniska system måste definitionen av det tekniska systemet innefatta alla relevanta krav (t.ex. regelbundet preventivt underhåll, eller reparationer vid fel), med en tillräcklig detaljnivå. Men hur underhållet ska organiseras och utföras på det därtill hörande tekniska systemet utgör inte någon del av definitionen av det tekniska systemet utan ska ingå i motsvarande underhållsmanualer.

A.3.4.3. Se även avsnitt A.3.1. i tillägg A.

A.3.5. Funktioner i tekniska system som omfattas av kriteriet för riskacceptans för tekniska system

A.3.5.1. Enligt definitionen av kriteriet för riskacceptans för tekniska system gäller kriteriet säkerhetsfarliga fel hos de funktioner som det tekniska systemet ska uppfylla om de har *”en sannolik **direkt** potential för katastrofala konsekvenser”*: se avsnitt 2.5.4. i {ref. 4}.

A.3.5.2. Kriteriet för riskacceptans för tekniska system kan också tillämpas på funktioner som omfattar tekniska system men vars fel **inte har** *”**direkt** potential för katastrofala konsekvenser”*. I detta fall måste kriteriet för riskacceptans för tekniska system tillämpas som ett övergripande mål för en uppsättning händelser som leder till den katastrofala konsekvensen. På grundval av detta övergripande mål måste det verkliga bidraget av varje händelse, och således de funktionella felen hos det tekniska system som ingår i scenariot i fråga, härledas enligt avsnitt A.3.6. i tillägg A.
En sådan tillämpning av kriteriet för riskacceptans för tekniska system måste diskuteras och en överenskommelse träffas med arbetsgruppen för gemensamma säkerhetsmetoder.

A.3.5.3. Vilka funktioner av det tekniska systemet omfattas av kriteriet för riskacceptans för tekniska system? Enligt standarden IEC 61226:2005 gäller följande:

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

(a) En funktion definieras i detta sammanhang som ett *specifikt syfte eller mål som ska uppnås som kan specificeras eller beskrivas utan hänvisning till de fysiska medel med vilka de uppnås*.
(b) En funktion (betraktad som en svart låda) överför ingående parametrar (t.ex. material, energi, information) till utgående parametrar som hör samman med målet (t.ex. material, energi, information).
(c) Analysen av funktionen är oberoende av dess tekniska genomförande.

A.3.5.4. Kriteriet för riskacceptans för tekniska system kan tillämpas på följande typer av funktioner:

(a) Exempel för ett fordonsbaserat ETCS-delsystem:

(1) ”Förser föraren med information som gör det möjligt för föraren att köra tåget på ett säkert sätt och framkalla en bromsansättning vid överhastighet.” På grundval av den information som tas emot från marken (tillåten hastighet) och beräkningen av tågets hastighet från den fordonsbaserade ETCS-utrustningen kan föraren och den fordonsbaserade ETCS-utrustningen övervaka att tåget inte överskrider den tillåtna hastigheten. Kriteriet för riskacceptans för tekniska system gäller utvärderingen av tågets hastighet med hjälp av den fordonsbaserade utrustningen eftersom

(i) det inte finns någon ytterligare barriär (direkt) då den information som föraren får tillgång till också är underskattad,
(ii) tågets överhastighet skulle kunna leda till urspårning vilket är en olycka med potential för katastrofala konsekvenser.

(2) ”Förser föraren med information som gör det möjligt för föraren att köra tåget på ett säkert sätt och framkalla en bromsansättning vid en överträdelse av det tillåtna körbeskedet.”

(b) Exempel för en spårledning: ”Upptäckt av att spåravsnittet är upptaget.” Kriteriet för riskacceptans för tekniska system kommer endast att vara tillämpbart som sådant på denna funktion om det inte finns någon funktion för ”sekvensövervakning” genomförd i signalställverket.
(c) Exempel för en punkt: ”Kontroll av punktens position.”

A.3.5.5. I vissa standarder definieras också funktioner som kriteriet för riskacceptans för tekniska system skulle kunna tillämpas på. Exempel:

(a) I standarden prEN 15380-4 {ref. 13} (ModTrain-arbete) definieras i dess normgivande del tre hierarkiska funktionsnivåer (som har utökats i de informativa bilagorna till fem nivåer). I hela prEN 15380-4 definieras flera hundra funktioner som hänför sig till tåg.
(b) I allmänhet rekommenderas val av funktioner från de tre första nivåerna enligt prEN 15380-4 (men inte lägre), varvid hänsyn också ska tas till produktnedbrytningens struktur.
(c) För funktioner som inte omfattas av prEN 15380-4 måste den korrekta funktionsnivån fastställas genom jämförelse under användning av en expertbedömning.

Dessa exempel på funktioner från prEN 15380-4 kommer byrån att behöva arbeta vidare med i sitt arbete med allmänt godtagbara risker och kriterier för riskacceptans.

A.3.5.6. Kriteriet för riskacceptans för tekniska system kan också tillämpas på exempelvis följande funktioner i prEN 15380-4: *”lutningskontroll”* (kod = CLB). Funktionen kan användas på systemnivå på två sätt:

(a) Fall ett: Tåget ska lutas i kurvorna för passagerarnas komfort och funktionen måste övervaka att tågets lastprofil överensstämmer med den markbaserade infrastrukturen.

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

(b) Fall två: Tåget ska lutas i kurvorna enbart för passagerarnas komfort men funktionen behöver inte övervaka att tågets lastprofil överensstämmer med den markbaserade infrastrukturen.

I det första fallet kommer kriteriet för riskacceptans för tekniska system att tillämpas men inte i det andra fallet eftersom ett fel på lutningsfunktionen inte leder till katastrofala konsekvenser.

A.3.5.7. Exempel (b) i punkt A.3.5.4. och exemplen i punkt A.3.5.6. i tillägg A visar tydligt att det inte kommer att vara möjligt att skapa en fördefinierad lista med funktioner för vilka kriteriet för riskacceptans för tekniska system gäller i alla lägen. Detta kommer alltid att vara beroende av hur dess delsystemsfunktioner kommer att användas i systemet.

A.3.5.8. Ett exempel på tillämpningen av kriteriet för riskacceptans för tekniska system ges i avsnitt C.15. i tillägg C.

A.3.6. Exempel på tillämpning av kriteriet för riskacceptans för tekniska system

A.3.6.1. Inledning

(a) I detta kapitel finns exempel som visar hur man ska bestämma felintensiteten för andra konsekvenser av faror och hur lägre säkerhetskrav än $10^{-9}\,h^{-1}$ kan härledas. I detta dokument varken föredras eller föreskrivs någon särskild metod. Dokumentet innehåller bara information om hur kriteriet för riskacceptans för tekniska system kan användas för att kalibrera några av de vanligaste använda metoderna. Det måste utvecklas ytterligare i byråns arbete med allmänt godtagbara risker och kriterier för riskacceptans.

(b) Kriteriet för riskacceptans för tekniska system kan i själva verket endast tillämpas direkt på ett litet antal fall eftersom det i praktiken inte är så många funktionella fel i tekniska system som leder direkt till olyckor med potentiellt katastrofala konsekvenser. För att tillämpa kriteriet på faror med icke-katastrofala konsekvenser och för att bestämma den eftersträvade felintensiteten är det därför möjligt att utföra avvägningar (t.ex. genom att kalibrera en riskmatris enligt detta kriterium) mellan olika parametrar, t.ex. allvarlighetsgrad mot frekvens.

A.3.6.2. Exempel 1: Avvägning för direkt risk

(a) Kriteriet för riskacceptans för tekniska system kan lätt tillämpas på scenarier för vilka endast ett fåtal oberoende parametrar skiljer sig från de referensförhållanden som definieras i kriteriet för riskacceptans för tekniska system i avsnitt 2.5.4. i förordningen om en gemensam säkerhetsmetod {ref. 3}.

(b) Antag att förhållandet till risk för en särskild parameter p är multiplikativt. Antag att p* förekommer i referensförhållandet, medan p kan tillämpas i scenariot p‘. I detta fall är endast parameterkvoten p*/p’ relevant och förekomstfrekvensen kan minskas. Detta förfarande kan itereras om parametrarna är oberoende.

(c) Exempel:

(1) Antag att den verkliga potentialen för en katastrofal konsekvens har bedömts genom en expertbedömning att vara tio gånger lägre än potentialen som gäller referensförhållandena i avsnitt 2.5.4 i förordningen om en gemensam säkerhetsmetod {ref. 3}. Då skulle kravet bli $10^{-8}\,h^{-1}$ i stället för $10^{-9}\,h^{-1}$.

(2) Antag att en ytterligare säkerhetsbarriär för ett annat tekniskt system (oberoende av konsekvenserna), som är effektivt i 50 % av fallen har identifierats.

(3) Då skulle säkerhetskravet bli $5*10^{-7}\,h^{-1}$ (dvs. $0{,}5*10^{-8}\,h^{-1}$) i stället för $10^{-9}\,h^{-1}$.

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

A.3.6.3. Exempel 2: Riskmatriskalibrering

(a) För att kunna använda kriteriet för riskacceptans för tekniska system på ett korrekt sätt i en riskmatris, måste riskmatrisen hänföra sig till den korrekta systemnivån (jämförbar med den som anges i avsnitt A.3.5. i tillägg A).

(b) Kriteriet för riskacceptans för tekniska system definierar ett fält i riskmatrisen som tolererbart som motsvarar koordinaten (katastrofal allvarlighetsgrad, 10^{-9} h^{-1} förekomstfrekvens): se det röda fältet i tabell 5. Alla fält som hör samman med en högre förekomst måste betecknas som ”ej tolererbara”. Lägg märke till att endast i ett fall med en trolig direkt potential för en katastrofal konsekvens är olycksfrekvensen den samma som frekvensen för ett funktionellt fel.

(c) Därefter kan resten av matrisen fyllas i. Effekter, såsom riskaversion eller skalning av kategorierna, måste dock beaktas. I det enklaste fallet med en linjär dekadisk skalning (så som visas i tabell 5 med hjälp av pilen) extrapoleras fältet med beteckningen ”godtagbar” enligt kriteriet för riskacceptans för tekniska system linjärt i förhållande till resten av matrisen. Detta innebär att alla fält i samma diagonal (eller under diagonalen) också betecknas som ”godtagbara”. Fälten under diagonalen kan också betecknas som ”godtagbara”.

Tabell 5: Typexempel på en kalibrerad riskmatris.

Förekomstfrekvens för en olycka (orsakad av en fara)	**Risknivåer**			
Frekvent (10^{-4} per h)	**Ej tolererbar**	**Ej tolererbar**	**Ej tolererbar**	**Ej tolererbar**
Sannolik (10^{-5} per h)	**Ej tolererbar**	**Ej tolererbar**	**Ej tolererbar**	**Ej tolererbar**
Tillfällig (10^{-6} per h)	**Godtagbar**	**Ej tolererbar**	**Ej tolererbar**	**Ej tolererbar**
Avlägsen (10^{-7} per h)	**Godtagbar**	**Godtagbar**	**Ej tolererbar**	**Ej tolererbar**
Osannolik (10^{-8} per h)	**Godtagbar**	**Godtagbar**	**Godtagbar**	**Ej tolererbar**
Otrolig (10^{-9} per h)	**Godtagbar**	**Godtagbar**	**Godtagbar**	**Godtagbar**
	Obetydlig	Marginell	Kritisk	Katastrofal
	Allvarlighetsgrader för farans konsekvens (dvs. olyckan)			

Riskvärdering	**Riskminskning/-kontroll**
Ej tolererbar	Risken ska elimineras.
Godtagbar	Risken är godtagbar. En oberoende bedömning krävs.

(d) När matrisen är fylld kan den även tillämpas på icke-katastrofala faror. Om exempelvis ett annat funktionellt fel har en konsekvens som är klassificerad som ”kritisk” kan den tolererbara olycksfrekvensen enligt den kalibrerade riskmatrisen inte vara mer än ”osannolik” (eller till och med lägre).

(e) Lägg märke till att användningen av riskmatrisen kan leda till överdrivet konservativa resultat då frekvenserna för funktionella fel tillämpas (dvs. för funktionella fel som inte direkt leder till olyckor).

A.3.6.4. Princip för kalibrering av andra riskanalysmetoder

Andra riskanalysmetoder, exempelvis det föreslagna riskprioritetsnummerschemat eller riskdiagrammet från VDV 331 eller IEC 61508 kan också kalibreras med hjälp av ett liknade förfarande som det som beskrivits för riskmatrisen:

(a) Steg ett: Klassificera referenspunkten enligt kriteriet för riskacceptans för tekniska system som tolererbar och punkter med högre frekvens eller högre allvarlighetsgrad som ett ej tolererbart kriterium för riskacceptans för tekniska system.

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

(b) Steg två: Använd avvägningsmekanismer för den specifika metoden för att extrapolera risktolererbarheten till icke-katastrofala faror (under användning av linjär riskavvägning som en startpunkt).
(c) Steg tre: För icke-katastrofala faror kan kriteriet för riskacceptans för tekniska system därefter härledas från den kalibrerade riskanalysmetoden genom jämförelse av (frekvens, konsekvens) koordinaten med den på detta sätt erhållna FN-kurvan.

A.3.7. Slutsatser om kriteriet för riskacceptans för tekniska system

A.3.7.1. I det allmänna ramverket för riskbedömning som föreslås i den gemensamma säkerhetsmetoden behövs kriterier för riskacceptans för att bedöma när den kvarvarande risknivån blir godtagbar och följaktligen när den uttryckliga riskuppskattningen ska avslutas.

A.3.7.2. Kriteriet för riskacceptans för tekniska system är ett konstruktionsmål ($10^{-9}\,h^{-1}$) för tekniska system.

A.3.7.3. De främsta målen med kriteriet för riskacceptans för tekniska system är

(a) att specificera en övre gräns för riskacceptans och följaktligen en referenspunkt, utifrån vilken riskanalysmetoderna för tekniska system kan kalibreras,
(b) att möjliggöra ett ömsesidigt erkännande av tekniska system eftersom de tillhörande risk- och säkerhetsbedömningarna kommer att utvärderas enligt samma kriterier för riskacceptans i alla medlemsstaterna,
(c) att spara kostnader eftersom det inte kräver onödigt höga kvantitativa säkerhetskrav,
(d) att underlätta konkurrensen mellan tillverkarna. Om antingen förslagsställaren eller en medlemsstat använder andra kriterier för riskacceptans skulle detta leda till att industrin skulle behöva utföra en rad olika demonstrationer för samma tekniska system. Detta skulle följaktligen äventyra tillverkarnas konkurrenskraft och göra produkterna onödigt dyra.

A.3.7.4. Det semikvantitativa kravet som finns i kriteriet för riskacceptans för tekniska system behöver inte alltid påvisas för tekniska system. Inom ramen för den gemensamma säkerhetsmetoden behöver kriteriet för riskacceptans för tekniska system endast tillämpas på tekniska system för vilka de identifierade farorna varken kan kontrolleras på ett adekvat sätt genom användning av handlingsregler eller genom jämförelse med referenssystem. Detta möjliggör att lägre säkerhetskrav kan anges under förutsättning att den globala säkerhetsnivån kan upprätthållas.

A.3.7.5. Endast då det saknas en handlingsregel eller ett referenssystem krävs ett harmoniserat semikvantitativt kriterium för riskacceptans för tekniska system.

A.3.7.6. Eftersom tillförlitlighetsnivån för systematiska felyttringar/fel är begränsad till SIL 4, måste tillförlitlighetsnivån för de slumpmässiga maskinvarufelen för tekniska system också begränsas till SIL 4. Detta motsvarar en maximal tolererbar risknivå (THR) på $10^{-9}\,h^{-1}$ (dvs. den maximala felintensiteten). Enligt Cenelec-standarden 50129 gäller att om mer krävande säkerhetskrav ställs kan detta inte uppnås med endast ett system. Systemets arkitektur måste ändras, till exempel genom att två system används, vilket oundvikligen ökar kostnaderna för det tekniska system drastiskt. Mer information finns i avsnitt A.3.1. i tillägg A.

