

Det Europæiske Jernbaneagentur

Samling af eksempler på risikovurderinger og nogle mulige værktøjer, der støtter CSM-forordningen

Reference i ERA:	ERA/GUI/02-2008/SAF
Version i ERA:	1.1
Dato:	06/01/2009

Dokument udarbejdet af	Det Europæiske Jernbaneagentur 160 Boulevard Harpignies BP 20392 F-59307 Valenciennes Cedex Frankrig
Type dokument:	Vejledning
Dokumentets status:	Offentlig

	Navn	Stilling
Udgivet af	Marcel VERSLYPE	Administrerende direktør
Revideret af	Anders LUNDSTRÖM Thierry BREYNE	Kontorchef, sikkerhedsafdelingen Sektorchef, sikkerhedsvurdering
Skrevet af (Forfatter)	Dragan JOVICIC	Sikkerhedsafdelingen - projektleder

DOKUMENTINFORMATION

Ændringsjournal

Tabel 1: Dokumentets status

Version Dato	Forfatter(e)	Afsnit nr.	Beskrivelse af ændringen
Gammel dokumenttitel og -struktur: "Vejledning i anvendelse af anbefalingen vedrørende den første fælles sikkerhedsmetode"			
"vejledning" version 0.1 15/02/2007	Dragan JOVICIC	Alle	Første version af "Vejledning i anvendelse", som hører sammen med version 1.0 af anbefalingen vedrørende den fælles sikkerhedsmetode. Dette er også første version af det dokument, der blev sendt til arbejdsgruppen om den fælles sikkerhedsmetode til formel revision.
"Vejledning" version 0.2 07/06/2007	Dragan JOVICIC	Alle	Omstrukturering af dokumentet for at tilpasse det til strukturen i version 4.0 af anbefalingen vedrørende den fælles sikkerhedsmetode. Ajourføring i forhold til <u>formel revisionsproces</u> ved arbejdsgruppen om den fælles sikkerhedsmetode af version 1.0 af anbefalingen.
		Alle	Ajourføring af dokumentet med yderligere oplysninger indsamlet under interne møder i ERA såvel som med anmodningerne fra taskforcen og arbejdsgruppen om den fælles sikkerhedsmetode om at udforme nye punkter.
		Figur 1	Ændring af figuren "risikostyringsrammer for den første serie af fælles sikkerhedsmetoder" i overensstemmelse med både revisionsbemærkningerne og ISO-terminologien.
"Vejledning" version 0.3 20/07/2007	Dragan JOVICIC	Bilag	Omorganisering af bilagene og udfærdigelse af nye bilag. Nyt bilag til samling af alle diagrammer, som illustrerer og letter læsningen og forståelsen af vejledningen.
		Alle afsnit	Dokument ajourført for: <ul style="list-style-type: none"> at udvikle bestående x-afsnit så meget som muligt at uddybe, hvad der henvises til med "påvisning af, at systemet opfylder sikkerhedskravene" at knytte en forbindelse til CENELEC's V-cyklus (dvs. figur 8 og figur 10 i EN 50 126) at forklare behovet for samarbejde og samordning mellem de forskellige aktører i jernbanesektoren, hvis virksomhed kan påvirke sikkerheden i jernbanesystemet at gøre nærmere rede for de beviser (f.eks. fareredegørelse og sikkerhedscases, som forventes at efterviser over for vurderingsorganerne, at risikovurderingsproceduren vedrørende den fælles sikkerhedsmetode anvendes korrekt. Dokument også ajourført i henhold til agenturets første interne revision.
"Vejledning" version 0.4 16/11/2007	Dragan JOVICIC	Alle afsnit	Dokument ajourført efter <u>den formelle revisionsproces</u> i henhold til de bemærkninger, der var indkommet til version 0.3 fra nedenstående medlemmer af arbejdsgruppen om den fælles sikkerhedsmetode eller diverse organisationer og aftalt med dem under telefonsamtaler: <ul style="list-style-type: none"> den belgiske, spanske, finske, norske, franske og danske nationale sikkerhedsmyndighed (NSA) SIEMENS (medlem af UNIFE) den norske infrastrukturforvalter (Jernbaneverket – EIM-medlem).
"Vejledning" version 0.5 27/02/2008	Dragan JOVICIC	Alle afsnit	Dokument ajourført i henhold til de bemærkninger, der var indkommet til version 0.3 fra nedenstående medlemmer af arbejdsgruppen om den fælles sikkerhedsmetode eller diverse organisationer og aftalt med dem under telefonsamtaler: <ul style="list-style-type: none"> CER den nederlandske NSA

Tabel 1: Dokumentets status

Version Dato	Forfatter(e)	Afsnit nr.	Beskrivelse af ændringen
		Alle afsnit	Dokument ajourført i overensstemmelse med den underskrevne version af anbefalingen vedrørende den fælles sikkerhedsmetode. Dokument ajourført i henhold til agenturets interne revisionsbemærkninger fra Christophe CASSIR og Marcus ANDERSSON.
		Alle afsnit Bilag	Komplet omnummerering af afsnit i dokumentet i forhold til anbefalingen. Vedlagte eksempler på anvendelsen af anbefalingen vedrørende den fælles sikkerhedsmetode.
Ny dokumenttitel og -struktur: "Samling af eksempler på risikovurderinger og nogle mulige værktøjer, der støtter CSM-forordningen"			
Vejledning version 0.1 23/05/2008	Dragan JOVICIC	Alle	Første version af dokumentet som følge af opsplitningen af "Vejledning i anvendelse" version 0.5 i to komplementære dokumenter.
Vejledning version 0.2 03/09/2008	Dragan JOVICIC	Alle	Dokument ajourført i overensstemmelse med: <ul style="list-style-type: none"> • Europa-Kommissionens forordning om den fælles sikkerhedsmetode {Ref. 3} • bemærkninger fra workshopen 1. juli 2008 med medlemmer af RISC (Railway Interoperability and Safety Committee) • bemærkningerne fra medlemmer af arbejdsgruppen om den fælles sikkerhedsmetode (den norske, finske, britiske og franske NSA, CER, EIM, Jens BRABAND (UNIFE) og Stéphane ROMEI (UNIFE).
Vejledning version 1.0 10/12/2008	Dragan JOVICIC	Alle	Dokument ajourført i overensstemmelse med Europa-Kommissionens forordning om den fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering {Ref. 3} vedtaget af RISC på plenarmødet den 25. november 2008.
Vejledning version 1.1 06/01/2009	Dragan JOVICIC	Alle	Dokument ajourført i henhold til bemærkninger om forordningen om den fælles sikkerhedsmetode fra Europa-Kommissionens juridiske og sproglige tjenestegrene.

Indholdsfortegnelse

DOKUMENTINFORMATION	2
Ændringsjournal	2
Indholdsfortegnelse	4
Figurfortegnelse.....	5
Tabelfortegnelse.....	6
0. INDLEDNING	7
0.1. Anvendelsesområde	7
0.2. Uden for anvendelsesområdet.....	7
0.3. Principper for dette dokument.....	8
0.4. Dokumentbeskrivelse	8
0.5. Referencedokumenter.....	9
0.6. Standarddefinitioner, termer og forkortelser	10
0.7. Specifikke definitioner	10
0.8. Specifikke termer og forkortelser	10
FORKLARING AF ARTIKLERNE I CSM-FORORDNINGEN	12
Artikel 1. Formål	12
Artikel 2. Anvendelsesområde	12
Artikel 3. Definitioner	14
Artikel 4. Væsentlige ændringer	15
Artikel 4 (1)	15
Artikel 4 (2)	16
Artikel 5. Risikostyringsproces	17
Artikel 6. Uafhængig vurdering	18
Artikel 7. Sikkerhedsvurderingsrapporter	19
Artikel 8. Ledelse af risikostyring/interne og eksterne revisioner	20
Artikel 9. Tilbage melding og tekniske fremskridt	21
Artikel 10. Ikrafttræden.....	22
BILAG I - FORKLARING AF PROCESSEN I CSM-FORORDNINGEN	23
1. GENERELLE PRINCIPPER FOR RISIKOSTYRINGSPROCESSEN.....	23
1.1. Generelle principper og forpligtelser	23
1.2. Styring af grænseflader.....	30
2. BESKRIVELSE AF RISIKOVURDERINGSPROCESSEN	33
2.1. Generel beskrivelse - Forbindelsen mellem CSM-risikovurderingsprocessen og CENELEC's V-cyklus	33
2.2. Fareidentifikation	40
2.3. Anvendelse af adfærdskodekser og risikoevaluering	43
2.4. Anvendelse af referencesystem og risikoevaluering	45
2.5. EksPLICIT risikoestimering og -evaluering	46
3. PÅVISNING AF OVERENSSTEMMELSE MED SIKKERHEDSKRAV	49
4. FAREHÅNDBTERING	52
4.1. Farehåndteringsprocessen	52
4.2. Udveksling af oplysninger	53

5. DOKUMENTATION FRA ANVENDELSEN AF RISIKOSTYRINGSPROCESSEN 56

BILAG II TIL CSM-FORORDNINGEN 59

Kriterier, som vurderingsorganerne skal opfylde 59

TILLÆG A: YDERLIGERE AFKLARING 60

A.1. Indledning..... 60

A.2. Fareklassificering 60

A.3. Risikoacceptkriterier for tekniske systemer (RAC-TS) 60

A.4. Beviser fra sikkerhedsvurdering..... 70

TILLÆG B: EKSEMPLER PÅ TEKNIKKER OG VÆRKTØJER, DER STØTTER RISIKOVURDERINGSPROCESSEN 74

TILLÆG C: EKSEMPLER 75

C.1. Indledning..... 75

C.2. Eksempler på anvendelse af væsentlige ændringskriterier i Artikel 4 (2) 75

C.3. Eksempler på grænseflader mellem jernbaneaktører 76

C.4. Eksempler på metoder til bestemmelse af bredt acceptable risici 77

C.5. Risikovurderingseksempel på en væsentlig organisatorisk ændring 78

C.6. Risikovurderingseksempel på en væsentlig driftsændring – Ændring af køretider..... 80

C.7. Risikovurderingseksempel på en væsentlig teknisk ændring (CCS)..... 82

C.8. Eksempel på svensk BVH 585.30 vejledning i risikovurdering af jernbanetunneler 85

C.9. Eksempel på risikovurdering på systemniveau for Københavns Metro 88

C.10. Eksempel på OTIF-vejledning i beregning af risiko som følge af jernbanetransport af
farligt gods..... 90

C.11. Risikovurderingseksempel på en ansøgning om godkendelse af nyt rullende materiel 92

C.12. Risikovurderingseksempel på en væsentlig driftsændring – ren lokoførerdrift 95

C.13. Eksempel på brug af et referencesystem til udledning af sikkerhedskrav til nye
elektroniske sammenkoblingssystemer i Tyskland..... 97

C.14. Eksempel på et eksplicit risikoacceptkriterium for radiobaseret togdrift med FFB
(FunkFahrBetrieb) i Tyskland..... 99

C.15. Eksempel på anvendelighedstest af RAC-TS..... 99

C.16. Eksempler på mulige strukturer for fareredegørelsen 101

C.17. Eksempel på en generisk fareliste for jernbanedrift 108

Figurfortegnelse

Figur 1: Risikostyringsrammerne i CSM-forordningen {Ref. 3}25

Figur 2: Harmoniseret SMS og CSM.....26

Figur 3: Eksempler på afhængighed mellem sikkerhedscases (uddraget af figur 9 i EN 50129 standarden).28

Figur 4: Forenklet V-cyklus i figur 10 i EN 50126-standardens.....33

Figur 5: Figur 10 i EN 50126 V-cyklus (CENELEC's systemlivscyklus).....34

Figur 6: Udvælgelse af tilstrækkelige sikkerhedsforanstaltninger til kontrol med risici39

Figur 7: Bredt acceptable risici42

Figur 8: Udfiltrering af farer, der er forbundet med en bredt acceptabel risiko42

Figur 9: Pyramide over risikoacceptkriterier (RAC).....47

Figur 10: Figur A.4 i EN 50129: Definition af farer med hensyn til systemets grænser49

Figur 11: Udledning af sikkerhedskrav for faser på lavere niveau50

Figur 12: Struktureret dokumentationshierarki56

Figur 13: Redundant arkitektur i et teknisk system63

Figur 14: Flowskema for anvendelighedstesten af RAC-TS	65
Figur 15: Eksempel på en ubetydelig ændring Telefonbesked til kontrol ved jernbaneoverskæring.....	75
Figur 16: Ændring af jordbaseret loop til et delsystem med radio infill	83

Tabelfortegnelse

Tabel 1: Dokumentets status.....	2
Tabel 2: Fortegnelse over referencedokumenter	9
Tabel 3: Termfortegnelse	10
Tabel 4: Fortegnelse over forkortelser	10
Tabel 5: Typisk eksempel på en kalibreret risikomatrix	69
Tabel 6: Eksempel på fareredegørelsen for den organisatoriske ændring i afsnit C.5. i tillæg C.....	103
Tabel 7: Eksempel på en fabrikants fareredegørelse for delsystemet mobil styringskontrol.....	104
Tabel 8: Eksempel på en fareredegørelse for overførsel af sikkerhedsrelateret information til andre aktører.....	106

0. INDLEDNING

0.1. Anvendelsesområde

- 0.1.1. Formålet med dette dokument er en yderligere præcisering af "Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i Europa-Parlamentets og Rådets direktiv 2004/49/EF" {Ref. 3}. Forordningen vil i nærværende dokument blive benævnt "CSM-forordningen" (Common Safety Method - den fælles sikkerhedsmetode).
- 0.1.2. Dette dokument er ikke retligt bindende, og indholdet af det må ikke fortolkes som den eneste måde at opfylde CSM-kravene på. Dokumentet har til formål at supplere vejledningen i anvendelse af forordningen om en fælles sikkerhedsmetode {Ref. 4} med hensyn til, hvordan processen i CSM-forordningen kan bruges og finde anvendelse. Den giver supplerende praktisk information uden på nogen måde at diktere obligatoriske procedurer, der skal følges, og uden at etablere juridisk bindende praksis. Denne information kan være nyttig for alle aktører⁽¹⁾, hvis virksomhed kan få indvirkning på sikkerheden i jernbanesystemerne, og som direkte eller indirekte skal anvende den fælles sikkerhedsmetode (CSM). Dokumentet giver eksempler på risikovurderinger og nogle mulige værktøjer, der støtter anvendelsen af CSM. Disse eksempler tjener kun som råd og vejledning. Aktørerne kan fortsat anvende deres egne eksisterende metoder til sikring af overensstemmelse med CSM, hvis de finder dem bedre egnede. Desuden er eksemplerne og den supplerende information i dette dokument ikke udtømmende og dækker ikke enhver mulig situation, hvor der foreslås væsentlige ændringer, og derfor er dokumentet udelukkende at betragte som informativt.
- 0.1.3. Dette informative dokument skal kun læses som en supplerende hjælp til anvendelsen af CSM-forordningen. Dokumentet bør anvendes sammen med CSM-forordningen {Ref. 3} og den tilhørende vejledning {Ref. 4} for at lette anvendelsen af CSM yderligere, men den erstatter ikke CSM-forordningen.
- 0.1.4. Dokumentet er udarbejdet af Det Europæiske Jernbaneagentur (ERA, European Railway Agency) med støtte fra eksperter fra jernbanesammenslutninger og nationale sikkerhedsmyndigheder, som sidder i arbejdsgruppen om den fælles sikkerhedsmetode (CSM-arbejdsgruppen). Det rummer en omfattende samling af tanker og oplysninger, som agenturet har opbygget under interne møder og møder med CSM-arbejdsgruppen og CSM-taskforce'erne. Når det er nødvendigt, vil ERA gennemgå og ajourføre dokumentet for at afspejle fremskridtene med de europæiske standarder, ændringerne i CSM-forordningen med hensyn til risikovurdering og eventuelle erfaringer med anvendelsen af CSM-forordningen. Da det i skrivende stund ikke er muligt at angive en tidsplan for denne revisionsproces, henvises læseren til Det Europæiske Jernbaneagentur, som oplyser om den senest tilgængelige version af dette dokument.

0.2. Uden for anvendelsesområdet

- 0.2.1. Dette dokument giver ikke vejledning i, hvordan man tilrettelægger, driver eller udformer (og anlægger) et jernbanesystem eller dele heraf. Det indeholder heller ikke en definition af de kontraktlige aftaler og ordninger, der måtte findes mellem visse aktører vedrørende

(1) De berørte aktører er ordregiverne som defineret i artikel 2, litra r), i direktiv 2008/57/EF om interoperabilitet i jernbanesystemet i Fællesskabet eller fabrikanterne, som alle er omtalt i forordningen som "initiativtagere", eller disses leverandører og tjenesteydere.

anvendelsen af risikostyringsprocessen. De projektspecifikke kontraktlige ordninger ligger uden for CSM-forordningen og den tilhørende vejledning om dette dokument.

0.2.2. Selv om aftaler, der er indgået mellem de relevante aktører, falder uden for dette dokumentets anvendelsesområde, kan de nedfældes i de relevante kontrakter ved projektstart, dog med forbehold af bestemmelserne i CSM. De kan f.eks. omfatte:

- (a) iboende omkostninger ved styring af sikkerhedsrelaterede risici ved grænsefladerne mellem aktørerne
- (b) iboende omkostninger ved overførsler af farer og tilknyttede sikkerhedsforanstaltninger mellem aktørerne, som endnu ikke kendes ved projektstart
- (c) løsning af konflikter, der opstår i løbet af projektet
- (d) osv.

Hvis der opstår uoverensstemmelser eller en konflikt mellem initiativtageren og dennes underleverandører i løbet af projekteringen, kan der henvises til de relevante kontrakter med hensyn til løsning af en konflikt.

0.3. Principper for dette dokument

0.3.1. Selv om dette dokument kan virke som et dokument, der kan læses fritstående, erstatter det ikke CSM-forordningen {Ref. 3}. For at gøre læsningen lettere er hver artikel i CSM-forordningen gentaget i dette dokument. Hvor det er nødvendigt, er den relevante artikel forklaret allerede i vejledningen til anvendelse af CSM-forordningen {Ref. 4}. Så gives der yderligere oplysninger i de følgende afsnit, hvis det anses for nødvendigt af hensyn til den videre forståelse af CSM-forordningens ordlyd.

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

0.3.3. Nærværende dokument har samme struktur som CSM-forordningen og den tilhørende vejledning for at hjælpe læseren.

0.4. Dokumentbeskrivelse

0.4.1. Dokumentet er opdelt i følgende dele:

- (a) kapitel 0., hvor dokumentets anvendelsesområde defineres, og der findes en liste over referencedokumenter
- (b) Bilag I og bilag II giver yderligere oplysninger for de tilsvarende afsnit af CSM-forordningen {Ref. 3} og den tilhørende vejledning {Ref. 4}
- (c) nye bilag giver yderligere oplysninger om specifikke aspekter og en række eksempler.