A.3.7.7. Slutligen, i avsnitt A.3.6. i tillägg A beskrivs hur kriteriet för riskacceptans för tekniska system kan användas som en referenspunkt för att kalibrera specifika riskanalysmetoder då tekniska system har en potential för konsekvenser som är mindre allvarliga än katastrofala.

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

A.4. Bevisning från säkerhetsbedömningen

A.4.1. I det har avsnittet ges vägledning om bevisning som normalt läggs fram för ett bedömningsorgan för att möjliggöra en oberoende bedömning och få ett säkerhetsgodkännande om inte annat föreskrivs i de nationella kraven i en medlemsstat. Vägledningen kan användas som en checklista för att kontrollera att alla tillhörande aspekter har tagits med och dokumenterats, där så är relevant, under tillämpning av den gemensamma säkerhetsmetoden.

A.4.2. Säkerhetsplan: I Cenelec rekommenderas att en säkerhetsplan tas fram i början av projektet, eller om detta inte passar för projektet, att den tillhörande beskrivningen ingår i ett annat relevant dokument. Om bedömningsorganen utses i början av projektet kan även säkerhetsplanen lämnas till dem för att få deras synpunkter på planen. I princip beskriver säkerhetsplanen följande:

(a) Den organisation som har inrättats och kompetensen hos de personer som har hand om utvecklingen och riskbedömningen.
(b) Alla säkerhetsrelaterade aktiviteter som är planerade för de olika faserna i projektet, liksom deras förväntade resultat.

A.4.3. Bevisning som krävs från systemdefinitionsfasen:

(a) Beskrivning av systemet:
    (1) Definition av systemets omfattning/gränser.
    (2) Beskrivning av funktioner.
    (3) Beskrivning av systemets struktur.
    (4) Beskrivning av de driftsrelaterade och miljömässiga förhållandena.
(b) Beskrivning av externa kontaktpunkter.
(c) Beskrivning av interna kontaktpunkter.
(d) Beskrivning av livscykelfaserna.
(e) Beskrivning av säkerhetsprinciperna.
(f) Beskrivning av de antaganden som definierar gränserna för riskbedömningen.

A.4.4. För att möjliggöra riskbedömning ingår det sammanhang, i vilket den planerade ändringen ska göras, i systemdefinitionen:

(a) Om den planerade ändringen är en ändring av ett befintligt system beskriver systemdefinitionen dels systemet före ändringen, dels den planerade ändringen.
(b) Om den planerade ändringen innebär att ett nytt system byggs är beskrivningen begränsad till systemdefinitionen, eftersom det inte finns någon beskrivning av något befintligt system.

A.4.5. Bevisning som krävs från fasen för identifiering av faror:

(a) Beskrivning av och motivering till (inklusive begränsningar) de metoder och verktyg som har använts för identifiering av faror (top-down, bottom-up, HAZOP etc.).
(b) Resultat:
    (1) Förteckning över faror:
    (2) System(gräns)faror.
    (3) Faror för delsystem.
    (4) Faror för kontaktpunkter.
    (5) De säkerhetsåtgärder som identifierades under denna fas.

A.4.6. Följande bevisning krävs också från riskanalysfasen:

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

(a) Då handlingsregler används för att kontrollera faror måste det påvisas att alla relevanta krav från handlingsreglerna är uppfyllda för det system som är föremål för bedömning. Detta omfattar att visa att de relevanta handlingsreglerna har tillämpats korrekt.

(b) Då liknande referenssystem används för att kontrollera farorna:

(1) Definition av säkerhetskraven från de relevanta referenssystemen för det system som är föremål för bedömning.
(2) Påvisande av att det system som är föremål för bedömning används under liknande driftsrelaterade och miljömässiga förhållanden som det relevanta referenssystemet. Om detta inte går måste det visas att avvikelserna från referenssystemet är korrekt bedömda.
(3) Bevisning om att säkerhetskraven från referenssystemen är korrekt genomförda i det system som är föremål för bedömning.

(c) Då uttrycklig riskuppskattning används för att kontrollera farorna:

(1) Beskrivning av och motivering (inklusive begränsningar) till de metoder och verktyg som har använts för riskanalysen (kvalitativ, kvantitativ, semikvantitativ, icke-regressionsanalys etc.).
(2) Identifiering av befintliga säkerhetsåtgärder och riskminskningsfaktorer för varje fara (inklusive aspekter om den mänskliga faktorn).
(3) Utvärdering och rankning av risken för varje fara:

(i) Uppskattning av konsekvenserna för faran och en motivering (med antaganden och villkor).
(ii) Uppskattning av frekvensen för faran och en motivering (med antaganden och villkor).
(iii) Rankning av farorna enligt deras allvarlighetsgrad och förekomstfrekvens.

(4) Identifiering av ytterligare lämpliga säkerhetsåtgärder som leder till godtagbara risker för varje fara (löpande process efter riskvärderingsfasen).

A.4.7. Bevisning som krävs för riskvärderingen:

(a) Då en uttrycklig riskuppskattning utförs:

(1) Definition av och motivering till riskvärderingskriterierna för varje fara.
(2) Påvisande av/motivering till att säkerhetsåtgärderna och säkerhetskraven täcker varje fara på en godtagbar nivå (enligt de ovanstående riskvärderingskriterierna).

(b) Enligt avsnitten 2.3.5 och 2.4.3 i förordningen om en gemensam säkerhetsmetod betraktas riskerna som omfattas av tillämpningen av handlingsregler och jämförelse med referenssystem implicit som godtagbara under förutsättning att (se prickad cirkel i figur 1)

(1) förhållandena för att tillämpa handlingsregler enligt avsnitt 2.3.2 är uppfyllda,
(2) förhållandena för att använda ett referenssystem enligt avsnitt 2.4.2 är uppfyllda.

Kriterier för riskacceptans är implicita för dessa två principer för riskacceptans.

A.4.8. Bevisning från hanteringen av faror:

(a) Registrering av alla faror i ett protokoll om faror som innehåller följande element:

(1) Den identifierade faran.
(2) De säkerhetsåtgärder som förhindrar förekomsten av faran eller mildrar dess konsekvenser.
(3) Säkerhetskraven för åtgärderna.
(4) Relevant del av systemet.
(5) Aktör som ansvarar för säkerhetsåtgärderna.
(6) Status för faran (t.ex. öppen, löst, borttagen, överförd, kontrollerad etc.).

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

(7) Datum för registrering, granskning och kontroll av varje fara.

(b) Beskrivning av hur farorna kommer att hanteras på ett effektivt sätt under hela livscykeln.

(c) Beskrivning av informationsutbytet mellan parterna för faror vid kontaktpunkterna och fördelning av ansvar.

A.4.9. Bevisning som hör samman med kvaliteten på riskvärderings- och riskbedömningsprocessen.

(a) Beskrivning av de personer som har deltagit i processen och deras kompetens.

(b) För uttryckliga riskuppskattningar: beskrivning av information, data och annan statistik som har använts under processen, och en motivering om deras tillräcklighet (t.ex. känslighetsstudie för de data som har använts).

A.4.10. Bevisning om att säkerhetskraven är uppfyllda:

(a) Förteckning över använda standarder.

(b) Beskrivning av konstruktionen och de driftsrelaterade principerna.

(c) Bevisning om att bra kvalitets- och säkerhetsstyrningssystem har använts för projektet: se punkt [G 3] i avsnitt 1.1.2.

(d) Sammanfattning av säkerhetsanalysrapporterna (t.ex. orsaksanalys för faran) som visar att säkerhetskraven uppfylls.

(e) Beskrivning av och motivering till de metoder och verktyg (FMECA, FTA etc.) som har använts vid orsaksanalysen för faran.

(f) Sammanfattning av säkerhetsverifierings- och valideringstesterna.

A.4.11. Säkerhetsbevisning: I Cenelec rekommenderas att alla tidigare nämnda bevisningar omgrupperas och summeras i ett dokument som lämnas till bedömningsorganet: se punkterna [G 4] och [G 5] i avsnitt 5.1.

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

TILLÄGG B: EXEMPEL PÅ TEKNIKER OCH VERKTYG SOM STÖDER RISKBEDÖMNINGSPROCESSEN

B.1. Exempel på tekniker och verktyg för att utföra riskbedömningsaktiviteterna i den gemensamma säkerhetsmetoden finns i bilaga E i vägledningen EN 50126-2 {ref. 9}. En sammanfattning av tekniker och verktyg finns i tabell E.1. Varje teknik beskrivs och vid behov hänvisas till andra standarder för mer information.

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

TILLÄGG C: EXEMPEL

C.1. Inledning

C.1.1. Syftet med detta tillägg är att underlätta läsningen av det aktuella dokumentet. Här finns alla de insamlade exemplen som syftar till att underlätta tillämpningen av den gemensamma säkerhetsmetoden.

C.1.2. De exempel på risk- eller säkerhetsbedömningar som finns i detta tillägg är inte ett resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom de har utförts innan förordningen om en gemensam säkerhetsmetod togs fram. Exemplen kan klassificeras i

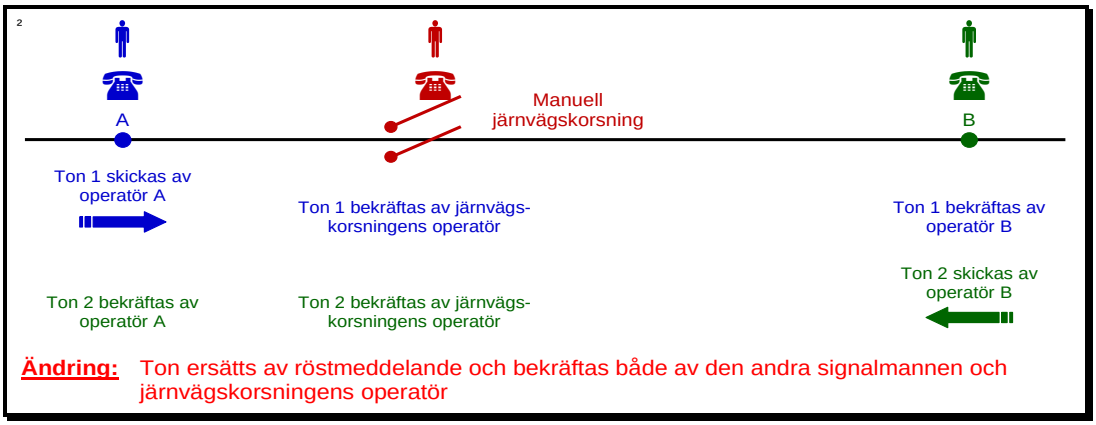
(a) exempel, med hänvisning till deras ursprung, som har erhållits från experterna i arbetsgruppen för den gemensamma säkerhetsmetoden,
(b) exempel, med avsikt utan hänvisning till deras ursprung, som har erhållits från experterna i arbetsgruppen för den gemensamma säkerhetsmetoden; experterna begärde att ursprunget skulle förbli konfidentiellt,
(c) exempel, vars ursprung inte nämns, och som har tagits fram av medlemmar i byråns personal baserat på deras tidigare personliga yrkeserfarenheter.

För varje exempel anges en spårbarhet mellan den tillämpade processen och den som krävs enligt den gemensamma säkerhetsmetoden, liksom en argumentation för och mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

C.2. Exempel på tillämpning av kriterierna för betydande ändring i artikel 4.2

C.2.1. Byrån arbetar på en definition av vad som kan betraktas som en ”betydande ändring”. Ett exempel från detta arbete finns i detta avsnitt och visar hur kriterierna i artikel 4.2 kan tillämpas.

C.2.2. Ändringen består av att modifiera hur signalmännen vid en manuellt manövrerad järnvägsövergång kommunicerar information om ett inkommande tågs riktning till järnvägsövergångens operatör. Ändringen visas i figur 15.



Figur 15: Exempel på en icke betydande ändring
Telefonmeddelande för styrning av en järnvägsövergång.

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

C.2.3. Befintligt system: Före den planerade ändringen indikerades informationen om riktningen för ett inkommande tåg automatiskt till järnvägskorsningens operatör genom telefonens ringsignal. Tonen var olika beroende på varifrån samtalet kom.

C.2.4. Planerad ändring: I takt med att det gamla telefonsystemet blir föråldrat och måste ersättas av ett nytt digitalt system är det inte längre tekniskt möjligt att låta den relevanta informationen ingå i tonen. Tonen är exakt den samma oberoende av vilken signalman den kommer ifrån. Det har därför beslutats att samma funktion ska uppnås genom en driftrutin:

(a) När tåget avgår informerar signalmannen verbalt järnvägskorsningens operatör om det inkommande tågets riktning.
(b) Informationen kontrolleras mot tidtabellen och bekräftas av både järnvägskorsningens operatör och den andra signalmannen för att undvika att operatören missförstår informationen.

Den planerade ändringen och den tillhörande driftrutinen visas i figur 15.

C.2.5. Även om ändringen verkar ha en potentiell inverkan på säkerheten (risk för att järnvägsövergångens bommar inte stängs i tid) kan andra kriterier i artikel 4.2 såsom

(a) låg komplexitet,
(b) avsaknad av innovation, och
(c) lätt att övervaka,

antyda att den avsedda ändringen inte är betydande.

C.2.6. I detta exempel krävs ändå viss säkerhetsanalys eller argumentation för att visa att ersättning av ett gammalt tekniskt system med en driftrutin (med personal som dubbelkontrollerar varandra) för denna säkerhetskritiska uppgift skulle leda till en liknande säkerhetsnivå. Frågan är om detta kräver att hela processen enligt den gemensamma säkerhetsmetoden tillämpas, med protokoll om faror, oberoende bedömning av ett bedömningsorgan etc. I detta fall är det diskutabelt om detta skulle ge något mervärde, vilket innebär att en sådan ändring därmed inte kan kvalificeras som betydande.

C.3. Exempel på kontaktpunkter mellan aktörer inom järnvägssektorn

C.3.1. Här är några exempel på kontaktpunkter och skäl till samarbete mellan aktörer inom järnvägssektorn:

(a) Infrastrukturförvaltare – infrastrukturförvaltare: Till exempel ska det i båda infrastrukturerna ingå säkerhetsåtgärder som säkerställer en säker överföring av tåg från den ena infrastrukturen till den andra.

(b) Infrastrukturförvaltare – järnvägsföretag: Till exempel skulle det kunna finnas specifika driftsregler beroende på infrastrukturen som tågföraren måste följa.

(c) Infrastrukturförvaltare – tillverkare: Till exempel skulle tillverkarens delsystem kunna ha begränsningar av användningen som infrastrukturförvaltaren måste uppfylla.

(d) Infrastrukturförvaltare – tjänsteleverantör: Till exempel skulle det kunna finnas särskilda underhållsbegränsningar för infrastrukturen som måste uppfyllas av underleverantören av underhåll.

(e) Järnvägsföretag – tillverkare: Till exempel skulle tillverkarens delsystem kunna ha begränsningar av användningen som järnvägsföretaget måste uppfylla.

(f) Järnvägsföretag – tjänsteleverantör: Till exempel skulle det kunna finnas särskilda underhållsbegränsningar för infrastrukturen som måste uppfyllas av underleverantören av underhåll.

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

(g) Järnvägsföretag – fordonsinnehavare: Till exempel skulle det kunna finnas specifika begränsningar av användningen för fordon som måste uppfyllas av det järnvägsföretag som använder dessa fordon.

(h) Tillverkare – tillverkare: Till exempel hanteringen av säkerhetsrelaterade tekniska kontaktpunkter mellan delsystemen från två olika tillverkare.

(i) Tillverkare – tjänsteleverantör: Till exempel tillverkarens hantering av protokoll om faror då arbete läggs ut på ett företag vars storlek är för liten för att ha en säkerhetsorganisation för projektet i fråga.