0.5. Referencedokumenter

Tabel 2: Fortegnelse over referencedokumenter

{Ref.nr.}	Titel	Reference	Version
{Ref. 1}	Europa-Parlamentets og Rådets direktiv 2004/49/EF af 29. april 2004 om jernbanesikkerhed i EU og om ændring af Rådets direktiv 95/18/EF om udstedelse af licenser til jernbanevirksomheder og direktiv 2001/14/EF om tildeling af jernbaneinfrastrukturkapacitet og opkrævning af afgifter for brug af jernbaneinfrastruktur samt sikkerhedscertificering ("jernbanesikkerhedsdirektivet")	2004/49/EF EUT L 164 af 30.4.2004, s. 44, berigtiget i EUT L 220 af 21.6.2004, s. 16	-
{Ref. 2}	Europa-Parlamentets og Rådets direktiv 2008/57/EF af 17. juni 2008 om interoperabilitet i jernbanesystemet i Fællesskabet	2008/57/EF EFT L 191 af 18.7.2008, s. 1	-
{Ref. 3}	Kommissionens forordning (EF) nr. .../... af [...] om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i Europa-Parlamentets og Rådets direktiv 2004/49/EF	xxxx/yy/EF	Vedtaget af RISC 25.11.2008
{Ref. 4}	Vejledning i anvendelse af Kommissionens forordning om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i jernbanesikkerhedsdirektivet	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Europa-Parlamentets og Rådets direktiv 2008/57/EF af 17. juni 2008 om interoperabilitet i jernbanesystemet i Fællesskabet	2008/57/EF EFT L 191 af 18.7.2008, s. 1	-
{Ref. 6}	Sikkerhedsledelsessystem- Vurderingskriterier for jernbanevirksomheder og infrastrukturforvaltere	Vurderingskriterier for sikkerhedsledelsessystem Del A Sikkerhedscertifikater og tilladelser	31/05/2007
{Ref. 7}	Jernbaneanvendelser – Kommunikation, signalering og databehandlingssystemer – Sikkerhedsrelaterede elektroniske systemer til signaludstyr	EN 50129	Februar 2003
{Ref. 8}	Jernbaneanvendelser- Specifikation og eftervisning af Pålidelighed, Tilgængelighed, Servicerbarhed og Sikkerhed (RAMS) – Del 1: selve standarden	EN 50126-1	September 2006
{Ref. 9}	Jernbaneanvendelser- Specifikation og eftervisning af Pålidelighed, Tilgængelighed, Servicerbarhed og Sikkerhed (RAMS) – Del 2: Vejledning i anvendelse af en EN 50126-1 i spørgsmål vedrørende sikkerhed	EN 50126-2 (Vejledning)	Endeligt udkast (august 2006)
{Ref. 10}	Generic Guideline for the Calculation of Risk inherent in the Carriage of Dangerous Goods by Rail (almene retningslinjer for beregning af risici i forbindelse med jernbanetransport af farligt gods)	OTIF-vejledning godkendt af RID-komiteen	24. november 2005
{Ref. 11}	Risikoacceptkriterium for tekniske systemer	Note 01/08	1.1 (25/01/2008)
{Ref. 12}	ERA Sikkerhedsafdelingen: Forundersøgelse – "Apportionment of safety targets (to TSI sub-systems) and consolidation of TSI from a safety point of view" WP1.1 - Vurdering af, om det er muligt at fordele de fælles sikkerhedsmål	WP1.1	1.0
{Ref. 13}	"Jernbaneanvendelser—Klassificeringssystemer for jernbanekøretøjer – Del 4: EN 0015380 Del 4: Funktionsgrupper".	EN 0015380 Part 4	

0.6. Standarddefinitioner, termer og forkortelser

- 0.6.1. De generelle definitioner, termer og forkortelser, der er anvendt i nærværende dokument, findes i en almindelig ordbog.
- 0.6.2. Nye definitioner, termer og forkortelser i denne vejledning er defineret i de følgende afsnit.

0.7. Specifikke definitioner

- 0.7.1. Se Artikel 3

0.8. Specifikke termer og forkortelser

- 0.8.1. I dette afsnit defineres de nye specifikke termer og forkortelser, der anvendes hyppigt i nærværende dokument.

Tabel 3: Termfortegnelse

Term	Definition
Agenturet	Det Europæiske Jernbaneagentur (ERA)
Vejledningen	"Vejledning i anvendelse af Kommissionens forordning (EF) nr. .../.. af [...] om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i Europa-Parlamentets og Rådets direktiv 2004/49/EF"
CSM-forordningen	"Kommissionens forordning (EF) nr. .../.. af [...] om vedtagelse af en fælles sikkerhedsmetode med hensyn til risikoevaluering og -vurdering som anført i artikel 6, stk. 3, litra a), i Europa-Parlamentets og Rådets direktiv 2004/49/EF" {Ref. 3}

Tabel 4: Fortegnelse over forkortelser

Forkortelse	Betydning
CCS	Control Command and Signalling - Styringskontrol og signaler
CSM	Common Safety Method(s) - fælles sikkerhedsmetode(r)
CST	Common Safety Targets - fælles sikkerhedsmål
EK	Europa-Kommissionen
ERA	European Railway Agency - Det Europæiske Jernbaneagentur
IM	Infrastructure Manager(s) - infrastrukturforvalter(e)
IF	Infrastrukturforvaltere
ISA	Independent Safety Assessor - uafhængigt sikkerhedsvurderingsorgan
OTIF	Den Mellemstatslige Organisation for Internationale Jernbanebefordringer
MS	Medlemsstat
NOBO	Notified Body - bemyndiget organ
ISA	Independent Safety Assessor, Uafhængig sikkerhedsgranskere
NSA	National Safety Authority - national sikkerhedsmyndighed
QMP	Quality Management Process - kvalitetsledelsesproces
QMS	Quality Management System - kvalitetsledelsessystem
RISC	Railway Interoperability and Safety Committee
RU	Railway Undertaking(s) - jernbanevirksomhed(er)
JV	Jernbanevirksomhed
SMP	Safety Management Process - sikkerhedsledelsesproces
SMS	Safety Management System - sikkerhedsledelsessystem

Tabel 4: Fortegnelse over forkortelser

Forkortelse	Betydning
SRT	Safety in Railway Tunnels - sikkerhed i jernbanetunneler
TBC	To be completed - færdiggøres
TSI	Technical Specifications for Interoperability - tekniske specifikationer for interoperabilitet
CENELEC	Comité Européen de Normalisation Electrotechnique, European Committee for Electrotechnical Standardization

FORKLARING AF ARTIKLERNE I CSM-FORORDNINGEN

Artikel 1. Formål

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] Yderligere forklaring anses ikke for nødvendig.

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 1] Yderligere forklaring anses ikke for nødvendig.

Artikel 2. Anvendelsesområde

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] CSM finder anvendelse på hele jernbanesystemet og dækker vurderingen af følgende ændringer i jernbanesystemerne, hvis de vurderes at være væsentlige i henhold til Artikel 4:

- (a) anlæg af nye linjer eller ændringer af eksisterende linjer
- (b) introduktion af nye og/eller ændrede tekniske systemer
- (c) driftsmæssige ændringer (f.eks. nye eller ændrede driftsregler og vedligeholdelsesprocedurer)
- (d) ændringer i JV/IF's organisation.

Termen "system" henviser i CSM til alle aspekter af et system, herunder udvikling, drift og vedligeholdelse heraf, frem til nedlukning eller bortskaffelse.

[G 2] CSM dækker de væsentlige ændringer af både:

- (a) "små og enkle" systemer, som kunne bestå af nogle få tekniske delsystemer eller elementer, og
- (b) "store og mere komplekse" systemer (f.eks. omfattende stationer og tunneler).

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] I overensstemmelse med jernbanesikkerhedsdirektivet {Ref. 1} og direktivet om interoperabilitet i jernbanenettet {Ref. 2} skal f.eks. en ny type rullende materiel til en højhastighedslinje være i overensstemmelse med TSI for rullende højhastighedsmateriel. Selv om størstedelen af det system, der vurderes, er dækket af TSI'en, er det vigtige punkt om menneskelige faktorer i forbindelse med førerrummet ikke med i TSI'en. For at sikre, at alle med rimelighed forudsigelige farer forbundet med den menneskelige faktor (dvs. med grænseflader mellem lokofører, det rullende materiel og resten af jernbanesystemet) identificeres og kontrolleres tilstrækkeligt, skal CSM-processen anvendes.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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;*
- (10) 'safety measures' means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk;*
- (11) 'proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC, the contracting entities or the manufacturers when they invite a notified body to apply the "EC" verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles;*
- (12) 'safety assessment report' means the document containing the conclusions of the assessment performed by an assessment body on the system under assessment;*
- (13) 'hazard' means a condition that could lead to an accident (EN 50126-2);*
- (14) 'assessment body' means the independent and competent person, organisation or entity which undertakes investigation to arrive at a judgment, based on evidence, of the suitability of a system to fulfil its safety requirements;*
- (15) 'risk acceptance criteria' means the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently*

- low that it is not necessary to take any immediate action to reduce it further;
- (16) 'hazard record' means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced;
- (17) 'hazard identification' means the process of finding, listing and characterising hazards (ISO/IEC Guide 73);
- (18) 'risk acceptance principle' means the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable;
- (19) 'code of practice' means a written set of rules that, when correctly applied, can be used to control one or more specific hazards;
- (20) 'reference system' means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison;
- (21) 'risk estimation' means the process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration (ISO/IEC 73);
- (22) 'technical system' means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;
- (23) 'catastrophic consequence' means fatalities and/or multiple severe injuries and/or major damages to the environment resulting from an accident (Table 3 from EN 50126);
- (24) 'safety acceptance' means status given to the change by the proposer based on the safety assessment report provided by the assessment body;
- (25) 'system' means any part of the railway system which is subject to a change;
- (26) 'notified national rule' means any national rule notified by Member States under Council Directive 96/48/EC⁽⁴⁾, Directive 2001/16/EC of the European Parliament and the Council⁽⁵⁾ and Directives 2004/49/EC and 2008/57/EC.

[G 1] Yderligere forklaring anses ikke for nødvendig.

Artikel 4. Væsentlige ændringer

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.

(4) EFT L 235 af 17.9.1996, s. 6.

(5) EFT L 110 af 20.4.2001, s. 1.

- [G 1] Hvis der ikke er en meddelt national forskrift, er beslutningen initiativtagerens ansvar. Betydningen af ændringen er baseret på en ekspertafgørelse. F.eks. hvis den planlagte ændring i et eksisterende system er kompleks, kan den evalueres som væsentlig, hvis risikoen for indvirkning på eksisterende funktioner⁽⁶⁾ i systemet er høj, selv om ændringen i sig selv ikke nødvendigvis er meget sikkerhedsrelateret.

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] **Eksempel på små ændringer:** Efter ibrugtagning af systemet kan en enkelt forøgelse af den maksimale strækningshastighed med 5 km/h være ubetydelig. Hvis den maksimale strækningshastighed imidlertid fortsat øges trinvis med 5 km/h, kunne summen af disse forøgelser (vurderet enkeltvis som ubetydelige ændringer) blive en væsentlig ændring i forhold til de oprindelige sikkerhedskrav til systemet.
- [G 2] For at vurdere, om en serie af flere på hinanden følgende (ikke-væsentlige) ændringer samlet set er væsentlig, skal alle farer og tilhørende risici forbundet med alle ændringerne vurderes. Serien af ændringer kan anses for ubetydelig, hvis den affødte risiko er bredt acceptabel.
- [G 3] Agenturets arbejde med væsentlige ændringer har vist:
- (a) at det ikke er muligt at identificere harmoniserede tærskler eller regler, der for en given ændring kan bruges som grundlag for at træffe beslutning om, hvorvidt ændringen er væsentlig, og
 - (b) at det ikke er muligt at opstille en udtømmende liste over væsentlige ændringer, og
 - (c) at beslutningen ikke kan være gyldig for alle initiativtagere og alle tekniske, driftsmæssige, organisatoriske og miljømæssige forhold.

⁽⁶⁾ Da funktionerne i et system ikke altid er uafhængige, kan ændringer af visse funktioner også indvirke på andre funktioner i systemet, selv om de kunne forekomme ikke at være direkte berørt af ændringerne.

Det er derfor afgørende at overlade ansvaret for beslutningen til initiativtagerne, som i overensstemmelse med artikel 4, stk. 3, i jernbanesikkerhedsdirektivet {Ref. 1} er ansvarlige for sikker drift og kontrol med de risici, der er forbundet med deres del af systemet.

[G 4] For at hjælpe initiativtageren gives der et eksempel på "evaluering og brug af kriterier" i afsnit C.2. af bilag C.

[G 5] CSM må ikke finde anvendelse, hvis en sikkerhedsrelateret ændring ikke anses for væsentlig. Men det betyder ikke, at der ikke skal foretages noget. Initiativtageren udfører (forhånds-)risikoanalyser under en given form for at beslutte, om ændringen er væsentlig. Disse risikoanalyser skal sammen med belæg og argumenter dokumenteres for at sætte NSA i stand til at foretage revision. Evalueringen af betydningen af en ændring og beslutningen om, at en ændring ikke er væsentlig, må ikke være genstand for et vurderingsorgans uafhængige vurdering.

Artikel 5. Risikostyringsproces

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] Yderligere forklaring anses ikke for nødvendig.

Artikel 5 (2)

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

[G 1] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

Artikel 6. Uafhængig vurdering

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] Det uafhængighedsniveau, der kræves af vurderingsorganet, afhænger af det sikkerhedsniveau, der er nødvendigt for det system, der vurderes. Mens vi afventer harmoniseringen af dette emne, kan bedste praksis på området findes i IEC 61508-1:2001 punkt 8 eller i afsnit 5.3.9. i standard EN 50129 {Ref. 7}. Afhængighedsgraden beror på, hvor alvorlige konsekvenserne er af den fare, der er forbundet med udstyret, og hvor ny den er. Afsnit 9.7.2 i EN 50126-2 og EN 50129 definerer afhængighedsniveauet i signalsystemerne. I princippet kunne dette også bruges til andre systemer.
- [G 2] Agenturet arbejder stadig på definitionen af de forskellige vurderingsorganers (NSA, NOBO og ISA) roller og ansvar samt de nødvendige grænseflader mellem dem. Definitionen fastlægger, hvem (om muligt) blandt disse vurderingsorganer der gør hvad, og hvordan det vil gøre det. Det vil til sidst gøre det muligt at definere:
- (a) hvordan det på basis af beviser kontrolleres, at risikostyrings- og risikovurderingsprocesserne, der er omfattet af CSM, anvendes korrekt, og
 - (b) hvordan initiativtageren støttes i sin beslutning om at acceptere den væsentlige ændring i det system, der vurderes.

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] Yderligere information vil blive tilføjet gennem agenturets arbejde med vurderingsorganernes roller og ansvar.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

Artikel 7. Sikkerhedsvurderingsrapporter

Artikel 7 (1)

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

[G 1] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Dette princip om gensidig anerkendelse er allerede accepteret i CENELEC-standarderne: se afsnit 5.5.2 i EN 50129 og afsnit 5.9 i EN 50126-2. I CENELEC anvendes princippet om krydsende accept eller gensidig anerkendelse af initiativtagere eller uafhængige sikkerhedsvurderingsorganer på generiske produkter og generiske anvendelser⁽⁷⁾, forudsat at sikkerhedsvurderingen og sikkerhedspåvisningen udføres i overensstemmelse med kravene i CENELEC-standarderne.

[G 2] Den gensidige anerkendelse skal også anvendes for accepten af nye eller ændrede systemer, hvis deres risikovurdering og påvisningen af systemets overensstemmelse med sikkerhedskravene udføres i overensstemmelse med bestemmelserne i CSM-forordningen {Ref. 3}.

Artikel 8. Ledelse af risikostyring/interne og eksterne 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] Yderligere forklaring anses ikke for nødvendig.

⁽⁷⁾ Se punkt [G 5] i afsnit 1.1.5 og fodnote ⁽⁹⁾ og ⁽¹⁰⁾ på side 28 samt Figur 3 i dette dokument med hensyn til yderligere forklaring af terminologien "generisk produkt og generisk anvendelse" og de deri indbyggede principper.

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] Yderligere forklaring anses ikke for nødvendig.

Artikel 9. Tilbage melding og tekniske fremskridt

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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

[G 1] Yderligere forklaring anses ikke for nødvendig.

Artikel 10. Ikrafttræden

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

BILAG I - FORKLARING AF PROCESSEN I CSM-FORORDNINGEN

1. GENERELLE PRINCIPPER FOR RISIKOSTYRINGSPROCESSEN

1.1. Generelle principper og forpligtelser

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.

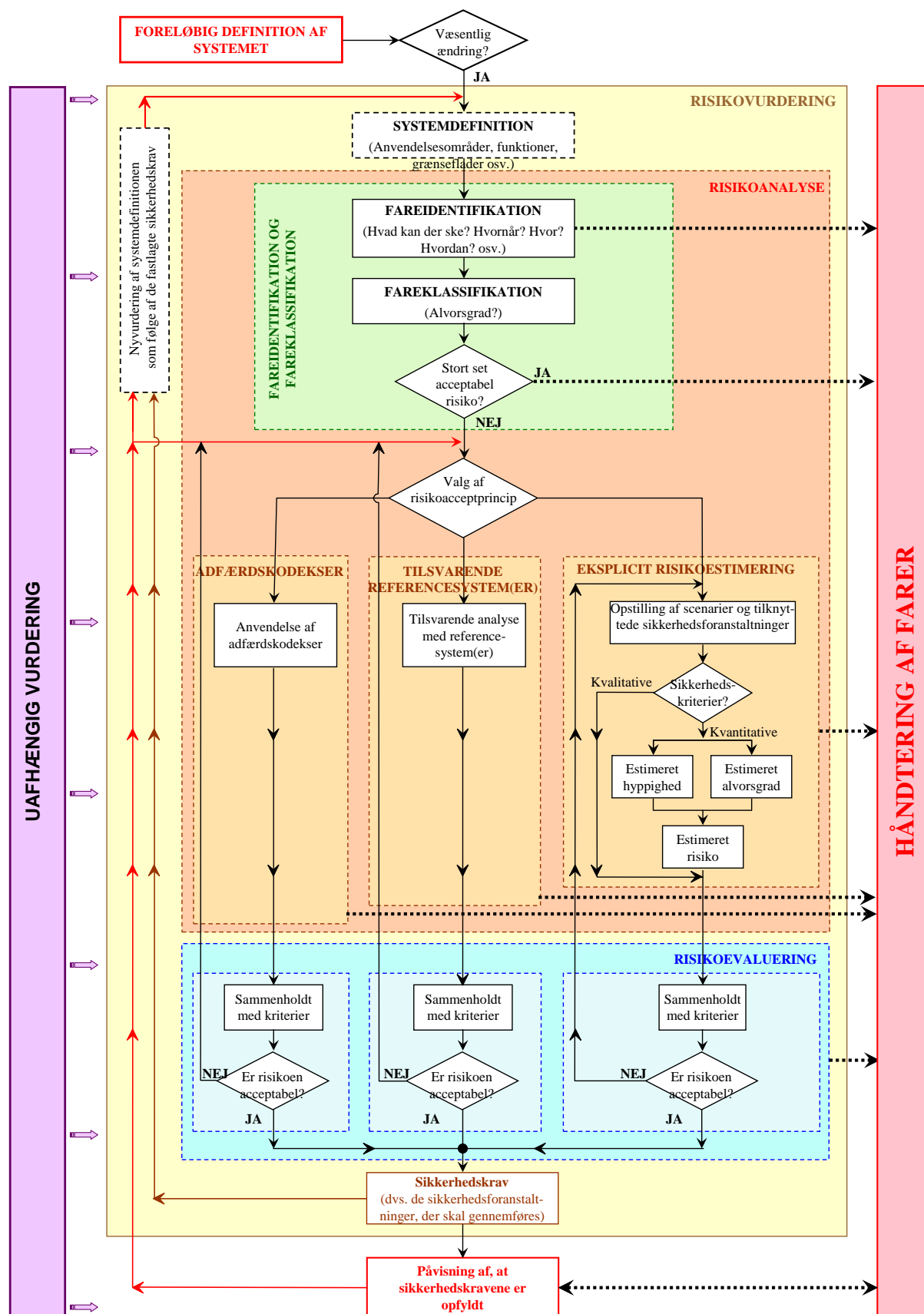
[G 1] Risikostyringsrammerne for CSM og den tilhørende risikovurderingsproces er illustreret i Figur 1. Når det anses for nødvendigt, er hver boks/aktivitet i denne figur beskrevet yderligere i et særskilt afsnit i dette dokument.