(j) Tjänsteleverantör – tjänsteleverantör: Liknande exempel som i punkt (j) ovan.

C.3.2. Tjänsteleverantörer sköter alla aktiviteter som antingen infrastrukturförvaltaren, järnvägsföretaget eller tillverkaren har lagt ut på entreprenad, t.ex. underhåll, biljettering, teknisk service etc.

C.3.3. Följande exempel ges för att åskådliggöra hanteringen av kontaktpunkter och den tillhörande identifieringen av faror. Exemplet hänför sig till en kontaktpunkt mellan en tågtillverkare och en förslagsställare (järnvägsföretag). Det beskriver hur de huvudkriterier som anges i punkt [G 3] i avsnitt 1.2.1 skulle kunna uppfyllas.

(a) Ledarskap: Förslagsställaren (järnvägsföretaget).

(b) Ingående data:

(1) Förteckning(ar) över relevanta faror från liknande projekt.
(2) Beskrivning av alla indata och utdata (I/O) för kontaktpunkten, inklusive prestandaegenskaper.

(c) Metoder: se tillägg A.2 i vägledningen EN 50126-2 {ref. 9}.

(d) Deltagare som behövs:

(1) Förslagsställarens (järnvägsföretagets) chef för säkerhetssäkringen.
(1) Tågtillverkarens chef för säkerhetssäkringen
(2) Förslagsställarens konstruktionsansvarige.
(3) Tågtillverkarens konstruktionsansvarige.
(4) Förslagsställarens underhållspersonal (delvis beroende av de analyserade indata/utdata).
(5) Tågförarna (delvis beroende av de analyserade indata/utdata).

(e) Utdata:

(1) Gemensamt överenskommen rapport över identifierade faror.
(2) Säkerhetsåtgärder för protokollet om faror med en klar beskrivning av ansvaret.

C.4. Exempel på metoder för att bestämma allmänt godtagbara risker

C.4.1. Inledning

C.4.1.1. En allmänt godtagbar risk definieras i förordningen om en gemensam säkerhetsmetod som varande *”så liten att det inte är rimligt att vidta några ytterligare säkerhetsåtgärder (för att ytterligare minska risken)”.* I identifieringen av faror innebär klassificeringen av vissa faror som förenade med allmänt godtagbara risker att dessa faror inte kan analyseras ytterligare i riskbedömningsprocessen. Definitionen av allmänt godtagbara risker som citeras ovan lämnar rum för viss tolkning. Det är därför som det anges i förordningen att beslutet att klassificera faror som allmänt godtagbara risker ska ske med expertbedömning.

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

C.4.1.2. Det är verkligen svårt att på ett enkelt sätt definiera ett mer explicit kriterium för allmänt godtagbara risker som skulle kunna tillämpas på alla olika möjliga systemnivåer där sådana faror skulle kunna identifieras och som också skulle förklara olika riskaversionsfaktorer som kan råda för olika tillämpningar. Eftersom det är viktigt att säkerställa att bedömningarna från experterna är lättförståeliga och spårbara är det emellertid av värde att det finns viss vägledning om hur risker ska definieras som allmänt godtagbara. Kriterier för att definiera allmänt godtagbara risker kan vara kvantitativa, kvalitativa eller semikvantitativa. Nedan följer några exempel på hur man härleder dessa kriterier som möjliggör en utvärdering av allmänt godtagbara risker på ett kvantitativt eller semikvantitativt sätt.

C.4.1.3. Exemplen nedan åskådliggör denna princip. De har tagits från skriften *”Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess”, Kurz, Milius, Signal + Draht (100) 9/2008.*

C.4.2. Härledning av ett kvantitativt kriterium

C.4.2.1. Man kan definiera allmänt godtagbara risker som risker som är mycket mindre än den godtagbara risken för en given klass av faror. Med hjälp av statistiska data kan det vara möjligt att beräkna vad den nuvarande risknivån för järnvägssystem är och därmed förklara denna beräknade nivå som godtagbar. Genom att dividera denna risknivå med antalet (N) faror (t.ex. kan man godtyckligt anta att det finns omkring N = 100 huvudkategorier av faror i ett järnvägssystem) fås en godtagbar risknivå per farokategori. Man skulle därefter kunna hävda att en fara med en risk som är två storleksordningar lägre än den godtagbara risknivån per fara (detta är parametern x % i punkt [G 1] i avsnitt 2.2.3) skulle kunna betraktas som en allmänt godtagbar risk.

C.4.2.2. En kontroll ska dock utföras så att bidraget av alla faror som hör samman med allmänt godtagbara risker inte överskrider en given andel (t.ex. y %) av den totala risken på systemnivå: se avsnitt 2.2.3 och förklaringen i punkt [G 2] i avsnitt 2.2.3.

C.4.3. Utvärdering av allmänt godtagbara risker

C.4.3.1. Gränsvärdena för allmänt godtagbara risker, enligt härledningen i exemplen ovan, kan därefter användas för att kalibrera kvalitativa verktyg, såsom en riskmatris, ett riskdiagram eller riskprioritetsnummer, för att underlätta för experten att fatta beslut om att klassificera risken som allmänt godtagbar. Det är viktigt att betona att det faktum att man har kvantitativa värden som kriterier för allmänt godtagbara risker inte innebär att det är nödvändigt att göra en exakt riskuppskattning eller riskanalys för att fatta beslut om att risken är allmänt godtagbar. Det är här som expertens bedömning ska tillämpas för att göra denna grova uppskattning under fasen för identifiering av faror.

C.4.3.2. Det är också viktigt att kontrollera att bidraget av alla faror som hör samman med i allmänt godtagbara risker inte överskrider en given andel (t.ex. y %) av den totala risken på systemnivå: se avsnitt 2.2.3 och förklaringen i punkt [G 2] i avsnitt 2.2.3.

C.5. Exempel på riskbedömning av en organisatorisk betydande ändring

C.5.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

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

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.5.2. Exemplet hänför sig till en organisatorisk ändring. Den ansågs betydande enligt den därtill hörande förslagsställaren. Ett riskbedömningsbaserat tillvägagångssätt tillämpades för att utvärdera ändringen.

C.5.3. En avdelning inom infrastrukturförvaltarens organisation, som utförde en del underhållsaktiviteter (utöver signalering och telematik) fram till ändringen, var tvungen att börja konkurrera med andra företag som var verksamma inom samma område. Den direkta konsekvensen av detta var ett behov av nedskärningar och omfördelning av personalen och uppgifterna inom den fristående avdelning i infrastrukturförvaltarens organisation som skulle konkurrensutsättas.

C.5.4. Betänkligheter hos den påverkade infrastrukturförvaltaren:

(a) Personalen hos infrastrukturförvaltaren som påverkades av förändringen ansvarade för akut underhåll och reparationer som krävdes vid plötsligt uppkomna fel på infrastrukturen. Personalen utförde också vissa planerade eller projektbaserade underhållsaktiviteter, såsom ballaststoppning, ballastrengöring, vegetationskontroll.
(b) Dessa uppgifter betraktades som kritiska för driftsäkerheten och punktligheten. De behövde därför analyseras för att hitta rätt åtgärder som skulle säkerställa att situationen inte skulle försämras, eftersom många av dem som var ansvariga för säkerheten skulle lämna infrastrukturförvaltarens organisation.
(c) Samma säkerhetsnivå och tågpunktlighet behövde upprätthållas under och efter organisationsändringen.

C.5.5. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg (se även figur 1):

(a) Systembeskrivning [avsnitt 2.1.2]:
    (1) Beskrivning av de uppgifter som utfördes av den befintliga organisationen (dvs. av infrastrukturförvaltarens organisation före ändringen).
    (2) Beskrivning av de planerade ändringarna inom infrastrukturförvaltarens organisation.
    (3) Kontaktpunkterna för den ”gren som skulle avknoppas” med andra omgivande organisationer eller med den fysiska miljön kunde endast beskrivas kortfattat. Gränserna kunde inte klart redovisas till 100 %.

(b) Identifiering av faror [avsnitt 2.2]:
    (1) Brainstormningsmöte med en grupp experter:
        (i) För att hitta alla faror med en relevant inverkan på den risk som uppkom på grund av den planerade organisatoriska ändringen.
        (ii) För att identifiera möjliga åtgärder för att kontrollera risken.

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

(2) Klassificering av farorna:

(i) Med avseende på allvarlighetsgraden för den tillhörande risken: hög, medel, låg risk.
(ii) Med avseende på inverkan av ändringen: ökad, oförändrad, minskad risk.

(c) Användning av ett referenssystem [avsnitt 2.4]:

Systemet före förändringen bedömdes ha en godtagbar säkerhetsnivå. Det användes därför som ”referenssystem” för att härleda kriterier för riskacceptans för ändringen av organisationen.

(d) Uttrycklig riskuppskattning och riskvärdering [avsnitt 2.5]:

För varje fara med ökad risk på grund av ändringen av organisationen identifierades riskminskningsåtgärder. Den kvarvarande risken jämfördes med kriterierna för riskacceptans från referenssystemet för att kontrollera om ytterligare åtgärder behövdes identifieras.

(e) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

(1) Riskanalysen och protokollet om faror visade att farorna inte kan kontrolleras förrän de har verifierats och förrän det har visats att säkerhetskraven (dvs. de valda säkerhetsåtgärderna) har genomförts.
(2) Riskanalysen och protokollet om faror var levande dokument. Effektiviteten hos de åtgärder som hade valts övervakades med regelbundna intervall för att kontrollera om förhållandena ändrades och om riskanalysen och riskvärderingen behövde uppdateras.
(3) Om de genomförda åtgärderna inte var tillräckligt effektiva uppdaterade riskanalysen, riskvärderingen och protokollet om faror och övervakades på nytt.

(f) Hantering av faror [avsnitt 4.1]:

De identifierade farorna och säkerhetsåtgärderna registrerades och förvaltades i ett protokoll om faror. En av slutsatserna från exemplet var att riskanalysen och protokollet om faror kontinuerligt behövde uppdateras eftersom beslut fattades och åtgärder vidtogs under ändringen av organisationen. Risken vid kontaktpunkterna mot exempelvis underleverantörer och entreprenörer omfattades också av riskanalysen.

Den struktur och de fält som användes i protokollet om faror, liksom ett utdrag med några rader, finns i avsnitt C.16.2. i tillägg C.

(g) Oberoende bedömning [artikel 6]:

En oberoende bedömning utfördes också av en tredje part för att

(1) kontrollera att riskhanteringen och riskbedömningen var korrekt utförda,
(2) kontrollera att den organisatoriska ändringen är lämplig och kommer att göra det möjligt att upprätthålla samma säkerhetsnivå som före ändringen.

C.5.6. Exemplet visar att de principer som krävs enligt den gemensamma säkerhetsmetoden är metoder som existerar inom järnvägssektorn och som redan tillämpas för att bedöma risker till följd av organisatoriska ändringar. Riskbedömningen i exemplet uppfyller alla krav enligt den gemensamma säkerhetsmetoden. I riskbedömningen används två av de tre principerna för riskacceptans som medges enligt det harmoniserade tillvägagångssättet i den gemensamma säkerhetsmetoden:

(a) Ett ”referenssystem” tillämpas för att bestämma de kriterier för riskacceptans som krävs för att utvärdera riskacceptansen för den organisatoriska ändringen.
(b) ”Uttrycklig riskuppskattning och riskvärdering”:

(1) För att analysera ändringens avvikelser från referenssystemet.

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

(2) För att identifiera riskminskningsåtgärder för den ökade risken som uppkommer på grund av ändringen.
(3) För att utvärdera om en godtagbar risknivå uppnås.

C.6. Exempel på riskbedömning av en driftsrelaterad betydande ändring – ändring av körtiderna

C.6.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.6.2. Exemplet är en driftsrelaterad ändring där järnvägsföretaget ville inrätta nya rutter och eventuellt nya arbetstider (inklusive rotations- och skiftscheman) för förarna.

C.6.3. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg (se även figur 1):

(a) Betydelsen av ändringen [artikel 4].

Järnvägsföretaget utförde en preliminär riskbedömning varvid slutsatsen drogs att den driftsrelaterade ändringen var betydande. Eftersom förarna var tvungna att köra nya rutter, och eventuellt utanför deras normala arbetstid, kunde risken för att passera stoppsignaler, köra för fort eller ignorera tillfälliga hastighetsbegränsningar inte negligeras.

Vid jämförelse av denna preliminära riskbedömning med kriterierna i artikel 4.2 i förordningen om en gemensam säkerhetsmetod skulle ändringen också kunna kategoriseras som betydande på grundval av följande kriterier:

(1) Säkerhetsrelevans: Ändringen är säkerhetsrelaterad eftersom inverkan av ändringen av förarnas arbetssätt skulle kunna vara katastrofal.
(2) Felkonsekvens: Förarnas fel som nämns ovan har potential att leda till katastrofala konsekvenser.
(3) Nyhetsgrad: Järnvägsföretaget skulle eventuellt kunna införa nya arbetssätt för förarna.
(4) Ändringens komplexitet: Ändringen av körtiderna skulle kunna vara komplex, eftersom detta skulle kunna kräva en fullständig bedömning och modifiering av befintliga arbetsförhållanden.

(b) Systemdefinition [avsnitt 2.1.2]:

Systemdefinitionen beskrevs initialt som

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

(1) de befintliga arbetsförhållandena: arbetstid, skiftscheman etc.,
(2) ändringar av arbetstiden,
(3) frågor som rör kontaktpunkterna (t.ex. med infrastrukturförvaltaren).

Under de olika iterationerna uppdaterades systemdefinitionen med säkerhetskrav från riskbedömningsprocessen. Viktiga personalföreträdare deltog i denna löpande process för identifieringen av faror och uppdateringen av systemdefinitionen.

(c) Identifiering av faror [avsnitt 2.2]:

Farorna och de möjliga säkerhetsåtgärderna identifierades i ett brainstormingmöte med en grupp experter, inklusive förarnas representanter, om de nya rutterna och skiftschemana. Förarnas uppgifter enligt de nya förhållandena granskades för att bedöma om de påverkade förarna, deras arbetsbelastning, den geografiska omfattningen och skiftsystemets tider.
Järnvägsföretagen rådfrågade också fackförbunden för att se om de kunde bidra med ytterligare information och undersökte om en eventuell ökning av övertiden på grund av förlängda resor på okända rutter skulle påverka risken för trötthet och sjukskrivningar.
Varje fara tilldelades en allvarlighetsgrad och konsekvens (hög, medel, låg) och hur den föreslagna ändringen som undersökts påverkade dem (ökad, oförändrad, minskad risk).

(d) Användning av ett referenssystem [avsnitt 2.3]:

Handlingsregler för arbetstid och risken för trötthet hos människor användes för att revidera befintliga arbetsförhållanden och fastställa nya säkerhetskrav. De driftsregler som behövdes togs fram i enlighet med handlingsreglerna för det nya skiftsystemet. Alla berörda parter deltog i revideringen av driftrutinerna och i överenskommelsen om att gå vidare med förändringen.

(e) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

De reviderade driftrutinerna infördes i järnvägsföretags säkerhetsstyrningssystem. De övervakades och en granskningsprocess infördes för att säkerställa att kontrollen av de identifierade farorna fortfarande var korrekt under driften av järnvägssystemet.

(f) Hantering av faror [avsnitt 4.1]:

Se punkten ovan om att järnvägsföretagens process för att hantera faror kan utgöra en del av deras säkerhetsstyrningssystem för att registrera och hantera risker. De identifierade farorna registrerades i ett protokoll om faror med säkerhetskraven (dvs. hänvisning till de reviderade driftrutinerna) som kontrollerade den tillhörande risken.
De reviderade rutinerna övervakades och granskades vid behov för att säkerställa att kontrollen av de identifierade farorna fortfarande var korrekt under driften av järnvägssystemet.