[G 2] CENELEC anbefaler, at risikostyrings- og risikovurderingsprocesserne beskrives i en sikkerhedsplan. Men hvis det ikke er hensigtsmæssigt for projektet, kan den tilhørende beskrivelse indarbejdes i ethvert andet relevant dokument: Se afsnit 1.1.6.

[G 3] Risikovurderingsprocessen tager udgangspunkt i en foreløbig systemdefinition. Under projektets udvikling opdateres den foreløbige systemdefinition gradvist og erstattes af systemdefinitionen. Hvis der ikke findes en foreløbig systemdefinition, anvendes den formelle systemdefinition til gennemførelse af risikovurderingen. Men da er det nyttigt, at alle aktører, der er berørt af den væsentlige ændring, mødes ved projektstart:

- (a) for at nå til enighed om de overordnede systemprincipper, systemfunktioner osv. I princippet kunne dette beskrives i en foreløbig systemdefinition
- (b) for at aftale projektorganisationen
- (c) for at aftale rolle- og ansvarsfordeling mellem de forskellige aktører, der allerede er involveret, bl.a. NSA, NOBO og ISA, hvor det er relevant.

En sådan koordinering i løbet af f.eks. den foreløbige systemdefinition giver initiativtageren, underleverandørerne, NSA, NOBO og ISA, hvis det er relevant, lejlighed til på et tidligt stadium at blive enige om adfærdskodekser eller referencesystemer, som er acceptable at bruge i projektet.



Figur 1: Risikostyringsrammerne i CSM-forordningen {Ref. 3}

1.1.2. This iterative risk management process:

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

- [G 1] Jernbanevirksomhedens og infrastrukturforvalterens sikkerhedsledelsessystem (SMS) indeholder den proces og de procedurer, som
- (a) overvåger, at systemet fortsætter med at være sikkert i hele sin livscyklus (dvs. under drift og vedligeholdelse)
 - (b) sikrer en sikker afvikling eller erstatning af det tilhørende system.
- Denne proces indgår ikke i CSM med hensyn til risikovurdering.
- [G 2] For at iværksætte CSM er det nødvendigt, at alle involverede parter er kompetente (dvs. har de rette færdigheder, viden og erfaring). Der er et generelt behov for kompetencestyring i organisationen hos jernbanesektorens aktører:
- (a) for infrastrukturforvalteres og jernbanevirksomheders vedkommende er dette dækket af deres sikkerhedsledelsessystem (SMS) i henhold til bilag III, stk. 2, litra e), i jernbanesikkerhedsdirektivet {Ref. 1}
 - (b) for så vidt angår de øvrige aktører, hvis aktiviteter kan have indvirkning på sikkerheden i jernbanesystemet, men for hvem SMS ikke er obligatorisk, i hvert fald ikke generelt på projektniveau (jf. punkt [G 1] i afsnit 5.1), så har de en kvalitetsledelsesproces (QMP) og/eller en sikkerhedsledelsesproces (SMP), som dækker dette krav.
- [G 3] De følgende afsnit af CENELEC-standard EN 50126-1 {Ref. 8} giver vejledning med hensyn til kompetence:
- (a) i medfør af afsnit 5.3.5.(b): *alle medarbejdere med ansvar inden for risikostyringsprocessen skal være kompetente til at varetage dette ansvar*
 - (b) i afsnit 5.3.5.(d) anføres, at kravene til risikostyring og risikovurdering skal gennemføres i forretningsprocesser understøttet af et kvalitetsledelsessystem (QMS), som er i overensstemmelse med kravene i EN ISO 9001, EN ISO 9002 eller EN ISO 9003, alt efter hvad der passer til det system", der vurderes. Der gives et eksempel på aspekter, der kontrolleres af kvalitetsledelsessystemet, i afsnit 5.2. i standarden EN 50129 {Ref. 7}.
- Disse afsnit dækker kvalitetssikringsaktiviteterne samt personalets/medarbejdernes kompetence og uddannelse, som er påkrævet for at støtte den proces, der er omfattet af CSM.
- [G 4] Meget ofte følges risikovurderingsprocessen op af et vurderingsorgan helt fra projektstart, men medmindre det kræves i henhold til national lov i en medlemsstat, er en så tidlig inddragelse af et vurderingsorgan ikke obligatorisk, om end det anbefales. Det uafhængige vurderingsorgan kunne være nyttigt, før der skiftes fra et trin i risikovurderingen til det næste. Se Artikel 6 med hensyn til yderligere detaljer om den uafhængige vurdering.

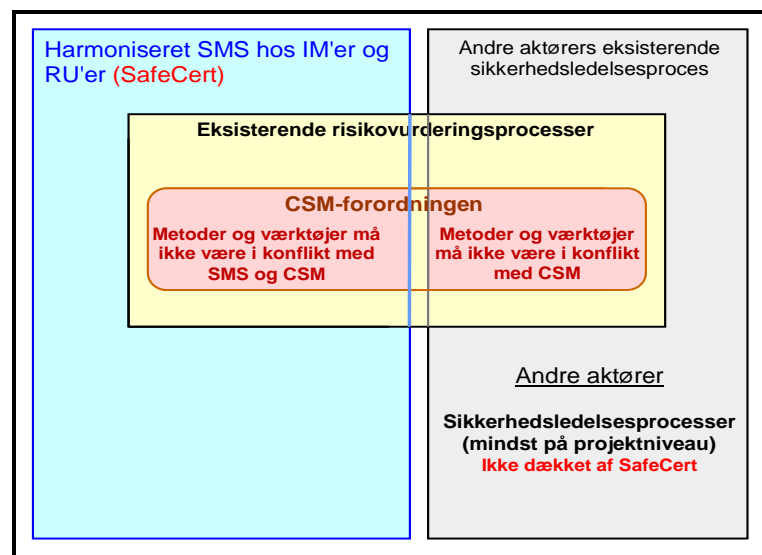
1.1.3. The proposer in charge of the risk management process required by this Regulation shall maintain a hazard record according to section 4.

[G 1] Yderligere forklaring anses ikke for nødvendig.

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 viser forholdet mellem CSM og "sikkerhedsledelsessystemerne og risikovurderingsprocesserne".



Figur 2: Harmoniseret SMS og CSM

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.*

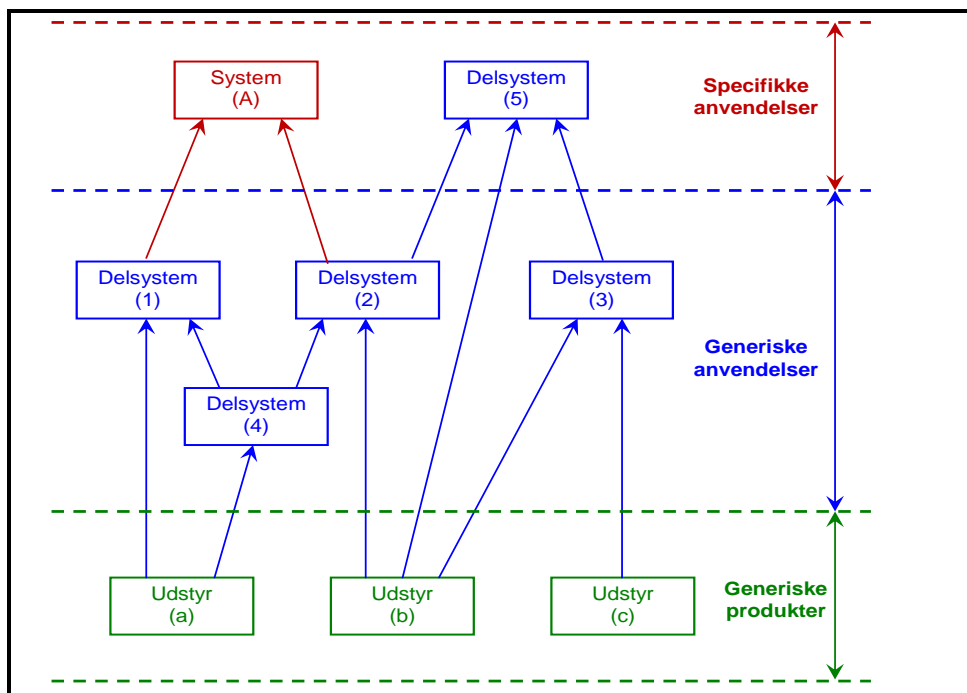
- [G 1] Hvis initiativtageren er en infrastrukturforvalter eller en jernbanevirksomhed, kan det sommetider være nødvendigt at inddrage andre aktører i processen⁽⁸⁾ (jf. afsnit 1.2.1). I visse tilfælde kan infrastrukturforvalteren eller jernbanevirksomheden udlicitere risikovurderingsarbejdet helt eller delvist. Hver aktørs roller og ansvar bliver normalt aftalt mellem de berørte aktører på et tidligt tidspunkt i projektforløbet.
- [G 2] Det er vigtigt at bemærke, at initiativtageren altid bevarer ansvaret for anvendelsen af CSM, for accepten af risikoen og dermed også for systemets sikkerhed. Det indebærer, at initiativtageren sikrer:
- (a) at der samarbejdes fuldt ud mellem de involverede aktører, så al nødvendig information udveksles, og
 - (b) at det står klart, hvem der skal opfylde de enkelte CSM-krav (f.eks. foretage risikoanalyse eller forvalte farededegørelsen).
- I tilfælde af uenighed mellem aktørerne om de sikkerhedskrav, de skal opfylde, kan man udbede sig en udtalelse fra NSA. Men ansvaret for at finde en løsning ligger fortsat hos initiativtageren og kan ikke overføres til NSA: se også afsnit 0.2.2.
- [G 3] Hvis opgaven udliciteres, har underleverandøren ikke pligt til at have sin egen sikkerhedsorganisation, hvis der ikke er tale om en infrastrukturforvalter eller en jernbanevirksomhed, og særlig ikke hvis underleverandørens struktur/størrelse er beskeden, eller hvis vedkommendes bidrag til det samlede system er begrænset. Ansvar for risikostyringen, herunder risikovurdering og farehåndteringsaktiviteter, kan fortsat påhvile den organisation, der ligger på det højere niveau (dvs. underleverandørens kunde). Imidlertid er underleverandøren altid ansvarlig for at tilvejebringe den rette og nødvendige information om sine aktiviteter til organisationen på højere niveau med henblik på opbygning af risikostyringsdokumentationen.
- De samarbejdende organisationer kan også aftale at etablere en fælles sikkerhedsorganisation, f.eks. for at optimere omkostningerne. I så fald vil kun en af organisationerne styre sikkerhedsaktiviteterne for alle de involverede organisationer. Ansvar for informationens nøjagtighed (dvs. farer, risici og sikkerhedsforanstaltninger) samt styringen af gennemførelsen af sikkerhedsforanstaltningerne ligger fortsat hos den organisation, der har til ansvar at kontrollere de farer, som disse sikkerhedsforanstaltninger er forbundet med.
- [G 4] initiativtageren vil normalt fastlægge de "sikkerhedsniveauer" og "sikkerhedskrav", der pålægges de aktører, der er involveret i projektet, og disse aktørers forskellige delsystemer og udstyr:
- (a) i kontrakterne mellem initiativtageren og de respektive aktører (underleverandører)

(8) Dette er i overensstemmelse med bilag A.4 i standard CENELEC EN 50129 {Ref. 7}.

- (b) i en sikkerhedsplan eller ethvert andet relevant dokument med samme formål sammen med beskrivelsen af den samlede projektorganisation og den enkelte aktørs ansvar, herunder initiativtagerens egne ansvarsområder: se afsnit 1.1.6
- (c) i initiativtagerens fareredegørelse(r): se afsnit 4.1.1.

Denne fordeling af systemets "sikkerhedsniveauer" og "sikkerhedskrav" ned til de underliggende delsystemer og det underliggende udstyr og derfor til de respektive aktører, herunder initiativtageren selv, kan finpudses/udvides i fasen "påvisning af systemets overensstemmelse med sikkerhedskravene": se Figur 1. I sammenligning med CENELEC's V-cyklus (jf. afsnit 2.1.1 og Figur 5 på side 34) svarer denne aktivitet til fase 5, der omhandler "fordeling af systemkrav" ned til de forskellige delsystemer og komponenter.

- [G 5] Artikel 5 (2) tillader, at andre aktører end RU og IM påtager sig det overordnede ansvar for overensstemmelse med CSM afhængigt af deres respektive behov. For f.eks. generiske produkter eller generiske anvendelser (9) kan fabrikanten udføre risikovurderingen på grundlag af en "generisk systemdefinition" med henblik på at specificere sikkerhedsniveauerne og sikkerhedskravene, der skal opfyldes af de generiske produkter og generiske anvendelser.



Figur 3: Eksempler på afhængighed mellem sikkerhedscases (uddraget af figur 9 i EN 50129 standarden)

- [G 6] CENELEC anbefaler, at fabrikanten tilvejebringer dokumentation fra risikovurderingen i sikkerhedscases og fareredegørelser for generiske produkter (henholdsvis generiske anvendelser⁽⁹⁾). Disse sikkerhedscases og fareredegørelser indeholder alle antagelser⁽¹⁰⁾ og

⁽⁹⁾ Terminologien "generisk anvendelse" og "generiske produktsikkerhedscases" er hentet fra CENELEC, hvor der anvendes tre forskellige kategorier af sikkerhedscases (se Figur 3):

- (a) **Generisk produktsikkerhedscase** (uafhængigt af anvendelsen). Et generisk produkt kan genanvendes til forskellige uafhængige anvendelser.

identificerede "anvendelsesrestriktioner" (dvs. sikkerhedsrelaterede anvendelsesbetingelser), som er gældende for de tilhørende generiske produkter (henholdsvis generiske anvendelser). Når et generisk produkt og en generisk anvendelse bruges i driften i en bestemt anvendelse, skal overensstemmelsen med alle disse antagelser⁽¹⁰⁾ og "anvendelsesrestriktioner" (eller sikkerhedsrelaterede anvendelsesbetingelser) derfor påvises i hver anvendelse for sig.

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] Medmindre andet er aftalt i kontrakterne ved projektstart, har hvert projekt meget ofte et ledsagende dokument, der beskriver risikostyringsaktiviteterne. De relevante dokumenter ajourføres og revideres, når der foretages væsentlige ændringer af det oprindelige system.
- [G 2] Et sådant dokument fastlægger organisationsstrukturen, ansvarsfordelingen blandt personalet og de processer, procedurer og aktiviteter, som tilsammen sikrer, at det system, der vurderes, opfylder de specificerede sikkerhedsniveauer og sikkerhedskrav. Dokumentet skal være i overensstemmelse med CSM, da det udgør en støtte og vejledning for vurderingsorganet. Ifølge CENELEC-standarderne anbefales det, at denne type information er inkluderet i en sikkerhedsplan eller i et andet dokument, hvoraf en del er viet til disse emner.

- (b) **Sikkerhedscase for generisk anvendelse** (for en anvendelseskategori). En generisk anvendelse kan genbruges for en kategori/type applikation med fælles funktioner.
- (c) **Sikkerhedscase for specifik anvendelse** (for en specifik anvendelse). En specifik anvendelse bruges kun til én bestemt installation.

Yderligere oplysninger om deres indbyrdes afhængighed findes i afsnit 9.4. og figur 9.1 i CENELEC's 50126-2 vejledning {Ref. 9}.

- (10) Disse antagelser og anvendelsesrestriktioner fastsætter grænserne for og gyldigheden af de "sikkerhedsvurderinger" og "sikkerhedsanalyser", der er forbundet med de tilknyttede sikkerhedscases for generiske produkter og generisk anvendelse. Hvis de ikke opfyldes af den pågældende specifikke anvendelse, er det nødvendigt at opdatere eller erstatte de tilhørende "sikkerhedsvurderinger" og "sikkerhedsanalyser" (f.eks. kausal analyse) med nye.

Dette falder i tråd med følgende generelle sikkerhedsprincip: "Når en specifik (del)systemkonstruktion er baseret på generiske anvendelser og generiske produkter, skal det påvises, at det specifikke (del)system er i overensstemmelse med alle de antagelser og anvendelsesrestriktioner (benævnt sikkerhedsrelaterede anvendelsesbetingelser i CENELEC), som er eksporteret i de tilsvarende sikkerhedscases for en generisk anvendelse og et generiske produkt (se Figur 3)."

Hvis der for en specifik anvendelse ikke kan opnås overensstemmelse med en række antagelser og anvendelsesrestriktioner på delsystemniveau (f.eks. hvis der er driftsmæssige sikkerhedskrav), kan de tilhørende antagelser og anvendelsesrestriktioner overføres til et højere niveau (dvs. sædvanligvis systemniveau). Disse antagelser og anvendelsesrestriktioner skal derefter tydeligt identificeres i "sikkerhedscasen for den specifikke anvendelse" for det tilhørende delsystem. Det er afgørende i sådanne tilfælde med afhængighed at sikre, at de sikkerhedsrelaterede anvendelsesbetingelser for hver sikkerhedscase er opfyldt i sikkerhedscasen på det højere niveau, eller også at de fremføres til de sikkerhedsrelaterede anvendelsesbetingelser for sikkerhedscasen på højeste niveau (dvs. systemsikkerhedscasen).

- *****
- [G 3] Navnlig initiativtagerens sikkerhedsplan eller ethvert andet relevant dokument skal præsentere den samlede projektorganisation. Den beskriver, hvordan roller og ansvar er fordelt mellem de involverede aktører. Med hensyn til detaljerede oplysninger henvises der til sikkerhedsplaner eller sikkerhedsorganisationer hos de forskellige involverede aktører. Sædvanligvis diskuteres og aftales ansvarsfordelingen mellem de forskellige aktører under den foreløbige systemdefinition (dvs. ved projektstart), hvis der foregår en sådan.
- [G 4] Sikkerhedsplanen er et levende dokument, der opdateres, når det er nødvendigt, i løbet af projektets levetid.
- [G 5] Der findes flere detaljer i EN 50126-1 standarden {Ref. 8} og den tilhørende vejledning 50126-2 {Ref. 9} om indholdet i en sikkerhedsplan.

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] Yderligere forklaring anses ikke for nødvendig..

1.2. Styling af grænseflader

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] Hvis f.eks. en jernbanevirksomhed af driftsmæssige årsager skal have en infrastrukturforvalter til at udføre definerede ændringer i infrastrukturen, overvåger jernbanevirksomheden i medfør af bilag III, stk. 2, litra g), i jernbanesikkerhedsdirektivet {Ref. 1} også det samlede arbejde for at sikre, at de forventede ændringer sker korrekt. Imidlertid fritager jernbanevirksomhedens lederskab ikke den berørte infrastrukturforvalter for ansvaret for at informere andre jernbanevirksomheder, hvis de også påvirkes af den pågældende ændring i infrastrukturen. Infrastrukturforvalteren skal måske endda udføre en risikovurdering i overensstemmelse med CSM, hvis pågældende ændring er væsentlig set fra IM's synspunkt.
- [G 2] Overførsel af ansvar mellem de forskellige aktører er mulig og under visse omstændigheder også nødvendig. Når flere aktører imidlertid er involveret i et system, udpeges en af dem meget ofte som den ansvarlige for det samlede system. Der er altid afhængigheder mellem delsystemer og driftselementer, som det kræver en særlig indsats at identificere. Det er derfor nødvendigt, at nogen overtager det samlede ansvar for sikkerhedsanalyserne og også får fuld adgang til al relevant dokumentation. Naturligvis har initiativtageren, som agter at indføre den væsentlige ændring, generelt det overordnede ansvar for, at risikovurderingen er systematisk og fuldstændig.
- [G 3] De primære kriterier, der skal aftales for styringen af en grænseflade mellem de berørte aktører, er:
- (a) lederskabet, som normalt varetages af initiativtageren, der agter at indføre den væsentlige ændring

- (b) de nødvendige input
- (c) metoderne til fareidentifikation og risikovurdering
- (d) de nødvendige deltagere med den nødvendige kompetence (dvs. kombination af viden, færdigheder og praktisk erfaring - se også definitionen af "personalekompetence" i punkt [G 2] (b) i artikel 3 i {Ref. 4})
- (e) de forventede resultater.

Disse kriterier er beskrevet i sikkerhedsplanerne (eller i ethvert andet relevant dokument) for de virksomheder, der er i berøring med de pågældende grænseflader.

[G 4] Der gives eksempler på grænseflader i afsnit C.3. i tillæg C samt et eksempel på anvendelse af hovedkriterierne for styringen af grænsefladerne mellem en togfabrikant og en infrastrukturforvalter eller en jernbanevirksomhed.

[G 5] Grænsefladestyringen består også i at tage de risici i betragtning, som kunne opstå ved grænsefladerne til menneskelige operatører (under drift og vedligeholdelse) for at kunne udforme disse grænseflader.

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 med overførsel af farer og tilknyttede sikkerhedsforanstaltninger mellem aktørerne er også gældende på lavere niveauer af CENELEC's V-cyklus i Figur 5 på side 34. Den kan anvendes, når det er nødvendigt at udveksle denne information f.eks. mellem en aktør og dennes underleverandører. Forskellen ved den samme proces på systemniveau er, at initiativtageren ikke behøver blive informeret om alle overførsler af farer og tilknyttede sikkerhedsforanstaltninger på delsystemniveau. Initiativtageren bliver kun informeret, når de overførte farer og tilknyttede sikkerhedsforanstaltninger er forbundet med grænseflader på højt niveau (dvs. når de indvirker på en grænseflade hos initiativtageren).

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] JV's og IF's sikkerhedsledelsessystem (SMS) omfatter ordninger og procedurer til sikring af, at sikkerhedsforanstaltningernes manglende overensstemmelse eller utilstrækkelighed forvaltes korrekt. Derfor indgår disse ordninger og procedurer ikke i CSM.

[G 2] I lighed hermed bliver ordninger og procedurer⁽¹¹⁾, der skal indføres af andre aktører⁽¹²⁾ til sikring af, at sikkerhedsforanstaltningernes manglende overensstemmelse eller utilstrækkelighed forvaltes korrekt, og om fornødent at sikkerhedsforanstaltningerne overføres til alle relevante aktører efter at være aftalt mellem de relevante aktører ved projektstart og beskrevet nærmere i deres sikkerhedsplan: se afsnit 0.2.

⁽¹¹⁾ *I princippet er disse ordninger og procedurer dækket af disse aktørers kvalitetsledelses- og/eller sikkerhedsledelsesproces, der som minimum er fastlagt på projektniveau (se også Figur 2).*

⁽¹²⁾ *Termen "andre aktører" betegner alle berørte aktører ud over IM'er og RU'er.*

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] Det vil således gøre det muligt at forvalte den eventuelle manglende overensstemmelse eller den utilstrækkelighed, som sikkerhedsforanstaltningen er behæftet med, i det system, der vurderes, eller i lignende systemer, hvor der anvendes samme foranstaltning.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

2. BESKRIVELSE AF RISIKOVURDERINGSPROCESSEN

2.1. Generel beskrivelse - Forbindelsen mellem CSM-risikovurderingsprocessen og CENELEC's V-cyklus

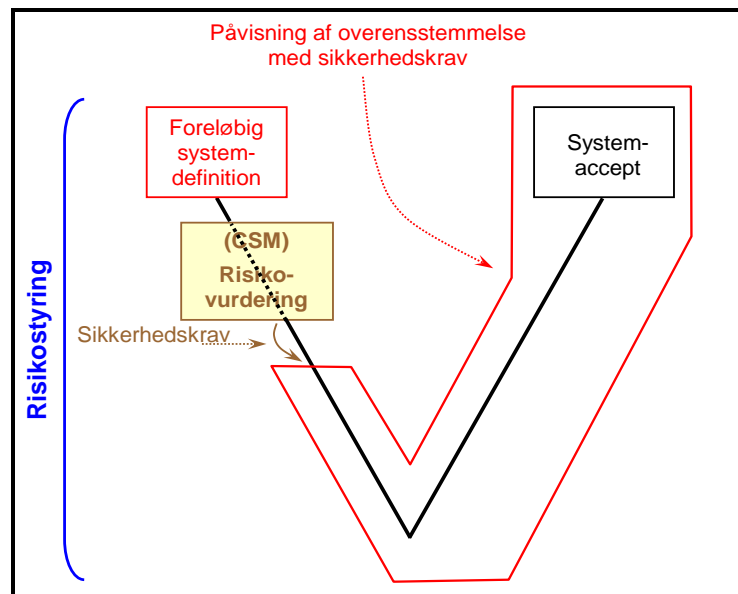
2.1.1. The risk assessment process is the overall iterative process that comprises:

- the system definition;
- the risk analysis including the hazard identification;
- the risk evaluation.

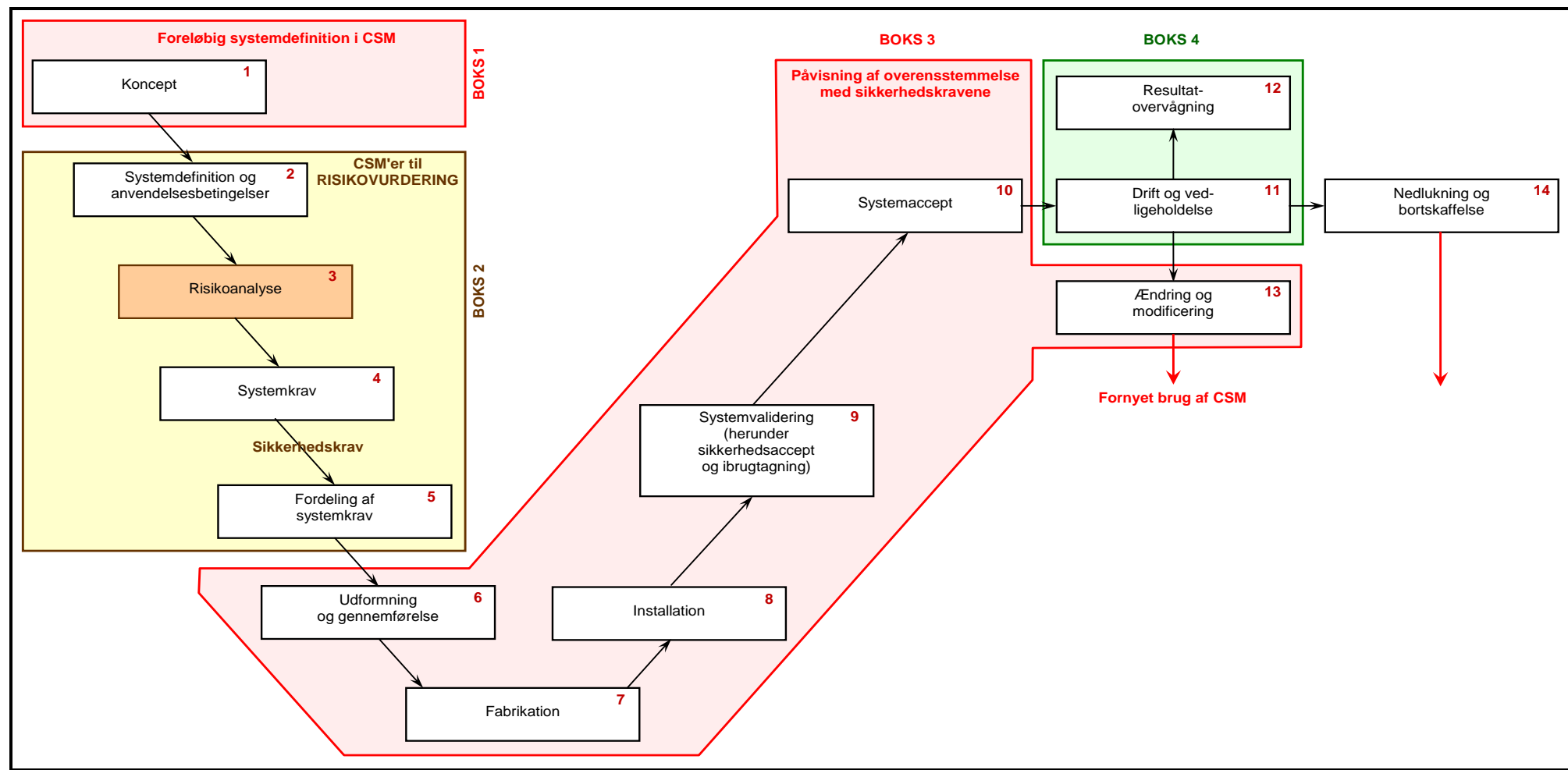
The risk assessment process shall interact with the hazard management according to section 4.1.

[G 1] Risikostyringsprocessen, der er omfattet af CSM, kan vises i en V-cyklus, som starter med den (foreløbige) systemdefinition og ender med accepten af systemet: se Figur 4. Denne forenklede V-cyklus har samme struktur som den klassiske V-cyklus i figur 10 i EN 50126-1 standarden [Ref. 8]. For at vise forbindelsen mellem CSM-risikostyringsprocessen i Figur 1 gives CENELEC's V-cyklus i figur 10 i Figur 5:

- (a) den "foreløbige systemdefinition" af CSM i Figur 1 svarer til fase 1 i CENELEC's V-cyklus, dvs. til definitionen af systemets "koncept" (jf. boks 1 i Figur 5)
- (b) "risikovurdering" af CSM i Figur 1 omfatter følgende faser af CENELEC's V-cyklus (jf. boks 2 i Figur 5):
 - (1) Fase 2 i Figur 5: "systemdefinition og anvendelsesbetingelser",
 - (2) Fase 3 i Figur 5: "risikoanalyse",
 - (3) Fase 4 i Figur 5: "systemkrav",
 - (4) Fase 5 i Figur 5: "fordeling af systemkrav" ned til de forskellige delsystemer og komponenter.



Figur 4: Forenklet V-cyklus i figur 10 i EN 50126-standarden



Figur 5: Figur 10 i EN 50126 V-cyklus (CENELEC's systemlivscyklus)

- *****
- [G 2] Resultaterne af risikovurderingsprocessen i CSM er (efter gentagelser - jf. Figur 1):
- (a) "systemdefinition" opdateret med "sikkerhedskravene", som hidrører fra "risikoanalysen" og "risikoevalueringen" (jf. afsnit 2.1.6)
 - (b) "fordeling af systemkrav" ned til de forskellige delsystemer og komponenter (fase 5 i Figur 5)
 - (c) "fareredegørelsen", hvor der registreres:
 - (1) alle de identificerede farer og de tilknyttede sikkerhedsforanstaltninger
 - (2) de deraf følgende sikkerhedskrav
 - (3) de antagelser, der er taget i betragtning for systemet, som fastsætter grænserne og gyldigheden af risikovurderingen (jf. punkt (g) i afsnit 2.1.2)
 - (d) og generelt alle beviser, der hidrører fra anvendelsen af CSM: se afsnit 5.
- Disse risikovurderingsresultater af CSM svarer til de sikkerhedsrelaterede resultater af fase 4 i CENELEC's V-cyklus, dvs. til systemkravspecifikationen i Figur 5.
- [G 3] Systemdefinitionen ajourført med resultaterne af risikovurderingen og fareredegørelsen udgør resultaterne, som systemet er udformet og accepteret i henhold til. "Påvisning af systemets overensstemmelse med sikkerhedskravene" i CSM svarer til følgende faser af CENELEC's V-cyklus (jf. boks 3 i Figur 5):
- (a) Fase 6 i Figur 5: "udformning og gennemførelse"
 - (b) Fase 7 i Figur 5: "fabrikation"
 - (c) Fase 8 i Figur 5: "installation"
 - (d) Fase 9 i Figur 5: "systemvalidering (herunder sikkerhedsaccept og ibrugtagning)"
 - (e) Fase 10 i Figur 5: "systemaccept".
- [G 4] Påvisningen af systemets overensstemmelse med sikkerhedskravene afhænger af, om den væsentlige ændring er teknisk, driftsmæssig eller organisatorisk. Så de forskellige trin i CENELEC's V-cyklus i Figur 5 egner sig muligvis ikke til alle væsentlige ændringer af den givne type. V-cyklussen i Figur 5 skal betragtes herefter og anvendes med passende skøn over, hvad der passer til hver enkelt anvendelse (f.eks. er der ingen fabrikationsfase for driftsmæssige og organisatoriske ændringer).
- [G 5] Det betyder, at "påvisning af systemets overensstemmelse med sikkerhedskravene" i CMS ikke kun omfatter "verifikation og validering" ved hjælp af prøver eller simulering. I praksis omfatter påvisningen alle faserne "6 til 10" (jf. listen ovenfor og Figur 5) i CENELEC's V-cyklus. De omfatter udformning, fabrikation, installation, verifikation og validering samt de tilhørende RAMS-aktiviteter (RAMS = Reliability Availability Maintainability and Safety) og systemaccepten.
- [G 6] Under "påvisning af systemets overensstemmelse med sikkerhedskravene" er det generelle princip at få risikovurderingen til kun at være fokuseret på sikkerhedsrelaterede funktioner og grænseflader i systemet. Det betyder, at når det er påkrævet risiko- og sikkerhedsvurderinger inden for en af faserne i CENELEC's V-cyklus i Figur 5, er der fokus på:
- (a) de sikkerhedsrelaterede funktioner og grænseflader
 - (b) delsystemer og/eller komponenter, der indgår i varetagelsen af de sikkerhedsrelaterede funktioner og/eller grænseflader, der blev vurderet under vurderingen af risici på højere niveau.

[G 7] Det følger herefter af sammenligningen med den klassiske udgave af CENELEC's V-cyklus i Figur 5:

- (a) at CSM dækker faserne "1-10" og "13" i denne V-cyklus. De omfatter den række aktiviteter, der er nødvendige for accepten af det system, der vurderes
- (b) at CSM ikke dækker faserne "11", "12" og "14" af systemets livscyklus:
 - (1) fase "11" og "12" vedrører henholdsvis "drift og vedligeholdelse" og "resultatovervågning" af systemet efter accepten baseret på CSM. Disse to faser er omfattet af JV's og IF's sikkerhedsledelsessystem (SMS) - (jf. boks 4 i Figur 5). Men hvis det under drift, vedligeholdelse eller udførelse af overvågning af systemet viser sig nødvendigt at ændre og modernisere systemet (fase 13 i Figur 5), selv om det allerede er i drift, skal CSM anvendes igen på de nye nødvendige ændringer i overensstemmelse med Artikel 2. Hvis ændringen er væsentlig, gælder derfor følgende:
 - (i) risikostyrings- og risikovurderingsprocesserne i CSM anvendes på disse nye ændringer
 - (ii) det er nødvendigt med en accept af disse nye ændringer i overensstemmelse med Artikel 6
 - (2) "nedlukning og bortskaffelse" af et system, der allerede er i drift (fase 14), kunne også betragtes som en væsentlig ændring, og derfor kunne CSM igen anvendes i overensstemmelse med Artikel 2 for fase 14 i Figur 5.

Yderligere information om afgrænsningen af hver fase eller aktivitet i CENELEC's V-cyklus angivet i Figur 5 gives i afsnit 6. af EN 50126-1 standarden {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] Yderligere forklaring anses ikke for nødvendig.

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

[G 1] Yderligere forklaring anses ikke for nødvendig.

2.1.4. The risk acceptability of the system under assessment shall be evaluated by using one

or more of the following risk acceptance principles:

- (a) the application of codes of practice (section 2.3);*
- (b) a comparison with similar systems (section 2.4);*
- (c) an explicit risk estimation (section 2.5).*

In accordance with the general principle referred to in section 1.1.5, the assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer.