(g) Oberoende bedömning [artikel 6]:

Riskbedömnings- och riskhanteringsprocessen bedömdes av en kompetent person inom järnvägsföretaget, som var oavhängig av bedömningsprocessen. Den kompetenta personen bedömde både processen och resultaten, dvs. de identifierade säkerhetskraven.

Järnvägsföretaget har grundat sitt beslut om att införa det nya systemet på den kompetenta personens rapport från den oberoende bedömningen.

C.6.4. Exemplet visar att de principer och den process som järnvägsföretaget använde ligger i linje med den gemensamma säkerhetsmetoden. Riskhanterings- och riskbedömningsprocessen uppfyllde alla krav enligt den gemensamma säkerhetsmetoden.

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

C.7. Exempel på riskbedömning av en teknisk betydande ändring (trafikstyrning och signalering)

C.7.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

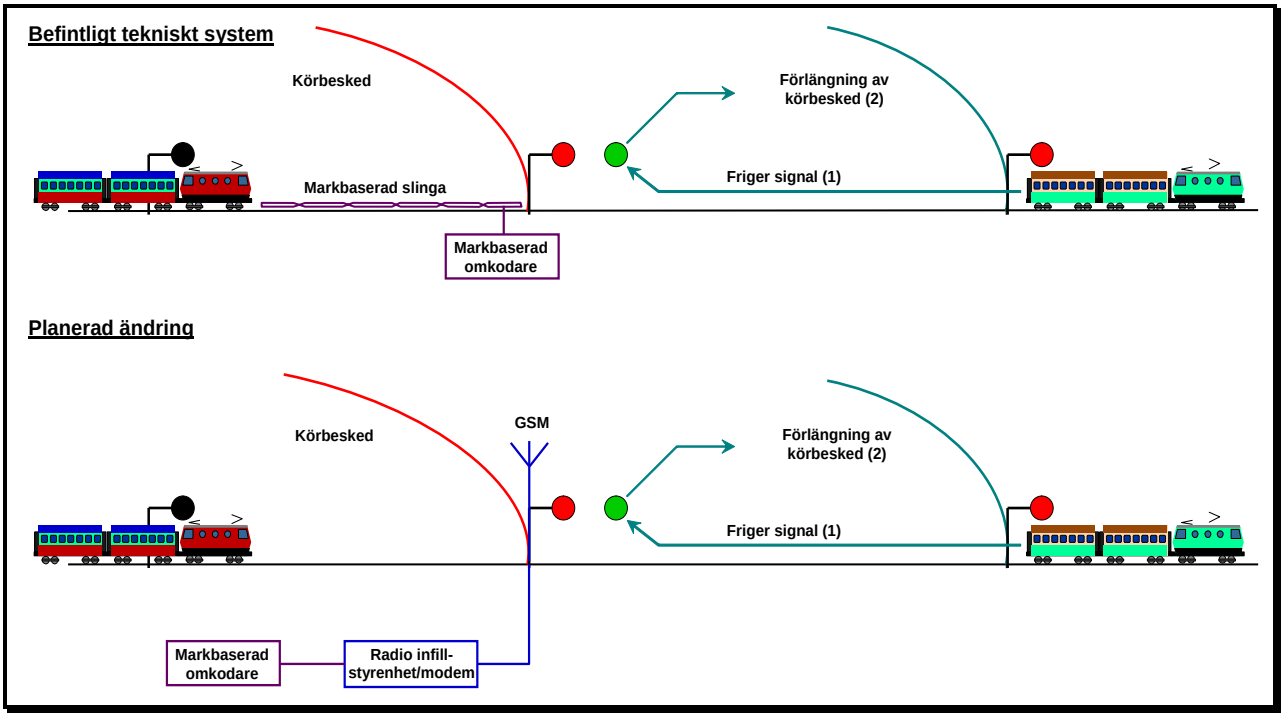
Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.7.2. Exemplet gäller en teknisk ändring av trafikstyrningssystemet. Den ansågs betydande enligt den därtill hörande förslagsställaren. Ett riskbedömningsbaserat tillvägagångssätt tillämpades för att utvärdera ändringen.

C.7.3. Beskrivning av ändringen: Ändringen består av att ersätta en markbaserad slinga som är belägen före en signal med ett ”radio infill + GSM”-delsystem (se figur 16).

C.7.4. Problem: att bibehålla säkerhetsnivån för systemet efter ändringen.

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



Figur 16: Ändring av en markbaserad loop till ett "radio infill"-delsystem.

C.7.5. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg (se även figur 1):

(a) Bedömning av betydelsen av ändringen [artikel 4]

Kriterierna i artikel 4.2 användes för att bedöma betydelsen av ändringen. Framför allt användes komplexiteten och nyhetsgraden för att bestämma om ändringen var betydande.

(b) Systembeskrivning [avsnitt 2.1.2]:

(1) Beskrivning av det befintliga systemet: slingan och dess funktioner i trafikstyrningssystemet.
(2) Beskrivning av den ändring som förslagsställaren och tillverkaren har planerat.
(3) Beskrivning av de funktionella och fysiska kontaktpunkterna mellan slingan och resten av systemet.

Funktionen hos "slingan + avkodaren" i det befintliga systemet är att avge en signal då ett tåg närmar sig när avsnittet bakom signalen (dvs. framför det närmande tåget) blir ledigt: se figur 16.

(c) Identifiering av faror [avsnitt 2.2]:

Den löpande riskbedömningsprocessen och identifieringen av faror (se avsnitt 2.1.1) tillämpades, baserat på ett brainstormingmöte med en grupp experter

(1) för att hitta alla faror med en relevant inverkan på den risk som uppkommer på grund av den planerade ändringen,
(2) för att identifiera möjliga åtgärder för att kontrollera risken.

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

Då slingan, och därmed ”radio infill”, avger signalen finns det risk för att tåget som närmar sig får ett farligt körbesked medan det föregående tåget fortfarande befinner sig i avsnittet framför signalen. Risken måste kontrolleras på en godtagbar nivå.

(d) Användning av ett referenssystem [avsnitt 2.4]:

Systemet före förändringen (slingan) bedömdes ha en godtagbar säkerhetsnivå. Det användes därför som ”referenssystem” för att härleda säkerhetskraven för ”radio infill”-delsystemet.

(e) Uttrycklig riskuppskattning och riskvärdering [avsnitt 2.5]:

(1) Skillnaden mellan ”slingans” delsystem och ”radio infill + GSM”-delsystemet analyserades med en uttrycklig riskuppskattning och riskvärdering. Följande nya faror identifierades för ”radio infill + GSM”-delsystemet:

(i) Överföring från hackare av osäker information i luftgapet, eftersom ”radio infill + GSM”-delsystemet är ett delsystem med öppen överföring.
(ii) Fördröjd överföring eller överföring av memorerade datapaket i luftgapet.

(2) Uttrycklig riskuppskattning och användning av kriterium för riskacceptans för tekniska system för ”radio infill”-styrenheten:

(f) Användning av ett referenssystem [avsnitt 2.3]:

(1) Standarden EN 50159-2 (”*Järnvägsanläggningar: Del 2: Överföring i öppna system av data av betydelse för säkerheten*”) innehåller säkerhetskrav för att kontrollera de nya farorna på en godtagbar nivå, t.ex.

(i) datakryptering och dataskydd,
(ii) sekvensering av meddelande och tidmärkning.

(2) Användning av t.ex. standarden EN 50128 för utveckling av programvaran till ”radio infill”-styrenheten.

(g) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

(1) Uppföljning av genomförande av säkerhetskraven genom utvecklingsprocessen för ”radio infill + GSM”-delsystemet.
(2) Verifiering av att systemet, när det är utformat och installerat, uppfyller säkerhetskraven.

(h) Hantering av faror [avsnitt 4.1]:

De identifierade farorna, säkerhetsåtgärderna, de resulterande säkerhetskraven som framkom under riskbedömningen och tillämpningen av de tre principerna för riskacceptans registrerades och hanterades i ett protokoll om faror.

(i) Oberoende bedömning [artikel 6]:

En oberoende bedömning utfördes också av en tredje part för att

(1) kontrollera att riskhanteringen och riskbedömningen var korrekt utförda,
(2) kontrollera att den tekniska ändringen är lämplig och kommer att göra det möjligt att upprätthålla samma säkerhetsnivå som före ändringen.

C.7.6. Exemplet visar att de tre principerna för riskacceptans som krävs enligt den gemensamma säkerhetsmetoden används på ett kompletterande sätt för att definiera säkerhetskraven för det system som är föremål för bedömning. Riskbedömningen i exemplet uppfyllde alla de krav i den gemensamma säkerhetsmetoden som finns sammanfattade i figur 1, inklusive hanteringen av ett protokoll om faror och en oberoende säkerhetsbedömning utförd av en tredje part.

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

C.8. Exempel på den svenska handboken BVH 585.30 för riskbedömning av järnvägstunnlar

C.8.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.8.2. Syftet med exemplet är att jämföra processen enligt den gemensamma säkerhetsmetoden med handboken BVH 585.30 som används av den svenska infrastrukturförvaltaren Banverket för att planera och verifiera att en tillräcklig säkerhetsnivå uppnås under planeringen och byggandet av nya järnvägstunnlar. De gemensamma punkterna och skillnaderna gentemot den gemensamma säkerhetsmetoden finns angivna nedan. De detaljerade riskbedömningskraven finns i handboken BVH 585.30.

C.8.3. I jämförelse med processen enligt den gemensamma säkerhetsmetoden i figur 1

(a) uppvisar handboken BVH 585.30 följande gemensamma punkter:

(1) Systembeskrivning [avsnitt 2.1.2]:

I handboken finns krav på en detaljerad systembeskrivning som innehåller följande:

(i) En beskrivning av tunneln.
(ii) En beskrivning av spåret.
(iii) En beskrivning av typen av rullande materiel (inklusive ombordpersonal).
(iv) En beskrivning av trafiken och den planerade driften.
(v) En beskrivning av extern assistans (inklusive räddningsinsatser).

(2) Identifiering av faror [avsnitt 2.2]:

I handboken finns inget explicit krav på identifiering av faror. Det finns ett krav på riskidentifiering och en ”olyckskatalog” som innehåller de typer av identifierade potentiella olyckor som anses ha en betydande inverkan på tunnelns risknivå och som måste ingå i den efterföljande bedömningen. Exempel på olyckor:

(i) ”Urspårning av passagerartåg”.
(ii) ”Urspårning av godståg”.
(iii) ”Olycka som omfattar farligt gods”.
(iv) ”Brand i fordon”.
(v) ”Kollision mellan passagerartåg och lätt/tungt föremål”.
(vi) Etc.

(3) Det finns inga bestämmelser om tillämpning av handlingsregler eller liknande referenssystem. Det anses att riskanalys alltid ska utföras.

(4) Uttrycklig riskuppskattning och riskvärdering [avsnitt 2.5]:

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

(i) I handboken rekommenderas generellt att ett fullständigt händelseträd ska tas fram för varje typ av olycka, baserat på en kvantitativ riskanalys. Men eftersom syftet med riskanalysen är att analysera den globala säkerhetsnivån för tunneln snarare än att analysera den enskilda säkerheten på mer detaljerade nivåer, läggs konsekvenserna för alla scenarier samman för att få den totala risknivån för tunneln.

(ii) Godtagbarheten för denna globala risknivå för tunneln ska jämföras med följande explicita kvantitativa kriterium för riskacceptans: *järnvägstrafik per kilometer i tunnlar ska vara lika säker som järnvägstrafiken per kilometer på öppna spår, exklusive plankorsningar*. Detta kriterium omvandlas till en FN-kurva som baseras på historiska data för järnvägsolyckor i Sverige och extrapoleras för att även omfatta konsekvenser som inte ingår i statistiken.

(iii) Utöver detta kriterium för den globala risknivån för tunneln, finns det även andra krav som måste uppfyllas, särskilt när det gäller evakuering av tunnlar och möjligheten till räddningsinsatser:

- Verifiera att självräddning är möjlig vid brand i ett tåg som ett ”troligt värsta fall” (kriterier för denna bedömning anges också).
- Tunneln ska planeras på ett sådant sätt att räddningsinsatser är möjliga för en given uppsättning scenarier.

(5) Resultat från riskbedömningen [avsnitt 2.1.6]:

Resultaten från riskbedömningen är

(i) en förteckning över säkerhetsåtgärder från minimistandarden baserad på TSD-SRT (Säkerhet i järnvägstunnlar) och nationella regler som ska användas vid konstruktionen av tunneln, och

(ii) alla övriga säkerhetsåtgärder som har identifierats som nödvändiga vid riskanalysen, med information om deras syfte. Det konstateras att åtgärderna ska fastställas enligt följande prioritetsordning:

- Förebyggande av olyckor.
- Minskning av konsekvenserna av olyckor.
- Underlättande av evakuering.
- Underlättande av räddningsinsatser.

(6) Hantering av faror [avsnitt 4.1]:

I handboken krävs inte explicit att ett protokoll om faror ska föras. Detta hör samman med det faktum att bedömningen sker på global nivå och att farorna därför inte utvärderas och kontrolleras individuellt. Godtagbarheten för den globala risken för tunneln utvärderas, utan någon fördelning av ett globalt kriterium för riskacceptans ned till de olika typerna av olyckor eller bakomliggande farorna.

Det finns emellertid en förteckning över alla säkerhetsåtgärder, både de som härrör från ”minimistandarden” och de som har identifierats som nödvändiga enligt riskanalysen: se punkt (a)(5)(ii) ovan. Det ska noteras i förteckningen över säkerhetsåtgärder om de gäller tunnelns infrastruktur, spåret, driften eller den rullande materielen och också vad deras avsedda effekt är enligt den numrerade listan i punkt (a)(5)(ii). I handboken finns inget krav på en explicit redovisning av vilka faror som säkerhetsåtgärderna kontrollerar och vem som ansvarar för åtgärderna.

(7) Oberoende bedömning [artikel 6]:

En oberoende bedömning som ska utföras av en tredje part är obligatorisk för att

(i) kontrollera om den riskbedömningsprocess som rekommenderas i handboken BVH 585.30 har utförts korrekt,

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

(ii) betrakta riskanalysen som godtagbar,
(iii) kontrollera om det tydligt anges hur framtida säkerhetsstyrning ska utföras i projektet.

Det slutliga riskanalysdokumentet ska undertecknas av den oberoende bedömaren och även av projektets säkerhetssamordnare.

(b) Handboken BVH 585.30 skiljer sig i fråga om följande aspekter:

(1) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

I handboken BVH 585.30 finns varken krav på att spåra hur de identifierade säkerhetskraven genomförs eller att verifiera att den slutliga tunnelkonstruktionen uppfyller de angivna säkerhetskraven. Den beskriver endast hur dessa krav ska överföras för att säkerställa att de genomförs under konstruktionsfasen.

I handboken finns säkerhetskrav som ska användas för att verifiera att riskanalysen har utförts på ett korrekt och öppet sätt och att den kan accepteras av projektet.

C.8.4. Sammanfattningsvis visar jämförelsen med den gemensamma säkerhetsmetoden att

(a) handboken BVH 585.30 uppfyller de relevanta delarna i den gemensamma säkerhetsmetoden, även om deras omfattning och syfte inte är exakt de samma,
(b) handboken BVH 585.30 bedömer den övergripande risknivån för en järnvägstunnel,
(c) farorna inte kontrolleras individuellt och att den därför är mindre inriktad på hantering av faror,
(d) påvisandet av överensstämmelse och verifiering av korrekt genomförande av alla säkerhetsåtgärder inte anges så explicit. I handboken anges dock att säkerhetssamordnarens roll inom projektet (en roll och kompetens som krävs enligt BVH 585.30) är att verifiera att slutsatserna av riskanalysen genomförs i konstruktionsdokumenten och ritningarna och även att kontrollera att de genomförs korrekt under konstruktionsfasen.