- [G 1] Generelt vil initiativtageren på baggrund af de specifikke krav til projektet samt initiativtagerens erfaring med de tre principper beslutte, hvilke risikoacceptprincipper der er de bedst egnede til at kontrollere de identificerede farer.
- [G 2] Det er ikke muligt altid at evaluere, om risikoen er acceptabel på systemniveau gennem anvendelse af kun et af de tre risikoacceptprincipper. Risikoaccepten vil ofte være baseret på en blanding af disse principper. Hvis der for en væsentlig fare er brug for at anvende mere end ét risikoacceptprincip til at kontrollere den tilhørende risiko, skal den pågældende fare deles op i underordnede farer, så hver enkelt underordnet fare kontrolleres tilstrækkeligt af kun ét risikoacceptprincip.
- [G 3] I beslutningen om at kontrollere en fare ved hjælp af et risikoacceptprincip skal der tages hensyn til faren og årsagerne til faren, som allerede er identificeret under fareidentifikationen. Hvis to forskellige og indbyrdes uafhængige årsager derfor er forbundet med samme fare, skal faren underinddeles i to forskellige underordnede farer. Hver underordnet fare vil derefter blive kontrolleret af et enkelt risikoacceptprincip. De to underordnede farer skal registreres og forvaltes i fareredegørelsen. Hvis f.eks. faren skyldes en konstruktionsfejl, kan dette styres af anvendelsen af en adfærdskodeks, mens dette måske ikke er tilstrækkeligt, hvis årsagen til faren er en vedligeholdelsesfejl. I så fald er anvendelsen af et andet risikoacceptprincip nødvendigt.
- [G 4] Nedbringelsen af risikoen til et acceptabelt niveau kan kræve flere gentagelser mellem risikoanalyse- og risikoevalueringsfasen, indtil der er identificeret passende sikkerhedsforanstaltninger.
- [G 5] Den aktuelle resterende risiko, der er udledt gennem erfaring fra anvendelse af eksisterende systemer og de systemer, der er baseret på anvendelse af adfærdskodekser (anerkendte regler), anerkendes som acceptabel. Risikoen, der hidrører fra eksplicit risikoestimering, er baseret på ekspertens afgørelser og forskellige antagelser under analysen eller på databaser over ulykker eller driftserfaring. Derfor kan den resterende risiko fra den eksplicitte risikoestimering ikke bekræftes umiddelbart gennem erfaring i felten. En sådan påvisning kræver tid til drift, overvågning og indhentning af repræsentativ erfaring med de relaterede systemer. Generelt har anvendelsen af adfærdskodekser og sammenligning med lignende referencesystemer den fordel, at man undgår en overspecificering af unødvendigt strenge sikkerhedskrav, som kan følge af overdrevent konservative (sikkerheds-)antagelser i eksplicitte risikoestimeringer. Imidlertid kunne det ske, at visse sikkerhedskrav fra adfærdskodekser eller lignende referencesystemer ikke behøver at blive opfyldt for det system, der vurderes. I så fald ville anvendelsen af eksplicit risikoestimering have den fordel, at man undgår unødigt overkonstruktion af systemet, der vurderes, og at det bliver muligt at frembringe en mere omkostningseffektiv konstruktion, der ikke er blevet afprøvet før.

- *****
- [G 6] Hvis de identificerede farer og tilhørende risici i systemet, der vurderes, ikke kan kontrolleres ved hjælp af anvendelsen af adfærdskodekser eller lignende referencesystemer, udføres en eksplicit risikoestimering baseret på kvantitative eller kvalitative analyser af farlige hændelser. Denne situation opstår, når systemet, der vurderes, er helt nyt (eller konstruktionen er nyskabende), eller når systemet afviger fra en adfærdskodeks eller et referencesystem. Den eksplicitte risikoestimering vil herefter afdække, om risikoen er acceptabel (dvs. yderligere analyse er unødvendig), eller om der er brug for supplerende sikkerhedsforanstaltninger for at reducere risikoen yderligere.
- [G 7] Vejledning i risikoreduktion og risikoaccept findes også i afsnit 8 af vejledningen EN 50126-2 {Ref. 9}.
- [G 8] Det risikoacceptprincip, der er brugt, og anvendelsen heraf skal vurderes af vurderingsorganet.

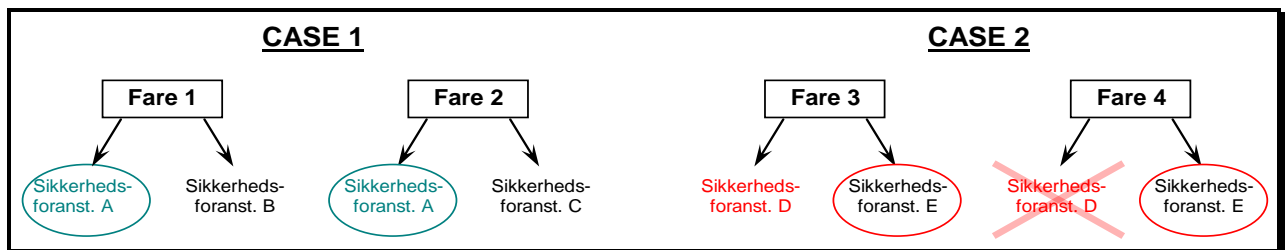
2.1.5. The proposer shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer shall also check that the selected risk acceptance principles are used consistently.

- [G 1] Hvis f.eks. anvendelsen af SIL 4-udviklingsprocessen i EN 50128-standarden, for så vidt angår softwaren til en komponent, er specificeret som sikkerhedskravet, vil det ved påvisning skulle bevises, at den proces, som standarden anbefaler, er gennemført. Dette inkluderer f.eks. påvisning af:
- (a) at kravene om uafhængighed i tilrettelæggelsen af softwarens udformning, verifikation og validering er opfyldt
 - (b) at de korrekte metoder i EN 50128-standarden for SIL 4-sikkerhedsintegritetsniveauet er anvendt
 - (c) osv.
- [G 2] Hvis f.eks. en dedikeret adfærdskodeks skal bruges til fremstilling af elektroventiler til nødbremser, vil det ved påvisning skulle bevises, at alle krav fra adfærdskodeksen er opfyldt under fremstillingen.

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] Der kan identificeres to slags sikkerhedsforanstaltninger:
- (a) "forebyggende sikkerhedsforanstaltninger", der forebygger forekomsten af farer eller årsagerne hertil, og
 - (b) "afbødende sikkerhedsforanstaltninger", der hindrer farer i at udvikle sig til ulykker eller mindsker konsekvenserne af ulykker efter disses opståen (beskyttelsesforanstaltninger).
- Af hensyn til driften er forebyggelse af årsager generelt mest effektivt.

- [G 2] Initiativtageren vil betragte de sikkerhedsforanstaltninger, der giver det bedste kompromis mellem omkostningen ved at opnå en risikoreduktion og niveauet for den resterende risiko, som de bedst egnede. De valgte sikkerhedsforanstaltninger bliver til sikkerhedskrav til det system, der vurderes.
- [G 3] Det er vigtigt at kontrollere, at sikkerhedsforanstaltningerne, der er valgt til at kontrollere én fare med, ikke er i konflikt med andre farer. Som vist i Figur 6 kan f.eks. følgende to situationer opstå⁽¹³⁾:
- (a) CASE 1: Hvis den samme sikkerhedsforanstaltning (foranstaltning A i Figur 6) kan kontrollere forskellige farer uden at skabe konflikt mellem dem, og hvis den tilknyttede sikkerhedsforanstaltning (hvis økonomisk berettiget) kunne vælges alene som tilhørende "sikkerhedskrav". Det samlede antal sikkerhedskrav, der skal opfyldes, er mindre end gennemførelsen af både foranstaltning B og C,



Figur 6: Udvælgelse af tilstrækkelige sikkerhedsforanstaltninger til kontrol med risici

- (b) CASE 2: Omvendt, hvis én sikkerhedsforanstaltning kan kontrollere én fare, men skaber en konflikt med en anden fare (foranstaltning D i Figur 6), kan den ikke vælges som "sikkerhedskrav". De øvrige sikkerhedsforanstaltninger for den pågældende fare skal i så fald anvendes (foranstaltning E og F i Figur 6):
- (1) Et typisk eksempel i styringskontrollsystemet er anvendelsen af togets placering på sporet enten til at kontrollere bremseanvendelsen eller til at tillade toget at accelerere. Anvendelsen af togets forende som togplacering (henholdsvis togets bagende) er ikke sikker i alle situationer:
 - (i) når ETCS's (European Train Control System) styringskontrollsystem skal udløse sikker anvendelse af nødbremserne, benyttes der MAXIMUM SAFE FRONT END, dvs. minimumsgrænse for sikker front, til at garantere, at togets forende faktisk stopper, før den når farepunktet
 - (ii) omvendt, når toget får tilladelse til at accelerere eksempelvis efter en hastighedsbegrænsning, benytter ETCS's styringskontrollsystem MINIMUM SAFE REAR END, dvs. minimumsgrænse for sikker bagende.
 - (2) Et andet eksempel er en sikkerhedsforanstaltning, som kunne være gyldig grund til at stoppe et tog under næsten alle omstændigheder undtagen i en tunnel eller på en bro for at gå i fejlsikret tilstand. I sidstnævnte tilfælde skal foranstaltning D i CASE 2 i Figur 6 ikke træffes.

⁽¹³⁾ Det skal bemærkes, at vejledningen ikke opregner alle situationer, hvor sikkerhedsforanstaltningerne kunne være i konflikt med andre identificerede farer. Der gives kun nogle få illustrative eksempler.

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] Alt efter f.eks. de tekniske valg i forbindelse med udformning af et system, dettes delsystemer og udstyr kunne der blive identificeret nye farer under "påvisningen af overensstemmelse med sikkerhedskravene" (f.eks. kunne anvendelse af visse malingstyper føre til giftige gasser i tilfælde af brand). Disse nye farer og de tilhørende risici skal betragtes som nye **input** til en ny sløjfe i den iterative risikovurderingsproces. Tillæg A.4.3 i EN 50129-standardens giver andre eksempler, hvor nye farer kunne optræde og ville skulle kontrolleres.

2.2. Fareidentifikation

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] Farerne udtrykkes så vidt muligt på samme detaljeniveau. Det kan ske under foreløbige fareanalyser, at farer på forskellige detaljeniveauer identificeres (f.eks. fordi der i forbindelse med en HAZOP er samlet mennesker med forskellig erfaring). Detaljeniveauet afhænger også af risikoacceptprincippet, som vælges til at kontrollere de identificerede farer med. Hvis f.eks. en fare er fuldstændig kontrolleret af en adfærdskodeks eller et lignende referencesystem, vil der ikke være brug for mere detaljeret fareidentifikation.
- [G 2] For alle de farer, der er blevet identificeret under risikovurderingsprocessen (herunder dem, der er forbundet med bredt acceptable risici), skal de tilknyttede sikkerhedsforanstaltninger og risici registreres i fareredegørelsen.
- [G 3] Afhængigt af arten af systemet, der skal analyseres, kan der anvendes forskellige metoder til fareidentifikation:
- (a) empirisk fareidentifikation kan bruges til at udforske hidtidig erfaring (f.eks. anvendelse af tjeklister eller generiske farelister)
 - (b) kreativ fareidentifikation kan anvendes til nye problemområder (proaktiv prognostisering, f.eks. strukturerede "WHAT-IF"-undersøgelser (**SWIFT**), **FMEA** eller HAZOP).
- [G 4] De empiriske og kreative metoder til fareidentifikation kan anvendes sammen for at supplere hinanden og sikre, at listen over potentielle farer og sikkerhedsforanstaltninger, hvor det er relevant, er udtømmende.
- [G 5] Som et foreløbigt skridt kunne fareidentifikationen starte med et brainstormingteam af eksperter, der har forskellige kompetencer fordelt på alle relevante aspekter af den væsentlige ændring. Når ekspertpanelet anser det for nødvendigt, kan empiriske metoder anvendes til at analysere specifikke funktioner eller driftsforhold.
- [G 6] Metoderne, der anvendes til fareidentifikation, afhænger af systemdefinitionen. Der gives nogle eksempler i tillæg B.

[G 7] Der findes flere oplysninger om fareidentifikationsteknikker og -metoder i tillæg A.2 og E i vejledningen EN 50126-2 {Ref. 9}.

[G 8] Et eksempel på en generisk fareliste findes i afsnit C.17. i tillæg 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.

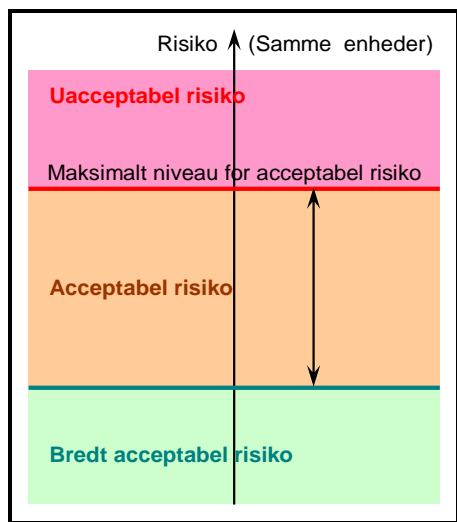
[G 1] For at befordre risikovurderingsprocessen kan de betydelige farer grupperes yderligere i forskellige kategorier. F.eks. kan de betydelige farer klassificeres eller ordnes efter den forventede alvorlighed og hyppighed. Vejledning til en sådan øvelse findes i CENELEC-standarderne: se afsnit A.2. i tillæg A.

[G 2] Risikoanalysen og -evalueringen, der er beskrevet i afsnit 2.1.4, anvendes på et prioriteret grundlag, hvor de høje strangerende farer står øverst.

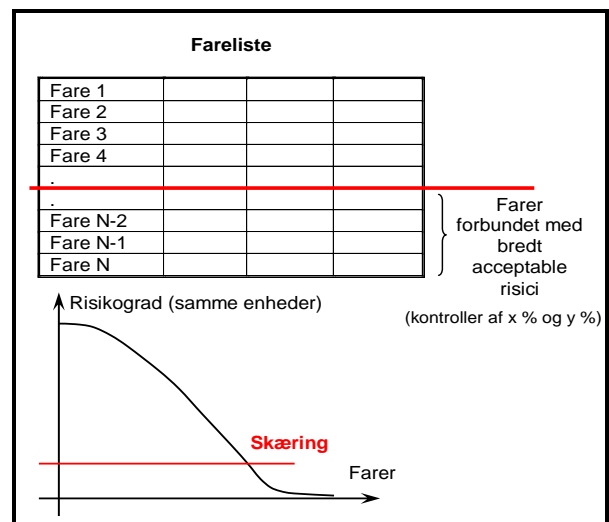
2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed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

[G 1] F.eks. kan en risiko forbundet med en fare anses for bredt acceptabel:

- (a) hvis risikoen er mindre end en given procent (f.eks. x %) af den maksimalt acceptable risiko for denne type fare. Værdien af x % kunne bygge på bedste praksis og erfaring med flere risikoanalysemetoder, f.eks. forholdet mellem bredt acceptabel risiko og uacceptabel risiko indtegnet i F-N-kurver (F = frekvens, N = antallet dræbte) eller i risikomatricer. Dette kan vises som i Figur 7
- (b) eller hvis tabet, der er forbundet med risikoen, er så lille, at det ikke er rimeligt at gennemføre afbødende sikkerhedsforanstaltninger.



Figur 7: Breddet acceptable risici



Figur 8: Udfiltrering af farer, der er forbundet med en bredt acceptabel risiko

- [G 2] Herudover skal der, hvis der identificeres farer med forskellige detaljeniveauer (dvs. alvorlige farer på den ene side og detaljerede underordnede farer på den anden side), træffes forholdsregler for at undgå at de klassificeres forkert som farer, der er forbundet med bredt acceptable risici. Bidraget fra alle farer, der er forbundet med bredt acceptable risici, kan ikke overstige en given andel (f.eks. y %) af den samlede risiko på systemplan. Denne kontrol er nødvendig for at hindre, at rationalet bliver udhulet, ved at farerne underinddeles i mange underordnede farer på lavt niveau. Hvis én fare udtrykkes som mange forskellige "mindre" underordnede farer, kan hver af disse nemlig let blive klassificeret som forbundet med bredt acceptable risici, hvis de blev evalueret uafhængigt af hinanden, men forbundet med betydelig risiko, når de evalueres under ét (dvs. som én alvorlig fare). Værdien af andelen (f.eks. y %) afhænger af de risikoacceptkriterier, der gælder på systemniveau. Den kan være baseret på og estimeret ud fra driftserfaring med lignende referencesystemer.
- [G 3] De to ovennævnte kontroller (dvs. imod x % og y %) gør det muligt at fokusere risikovurderingen på de vigtigste farer og at sikre, at enhver betydelig risiko bliver kontrolleret (jf. Figur 8). Med forbehold af lovkravene i en given medlemsstat er initiativtageren ansvarlig for på basis af en ekspertafgørelse at definere værdierne x % og y % og at få dem uafhængigt vurderet af et vurderingsorgan. Et eksempel på størrelsesordenen kan være x = 1 % og y = 10 %, hvis det betragtes som acceptabelt i henhold til ekspertafgørelsen.
- [G 4] I afsnit 2.2.2 kræves, at klassifikationen i "bredt acceptable risici" vurderes uafhængigt af et vurderingsorgan.

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] Det primære formål med aktiviteten er identifikation af farer, som er forbundet med ændringen. Hvis der allerede er identificeret sikkerhedsforanstaltninger, skal de registreres i fareredegørelsen. Foranstaltningernes art afhænger af ændringen. De kan være procedurerelaterede, tekniske, driftsrelaterede eller organisatoriske.

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] Selv om en risiko er holdt på et acceptabelt niveau, kan initiativtageren stadig beslutte, at det er nødvendigt med mere detaljeret fareidentifikation. En grund hertil kunne være, at en mere detaljeret fareidentifikation sandsynligvis kan afdække mere omkostningseffektive risikokontrolrelaterede sikkerhedsforanstaltninger.

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] Yderligere forklaring anses ikke for nødvendig.

2.3. Anvendelse af adfærdskodekser og risikoevaluering

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

2.4. Anvendelse af referencesystem og risikoevaluering

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] Der findes flere oplysninger om disse principper i afsnit 8 i vejledningen EN 50126-2 {Ref. 9}.

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

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

[G 1] F.eks. kunne et gammelt styringskontrollsystem, som under drift beviseligt har et acceptabelt sikkerhedsniveau, blive afløst af et andet system med nyere teknologi og bedre sikkerhedsresultater. Når der anvendes et referencesystem, er det således relevant at kontrollere hver gang, om det fortsat er berettiget til accept.

[G 2] Da f.eks. visse aspekter af tunnelsikkerhed eller sikkerhed ved transport af farligt gods kunne være specifikke og afhænge af drifts- og miljøforhold, er det nødvendigt at kontrollere for hvert projekt, at systemet vil blive brugt under de samme forhold.

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] Yderligere forklaring anses ikke for nødvendig.

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] Der findes flere oplysninger om lighedsanalyser i afsnit 8.1.3 i vejledningen 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] Yderligere forklaring anses ikke for nødvendig.

2.5. EksPLICIT risikoestimering og -evaluering

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] Yderligere forklaring anses ikke for nødvendig.