C.8.5. Den gemensamma säkerhetsmetoden är mer allmängiltig än handboken BVH 585.30 i den meningen att den erbjuder tillämpning av tre olika principer för riskacceptans. Att tillämpa handboken BVH 585.30 i den gemensamma säkerhetsmetoden ger dock inte upphov till några problem eftersom den är förenlig med användningen av den tredje principen om uttrycklig riskuppskattning.

C.9. Exempel på riskbedömning på systemnivå för Köpenhamns metro

C.9.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

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

C.9.2. Detta exempel hänför sig till ett fullständigt och komplext förarlöst metrosystem, inklusive bakomliggande tekniska delsystem (t.ex. automatisk hastighetsövervakning och rullande materiel) samt drift och underhåll av systemet. En riskbedömningsbaserad metod tillämpades för att utvärdera systemet och de bakomliggande delsystemen. Projektet omfattade också certifiering av säkerhetsstyrningssystemet hos det företag som skulle ha hand om driften av systemet. Detta hänför sig till järnvägsföretagets och infrastrukturförvaltarens förmåga att på ett säkert sätt hantera och underhålla hela systemet under systemets livscykel.

C.9.3. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg (se även figur 1):

(a) Systembeskrivning [avsnitt 2.1.2]:

(1) Beskrivning av kraven för systemets prestanda.
(2) Beskrivning av driftsreglerna.
(3) En tydlig beskrivning av kontaktpunkterna och ansvarsområdena mellan de olika aktörerna, särskilt mellan de tekniska delsystemen.
(4) Definition av systemkraven på hög nivå (i fråga om godtagbar olycksfrekvens och definition av ett ALARP-område).

(b) Identifiering av faror [avsnitt 2.2]:

(1) En preliminär analys av faror på systemnivå.
(2) En funktionell analys på systemnivå som belyser alla delsystem, och inte enbart dem som uppenbarligen är säkerhetskritiska (t.ex. automatisk hastighetsövervakning och rullande materiel) som bidrar till säkerhetsfunktionerna och har en aktiv roll för att garantera passagerarnas och personalens säkerhet.
(3) Intensiv samordning mellan aktörerna (underleverantörer, delsystemsleverantörer av tekniska delsystem och byggnadsarbeten)

(i) för att systematiskt identifiera alla rimligen förutsebara faror,
(ii) för att identifiera eventuella åtgärder för att kontrollera alla risker som hör samman med de identifierade farorna på en godtagbar nivå.

(c) Användning av ett referenssystem [avsnitt 2.3]:

Olika handlingsregler, standarder och förordningar användes, t.ex.

(1) BOStrab-förordningen om konstruktion och drift av spårvagnar (tysk förordning som gäller järnvägssystem inom tättbebyggt område) och om förarlös drift,
(2) VDV-dokument (tyska handlingsregler) som hänför sig till kraven på utrustning för att säkerställa passagerarnas säkerhet på stationer med förarlös drift,
(3) Cenelec-standarder för järnvägssystem (EN 50126, 50128 och 50129). Dessa standarder gäller särskilt för tekniska järnvägssystem. Men de innehåller också ett metodiskt tillvägagångssätt som har allmän giltighet. De har använts i stor utsträckning för Köpenhamns metro:

(i) EN 50126 användes för säkerhetsstyrnings- och riskbedömningsaktiviteterna för hela järnvägssystemet.
(ii) EN 50129 användes för hela signalsystemet.
(iii) EN 50128 användes för programvaruutvecklingen (inklusive verifiering och validering) för de tekniska delsystemen.

(4) Brandskyddsstandarder för tunnlar (NEPA 130).
(5) Standarder för väg- och vattenbyggnad och byggnadsarbeten (Eurokoder).

(d) Användning av ett referenssystem [avsnitt 2.4]:

Metron skulle uppnå en säkerhetsnivå som motsvarade moderna installationer i Tyskland, Frankrike och Storbritannien. Dessa befintliga system användes som liknande

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

referenssystem för att härleda kriterierna för riskacceptans i fråga om godtagbara olycksfrekvenser för Köpenhamns metro.

(e) Uttrycklig riskuppskattning och riskvärdering [avsnitt 2.5]:

(1) För uppskattning av risker som hör samman med specifika faror.
(2) För styrning av nödventilationen i tunnlar (inklusive mänskliga faktorer som berör brandkår/räddningstjänst).
(3) För identifiering av riskminskningsåtgärder.
(4) För utvärdering om en godtagbar risknivå har uppnåtts för hela systemet.

(f) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

(1) Ledningens insatser och de tekniska insatserna var förenliga med systemets komplexitet för att påvisa systemets säkerhet.
(2) Fördelning av systemets säkerhetskrav ned till tekniska delsystem och byggnadsarbeten, liksom alla säkerhetsrelaterade funktioner gällande metron.
(3) Påvisande av att varje delsystem uppfyller, så som de är konstruerade, sina säkerhetskrav.
(4) För säkerhetsfunktioner som utförs av mer än ett delsystem kunde påvisandet av att säkerhetskraven har uppfyllts inte slutföras på delsystemnivå. Det utfördes på systemnivå genom integrering av de olika delsystemen, verktygen och förfarandena.
(5) Påvisande av att hela systemet uppfyllde säkerhetskraven på hög nivå.

(g) Hantering av faror [avsnitt 4.1]:

Identifieringen av faror, tillhörande säkerhetsåtgärder och de resulterande säkerhetskraven registrerades och hanterades med hjälp av ett centralt protokoll om faror. Den övergripande säkerhetschefen för projektet ansvarade för detta protokoll om faror. De driftsrelaterade farorna som uppkom under konstruktionen och installationen, liksom faror som hänförde sig till drift och underhåll ingick i protokollet om faror.

(h) Bevisning från riskhanteringen och riskbedömningen [avsnitt 5]:

Resultaten från riskbedömningen dokumenterades formellt och stöddes av en säkerhetsbevisning som uppfyllde kraven enligt Cenelec-standarderna:

(1) Säkerhetsbevisning för hela systemet.
(2) Säkerhetsbevisning för varje tekniskt delsystem (inklusive delsystem för signalering och byggnadsarbeten).
(3) Säkerhetsbevisning för byggnadsarbeten (stationer, tunnlar, viadukter, banvallar).
(4) Säkerhetsbevisning för installationen.
(5) Säkerhetsbevisning för fordonen.
(6) Säkerhetsbevisning för operatörer (som stöder järnvägsföretagets och infrastrukturförvaltarens certifiering av säkerhetsstyrningssystemet, dvs. påvisar förslagsställarens förmåga att driva och underhålla systemet på ett säkert sätt).

(i) Oberoende bedömning [artikel 6]:

Hela processen följdes upp och bedömdes av en oberoende säkerhetsbedömare, som agerade på uppdrag av den tekniska tillsynsmyndigheten (dvs. det danska transportministeriet). Den oberoende säkerhetsbedömarens roller beskrivs i en relevant handlingsregel. Dessa omfattar

(1) att kontrollera att riskhanteringen och riskbedömningen är korrekt,
(2) att kontrollera att systemet är lämpligt för dess ändamål och att det kommer att drivas och underhållas på ett säkert sett under hela dess livscykel,
(3) en rekommendation om godkännande till den tekniska tillsynsmyndigheten.

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

C.9.4. Hela projektet stöddes av en lämplig kvalitetsstyrningsprocess.

C.9.5. I projektet överlämnades säkerhetsbevisningar från leverantörerna (dvs. säkerhetsbevisningar och detaljerad stödjande dokumentation för det tekniska delsystemet och byggnadsarbetet) till förslagsställarens säkerhetschef. Dessa bevisningar granskades därefter av säkerhetsstyrningsorganisationen, liksom av den oberoende säkerhetsbedömaren vars slutsatser rapporterades i en bedömningsrapport.
Rapporten från den oberoende säkerhetsbedömningen granskades av förslagsställarens säkerhetsstyrningsorganisation och överlämnades till förslagsställaren som vidarebefordrade alla dokument till den tekniska tillsynsmyndigheten (dvs. det danska transportministeriet) för ett slutligt godkännande.

C.90,6. Exemplet visar att de principer som krävs enligt den gemensamma säkerhetsmetoden är metoder som används inom järnvägssektorn. Riskbedömningen i exemplet uppfyller alla krav enligt den gemensamma säkerhetsmetoden. I riskbedömningen används särskilt två av de tre principerna för riskacceptans som medges enligt det harmoniserade tillvägagångssättet i den gemensamma säkerhetsmetoden:

C.10. Exempel på riktlinjer från Otif för att beräkna risker i samband med järnvägstransport av farligt gods

C.10.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.10.2. Den övergripande filosofin i riktlinjerna från Otif ligger i linje med den gemensamma säkerhetsmetodens syfte, men riktlinjerna har ett mindre tillämpningsområde. Syftet med Otifs *riktlinjer är att uppnå ett mer enhetligt tillvägagångssätt för riskbedömningen av transport av farligt gods i Cotifs medlemsstater och på så sätt göra de individuella riskbedömningarna jämförbara*. Den stöder således korsacceptans mellan Cotifs medlemsstater för riskbedömningar av järnvägstransport av farligt gods.

C.10.3. Jämfört med den gemensamma säkerhetsmetoden och flödesschemat i figur 1 gäller följande:

(a) Otifs riktlinjer uppvisar följande gemensamma punkter med den gemensamma säkerhetsmetoden:

(1) Det är ett gemensamt synsätt för riskbedömning, likväl endast baserat på uttrycklig riskuppskattning (dvs. den tredje principen för riskacceptans enligt den gemensamma säkerhetsmetoden).
(2) Otifs riskbedömning består av följande:

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

(i) En riskanalysfas som omfattar

- en fas för identifiering av faror,
- en fas för riskuppskattning.

(ii) En fas för riskvärdering som baseras på kriterier för en (godtagbar) risknivå som ännu inte är harmoniserade. En rad nationella särdrag kan påverka dessa kriterier.

(b) Otifs riktlinjer skiljer sig från den gemensamma säkerhetsmetoden i fråga om följande aspekter:

(1) Dess tillämpningsområde är annorlunda. Medan den gemensamma säkerhetsmetoden endast har tillämpats på betydande ändringar av ett järnvägssystem, ska Otifs riktlinjer tillämpas för att bedöma riskerna i samband med järnvägstransport av farligt gods, oberoende om detta utgör en betydande ändring eller inte för järnvägssystemet.
(2) Det finns ingen möjlighet att välja mellan de tre principerna för riskacceptans för att kontrollera riskerna. Den tredje principen, dvs. uttrycklig riskuppskattning, är den enda som är tillåten. Vidare måste den uteslutande baseras på en kvantitativ uppskattning i stället för en kvalitativ. Den kvalitativa riskanalysen är eventuellt endast lämplig för att jämföra alternativa (säkerhets-)åtgärder för riskminskning.
(3) Det krävs att ALARP-principen tillämpas för att fastställa om ytterligare säkerhetsåtgärder skulle kunna minska den bedömda risken ytterligare till en rimlig kostnad.
(4) Begreppet ”faror som hör samman med allmänt godtagbara risker” som gör det möjligt att inrikta riskbedömningsinsatsen mot de mest bidragande farorna saknas. Likväl rekommenderas att antalet potentiella olycksscenarier minskas till ett rimligt antal grundscenarier (se avsnitt 3.2 i {ref. 10}).
(5) Processen är inriktad på riskbedömning men omfattar inte

(i) processen för att välja och genomföra (säkerhets-)åtgärder för att modifiera risken,
(ii) processen för riskacceptans,
(iii) processen för att påvisa att systemet uppfyller säkerhetskraven,
(iv) processen för att kommunicera risken till andra berörda aktörer (se punkten nedan).

(6) Inga direktiv ges om vilka bevisningar som riskbedömningsprocessen ska leda till.
(7) Krav på hantering av faror saknas.
(8) Krav på en oberoende bedömning utförd av en tredje part för att bedöma att den gemensamma modellen har tillämpats korrekt saknas.

C.10.4. Jämförelsen mellan Otifs riktlinjer och den gemensamma säkerhetsmetoden visar att båda är förenliga, även om deras tillämpningsområde och syfte inte är exakt lika. Den gemensamma säkerhetsmetoden är mer allmängiltig än Otifs riktlinjer, i den meningen att den är mer flexibel. Å andra sidan omfattar den gemensamma säkerhetsmetoden även fler riskhanteringsaktiviteter:

(a) Den medger användning av tre principer för riskacceptans som är baserade på befintliga regler inom järnvägssektorn: se avsnitt 2.1.4.
(b) Dess tillämpning krävs endast för betydande ändringar och ytterligare riskanalys krävs endast för faror som inte hör samman med en allmänt godtagbar risk.
(c) Den omfattar val och genomförande av säkerhetsåtgärder som förväntas kontrollera de identifierade farorna och de tillhörande riskerna.
(d) Den harmoniserar riskhanteringsprocessen, däribland

(1) harmoniseringen av kriterier för riskacceptans som behandlas inom ramen för byråns arbete med allmänt godtagbara risker och kriterier för riskacceptans,

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

(2) påvisandet av att systemet uppfyller säkerhetskraven,
(3) resultaten och bevisningen från riskbedömningsprocessen,
(4) utbytet av säkerhetsrelaterad information mellan de berörda aktörerna vid kontaktpunkterna,
(5) hanteringen av ett protokoll om alla identifierade faror och tillhörande säkerhetsåtgärder,
(6) den oberoende bedömningen som utförs av en tredje part för att bedöma om den gemensamma säkerhetsmetoden tillämpats korrekt.

C.10.5. Att tillämpa Otif-riktlinjerna inom ramen för den gemensamma säkerhetsmetoden (i det fall då transport av farligt gods utgör en betydande ändring för en infrastrukturförvaltare eller ett järnvägsföretag) utgör dock inga problem eftersom det är förenligt med användningen av den tredje principen för uttrycklig riskuppskattning.

C.11. Exempel på riskbedömning av en ansökan om godkännande för en ny typ av rullande materiel

C.11.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.11.2. Detta exempel på riskbedömning hänför sig till ansökan om godkännande av en ny typ av rullande materiel. En riskanalys utfördes för att utvärdera riskerna i samband med införandet av en ny godsvagn.

C.11.3. Syftet med ändringen var att öka effektiviteten, kapaciteten, prestandan och tillförlitligheten för transport av bulkvaror på en specifik fraktlinje. Eftersom vagnarna var avsedda för gränsöverskridande trafik krävdes också godkännande från två olika nationella säkerhetsmyndigheter. Förslagsställaren var fraktoperatören som i sin tur ägdes av företaget som tillverkade varorna som skulle transporteras.

C.11.4. Projektutvecklingen omfattade konstruktion, tillverkning, montering, idrifttagande och verifiering av den nya rullande materielen. En riskanalys utfördes för att verifiera att den nya konstruktionen uppfyllde säkerhetskraven för varje delsystem liksom för hela systemet.

C.11.5. I riskanalysen hänvisades till förfarandena och definitionerna i Cenelec EN 50126 och riskvärderingen utfördes enligt denna standard.

C.11.6. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg:

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

(a) Systembeskrivning [avsnitt 2.1.2]:

För varje konstruktionsfas fanns det krav på säkerhetsverifieringsdokumentation och beskrivning av systemets konstruktion:

(1) Den konceptuella fasen: preliminär beskrivning av operatörens driftskrav,

(2) Specifikationsfasen: funktionell specifikation, tillämpliga tekniska standarder, plan för testning och verifiering. Kraven från operatören på drift och underhåll av vagnen ingick också.

(3) Tillverkningsfasen: teknisk dokumentation från tillverkaren, inklusive ritningar, standarder, beräkningar etc. Djupgående analys av nya eller innovativa utformningar eller nya användningsområden.

(4) Verifikationsfasen:

(i) Tillverkarens verifikation av vagnens tekniska prestanda (testrapporter, beräkningar, verifikationer i överensstämmelse med standarder och funktionella krav).
(ii) Dokumentation om riskminskningsåtgärder och testrapporter som bevisade vagnens förenlighet med järnvägsinfrastrukturen.
(iii) Underhålls- och utbildningsdokument, användarmanualer etc.