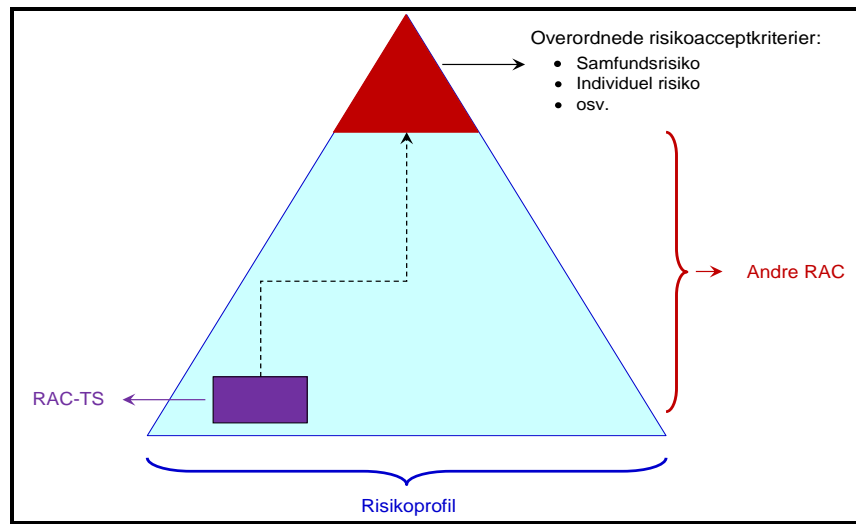
2.5.2. *The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated 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] For at vurdere, om risiciene fra systemet, der vurderes, er acceptable eller ikke, skal der bruges risikoacceptkriterier (jf. boks om "risikoevaluering" i Figur 1). Risikoacceptkriterierne kan være enten implicitte eller eksplicitte:

- (a) Implicitte risikoacceptkriterier: I henhold til afsnit 2.3.5 og 2.4.3 bliver risici, der er omfattet af anvendelse af adfærdskodekser og sammenligning med referencesystemer, implicit betragtet som acceptable, forudsat henholdsvis (jf. prikket cirkel i Figur 1):
 - (1) at betingelserne for anvendelse af adfærdskodekser i afsnit 2.3.2 er opfyldt
 - (2) at betingelserne for anvendelse af et referencesystem i afsnit 2.4.2 er opfyldt.
- (b) Eksplicitte risikoacceptkriterier: For at vurdere, om risikoen(risiciene), der kontrolleres ved anvendelse af eksplicit risikoestimering, er acceptabel(le) eller ikke, skal der bruges eksplicitte risikoacceptkriterier (jf. ubrudt cirkel i Figur 1 for det tredje princip). Disse kan defineres på forskellige niveauer i et jernbanesystem. De kan ses som en "kriteriepyramide" (jf. Figur 9), der starter med de alvorlige risikoacceptkriterier (udtrykt f.eks. som samfundsrisiko eller individuel risiko) og går ned til delsystemer og komponenter (for at dække tekniske systemer) og omfatter menneskelige operatører under drift og vedligeholdelse af systemet og delsystemerne. Selv om risikoacceptkriterierne bidrager til at nå systemets sikkerhedsresultater og dermed er forbundet med de fælles sikkerhedsmål (CST) og de nationale referenceværdier (NRV), er det meget vanskeligt at opbygge en matematisk model mellem dem: jf. {Ref. 12}, hvor der findes flere detaljer.

Det niveau, som de eksplicitte risikoacceptkriterier defineres på, skal passe sammen med graden og kompleksiteten af den væsentlige ændring. Det er f.eks. ikke nødvendigt at evaluere den overordnede jernbanesystemrisiko, når man ændrer en akseltype i det rullende materiel. Definitionen af risikoacceptkriterierne kan fokusere på sikkerheden for det rullende materiel. Omvendt bør store ændringer eller tilføjelser til et eksisterende jernbanesystem ikke kun vurderes på basis af sikkerhedsresultatniveauet for de enkelte funktioner eller ændringer, der er tilføjet. Det bør også verificeres på jernbanesystemniveau, at ændringen er acceptabel i sin helhed.



Figur 9: Pyramide over risikoacceptkriterier (RAC)

- [G 2] De eksplicitte risikoacceptkriterier, som skal bruges til at understøtte den gensidige anerkendelse mellem medlemsstaterne, vil blive harmoniseret i det løbende arbejde, som agenturet udfører vedrørende risikoacceptkriterier. Når yderligere oplysninger bliver tilgængelige, vil de blive indarbejdet i dette dokument.
- [G 3] I mellemtiden kan risiciene evalueres ved hjælp af f.eks. risikomatricen, som findes i afsnit 4.6 i EN 50126-1-standarden {Ref. 8}. Andre typer egnede kriterier kan også bruges, forudsat at disse kriterier vurderes at sikre et acceptabelt sikkerhedsniveau i det pågældende tilfælde.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere detaljer om RAC-TS samt hvilke aspekter og funktioner i det tekniske system, som kriteriet gælder, er angivet i et særskilt notat fra agenturet, som udgør et tillæg til nærværende dokument: se afsnit A.3. i tillæg A og referencedokument {Ref. 11}.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

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] Yderligere forklaring anses ikke for nødvendig.

3. PÅVISNING AF OVERENSSTEMMELSE MED SIKKERHEDSKRAV

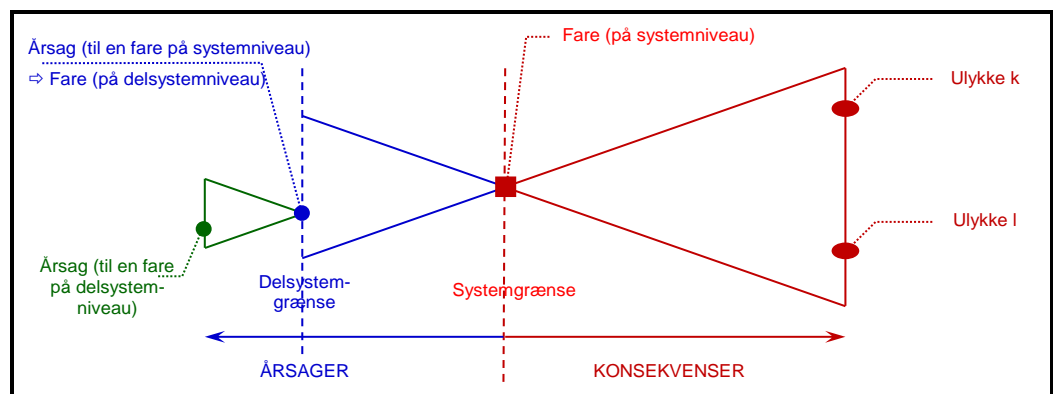
3.1. *Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.*

[G 1] Som forklaret i punkt [G 3] til [G 6] i afsnit 2.1.1 omfatter "påvisningen af systemets overensstemmelse med sikkerhedskravene" fase "6-10" af CENELEC's V-cyklus (jf. boks 3 i Figur 5). Se punkt [G 3] i afsnit 2.1.1.

[G 2] Se også punkt [G 4] i afsnit 2.1.1 i nærværende 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.*

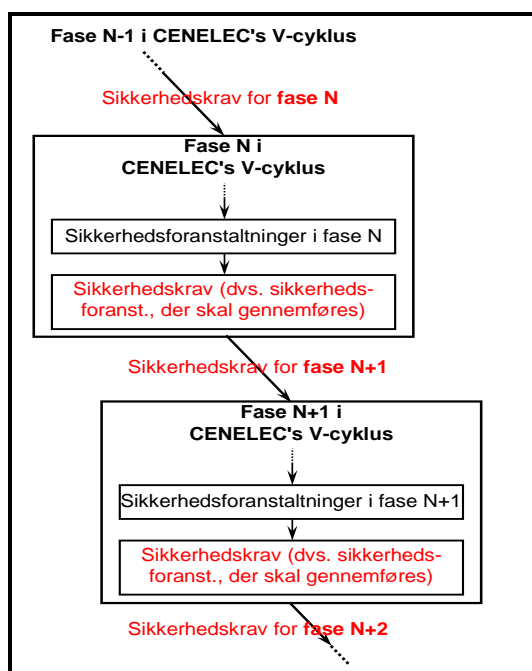
[G 1] Et eksempel på sikkerhedsvurderinger og sikkerhedsanalyser, som kan udføres på delsystemniveau, er kausale analyser: Se Figur 10. Men enhver anden metode kan bruges til at påvise delsystemets overensstemmelse med inputsikkerhedskravene.



**Figur 10: Figur A.4 i EN 50129:
Definition af farer med hensyn til systemets grænser**

[G 2] Den hierarkiske strukturering af farer og årsager, for så vidt angår systemer og delsystemer, kan gentages for hver fase på lavere niveau i CENELEC's V-cyklus i Figur 5. Fareidentifikationen og den kausale analyse (eller enhver relevant metode) samt brugen af adfærdskodekser, lignende referencesystemer og eksplicite analyser og evalueringer kan også gentages for hver fase i systemudviklingscyklussen for – af de sikkerhedsforanstaltninger, der er identificeret på delsystemniveau – at udlede, hvilke sikkerhedskrav der skal opfyldes i næste fase. Det er illustreret i Figur 11.

[G 3] Se også punkt [G 4] i afsnit 2.1.1 i nærværende dokument.



Figur 11: Udledning af sikkerhedskrav for faser på lavere niveau

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] Alle aktiviteter vist i boks3⁽¹⁴⁾ i CENELEC's V-cyklus i Figur 5 bliver derfor også vurderet uafhængigt.
- [G 2] Detaljetyper og -graden af den uafhængige vurdering, der udføres af et vurderingsorgan (dvs. detaljeret eller makroskopisk vurdering), er omhandlet i forklaringerne til 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] F.eks. kunne brandslukningsmetoden føre til en ny fare (kvælning), som vil kræve nye sikkerhedskrav (f.eks. en specifik procedure for evakuering af passagerer). Et andet eksempel er anvendelse af hærdet glas til at undgå, at vinduerne springer i stykker ved sammenstød, og at passagererne kvæstes af glas eller endda kastes ud af toget. Den nye fare, der påføres, er, at evakuering af vognene gennem vinduerne i nødsituationer vanskeliggøres betydeligt, hvilket kan

⁽¹⁴⁾ Sammenhængen i aktiviteterne mellem de fælles sikkerhedsmetoder og Figur 5 (dvs. figur 10 i CENELEC's 50126 V-cyklus) er beskrevet i afsnit 2.1.1. Navnlig punkt [G 3] i afsnit 2.1.1 opregner, hvilke CENELEC-aktiviteter der er omfattet af den fælles sikkerhedsmetodes fase "påvisning af systemets overensstemmelse med sikkerhedskravene".

resultere i sikkerhedskrav om, at visse vinduer skal være specifikt udformet til at tillade evakuering.

[G 2] Eksempel på en driftsændring: Det kræves, at al transport af farligt gods forbydes på strækninger, der går gennem tætbefolkede områder. I stedet skal den foregå ad alternative ruter med tunneler og skaber derfor andre typer fare.

[G 3] Andre eksempler på nye farer, som kunne blive identificeret under påvisningen af systemets overensstemmelse med sikkerhedskravene, findes i tillæg A.4.3 i EN 50129-standard.

4. FAREHÅNTERING

4.1. Farehåndteringsprocessen

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] Anvendelsen af en fareredegørelse (hasardlog) til registrering, styring og kontrol med sikkerhedsrelevant information anbefales også i henhold til CENELEC-standarderne 50126-1 {Ref. 8} og 50129 {Ref. 7}.
- [G 2] F.eks. kunne en aktør alt efter systemets kompleksitet have enten en eller flere fareredegørelser. I begge tilfælde skal vurderingsorganet(erne) foretage en uafhængig vurdering af fareredegørelsen/fareredegørelserne. F.eks. kunne en mulig løsning være at have:
- (a) en "intern fareredegørelse" til styring af alle interne sikkerhedskrav, der gælder for delsystemet, som aktøren er ansvarlig for. Størrelsen og håndteringsarbejds omfang afhænger af redegørelsens struktur og naturligvis af delsystemets kompleksitet. Da den imidlertid bruges til interne håndteringsformål, skal fareredegørelsen ikke kommunikeres til andre aktører. Den interne fareredegørelse indeholder alle de identificerede farer, som er kontrolleret, samt de tilknyttede sikkerhedsforanstaltninger, som er valideret
 - (b) en "ekstern fareredegørelse" til overførsel til andre aktører af farer og de tilknyttede sikkerhedsforanstaltninger (som aktøren ikke kan gennemføre fuldt ud alene) i overensstemmelse med afsnit 1.2.2. Sædvanligvis er denne anden fareredegørelse mindre og kræver mindre håndteringsarbejde (jf. eksemplet i afsnit C.16.3. i tillæg C).
- [G 3] Hvis det forekommer kompliceret at styre flere forskellige fareredegørelser, er en anden mulig løsning at styre alle farer og de tilknyttede sikkerhedsforanstaltninger, som er omfattet af punkt (a) og (b) ovenfor, i en enkelt fareredegørelse, men med mulighed for at udskrive to fareredegørelsesrapporter (jf. eksemplet i afsnit C.16.3. i tillæg C):
- (a) en intern fareredegørelsesrapport, som endda måske er overflødig, hvis fareredegørelsen er velstruktureret for at muliggøre uafhængig vurdering
 - (b) en ekstern fareredegørelsesrapport til overførsel af farer og de tilknyttede sikkerhedsforanstaltninger til andre aktører.
- [G 4] Som forklaret i afsnit 4.2 sker følgende ved afslutningen af projektet, når systemet er accepteret:
- (a) Alle farer, som er overført til andre aktører, er kontrolleret i den eksterne fareredegørelse hos den aktør, der overfører dem. Da de importeres og styres i den interne fareredegørelse hos de øvrige aktører, skal de ikke styres yderligere af den pågældende aktør i løbet af delsystemets livscyklus.
 - (b) Imidlertid bør ikke alle de tilknyttede sikkerhedsforanstaltninger valideres i fareredegørelsen af årsager, der er forklaret i punkt [G 9] i afsnit 4.2. Det er nemlig

nyttigt, at organisationen, der eksporterer anvendelsesrestriktionerne, klart påpeger i sin fareredegørelse, at de tilknyttede sikkerhedsforanstaltninger ikke var validerede.

- [G 5] Omvendt vedligeholdes alle interne fareredegørelser i hele (del)systemets livscyklus. Dette gør det muligt at spore fremskridtene med hensyn til overvågning af risici forbundet med de identificerede farer i løbet af (del)systemets drift og vedligeholdelse, dvs. også efter ibrugtagning: Se boks 4 i CENELEC's V-cyklus 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] Informationen om farer og de tilknyttede sikkerhedsforanstaltninger, som modtages fra andre aktører (jf. afsnit 1.2.2) inkluderer også alle de antagelser⁽¹⁵⁾ og anvendelsesrestriktioner⁽¹⁵⁾ (også kaldet sikkerhedsrelaterede anvendelsesbetingelser), der gælder for de forskellige delsystemer og de generiske anvendelses- og generiske produktsikkerhedscases (safety case benævnes også sikkerhedsdokumentation på dansk), som udarbejdes af fabrikanterne, hvor det er relevant.
- [G 2] Et eksempel på en eventuel struktur for fareredegørelsen er beskrevet i afsnit C.16. i tillæg C.

4.2. Udveksling af oplysninger

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] F.eks. kan fabrikanten, for så vidt angår delsystemet vejimpuls giver i ETCS's mobile udstyr, validere algoritmerne i laboratoriet ved at simulere de teoretiske signaler, som kunne blive genereret af de tilhørende vejimpuls giversensorer. Den fuldstændige validering af delsystemet vejimpuls giver kræver imidlertid hjælp fra JV og I til at udføre valideringen ved brug af et rigtigt tog og den rigtige kontakt mellem togets hjul og skinnerne.
- [G 2] Andre eksempler kunne være overførsler fra fabrikanterne til jernbanevirksomhederne af drifts- eller vedligeholdelsessikkerhedsforanstaltninger til teknisk udstyr. Disse sikkerhedsforanstaltninger skal iværksættes af jernbanevirksomheden.
- [G 3] For at behandle disse farer, de tilknyttede sikkerhedsforanstaltninger og risici, der skal revurderes i fællesskab af de berørte organisationer, er det nyttigt, hvis organisationen, der har identificeret dem, tilvejebringer alle de forklaringer, der er nødvendige for at få klarlagt

⁽¹⁵⁾ Se punkt [G 5] i afsnit 1.1.5 og fodnote ⁽⁹⁾ og ⁽¹⁰⁾ på side 28 i dette dokument med hensyn til yderligere forklaring af terminologien "generiske produkt- og generiske anvendelsessikkerhedscases", "antagelser og anvendelsesrestriktioner".

problemet fuldt ud. Det er muligt, at farebeskrivelsens, sikkerhedsforanstaltningernes og risicienes oprindelige ordlyd skulle ændres for at gøre dem forståelige, uden at de skulle drøftes igen i fællesskab. Den fælles revurdering af farerne kunne medføre identifikation af nye sikkerhedsforanstaltninger.

[G 4] Den modtagende aktør, der er ansvarlig for gennemførelse, verificering og validering af de modtagne eller nye sikkerhedsforanstaltninger, registrerer alle de relaterede farer i sin egen fareredegørelse sammen med de tilknyttede sikkerhedsforanstaltninger (både importerede og dem, der er identificeret i fællesskab).

[G 5] Når en sikkerhedsforanstaltning ikke er fuldt valideret, skal en klar anvendelsesbegrænsning (f.eks. driftsmæssige afbødningsforanstaltninger) udarbejdes og registreres i fareredegørelsen. Det kan nemlig ske, at tekniske/konstruktionsmæssige sikkerhedsforanstaltninger:

- (a) ikke er korrekt gennemført eller
- (b) ikke er fuldt gennemført eller
- (c) bevidst ikke er gennemført, f.eks. fordi der er gennemført andre sikkerhedsforanstaltninger end dem, der er registreret i fareredegørelsen (f.eks. til omkostningsformål). Da de ikke er valideret, skal disse sikkerhedsforanstaltninger tydeligt identificeres i fareredegørelsen. Og der skal tilvejebringes bevis/belæg for, hvorfor de sikkerhedsforanstaltninger, der er gennemført i stedet for⁽¹⁶⁾, er egnede, samt en påvisning af, at systemet med de andre sikkerhedsforanstaltninger stemmer overens med sikkerhedskravene
- (d) osv.

I disse tilfælde kan de tilhørende tekniske/konstruktionsmæssige sikkerhedsforanstaltninger ikke verificeres og valideres under farehåndteringen. De relaterede farer og sikkerhedsforanstaltninger skal derefter forblive åbne i fareredegørelsen for at undgå forkert brug af sikkerhedsforanstaltningerne til andre systemer ved anvendelse af risikoacceptprincippet "et lignende referencesystem".

[G 6] Normalt påvises de sikkerhedsforanstaltninger, der er "ikke korrekt" og/eller "ikke fuldt" gennemført, tidligt i systemets livscyklus og korrigeres før systemaccept. Hvis en teknisk sikkerhedsforanstaltning imidlertid påvises for sent til at blive gennemført korrekt og fuldt ud, skal den organisation, som er ansvarlig for gennemførelse og styring, identificere og i fareredegørelsen registrere klare anvendelsesrestriktioner for det system, der vurderes. Disse anvendelsesrestriktioner er ofte driftsmæssige anvendelsesbegrænsninger for det system, der vurderes.

[G 7] Det kunne også være nyttigt at registrere i fareredegørelsen, om de tilknyttede sikkerhedsforanstaltninger vil blive korrekt gennemført på et senere stadium i systemets livscyklus, eller om systemet fortsat vil blive brugt med de identificerede anvendelsesbegrænsninger. Det kunne også være nyttigt at registrere i fareredegørelsen, hvad begrundelsen er for ikke at gennemføre de tilknyttede tekniske sikkerhedsforanstaltninger korrekt/fuldt ud.

[G 8] Aktøren, som modtager anvendelsesrestriktionerne:

- (a) importerer dem alle i sin egen fareredegørelse

⁽¹⁶⁾ Hvis der iværksættes andre sikkerhedsforanstaltninger end de oprindeligt specificerede, skal de også registreres i fareredegørelsen.