(5) Godkännandefasen:

(i) Tillverkarens säkerhetsdeklaration och säkerhetsbevisning.
(ii) Operatörens godkännande av både fraktvagnen och dess dokumentation.

(b) Identifiering av faror [avsnitt 2.2]:

Detta utfördes kontinuerligt under alla konstruktionsfaser. Först användes en ”bottom-up”-modell där olika tillverkare utvärderade risksekvenser som uppstod på grund av felyttringar hos komponenter i deras delsystem. Uppdelningen i delsystem såg ut på följande sätt:

(1) chassier,
(2) bromssystem,
(3) central koppling,
(4) etc.

En kompletterande ”top-down”-modell tillämpades därefter för att söka efter luckor eller informationsbrister. Risker som inte omedelbart kunde godkännas överfördes till protokollet om faror för ytterligare behandling och klassificering.

(c) Användning av ett referenssystem [avsnitt 2.1.4]:

En uttrycklig riskuppskattning utfördes på systemet som helhet. Handlingsregler eller liknande referenssystem kunde dock användas för att bedöma enskilda faror. Principen är att varje delsystem ska vara minst lika säkert som det delsystem som det ska ersätta, vilket leder till ett nytt, fullständigt system med en högre säkerhetsnivå än det tidigare. Riskmatrisen i EN 50126 användes för att plotta de identifierade farorna. Olika andra kriterier för riskacceptans tillämpades också, bland annat följande:

(1) En enstaka felyttring ska inte leda till en situation med allvarlig inverkan på människor, material eller miljö.
(2) Om detta inte kan undvikas med tekniska konstruktionsmedel ska det förhindras genom driftsregler eller underhållskrav; detta gällde endast faror för vilka det var möjligt att identifiera den uppkomna felyttringen innan den leder till en farlig situation.

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

(3) För komponenter med en hög sannolikhet för felyttring eller då felyttringar inte kan upptäckas i förväg eller förhindras genom underhåll eller driftsregler, kan ytterligare säkerhetsfunktioner och barriärer övervägas.
(4) Redundanta system med komponenter som kan utveckla felyttringar under drift som inte går att upptäcka ska skyddas genom underhållsåtgärder för att minska en minskad redundans.
(5) Den resulterande slutliga säkerhetsnivån var ett ledningsbeslut, som var baserat på kvantitativ och kvalitativ riskanalys.

(d) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

Alla identifierade risker och faror registrerades och förteckningen konsulterades och uppdaterades kontinuerligt. Kvarvarande faror registrerades i protokollet om faror tillsammans med motsvarande förteckning över riskminskande åtgärder som skulle vidtas under konstruktion, drift och underhåll. På grundval av detta togs en slutlig säkerhetsrapport fram med verifieringen av att säkerhetskraven hade genomförts.

(e) Hantering av faror [avsnitt 4.1]:

Så som anges ovan registrerades farorna och deras tillhörande säkerhetsåtgärder i ett protokoll om faror för att hålla reda på alla identifierade faror och säkerhetsåtgärder. Faror som hörde samman med risker som var godtagbara utan några åtgärder ingick dock inte i protokollet om faror.

(f) Oberoende bedömning [artikel 6]:

Ingen oberoende bedömning nämndes i de dokument som togs emot om denna betydande ändring.

C.11.7. Exemplet på riskbedömning är baserat på Cenelec-standarden EN 50126 och motsvarar mycket väl processen enligt den gemensamma säkerhetsmetoden. Riskbedömningen i exemplet uppfyller alla krav enligt den gemensamma säkerhetsmetoden, med undantag av kraven på en oberoende bedömning som inte klargjordes explicit i de mottagna dokumenten. Explicita kriterier för riskacceptans användes och angavs tydligt.

C.12. Exempel på riskbedömning av en driftsrelaterad betydande ändring – drift med enbart tågförare

C.12.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

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

C.12.2. Exemplet är en driftsrelaterad ändring där järnvägsföretaget beslutade att tåget skulle köras med enbart tågförare (drift med enbart tågförare – DOO) på en rutt där det tidigare fanns en konduktör ombord som hjälpte föraren med tågklareringen.

C.12.3. I jämförelse med processen enligt den gemensamma säkerhetsmetoden tillämpades följande steg (se även figur 1):

(a) Betydelsen av ändringen [artikel 4].

Järnvägsföretaget utförde en preliminär riskbedömning varvid slutsatsen drogs att den driftsrelaterade ändringen var betydande. Eftersom tågföraren skulle arbeta ensam, utan assistans, kunde risken för att passagerarna fastnar i dörrarna eller faller ned på spåret (t.ex. om dörrarna öppnas på fel sida) inte negligeras.

Vid jämförelse av denna preliminära riskbedömning med kriterierna i artikel 4 i förordningen om en gemensam säkerhetsmetod skulle ändringen också kunna kategoriseras som betydande på grundval av följande kriterier:

(1) Säkerhetsrelevans: Ändringen är säkerhetsrelaterad eftersom inverkan av kravet på ett helt annat sätt att hantera driften av tågtjänsten skulle kunna vara katastrofal.
(2) Felkonsekvens: Den potentiella effekten på förarens prestationsförmåga skulle kunna leda till katastrofala konsekvenser om inte driften kontrolleras på ett effektivt sätt.
(3) Nyhetsgrad: Drift med enbart förare skulle kunna kräva innovativa sätt att köra tågen, vars risker måste bedömas.

(b) Systemdefinition [avsnitt 2.1.2]:

Systemdefinitionen beskrev

(1) det befintliga systemet, med tydlig förklaring av vilka uppgifter som föraren utförde och vilka uppgifter som utfördes av ombordpersonalen (eller konduktören) för att hjälpa föraren,
(2) ändringen av förarens ansvarsområden på grund av borttagandet av den assisterande ombordpersonalen,
(3) de tekniska kraven på systemet för att täcka de driftsrelaterade ändringarna,
(4) de befintliga kontaktpunkterna mellan den assisterande ombordpersonalen, föraren och infrastrukturförvaltarens spårpersonal.

Under de olika iterationerna uppdaterades systemdefinitionen med säkerhetskrav från riskbedömningsprocessen. Viktiga personer (däribland förare, personalföreträdare och infrastrukturförvaltaren) deltog i denna löpande process för identifiering av faror och uppdatering av systemdefinitionen.

(c) Identifiering av faror [avsnitt 2.2]:

Farorna och möjliga säkerhetsåtgärder identifierades vid ett brainstormingmöte med en grupp experter och omfattade bland annat

(1) förarnas och personalens företrädare, med sin driftsmässiga erfarenhet,
(2) företrädare för infrastrukturförvaltaren eftersom infrastrukturen också skulle kunna påverkas av ändringen, inbegripet exempelvis ändringar av stationerna (t.ex. installation av speglar, kameraövervakning [CCTV] på perrongerna).

De extrauppgifter som förarna skulle utföra granskades för att identifiera alla förutsebara faror som skulle kunna uppträda efter att den assisterande ombordpersonalen hade tagits bort. I synnerhet undersökte man vid identifieringen av faror vilka de viktiga driftsrelaterade farorna skulle kunna vara vid stationerna, på de befintliga rutterna på vilka det fanns assistans från ombord- eller spårpersonalen inklusive säker klarering av

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

tågen, särskilda frågor som hörde samman med föraren, den rullande materielen (t.ex. kontroll vid dörröppning/-stängning), underhållskrav etc.

Varje identifierad fara tilldelades en allvarlighetsgrad och konsekvenser (hög, medel, låg) och hur den föreslagna ändringen som undersökts påverkade dem (ökad, oförändrad, minskad risk).

(d) Användning av handlingsregler [avsnitt 2.3] och användning av liknande referenssystem [avsnitt 2.4]:

Både handlingsreglerna (dvs. en uppsättning standarder för drift med enbart förare) och liknande referenssystem användes för att definiera säkerhetskraven för de identifierade farorna. Dessa säkerhetskrav omfattade

(1) de reviderade driftrutinerna för föraren som krävs för att köra tågen på ett säkert sätt utan assistans från ombordpersonal,
(2) eventuell ytterligare utrustning som krävs ombord eller på spåret för att säkerställa säkra och tillförlitliga medel för tågklareringen,
(3) en checklista för att säkerställa att förarhytten var lämplig med hänsyn tagen till kontaktpunkten mellan järnvägssystemet (både ombord och på spåret) och föraren.

De driftsregler som krävdes reviderades så att de uppfyllde kraven i de tillämpliga handlingsreglerna och de relevanta referenssystemen. Alla berörda parter deltog i revideringen av driftrutinerna och i överenskommelsen om att gå vidare med förändringen.

(e) Påvisande av att systemet uppfyller säkerhetskraven [avsnitt 3]:

Systemet genomfördes i enlighet med de identifierade säkerhetskraven (ytterligare utrustning och reviderade förfaranden). Dessa verifierades som lämpliga medel för att säkerställa en tillräcklig säkerhetsnivå för det system som var föremål för bedömning.

De reviderade driftrutinerna infördes i järnvägsföretags säkerhetsstyrningssystem. De reviderade rutinerna övervakades och granskades vid behov för att säkerställa att kontrollen av de identifierade farorna fortfarande var korrekt under driften av järnvägssystemet.

(f) Hantering av faror [avsnitt 4.1]:

Se punkten ovan om att järnvägsföretagens process för att hantera faror kan utgöra en del av deras säkerhetsstyrningssystem för att registrera och hantera risker. De identifierade farorna registrerades i ett protokoll om faror med de säkerhetskrav som kontrollerade den tillhörande risken, dvs. hänvisning till extrautrustning ombord och på spåret liksom de reviderade driftrutinerna.
De reviderade rutinerna övervakades och granskades vid behov för att säkerställa att kontrollen av de identifierade farorna fortfarande var korrekt under driften av järnvägssystemet.

(g) Oberoende bedömning [artikel 6]:

Riskbedömnings- och riskhanteringsprocessen bedömdes av en kompetent person inom järnvägsföretaget, som var oavhängig av bedömningsprocessen. Den kompetenta personen bedömde både processen och resultaten, dvs. de identifierade säkerhetskraven.

Järnvägsföretag har grundat sitt beslut om att införa det nya systemet på den kompetenta personens rapport från den oberoende bedömningen.

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

C.12.4. Exemplet visar att de principer och den process som järnvägsföretaget använder ligger i linje med den gemensamma säkerhetsmetoden. Riskhanterings- och riskbedömningsprocessen uppfyllde alla krav enligt den gemensamma säkerhetsmetoden.

C.13. Exempel på användning av ett referenssystem för att härleda säkerhetskrav för nya elektroniska signalställverkssystem i Tyskland

C.13.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring. Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.13.2. För att härleda standardmässiga säkerhetskrav för framtida elektroniska ställverkssystem hade Deutsche Bahn genomfört en riskanalys på ett redan godkänt elektroniskt system. Det senare systemet hade tidigare godkänts i enlighet med tysk standard (Mü 8004).

C.13.3. Riskanalysen utfördes i enlighet med Cenelec-standarderna (EN 50126 och EN 50129) och omfattade följande steg:

(a) Systemdefinition.
(b) Identifiering av faror.
(c) Analys och kvantifiering av faror.

C.13.4. När det gäller systemdefinitionen hade man varit noga med att definiera systemets gränser, dess funktioner och kontaktpunkter. Den största utmaningen var att definiera systemet på ett sådant sätt att det var oberoende av den interna arkitekturen hos ett ställverkssystem samtidigt som det förblev förenligt med befintliga ställverkssystem. Särskild uppmärksamhet ägnades därvid att på ett mycket tydligt sätt definiera kontaktpunkterna med externa system som interagerade med ställverket utan att specificera ställverkets inre funktioner.

C.13.5. Farorna identifierades därefter endast vid kontaktpunkterna för att förbli generiska (dvs. för att undvika att de blev beroende av specifika arkitekturer). Hänsyn togs endast till faror som uppkom på grund av tekniska fel. För varje kontaktpunkt identifierades således två generiska faror:

(a) Felaktiga utdata från ställverket som överfördes till kontaktpunkten.
(b) (Korrekta) indata som blev korrupta vid kontaktpunkten.

C.13.6. Dessa generiska faror försågs sedan med mer specifika egenskaper för varje kontaktpunkt.

C.13.7. I den följande fasen analyserades bidragen från det befintliga systemets komponenter till var och en av de identifierade farorna som sedan samlades i ett felträd. Detta gjorde det möjligt

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

att på grundval av de uppskattade felintensiteterna för komponenterna beräkna förekomstfrekvensen för varje fara och använda dessa frekvenser som tolererbara risknivåer (THR) för framtida generationer av elektroniska ställverk.

C.13.8. Riskanalysen följdes upp och bedömdes av den nationella säkerhetsmyndigheten (EBA – Eisenbahnbundesamt).

C.13.9. En analys av det elektroniska systemets styr- och visningsfunktioner utfördes också som en del av riskanalysen. Än en gång användes ett befintligt, elektroniskt ställverkssystem som referens för att härleda säkerhetskraven för funktionerna för samspelet mellan människa och teknik (MMI) för att kontrollera både slumpmässiga felyttringar och fel och för att kontrollera systematiska fel. Som ett resultat fastställdes tillförlitlighetsnivåerna (SIL) för olika funktioner: För MMI-funktioner vid normaldrift, för MMI-funktioner vid kommandofrigivningsdrift (störning) och för visningsfunktionalitet.

C.13.10. Riskanalysen följdes också upp och bedömdes av den nationella säkerhetsmyndigheten (EBA).

C.13.11. Dessa riskbedömningsexempel åskådliggör hur den andra riskacceptansen (referenssystem) enligt den gemensamma säkerhetsmetoden kan användas för att härleda säkerhetskrav för nya system. Dessutom grundade de sig på Cenelec-standarder och stämmer därför bra överens med processen enligt den gemensamma säkerhetsmetoden. Riskbedömningen i exemplen uppfyller kraven enligt den gemensamma säkerhetsmetoden som hör samman med de faser som den omfattar. Men eftersom ingen konstruktionsaktivitet ingår finns det varken någon hänvisning till hantering av protokoll om faror eller något påvisande om att det system som är föremål för bedömning uppfyller de identifierade säkerhetskraven.

C.13.12. Ytterligare information om dessa riskanalyser finns i följande referenser:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *”Erfahrungen mit der Risikoanalyse ESTW (DB AG)”*, Signal+Draht, 10, 2003, 10–15, och

(b) Bock, H., Braband, J., och 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. Exempel på ett explicit kriterium för riskacceptans för radiobaserad tågdrift (FFB – FunkFahrBetrieb) i Tyskland

C.14.1. **Anmärkning:** Detta exempel på riskbedömning är inte något resultat av tillämpningen av processen enligt den gemensamma säkerhetsmetoden eftersom den utfördes innan den gemensamma säkerhetsmetoden existerade. Syftet med detta exempel är

(a) att identifiera likheter mellan befintliga riskbedömningsmetoder och processen enligt den gemensamma säkerhetsmetoden,
(b) att åstadkomma en spårbarhet mellan en befintlig process och den som krävs enligt den gemensamma säkerhetsmetoden,
(c) att motivera mervärdet av att utföra de ytterligare steg (om det finns några) som krävs enligt den gemensamma säkerhetsmetoden.

Det måste betonas att detta exempel enbart är informativt. Dess syfte är att underlätta för läsaren att förstå processen i den gemensamma säkerhetsmetoden. Men exemplet i sig ska inte omvandlas till eller användas som referenssystem för en annan betydande ändring.

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

Riskbedömningen ska utföras för varje betydande ändring i överensstämmelse med förordningen om en gemensam säkerhetsmetod.