- (b) sikrer, at betingelserne for brug af det system, der vurderes, er i overensstemmelse med alle de modtagne anvendelsesrestriktioner, og
- (c) verificerer og validerer, at systemet, der vurderes, overholder disse anvendelsesrestriktioner.

[G 9] Afhængigt af beslutningerne, der er truffet i fællesskab af de berørte organisationer:

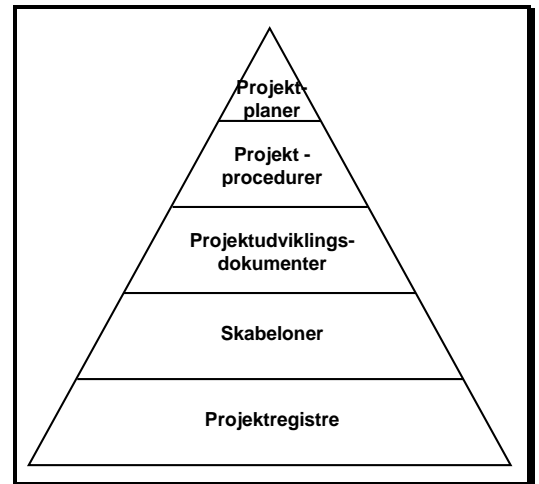
- (a) bliver enten de tilknyttede tekniske sikkerhedsforanstaltninger gennemført korrekt i konstruktionen på et senere stadium.
Organisationen, der eksporterer anvendelsesrestriktionerne, fortsætter med at spore den korrekte tekniske gennemførelse af de tilknyttede sikkerhedsforanstaltninger. Følgelig kan de tilhørende sikkerhedsforanstaltninger ikke valideres, og farer, der er forbundet med dem, kan ikke kontrolleres i fareredegørelsen hos denne organisation, så længe den tilsvarende tekniske sikkerhedsforanstaltning ikke er fuldt gennemført. Dette skal sikres, selv om de eksporterede anvendelsesrestriktioner i mellemtiden er blevet indført
- (b) eller de tilknyttede tekniske sikkerhedsforanstaltninger bliver ikke gennemført i konstruktionen på et senere stadium. Systemet vil dermed fortsat blive brugt i hele sin livscyklus med de tilhørende anvendelsesrestriktioner. I dette tilfælde kan der enten foregå det:
 - (1) at organisationen, der eksporterer anvendelsesrestriktionerne, ikke registrerer de tilknyttede sikkerhedsforanstaltninger som "validerede" i fareredegørelsen. På denne måde vil de tilsvarende sikkerhedsproblemer ikke blive overset, når det relaterede system bruges som referencesystem i andre projekter. Så selv om en anden aktør accepterer at styre de tilhørende risici anderledes, er det nyttigt, at organisationen, der eksporterer anvendelsesrestriktionerne, tydeligt påpeger i sin fareredegørelse, at de tilknyttede sikkerhedsforanstaltninger ikke blev valideret, eller
 - (2) at systembeskrivelsen ændres, så den omfatter anvendelsesrestriktioner for systemets anvendelse (dvs. antagelserne for systemet) og i sikkerhedskravene. Det vil gøre det muligt at kontrollere farerne. Så hvis systemet bruges som et referencesystem i en anden anvendelse:
 - (i) vil det nye system skulle anvendes på de samme betingelser (dvs. overholde de anvendelsesrestriktioner, der er forbundet med disse antagelser), eller
 - (ii) initiativtageren skal foretage en yderligere risikovurdering med hensyn til afvigelserne i forhold til disse antagelser.

5. Dokumentation FRA ANVENDELSEN AF RISIKOSTYRINGSPROCESSEN

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] Der er allerede taget højde for disse krav i infrastrukturforvalterens og jernbanevirksomhedens sikkerhedsledelsessystem (SMS). For så vidt angår de øvrige aktører i jernbanesektoren, der er involveret i den væsentlige ændring, men for hvem SMS ikke er obligatorisk, i hvert fald ikke generelt på projektniveau, så har de en kvalitetsledelsesproces (QMP) og/eller en sikkerhedsledelsesproces (SMP). Begge disse processer bygger på et struktureret dokumentationshierarki enten på virksomhedsniveau eller som minimum på projektniveau. De dækker også dokumentationsbehovet vedrørende RAMS. En sådan struktureret dokumentation kan grundlæggende opbygges af følgende (jf. også Figur 12):

- (a) **Projektplaner** udarbejdet for at beskrive den organisation, der skal opbygges for at styre en aktivitet i et givet projekt
- (b) **Projektprocedurer** udarbejdet for at beskrive i detaljer, hvordan en bestemt opgave skal udføres. Sædvanligvis findes der procedurer og instrukser i virksomheden, der også bruges som sådan. Nye projektprocedurer udarbejdes kun, hvis der er behov for at beskrive en specifik opgave i det pågældende projekt
- (c) **Projektudviklingsdokumenter** udarbejdet i løbet af systemets livscyklus og vist i Figur 5
- (d) **Virksomheds- eller som minimum projektskabeloner** findes for de forskellige typer dokumenter, der skal udfærdiges
- (e) **Projektregistre** udarbejdet i løbet af systemets livscyklus og nødvendige for at påvise, at virksomhedens kvalitetsledelses- og sikkerhedsledelsesprocesser er overensstemmende.



Figur 12: Struktureret dokumentationshierarki

Det er en af måderne at opfylde behovet for dokumenteret bevis på. Der kan være andre måder at gøre det på, blot CSM-kravene er opfyldt.

[G 2] CENELEC-standarderne anbefaler at påvise systemets overensstemmelse med funktions- og sikkerhedskrav i et sikkerhedscasedokument (eller en sikkerhedsrapport). Selv om det ikke er obligatorisk, tilvejebringer sikkerhedscasen følgende i et struktureret dokument, som giver belæg for sikkerheden:

- (a) bevis for kvalitetsledelse
- (b) bevis for sikkerhedsledelse
- (c) bevis for funktionssikkerhed og teknisk sikkerhed.

Samtidig har det den fordel, at det støtter og vejleder vurderingsorganet(erne) i den uafhængige vurdering af den korrekte anvendelse af CSM.

[G 3] Sikkerhedscasen beskriver og resumerer, hvordan projektdokumenterne, der hidrører fra anvendelsen af kvalitets- og/eller sikkerhedsledelsesprocesserne på virksomheds- eller projektniveau, er forbundet indbyrdes i systemudviklingsprocessen med henblik på at påvise systemets sikkerhed. Normalt indeholder sikkerhedscasen ikke store mængder detaljerede beviser og understøttende dokumentation, men giver præcise henvisninger til disse dokumenter.

[G 4] **Sikkerhedscase vedrørende tekniske systemer:** CENELEC-standarderne kan bruges som retningslinjer for udfærdigelse og/eller strukturering af sikkerhedscases:

- (a) Se EN 50129-standardens {Ref. 7} for "Jernbaneanvendelser – Kommunikation, signalering og databehandlingssystemer og sikkerhedsrelaterede elektroniske systemer til signaludstyr". Tillæg H.2 til vejledningen hertil, vejledningen EN 50126-2 {Ref. 9} giver også forslag til en struktur for sikkerhedscasen vedrørende signalsystemer
- (b) Se tillæg H.1 til vejledningen, EN 50126-2 {Ref. 9} til struktur for sikkerhedscasen vedrørende rullende materiel
- (c) Se tillæg H.3 til vejledningen EN 50126-2 {Ref. 9} om strukturen for sikkerhedscasen vedrørende infrastruktur

Som det fremgår af disse referencer, afhænger såvel struktur som indhold af sikkerhedscasen vedrørende tekniske systemer af det system, hvis sikkerhedsoverensstemmelse skal påvises.

Sikkerhedscasen beskrevet i tillæg H til vejledningen EN 50126-2 {Ref. 9} giver kun eksempler og er muligvis ikke egnet til alle systemer af den givne type. Derfor skal beskrivelsen anvendes med et passende skøn af, hvad der egner sig til den enkelte anvendelse.

[G 5] **Sikkerhedscase vedrørende organisatoriske og driftsmæssige aspekter af jernbanesystemer:**

Der findes i dag ikke en særlig standard, der leverer struktur og indhold samt retningslinjer for udfærdigelse af sikkerhedscasen vedrørende organisatoriske og driftsmæssige aspekter af et jernbanesystem. Da sikkerhedscasen imidlertid har til formål på struktureret vis at påvise systemets overensstemmelse med sikkerhedskravene, kan der anvendes samme type sikkerhedscasestruktur som for tekniske systemer. Referencerne i punkt [G 4] i afsnit 5.1 giver da også råd og en tjekliste over punkter, der skal gennemgås, uanset hvilken type system, der vurderes. Styring af organisatoriske og driftsmæssige ændringer kræver samme type kvalitetsledelses- og sikkerhedsledelsesprocesser som tekniske ændringer, herunder påvisning af systemets overensstemmelse med de specificerede sikkerhedskrav. De krav i CENELEC-standarderne, der ikke gælder organisatoriske og driftsmæssige aspekter, er krav, som udelukkende er knyttet til tekniske systemkonstruktionsfaciliteter, f.eks. principper om "inherent hardware fail-safety", elektromagnetisk kompatibilitet (EMC, Electro-Magnetic Compatibility) osv.

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] Afhængigt af systemets kompleksitet kan disse beviser samles i en eller flere sikkerhedscases. Se henholdsvis punkt [G 4] og [G 5] i afsnit 5.1 med hensyn til strukturen i sikkerhedscasen for tekniske systemer og for organisatoriske og driftsmæssige aspekter.
- [G 2] Se også afsnit A.4. i tillæg A med hensyn til mulige eksempler på beviser.
- [G 3] Tekniske systemer og delsystemer i jernbanesektoren forventes generelt at have en levetid på ca. 30 år. Over så lang en periode må der også forventes at blive foretaget en række væsentlige ændringer i disse systemer. Derfor vil der formentlig blive gennemført risikovurderinger af disse systemer og deres grænseflader med ledsagende dokumentation, som skal gennemgås, suppleres og overføres mellem forskellige aktører og organisationer ved hjælp af fareredegørelser. Dette indebærer temmelig strenge krav til dokumentationskontrol og konfigurationsstyring.
- [G 4] Det er derfor nyttigt, at virksomheden, der arkiverer alle risikovurderinger og risikostyringsoplysninger, garanterer, at resultater/oplysninger gemmes på et fysisk medium, som kan læses/gøres tilgængeligt under hele systemets levetid/livscyklus (f.eks. 30 år).
- [G 5] De primære grunde til dette krav er bl.a.:
- (a) at det skal sikres, at alle sikkerhedsanalyser og sikkerhedslogger vedrørende det system, der vurderes, er tilgængelige i hele systemets levetid. F.eks.:
 - (1) at den seneste systemdokumentation er tilgængelig i tilfælde af yderligere væsentlige ændringer af samme system
 - (2) at det er nyttigt i tilfælde af problemer i systemets levetid at kunne gå tilbage i de tilhørende sikkerhedsanalyser og sikkerhedslogger
 - (b) at sikkerhedsanalyserne og sikkerhedsloggerne for det system, der vurderes, skal være tilgængelige, såfremt systemet bruges i en anden anvendelse som et lignende referencesystem.

BILAG II TIL CSM-FORORDNINGEN

Kriterier, som vurderingsorganerne skal opfylde

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] Yderligere forklaring anses ikke for nødvendig.

TILLÆG A: YDERLIGERE AFKLARING

A.1. Indledning

- A.1.1. Formålet med dette tillæg er at lette læsningen af nærværende dokument. I stedet for at give store mængder information i dokumentet forklares mere komplekse emner yderligere i dette tillæg.

A.2. Fareklassificering

- A.2.1. Der gives en vejledning i afsnit 4.6.3. i EN 50126-1-standarden {Ref. 8} samt i tillæg B.2 til vejledningen EN 50126-2 {Ref. 9} til, hvordan man klassificerer/ordner farer.

A.3. Risikoacceptkriterier for tekniske systemer (RAC-TS)

A.3.1. Øvre grænse for risikoaccept for tekniske systemer

- A.3.1.1. RAC-TS er beskrevet i afsnit 2.5.4. i {Ref. 4}.
- A.3.1.2. Formålet med RAC-TS er at specificere en øvre grænse for risikoaccept for tekniske systemer, for hvilke sikkerhedskravene hverken kan udledes af anvendelsen af adfærdskodekser eller ved sammenligning med lignende referencesystemer. RAC-TS definerer derfor et referencepunkt, ud fra hvilket risikoanalysemetoderne for de tekniske systemer kan kalibreres. Som beskrevet i afsnit A.3.6. i tillæg A til dette dokument kunne dette referencepunkt eller denne øvre grænse for risikoaccept også bruges til at fastslå de risikoacceptkriterier for andre funktionssvigt i tekniske systemer, som ikke har et muligt direkte potentiale for katastrofale følger (dvs. for andre alvorligheder). Men RAC-TS er ikke en metode til risikoanalyse.
- A.3.1.3. RAC-TS er et semikvantitativt kriterium. Det gælder både for tilfældige hardwaresvigt og systematiske svigt/fejl i det tekniske system. De systematiske svigt/fejl i det tekniske system, der potentielt kan hidrøre fra menneskelige fejl under udvikling af det tekniske system (dvs. specifikation, konstruktion, gennemførelse og validering) er dermed også dækket. Men de menneskelige fejl under drift og vedligeholdelse af de tekniske systemer er ikke dækket af RAC-TS.
- A.3.1.4. Ifølge tillæg A.3 og A.4 til CENELEC 50129-standardens er systematiske svigt/fejl ikke kvantificerbare, hvorfor de kvantitative mål kun skal påvises, for så vidt angår tilfældige hardwaresvigt, mens de systematiske svigt/fejl behandles med kvalitative metoder⁽¹⁷⁾. *"Fordi det ikke er muligt at vurdere systematisk fejlintegritet ved hjælp af kvantitative metoder, anvendes sikkerhedsintegritetsniveauer (SIL) til at gruppere metoder, værktøjer og teknikker, som brugt effektivt anses for at sikre et passende konfidensinterval i virkeliggørelsen af et system til et angivet integritetsniveau."*

⁽¹⁷⁾ Ifølge CENELEC-standarderne 50126, 50128 og 50129 skal mængdetallet for tilfældige hardwaresvigt altid forbindes med et sikkerhedsintegritetsniveau, der kan håndtere de systematiske svigt/fejl. Derfor kræver RAC-TS-tallet $10^{-9} h^{-1}$ også, at der indføres en tilstrækkelig proces med henblik på at håndtere de systematiske svigt/fejl korrekt. Men for at lette læsningen af noten henvises der ofte kun til tilfældige hardwaresvigt i det tekniske system.

A.3.1.5. Ligeledes ifølge CENELEC-standarderne er integriteten i tekniske systemers software ikke kvantificerbar. CENELEC 50128 standarden giver vejledning i udvikling af sikkerhedsrelateret software alt efter det påkrævede sikkerhedsintegritetsniveau. Heri indgår konstruktion, verifikation, validering og kvalitetssikringsprocesser for softwaren. Ifølge CENELEC 50128-standarden er det højest mulige sikkerhedsintegritetsniveau for softwareudviklingsprocessen for et programmerbart elektronisk kontrolsystem, der gennemfører sikkerhedsfunktioner, SIL 4, som svarer til en kvantitativ acceptabel farerisiko på 10^{-9} h^{-1} .

A.3.1.6. Da de systematiske svigt/fejl ikke kan kvantificeres, skal de derfor i stedet styres kvalitativt ved at indføre en kvalitets- og sikkerhedsproces, som er forenelig med det sikkerhedsintegritetsniveau, der er nødvendigt for det system, der vurderes.

- (a) Formålet med kvalitetsprocessen er *"at minimere indvirkningen af menneskelige fejl på det enkelte stadium i livscyklussen og dermed reducere risikoen for systematiske svigt i systemet"*.
- (b) Formålet med sikkerhedsprocessen er *"at reducere indvirkningen af sikkerhedsrelaterede menneskelige fejl yderligere gennem hele livscyklussen og dermed minimere den resterende risiko for sikkerhedsrelaterede systematiske svigt."*

A.3.1.7. Der gives i nedenstående standarder vejledning i styring af indvirkningen af systematiske svigt/fejl samt vejledning i eventuelle konstruktionsmæssige foranstaltninger for at beskytte mod Common Cause/Mode Failures (CCF/CMF) og sikre, at det tekniske system går i en fejlsikret tilstand i tilfælde af sådanne svigt/fejl:

- (a) CENELEC 50126-1-standardens {Ref. 8} og den tilhørende vejledning 50126-2 {Ref. 9} opregner bestemmelserne i CENELEC 50129 og deres anvendelighed som dokumenteret bevis på andre systemer end signalering: Se tabel 9.1 i vejledning 50126-2 {Ref. 9}. Listen indeholder henvisninger til vejledningen i, hvordan man håndterer såvel de svigt, der hidrører fra systemet selv, som miljøpåvirkningen af det system, der vurderes.

F.eks. gives der teknikker/foranstaltninger for konstruktionsdata i *tabel E.5: Konstruktionsegenskaber (som der henvises til i 5.4)"* i CENELEC 50129-standardens {Ref. 7}, *for at undgå og kontrollere fejl, som forårsages af:*

- (1) *eventuelle resterende konstruktionsfejl*
- (2) *miljøbetingelser*
- (3) *fejlagtig anvendelse eller driftsrelaterede fejl*
- (4) *eventuelle resterende fejl i softwaren*
- (5) *menneskelige faktorer.*

Tillæg D og E til CENELEC 50129-standardens {Ref. 7} giver teknikker og foranstaltninger til forebyggelse af systematiske fejl og kontrol med tilfældige hardwaresvigt/fejl og systematiske svigt/fejl i sikkerhedsrelaterede elektroniske systemer inden for signalering. Mange af dem kan udvides til andre systemer end signalering via en reference til disse retningslinjer i tabel 9.1 i vejledningen 50126-2 {Ref. 9}.

- (b) CENELEC 50128-standardens giver vejledning i udvikling af sikkerhedsrelateret software alt efter det sikkerhedsintegritetsniveau (SIL 0 til SIL 4), der er påkrævet for softwaren i det system, der vurderes.

A.3.1.8. RAC-TS repræsenterer også det højeste integritetsniveau, der kan kræves ifølge både CENELEC- og IEC-standarderne. For at befordre læsningen er kravene i IEC 61508-1 og CENELEC 50129 citeret her:

- (a) IEC 61508-1: *"Denne standard fastsætter en nedre grænse i en farlig svigttilstand for de måltal for fejloperationer, der kan stilles krav om. Disse specificeres som de nedre grænser for SIL 4. Det er måske muligt at konstruere sikkerhedsrelaterede systemer med lavere værdier for måltal for fejloperationer for ikkekomplekse systemer, men det vurderes, at tallene i tabellen udgør grænsen for, hvad der kan opnås for relativt komplekse systemer (f.eks. programmerbare elektroniske sikkerhedsrelaterede systemer) på nuværende tidspunkt."*
- (b) EN 50129: *"En funktion, der stiller mere krævende kvantitative krav end $10^{-9} h^{-1}$, skal behandles på en af følgende måder:*
 - (1) *hvis det er muligt at dele funktionen i funktionelt uafhængige delfunktioner, kan THR deles mellem disse delfunktioner og et SIL, der er beregnet for hver delfunktion;*
 - (2) *hvis funktionen ikke kan deles, skal som minimum de tal og metoder, der gælder i forbindelse med SIL 4, være overholdt, og funktionen skal anvendes i kombination med andre tekniske regler eller driftsregler for at nå den nødvendige THR."*

A.3.1.9. Alle tekniske systemer skal dernæst begrænse de kvantitative sikkerhedskrav til det tal. Hvis der er behov for et højere beskyttelsesniveau, kan det ikke nås med kun ét system. Systemets arkitektur skal ændres, f.eks. ved at bruge to uafhængige systemer parallelt, som krydstjekker hinanden indbyrdes, så der genereres sikre resultater. Men dette øger absolut omkostningerne ved udviklingen af det tekniske system.