C.14.2. En riskanalys i enlighet med Cenelec-standarderna utfördes för en helt ny driftrutin som var planerad (men aldrig införd) för konventionella järnvägslinjer i Tyskland. Konceptet bestod av att köra tågen på ett säkert sätt med enbart radiobaserad styrning (av rutt och tåg). Eftersom det saknades handlingsregler (erkända tekniska regler) och referenssystem för ett sådant nytt system, utfördes en uttrycklig riskuppskattning för att påvisa den nya rutinens säkerhet. Det var nödvändigt att visa att risknivån för en passagerare till följd av det nya systemet inte skulle överstiga ett godtagbart riskvärde (explicit kriterium för riskacceptans).

C.14.3. Detta explicita kriterium för riskacceptans uppskattades på grundval av olycksstatistik i Tyskland som tillskrevs signal- och styrsystem, och dess sannolikhet jämfördes också med MEM-kriteriet (MEM – minimum endogenous mortality). Ett sådant påvisande av säkerheten överensstämmer med det tyska kravet enligt EBO (Eisenbahn Bau- und Betriebsordnung) om ”samma säkerhetsnivå” vid avvikelser från tekniska regler. Riskanalysen följdes också upp och bedömdes av den nationella säkerhetsmyndigheten (EBA).

C.14.4. Detta riskbedömningsexempel visar hur ett globalt explicit kriterium (för den tredje principen för riskacceptans i den gemensamma säkerhetsmetoden) kan härledas för nya system utan tillämpliga handlingsregler och referenssystem. Den efterföljande riskanalysen för det nya systemet baserades på Cenelec-standarderna och överensstämmer således väl med processen enligt den gemensamma säkerhetsmetoden. Riskbedömningen i exemplet uppfyller kraven enligt den gemensamma säkerhetsmetoden, men det finns varken någon hänvisning till hantering av protokoll om faror eller påvisandet till att det system som är föremål för bedömning uppfyller de identifierade säkerhetskraven.

C.14.5. Ytterligare information om dessa riskanalyser finns i följande referens: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *”Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)”*, Signal + Draht, Nr.5, 2001, 10–15.

C.15. Exempel på tillämplighetstest för kriteriet för riskacceptans för tekniska system

C.15.1. Syftet med detta tillägg är att med ett exempel på en funktion i det fordonsbaserade ETCS-delsystemet visa hur kriteriet i avsnitt 2.5.4 ska användas och hur man fastställer om kriteriet för riskacceptans för tekniska system kan tillämpas.

C.15.2. Det fordonsbaserade ETCS-delsystemet är ett tekniskt system. Följande funktion betraktas: *”Förse föraren med information som gör det möjligt för föraren att köra tåget på ett säkert sätt och framkalla en bromsansättning vid överhastighet.”*

Beskrivning av funktionen: Baserat på den markbaserade informationen (tillåten hastighet) och tågets hastighet som beräknas med det fordonsbaserade ETCS-delsystemet

(a) kör föraren tåget och säkerställer att tåghastigheten inte överskrider den tillåtna,
(b) övervakar samtidigt det fordonsbaserade ETCS-delsystemet att tåget inte överskrider den tillåtna hastighetsgränsen. Vid överhastighet slås bromsarna till automatiskt.

Både föraren och det fordonsbaserade ETCS-delsystem använder den utvärdering av tåghastigheten som beräknas av det fordonsbaserade ETCS-delsystemet.

C.15.3. Fråga: ”Gäller kriteriet för riskacceptans för tekniska system för det fordonsbaserade ETCS-delsystemets utvärdering av tåghastigheten?”

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

C.15.4. Tillämpning av flödesschemat i figur 14 och svar på de olika frågorna:

(a) Betraktad fara för det tekniska systemet:

"*Överskridande av den säkra hastigheten enligt rekommendation till ETCS*" (se UNISIG SUBSET 091).

(b) Kan faran kontrolleras med hjälp av en handlingsregel eller ett referenssystem?

NEJ. Det antas att ETCS-systemet är en ny och innovativ konstruktion. Därför finns det inga handlingsregler eller referenssystem som kan möjliggöra kontroll av faran till en godtagbar risknivå.

(c) Är det troligt att faran kan leda till en katastrofal konsekvens?

JA eftersom "*överskridande av den säkra hastigheten enligt rekommendation till ETCS*" kan leda till en tågurspårning som eventuellt kan leda till "*dödsfall och/eller flera svåra skador och/eller stora skador på miljön*".

(d) Är den katastrofala konsekvensen ett direkt resultat av felyttringen i det tekniska systemet?

JA om det saknas ytterligare säkerhetsbarriärer. Samma utvärdering av tåghastigheten, som beräknas av det fordonsbaserade ETCS-delsystemet, överförs till både föraren och det fordonsbaserade ETCS-delsystemets bromsregleringsfunktion. Om man antar att föraren kör tåget (av prestandaskäl) vid den högsta hastigheten som tillåts på spåren kommer varken föraren eller det fordonsbaserade ETCS-delsystemet att upptäcka att tåget överskrider hastigheten om tåghastigheten underskattas. Detta har en potential att leda till en tågurspårning med katastrofala konsekvenser.

(e) Slutsatser:

(1) För de kvantitativa kraven: Tillämpa en THR på $10^{-9}\ h^{-1}$ för slumpmässiga maskinvarufel hos det fordonsbaserade ETCS-delsystemet för att säkerställa att

(i) hänsyn tas vid utvärderingen av detta kvantitativa mål för redundanta system för de gemensamma komponenterna (t.ex. enskilda eller gemensamma indata till alla kanaler, gemensam strömförsörjning, komparatorer, väljare etc.),
(ii) de vilande eller latenta felupptäcktstiderna täcks,
(iii) en analys av gemensam felorsak/felyttring (CCF/CMF) utförs,
(iv) en oberoende bedömning utförs.

(2) För processkraven: Tillämpa en SIL 4-process för att hantera systematiska felyttringar/fel hos det fordonsbaserade ETCS-delsystemet. Detta kräver tillämpning av följande:

(i) En kvalitetsstyrningsprocess som överensstämmer med SIL 4.
(ii) En säkerhetsstyrningsprocess som överensstämmer med SIL 4.
(iii) Relevanta standarder, t.ex.

- standarden EN 50128 för programvaruutvecklingen,
- standarderna EN 50121-3-2, EN 50121-4, EN 50124-1, EN 50124-2, EN 50125-1 EN 50125-3, EN 5050081, EN 50155, EN 61000-6-2, etc. för maskinvaruutvecklingen.

(3) En oberoende bedömning av processerna.

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

C.16. Exempel på möjliga strukturer för protokoll om faror

C.16.1. Inledning

C.16.1.1. De minimikrav som gäller det som ska registreras i ett protokoll om faror har fastställts i avsnitt 4.1.2 i förordningen om en gemensam säkerhetsmetod. Dessa är markerade med en skuggad bakgrund i exemplen nedan på protokoll om faror.

C.16.1.2. Det kan finnas olika sätt att strukturera ett protokoll om faror, liksom övrig information som skulle kunna karakterisera farorna och de tillhörande säkerhetsåtgärderna. Exempelvis kan farorna och de tillhörande säkerhetsåtgärderna förses med ett fält per uppgift. Oberoende av vilken struktur som används är det viktigt att protokollet om faror anger tydliga kopplingar mellan farorna och de tillhörande säkerhetsåtgärderna. En möjlig lösning är att protokollet om faror innehåller minst ett fält för varje fara och för varje säkerhetsåtgärd med följande information

(a) En tydlig beskrivning inklusive referenser till dess ursprung och till den princip för riskacceptans som har valts för att kontrollera den tillhörande faran. Detta fält gör det möjligt att förstå faran och de tillhörande säkerhetsåtgärderna, och ger vidare information om i vilka säkerhetsanalyser de har identifierats.

Eftersom protokollet om faror används och förvaltas under hela systemets livscykel (dvs. under driften och underhållet av systemet), är det praktiskt med en tydlig spårbarhet, eller koppling, mellan varje fara och

(1) den tillhörande risken,
(2) orsakerna till faran då de redan har identifierats,
(3) de tillhörande säkerhetsåtgärderna liksom de antaganden som definierar gränserna för det system som är föremål för bedömning,
(4) de tillhörande säkerhetsanalyserna i vilka faran är identifierad.

Vidare måste formuleringen av säkerhetsåtgärderna (särskilt de som ska överföras till andra aktörer, såsom förslagsställaren) och formuleringen av de tillhörande farorna och riskerna vara tydliga och tillräckliga. Med ”tydlig och tillräcklig” menas att det ska gå att förstå vilka risker som säkerhetsåtgärderna och de tillhörande farorna förväntas kontrollera utan att man behöver gå tillbaka till de därtill hörande säkerhetsanalyserna.

(b) Den princip för riskacceptans som har använts för att kontrollera faran för att stödja ett ömsesidigt erkännande och underlätta för bedömningsorganet att bedöma att den gemensamma säkerhetsmetoden har tillämpats korrekt.

(c) Klar information om dess status. Detta fält anger om den därtill hörande faran/säkerhetsåtgärden fortfarande är öppen eller kontrollerad/validerad.

(1) En öppen fara/säkerhetsåtgärd följs upp tills den är kontrollerad/validerad.
(2) Omvänt följs inte kontrollerade/validerade faror/säkerhetsåtgärder upp längre såvida inte betydande ändringar av driften eller underhållet av systemet görs: se punkt [G 6](b) i avsnitt 2.1.1. Om detta inträffar

(i) ska den gemensamma säkerhetsmetoden tillämpas igen på de ändringar som krävs i enlighet med artikel 2, se även punkt [G 6](b)(1) i avsnitt 2.1.1,
(ii) ska alla kontrollerade faror och säkerhetsåtgärder betraktas på nytt för att kontrollera att de inte påverkas av ändringarna. Om de påverkas öppnas de därtill hörande farorna och tillhörande säkerhetsåtgärderna igen och behandlas på nytt i protokollet om faror.

Det kan hända att andra säkerhetsåtgärder har genomförts än dem som är registrerade i protokollet om faror (t.ex. av kostnadsskäl). De genomförda

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

säkerhetsåtgärderna registreras då i protokollet om faror med bevisning/motivering om varför de är lämpliga och påvisande om att systemet med dessa åtgärder uppfyller säkerhetskraven.

(d) Hänvisning till den tillhörande bevisningen som kontrollerar en fara eller validerar en säkerhetsåtgärd. Detta fält gör det möjligt att senare hitta den bevisning som har tillåtit att faran kontrolleras och att de tillhörande säkerhetsåtgärderna valideras.

En fara kan endast kontrolleras i protokollet om faror då alla tillhörande säkerhetsåtgärder som hör samman med faran har validerats i förväg.

(e) Den organisation eller enhet som ansvarar för att förvalta protokollet.

C.16.1.3. Ett annat exempel på vad som kan ingå i ett protokoll om faror finns i tillägg A.3 i vägledningen EN 50126-2 {ref. 9}.

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

C.16.2. Exempel på protokollet om faror för den organisatoriska ändringen i avsnitt C.5. i tillägg C

Tabell 6: Exempel på protokoll om faror för den organisatoriska ändringen i avsnitt C.5. i tillägg C.

Beskrivning av fara	**Säkerhetsåtgärder**	**Prioritet/säkerhet Punktlighet**	**Genomförande ([16])**	**Anmärkningar**	**Ansvarig ([16])**	**Källa**	**Använd princip för riskacceptans**	**Ansvarig för verifiering**	**Verifierings-sätt**	**Status xx.xx.xx**
Minskad motivation bland de anställda att stanna kvar i företaget. Personalen lämnar därför företaget kontinuerligt. Omotiverade/utbrända chefer	Ny omgång av motiverande arbete för personalen, som ska utföras i små grupper. Omfördelning av medel så att företaget får meningsfulla uppgifter att utföra. Fler inspektioner av den spåransvarige. Tilldelning av medel för att säkerställa att nyckelpersonal stannar kvar under hela processen. Särskilt se till att information och kunskap överförs från anställda som slutar till dem som tar över uppgifterna. Etc.	Hög/hög	Samordnas av XYZ. Regionerna måste titta på åtgärder för att öka kontrollen av spåren, anställda som överlappar varandra och uppföljning av linjeansvarig.	Större antal inspektioner måste ingå i avtalen. Etc.	Företagets chef	Brainstorming HAZID-rapport R_X	Inte tillämpbar			Ändring av villkor eller förhållanden har minskat denna risk betydligt. Analys av arbetsmiljön och viss utbildning av personalen.
Entreprenörernas underleverantör saknar kunskap, kompetens och kvalitetskontroll.	Ökad efterfrågan på dokumenterad kompetens. Systematisk kontroll av utförda uppgifter.	Hög/ medelhög	Infrastrukturförvaltaren måste samordna. Regionerna måste vidta åtgärder för att kräva kompetens och kontrollera arbetet.	Genomförd vid uppföljning av avtal. Indata till revisionsplanering.	Infrastrukturförvaltaren	Brainstorming HAZID-rapport R_X	Inte tillämpbar	Säkerhetschefen		Ökat fokus på rutiner för kontroll (2 operativa kontroller per månad och driftområde).
Osäkerhet om roller och ansvar vid kontaktpunkten	Definiera roller och ansvarsområden. Kartlägga alla kontaktpunkter och definiera vem som ansvarar för kontaktpunkten.	Medelhög/medelhög	Separat i varje region.	Genomförd via underhållsavtal och strategi-	Regionchefer	Brainstorming	Inte tillämpbar	Säkerhetschefen		Regionerna har presenterat

([16]) *Dessa två kolumner hänför sig till information/fält om de aktörer som har ansvaret för att kontrollera de identifierade farorna.*

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

Tabell 6: Exempel på protokoll om faror för den organisatoriska ändringen i avsnitt C.5. i tillägg C.

Beskrivning av fara	Säkerhetsåtgärder	Prioritet/säkerhet Punktlighet	Genomförande ([16])	Anmärkningar	Ansvarig ([16])	Källa	Använd princip för riskacceptans	Ansvarig för verifiering	Verifierings-sätt	Status xx.xx.xx
mellan företaget och infrastruktur-förvaltaren (den spåransvarige).				planen för omorganisationen.		HAZID-rapport R_X				sina strategier.

C.16.3. Exempel på ett komplett protokoll om faror för ett fordonsbaserat trafikstyrningsdelsystem

C.16.3.1. I detta avsnitt finns ett exempel på ett enskilt protokoll om faror (se punkt [G 3] i avsnitt 4.1.1) för hanteringen av både

(a) alla interna säkerhetskrav som kan tillämpas på det delsystem som aktören ansvarar för och
(b) alla identifierade faror och tillhörande säkerhetsåtgärder som aktörerna inte kan genomföra och som måste överföras till andra aktörer.

Tabell 7: Exempel på en tillverkares protokoll om faror för ett fordonsbaserat trafikstyrningsdelsystem.

Fara nr	Källa	Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Använd princip för riskacceptans	Exporterad	Status
1	HAZOP-rapport R_X	Tågsättets högsta hastighet (Vmax) är för hög	Felaktig specifik konfigurering av det fordonsbaserade delsystemet (underhållspersonal). Felaktig datainmatning ombord (föraren).	Järnvägsföretaget	• Definiera en rutin för att godkänna konfigureringsdata för det fordonsbaserade delsystemet. • Definiera en driftrutin för hur data ska matas in av föraren.	Uttrycklig riskuppskattning	Ja	Kontrollerad (exporterad till järnvägsföretaget). Se även avsnitt C.16.4.2. i tillägg C.
2	HAZOP-rapport R_X	Bromskurvor (dvs. körbesked) i det fordonsbaserade delsystemets konfigureringsdata är alltför tillåtande.	Förfarandet för den specifika konfigureringen av det fordonsbaserade delsystemet beror på • de säkerhetsmarginaler som används för tågets bromssystem, • reaktionsfördröjningen för tågets bromssystem (denna är direkt beroende av tågets längd, särskilt för godståg).	Järnvägsföretaget	• Göra en korrekt specificering av systemkraven i systemdefinitionen. • Ange tillräckliga säkerhetsmarginaler för bromssystemet för det specifika tåget.	Uttrycklig riskuppskattning	Ja	Kontrollerad (exporterad till järnvägsföretaget). Se även avsnitt C.16.4.2. i tillägg C.

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

Tabell 7: Exempel på en tillverkares protokoll om faror för ett fordonsbaserat trafikstyrningsdelsystem.

Fara nr	Källa	Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Använd princip för riskacceptans	Export-erad	Status
3	HAZOP-rapport R_X	• Tågsättets högsta hastighet (Vmax) är för hög • Bromskurvor (dvs. körbesked) i det fordonsbaserade delsystemets konfigureringsdata är alltför tillåtande.	Tågets hjuldiameter i den specifika konfigureringen för det fordonsbaserade delsystemet har inte uppdaterats (underhållspersonal).	Järnvägs-företaget	• Definiera en rutin för underhållspersonalen för att mäta tågets hjuldiameter. • Definiera en rutin för att regelbundet uppdatera tågets hjuldiameter i det fordons-baserade delsystemet.	Uttrycklig risk-uppskattning	Ja	Kontrollerad (exporterad till järnvägsföretaget). Se även avsnitt C.16.4.2. i tillägg C.
			Fel i tillverkarens rutin för att ta fram och ladda upp konfigureringsdata i det fordonsbaserade delsystemet	Tillverkaren	Definiera en rutin för att uppdatera tågets hjuldiameter i de fordons-baserade konfigureringsdata.	Uttrycklig risk-uppskattning	Ja	Kontrollerad av rutin P_X
4	HAZOP-rapport R_X	Ett tåg kommer in på ett spår med hög hastighet (160 km/h om signalen längs spåret visar fritt) utan att det fordons-baserade delsystemet är aktivt och utan signalering längs spåret.	Kan endast kontrolleras genom förarens vaksamhet. Inkörsel i ett område som är utrustat med mark-baserad ATP är beroende av en bekräftelserutin som föraren genomför före övergångsplatsen. Om bekräftelse saknas sker en automatisk ansättning av tågets bromsar med hjälp av det fordonsbaserade trafikstyrningsdelsystemet.	Infrastruktur-förvaltaren	Infrastrukturförvaltaren ska se till att tåg som inte är utrustade med ett aktivt fordonsbaserat trafikstyrnings-delsystem inte kan köra in på det relevanta spåret. Definiera en rutin för trafikledningen.	Uttrycklig risk-uppskattning	Ja	Kontrollerad (exporterad till infrastruktur-förvaltaren). Se även avsnitt C.16.4.2. i tillägg C.
				Järnvägs-företaget	Se till att föraren utbildas i hur man kör in ett område med markbaserad ATP.	Uttrycklig risk-uppskattning	Ja	Kontrollerad (exporterad till järnvägsföretaget). Se även avsnitt C.16.4.2. i tillägg C.
5	HAZOP-rapport R_X	Tågsättets högsta hastighet (Vmax) som visas för föraren är för hög	Den information som visas vid kontaktpunkten med föraren övervakas av det fordonsbaserade trafikstyrningsdelsystemet med SIL 4 som slår till nödbromsarna om det finns en brist på överensstämmelse mellan det visade och det förväntade värdet. Vid bristande överensstämmelse med körbeskedet slår det fordonsbaserade trafikstyrningsdelsystemet till nödbromsarna.	Tillverkaren	Utveckla ett fordonsbaserat trafikstyrningsdelsystem med SIL 4.	Uttrycklig risk-uppskattning	Ja	Säkerhetsbevisning som påvisar att ett SIL 4-delsystem har bedömts av en oberoende säkerhetsbedömare.
6	HAZOP-rapport	Tåget avgår utan operatörssystem.	Förlust av redundant arkitektur för fordonsbaserat delsystem.	Tillverkaren	Utveckla ett fordonsbaserat trafikstyrningsdelsystem med SIL 4.	Uttrycklig risk-	Ja	Säkerhetsbevisning som påvisar att ett

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

Tabell 7: Exempel på en tillverkares protokoll om faror för ett fordonsbaserat trafikstyrningsdelsystem.

Fara nr	Källa	Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Använd princip för riskaccepta ns	Export-erad	Status
	R_X					uppskattning		SIL 4-delsystem har bedömts av en oberoende säkerhetsbedömare.
Etc.								

C.16.4. Exempel på protokoll om faror för överföring av information till andra aktörer

C.16.4.1 I detta avsnitt finns ett exempel på ett protokoll om faror för att överföra de identifierade farorna och tillhörande säkerhetsåtgärder, som en berörd aktör inte kan genomföra, till andra aktörer: se punkt [G 1] i avsnitt 4.1.1.
Detta är samma exempel som exemplet i avsnitt C.16.3. i tillägg C. Enda skillnaden är att alla de interna farorna och säkerhetsåtgärderna som skulle kunna kontrolleras av den berörda aktören har tagits bort.

C.16.4.2. Den sista kolumnen i tabell 8 används för att uppfylla kravet enligt avsnitt 4.2 i förordningen om en gemensam säkerhetsmetod. Det finns olika lösningar för att uppnå detta. Ett sätt kan vara att hänvisa till den bevisning som används av en aktör som tar emot den exporterade säkerhetsinformationen. Ett annat sätt kan vara att de två aktörerna har ett möte där de tillsammans försöker hitta en lämplig lösning för att kontrollera de tillhörande riskerna. Resultatet av ett sådant möte kan rapporteras i ett överenskommet dokument (t.ex. ett mötesprotokoll) till vilket den aktör som exporterar den säkerhetsrelaterade informationen kan hänvisa för att stänga de tillhörande farorna i sitt protokoll om faror.

Tabell 8: Exempel på ett protokoll om faror för att överföra säkerhetsrelaterad information till andra aktörer.

Fara nr	Källa för faran		Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Kommentar från mottagaren
	Nr i tabell 7	Övriga					
1	Nr 1	HAZOP-rapport R_X	Tågsättets högsta hastighet (Vmax) är för hög	Felaktig specifik konfigurering av det fordonsbaserade delsystemet (underhållspersonal). Felaktig datainmatning ombord (föraren).	Järnvägs-företaget	• Definiera en rutin för att godkänna konfigurerings-data för det fordons-baserade delsystemet. • Definiera en driftrutin för	• Det fordonsbaserade trafikstyrningsdelsystemets konfigureringsdata beror på den rullande materielens fysiska egenskaper. • Säkerhetsmarginaler tillämpas därefter på dessa data i ett samarbete mellan infrastrukturförvaltaren och järnvägsföretaget. • Dessa data laddas därefter upp i det fordonsbaserade delsystemet i

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

Tabell 8: Exempel på ett protokoll om faror för att överföra säkerhetsrelaterad information till andra aktörer.

Fara nr	Källa för faran		Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Kommentar från mottagaren
	Nr i tabell 7	Övriga					
						hur data ska matas in av föraren.	överensstämmelse med lämplig tillverkares rutiner under installationen, integreringen i den rullande materielen och godkännandet av trafikstyrningsdelsystemet. • Förarna utbildas och testas mot rutin D_P. • Förarna testas också av infrastrukturförvaltare enligt de regler som är tillämpliga för infrastrukturförvaltarens infrastruktur.
2	Nr 2	HAZOP-rapport R_X	Bromskurvor (dvs. körbesked) i det fordonsbaserade delsystemets konfigureringsdata är alltför tillåtande.	Förfarandet för den specifika konfigureringen av det fordonsbaserade delsystemet beror på • de säkerhetsmarginaler som används för tågets broms-system, • reaktionsfördröjningen för tågets bromssystem (denna är direkt beroende av tågets längd, särskilt för godståg).	Järnvägs-företaget	• Göra en korrekt specificering av systemkraven i systemdefinitionen. • Ange tillräckliga säkerhetsmarginaler för bromssystemet för det specifika tåget.	Hänvisning till kommentar för rad 1 här ovan.
3	Nr 3	HAZOP-rapport R_X	• Tågsättets högsta hastighet (Vmax) är för hög • Bromskurvor (dvs. körbesked) i det fordonsbaserade delsystemets konfigureringsdata är alltför tillåtande.	Tågets hjuldiameter i den specifika konfigureringen för det fordonsbaserade delsystemet har inte uppdaterats (underhållspersonal).	Järnvägs-företaget	• Definiera en rutin för underhållspersonalen för att mäta tågets hjuldiameter. • Definiera en rutin för att regelbundet uppdatera tågets hjuldiameter i det fordonsbaserade delsystemet.	• Underhållet av det fordonsbaserade trafikstyrningsdelsystemet har utförts i enlighet med ”Underhållsrutin MP_Z”. • Tågets hjuldiameter uppdateras med fastställda intervall i enlighet med rutin P_W. • Tågförarna får utbildning i hur man matar in data och testas utifrån ”Rutin P_{DE}”.
4	Nr 4	HAZOP-rapport R_X	Ett tåg kommer in på ett spår med hög hastighet (160 km/h om signalen längs spåret visar fritt) utan att det fordonsbaserade delsystemet är aktivt och utan signalering längs spåret.	Kan endast kontrolleras genom förarens vaksamhet. Inkörsel i ett område som är utrustat med markbaserad ATP är beroende av en bekräftelserutin som föraren genomför före övergångsplatsen. Om bekräftelse saknas sker en automatisk ansättning av tågets bromsar med hjälp av det fordonsbaserade trafikstyrnings-	Infrastruktur-förvaltaren	Infrastrukturförvaltaren ska se till att tåg som inte är utrustade med ett aktivt fordonsbaserat trafikstyrningsdelsystem inte kan köra in på det relevanta spåret. Definiera en rutin för trafikledningen.	Trafikledningen i infrastrukturförvaltarens infrastrukturer styrs av en uppsättning regler R_{TM}.

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

Tabell 8: Exempel på ett protokoll om faror för att överföra säkerhetsrelaterad information till andra aktörer.

Fara nr	Källa för faran		Beskrivning av fara	Ytterligare upplysningar	Ansvarig aktör	Säkerhetsåtgärd	Kommentar från mottagaren
	Nr i tabell 7	Övriga					
				delsystemet.			
					Järnvägs-företaget	Se till att föraren utbildas i hur man kör in ett område med markbaserad ATP.	• Förarna utbildas med regelbundna intervall i enlighet infrastrukturförvaltarens rutin P_{IM_DP}. • Förarna testas också av infrastrukturförvaltare enligt de regler (S_R) som är tillämpliga för infrastrukturförvaltarens infrastruktur.
Etc.							

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

C.17. Exempel på en generisk förteckning över faror för järnvägsdrift

C.17.1. I ROSA (Rail Optimisation Safety Analysis), ett projekt inom ramen för DEUFRAKO (ett samarbete mellan Frankrike och Tyskland), gjordes ett försök att upprätta en generisk och uttömmande förteckning över faror som omfattande standardmässig järnvägsdrift. Målet och utmaningen var att definiera dessa faror med så hög detaljnivå som möjligt, utan att återspegla särdragen hos järnvägarna i Frankrike och Tyskland. Förteckningen upprättades med hjälp av aktuella befintliga förteckningar över faror från båda länderna (SNCF och DB) och dubbelkontrollerades också mot förteckningar över faror från andra länder. Trots det uttalade målet om att vara uttömmande och generisk ingår förteckningen här endast som ett vägledande exempel som kan vara till hjälp för aktörerna när de ska identifiera faror för ett särskilt projekt. Det förväntas att farorna som anges i förteckningen förmodligen behöver förfinas eller kompletteras för att återspegla eventuella särdrag för ett projekt.

C.17.2. Farorna som anges i förslaget till förteckning nedan kallas *startpunktsfaror* (SPH – starting point hazards). Med detta menas faror som kan användas som utgångspunkt för både en konsekvensanalys och en orsaksanalys för att fastställa säkerhetsåtgärder/barriärer och säkerhetskrav för att kontrollera farorna.

C.17.3. ROSA-projektets förteckning över faror:

SPH 01	Initialt felaktig bestämning av hastighetsgränsen (i förhållande till infrastrukturen)
SPH 02	Felaktig bestämning av hastighetsgränsen (tågrelaterad)
SPH 03	Felaktigt fastställt bromsavstånd/felaktig hastighetsprofil/felaktiga bromskurvor
SPH 04	Otillräcklig hastighetsminskning (fysiska orsaker)
SPH 05	Felaktigt/olämpligt hastighets-/bromskommando
SPH 06	Felaktig hastighet registrerad (felaktig tåghastighet)
SPH 07	Fel vid kommunikation av hastighetsgräns
SPH 08	Tåget rullar iväg
SPH 09	Felaktig färdriktning/avsiktlig rörelse bakåt – (kombination av SPH 08 och SPH 14)
SPH 10	Felaktig absolut/relativ position registrerad
SPH 11	Tågdetektionsfel
SPH 12	Förlust av tågintegritet (att tågsättet är komplett)
SPH 13	Eventuellt felaktig rutt för tåget
SPH 14	Fel vid överföring/kommunikation av tidtabell/körbesked
SPH 15	Strukturellt fel på spåret
SPH 16	Defekt växelkomponent
SPH 17	Felaktigt växelkommando
SPH 18	Felaktig växelstatus
SPH 19	Systemföremål på spåret/inom fria rummet (exkl. ballast)
SPH 20	Främmande föremål på spåret/inom fria rummet
SPH 21	Vägtrafikanvändare i järnvägskorsning
SPH 22	Luftströmseffekter på ballasten
SPH 23	Påverkan av aerodynamiska krafter på tåget
SPH 24	Tågets utrustning/komponenter/last inkräktar på det fria rummet för tåget
SPH 25	Felaktigt fritt rum för tåget (längs vägen)
SPH 26	Felaktig fördelning av lasten
SPH 27	Defekt hjul, defekt axel
SPH 28	Varm axel/varmt hjul/varmt lager
SPH 29	Fel på boggi/upphängning, dämpning
SPH 30	Fel på fordonsramen/karossen
SPH 31	Intrång (säkerhetsaspekt)

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

SPH 32	Behörig person korsar spåret
SPH 33	Personal arbetar på spåret
SPH 34	Obehörig person gör intrång på spåret (oaktsamhet)
SPH 35	Person faller från perrongkanten ned på spåret
SPH 36	Luftström/person för nära perrongkanten.
SPH 37	Personal arbetar nära spåret, t.ex. på ett angränsande spår
SPH 38	Person lämnar avsiktligt tåget (exkl. passagerarbyte)
SPH 39	Person faller ut genom (sido-)dörr
SPH 40	Person faller ut genom gaveldörr
SPH 41	Tåget avgår/rullar med öppna dörrar (inkräktar inte på fria rummet)
SPH 42	Person faller i gången mellan två vagnar
SPH 43	Passagerare lutar sig ut genom dörr
SPH 44	Passagerare lutar sig ut genom fönster
SPH 45	Personal/tågvärd lutar sig ut genom dörr
SPH 46	Personal/tågvärd lutar sig ut genom fönster
SPH 47	Växlingspersonal på fordonet lutar sig ut från trappsteg
SPH 48	Person faller ned från/klättrar upp på perrong i utrymmet mellan fordonet och perrongen
SPH 49	Person faller ut från/lämnar tåget utan att det finns någon perrong
SPH 50	Person faller i dörrområdet vid passagerarbyte
SPH 51	Tågets dörrar stängs med person i dörrområdet
SPH 52	Tåget rör sig under passagerarbyte
SPH 53	Risk för skadad person i tåget
SPH 54	Brand-/explosionsfara (i/vid tåget) – olyckskategori, konsekvens av SPH 55, SPH 56)
SPH 55	Felaktig temperatur (i tåget)
SPH 56	Förgiftning/kvävning (i/vid tåget)
SPH 57	Dödsfall på grund av elektrisk ström (i/vid tåget)
SPH 58	Person faller på perrongen (förutom vid passagerarbyte)
SPH 59	Felaktig temperatur (på perrongen)
SPH 60	Förgiftning/kvävning (på perrongen)
SPH 61	Dödsfall på grund av elektrisk ström (på perrongen)

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