Bemærkning: Hvis der findes eksisterende funktioner, f.eks. rent mekaniske systemer, som måske baseret på driftserfaring kan have nået et højere integritetsniveau, kan sikkerhedsniveauet beskrives ved en bestemt adfærdskodeks, eller sikkerhedskravene kan blive fastsat ved en analyse af ligheden med det eksisterende system. I forbindelse med CSM skal RAC-TS kun bruges, hvis der ikke findes en adfærdskodeks eller et referencesystem.

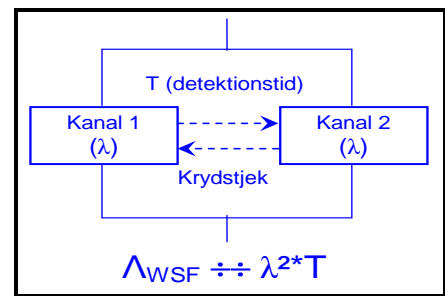
A.3.1.10. Der kan herefter opsummeres som følger:

- (a) Ifølge CENELEC-standarderne 50126, 50128 og 50129 er systematiske svigt/fejl i udviklingsprocessen ikke kvantificerbare.
- (b) Indvirkningen af systematiske svigt/fejl samt den resterende risiko skal kontrolleres og styres ved anvendelse af egnede kvalitets- og sikkerhedsprocesser, som er forenelige med det sikkerhedsintegritetsniveau, som er påkrævet for det system, der vurderes.
- (c) Det højeste opnåelige sikkerhedsintegritetsniveau er SIL 4 både for tilfældige hardwaresvigt og de systematiske svigt/fejl i tekniske systemer.
- (d) Denne grænse for sikkerhedsintegritetsniveauet på SIL 4 indebærer, at den maksimale acceptable farerisiko (dvs. den maksimale svigtrate) for tekniske systemer også skal begrænses til $10^{-9} h^{-1}$.

A.3.1.11. En maksimal acceptabel farerisiko på 10^{-9} h^{-1} kan nås af det tekniske system med enten en "fejsikret arkitektur" (som pr. definition opfylder et sådant sikkerhedsniveau) eller en "redundant arkitektur" (f.eks. to indbyrdes uafhængige behandlingskanaler, der krydstjekker hinanden).

For en redundant arkitektur gælder, at det kan vises, at den overordnede defekt i sikringsanlæg (Λ_{WSF}) (WSF = Wrong Side Failure) i det tekniske system er proportional med $\lambda^2 \cdot T$, hvor:

- λ^2 er kvadratet på defektraten på én kanal
- T er den tid, der er nødvendig for, at én kanal kan påvise defekter i sikringsanlæg på den anden kanal. Dette er normalt et multiplum af behandlingstiden/-cyklussen i en kanal. Normalt er T langt under 1 sekund.



Figur 13: Redundant arkitektur i et teknisk system

A.3.1.12. På basis af denne formel ($\lambda^2 \cdot T$) kan det teoretisk set påvises (kun med hensyn til tilfældige hardware-sigt i det tekniske system – jf. også punkt A.3.1.13. i tillæg A), at et kvantitativt krav til RAC-TS på 10^{-9} h^{-1} kan opfyldes. De systematiske svigt/fejl skal styres af en proces: Se punkt A.3.1.6. i tillæg A. For eksempel:

- med en MTBF (Mean Time Between Failures) på 10.000 timer som troværdighedstal for en kanal og den konservative antagelse, at alle kanalsvigt er usikre, er defekten i sikringsanlægget på kanalen 10^{-4} h^{-1}
- selv med en tid på 10 minutter (dvs. $\approx 2 \cdot 10^{-3}$ timer) til at påvise defekterne i sikringsanlægget i den anden kanal, hvilket også er en konservativ antagelse,

er den overordnede defekt i sikringsanlægget $\Lambda_{\text{WSF}} \approx 2 \cdot 10^{-10} \text{ h}^{-1}$.

A.3.1.13. I praksis skal der i en sådan redundant arkitektur, når de kvantitative overordnede defekter i sikringsanlæggets hardware evalueres, tages hensyn til de foranstaltninger, der er truffet i konstruktionen for at beskytte mod Common Cause/Mode Failures (CCF/CMF) og sikre, at det tekniske system går i en fejlsikret tilstand i tilfælde af et svigt/en fejl af typen CCF/CMF. Denne evaluering af den overordnede defekt i sikringsanlæg (Λ_{WSF}) skal altså omfatte:

- de komponenter, der er fælles for alle kanaler, f.eks. enkelt eller fælles input til alle kanaler, fælles strømforsyning, komparatorer, overvågningsudstyr osv.
- den tid, der skal til for at påvise hvilende eller latente svigt. For komplekse tekniske systemer kan denne tid være adskillige størrelsesordner længere end 1 sekund
- virksomheden af Common Cause/Mode Failures (CCF/CMF).

Der findes vejledning til disse emner i standarderne, som der henvises til i punkt A.3.1.7. i tillæg A i dette dokument.

A.3.2. Flowskema for anvendelighedstesten af RAC-TS

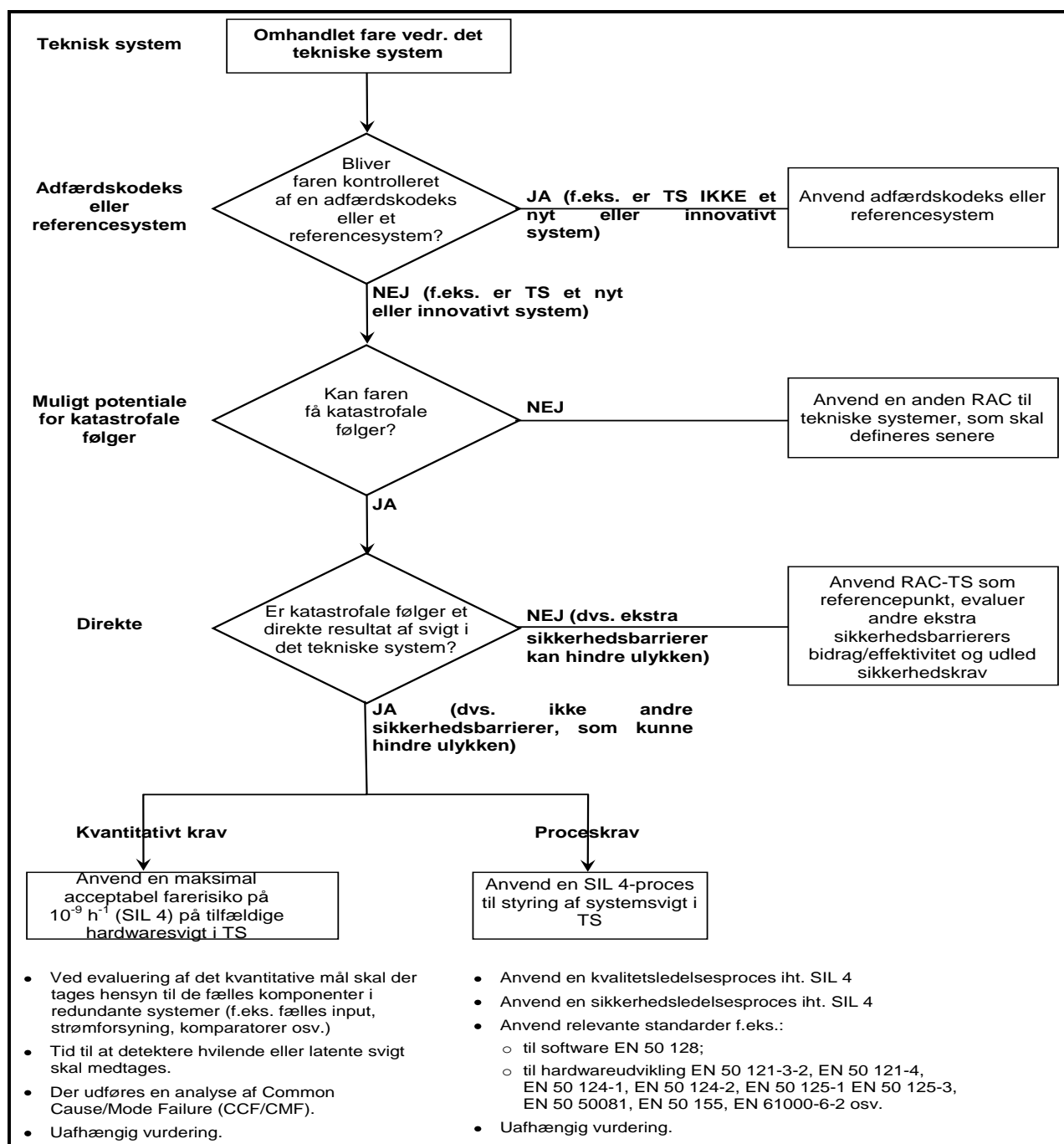
A.3.2.1. Den måde, hvorpå RAC-TS skal anvendes på farer, der opstår som følge af svigt i tekniske systemer, kan opstilles som vist i Figur 14.

A.3.2.2. Anvendelsen af dette flowskema på et eksempel gives i afsnit C.15. i tillæg C.

A.3.3. Definition af et teknisk system fra CSM

- A.3.3.1. RAC-TS gælder kun tekniske systemer. I Artikel 3(22) i CSM-forordningen gives følgende definition af et "teknisk system":

‘teknisk system’: et produkt eller en helhed af produkter, herunder udformning, implementering og dokumentation. Udviklingen af et teknisk system indledes med kravspecifikationer til dette og afsluttes med en godkendelse af systemet. Selv om udformningen af grænseflader, hvor menneskelig adfærd får betydning, tages i betragtning, inddrages menneskelige operatører og deres handlinger ikke i et teknisk system. Vedligeholdelsesprocessen beskrives i vedligeholdelseshåndbøgerne, men er ikke i sig selv en del af det tekniske system.



Figur 14: Flowskema for anvendelighedstesten af RAC-TS

A.3.4. Forklaring til definitionen af "teknisk system"

A.3.4.1. Denne definition af et teknisk system beskriver det tekniske systems anvendelsesområde: *"teknisk system": et produkt eller en helhed af produkter, herunder udformning, implementering og dokumentation.* Derfor består det af og omfatter:

(a) de fysiske dele, der udgør det tekniske system

- (b) den (eventuelle) tilhørende software
- (c) konstruktion og gennemførelse af det tekniske system, herunder hvis relevant konfigurerings eller parameterisering af et generisk produkt til specifikke krav til den specifikke anvendelse
- (d) støttedokumentation, der er nødvendig for:
 - (1) udvikling af det tekniske system
 - (2) drift og vedligeholdelse af det tekniske system.

A.3.4.2. Notaterne til denne definition specificerer yderligere afgrænsningen af det tekniske system:

- (a) *"Udviklingen af et teknisk system indledes med kravspecifikationer til dette og afsluttes med en godkendelse af systemet".* Det inkluderer faserne 1-10 af V-cyklussen vist i figur 10 i CENELEC 50126-1-standardens {Ref. 8}.
- (b) *"Selv om udformningen af grænseflader, hvor menneskelig adfærd får betydning, tages i betragtning, inddrages menneskelige operatører og deres handlinger ikke i et teknisk system."* Selv om menneskelige fejl under drift og vedligeholdelse af det tekniske system ikke indgår i selve det tekniske system, skal udformningen af grænsefladerne til menneskelige operatører tages i betragtning. Formålet er at minimere sandsynligheden for menneskelige fejl på grund af en ringe udformning af de relevante grænseflader til menneskelige operatører.
- (c) *"Vedligeholdelsesprocessen beskrives i vedligeholdelseshåndbøgerne, men er ikke i sig selv en del af det tekniske system."* Det betyder, at RAC-TS ikke behøver at blive anvendt på drift og vedligeholdelse af det tekniske system, som er stærkt afhængigt af processer og handlinger, der udføres af menneskeligt personale. For at støtte vedligeholdelsen af de tekniske systemer skal den tekniske systemdefinition imidlertid omfatte ethvert relevant krav (f.eks. periodisk forebyggende vedligeholdelse eller korrigerende vedligeholdelse i tilfælde af svigt) med et tilstrækkeligt detaljeniveau. Men hvordan vedligeholdelsen skal tilrettelægges og udføres på det tilhørende tekniske system, er ikke led i den tekniske systemdefinition, men indgår i de tilhørende vedligeholdelsesmanualer.

A.3.4.3. Se også afsnit A.3.1. i tillæg A.

A.3.5. Funktioner i de tekniske systemer, som RAC-TS anvendes på

- A.3.5.1. Ifølge definitionen af RAC-TS gælder den defekter i sikringsanlæg i funktioner, der skal varetages af det tekniske system, hvis de har "et muligt direkte potentiale for katastrofale følger" *"troværdigt direkte potentiale for katastrofale følger"*: Se afsnit 2.5.4. i {Ref. 4}.
- A.3.5.2. RAC-TS kan også anvendes på funktioner, som involverer tekniske systemer, men hvor svigtene **ikke har et** *"direkte potentiale for katastrofale følger"*. I dette tilfælde skal RAC-TS anvendes som et overordnet mål for den serie hændelser, der fører til de katastrofale følger. På basis af dette overordnede mål skal det faktiske bidrag fra hver hændelse og dermed de funktionelle svigt i det tekniske system, som er involveret i det pågældende scenario, udledes i henhold til afsnit A.3.6. i tillæg A. Denne brug af RAC-TS skal stadig drøftes og aftales med CSM-arbejdsgruppen.
- A.3.5.3. På hvilke af det tekniske systems funktioner finder RAC-TS anvendelse? Ifølge standarden IEC 61226:2005:

- (a) defineres en funktion i denne sammenhæng som et specifikt formål eller mål, der skal nås, og som kan specificeres eller beskrives uden henvisning til fysiske midler til at nå det
- (b) overfører en funktion (betragtet som en sort boks) en række inputparametre (f.eks. materiale, energi, information) til målrelaterede outputparametre (f.eks. materiale, energi, information)
- (c) er analysen af funktionen uafhængig af dens tekniske udførelse.

A.3.5.4. RAC-TS gælder alle følgende typer funktioner:

- (a) Eksempler til det mobile delsystem ETCS:
 - (1) "Giv lokoføreren information, der sætter ham i stand til at føre toget sikkert, og igangsæt en bremsefunktion i tilfælde af for høj hastighed". På grundlag af information modtaget fra de faste anlæg (tilladt hastighed) og togets hastighedscomputer i det mobile ETCS, kan lokoføreren og det mobile ETCS overvåge, at toget ikke overskrider den tilladte hastighed. RAC-TS finder anvendelse på det mobile delsystems evaluering af toghastigheden, eftersom:
 - (i) der ikke er yderligere (direkte) barrierer, idet informationen til lokoføreren også er underevalueret
 - (ii) for stor toghastighed kunne medføre afsporing, som er en ulykke med potentiale for katastrofale følger.
 - (2) "Giv lokoføreren information, der sætter ham i stand til at føre toget sikkert, og igangsæt en bremsefunktion i tilfælde af overtrædelse af den strækning, der er givet tilladelse til at tilbagelægge".
- (b) Eksempel til en sporstrømkreds: "Detektér tilstedeværelse på sporafsnittet". RAC-TS vil kun finde anvendelse som sådan på denne funktion, hvis der ikke er indlagt en "sekvensovervågningsfunktion" i sikringsystemet,
- (c) Eksempel til et punkt: "Kontrollér punktposition".

A.3.5.5. Nogle standarder definerer også funktioner, som RAC-TS kunne finde anvendelse på. For eksempel:

- (a) Standarden prEN 0015380-4 {Ref. 13} (ModTrain Work) definerer i sin normative del tre hierarkiske funktionsniveauer (udvidet i informative bilag op til fem niveauer). I alt definerer prEN 0015380-4 flere hundrede funktioner i forbindelse med tog.
- (b) Generelt anbefales det at udvælge funktioner fra de første tre niveauer af prEN 0015380-4 (men ikke under) under hensyntagen til produktprogramformen.
- (c) For funktioner, som ikke ligger inden for prEN 0015380-4-standardens anvendelsesområde, skal det passende funktionsniveau bestemmes ved sammenligning ved hjælp af en ekspertafgørelse.

Disse eksempler på funktioner fra prEN 0015380-4 kræver endnu noget bearbejdning fra agenturets side i forbindelse med arbejdet med de bredt acceptable risici og risikoacceptkriterier.

A.3.5.6. RAC-TS finder også anvendelse på f.eks. følgende funktion i prEN 0015380-4: "*control tilting*" "kurvestyring" (kode = CLB). Funktionen kunne anvendes på systemniveau på følgende to måder:

- (a) A: Toget skal kurvestyres af hensyn til passagerernes komfort og skal overvåge togprofilens overensstemmelse med den jordbaserede infrastruktur.

- (b) B: Toget skal kun kurvestyres af hensyn til passagerernes komfort, men behøver ikke overvåge togprofilets overensstemmelse med den jordbaserede infrastruktur.

I tilfælde A vil RAC-TS blive anvendt, men ikke i tilfælde B, idet svigtende kurvestyring ikke har katastrofale følger.

A.3.5.7. Eksempel (b) i punkt A.3.5.4. og eksemplerne i punkt A.3.5.6. i tillæg A viser tydeligt, at det ikke bliver muligt at opbygge en foruddefineret liste over funktioner, som RAC-TS finder anvendelse på i alle tilfælde. Det vil altid afhænge af, hvordan systemet vil bruge disse delsystemfunktioner.

A.3.5.8. Der gives et eksempel på anvendelse af RAC-TS i afsnit C.15. i tillæg C.

A.3.6. Eksempler på anvendelse af RAC-TS

A.3.6.1. Indledning

- (a) Dette kapitel viser eksempler på, hvordan man bestemmer svigtraten for de øvrige konsekvenser af farer, og hvordan mildere sikkerhedskrav end $10^{-9} h^{-1}$ kan udledes. Der foretrækkes eller foreskrives ikke nogen bestemt metode i nærværende dokument. Det vises blot til oplysning, hvordan RAC-TS kan bruges til at kalibrere nogle udbredte metoder. Der skal arbejdes videre med dette i agenturets arbejde med bredt acceptable risici og risikoacceptkriterier.
- (b) Faktisk kan RAC-TS kun anvendes direkte på et lille antal tilfælde, idet der ikke i praksis er mange funktionelle svigt i tekniske systemer, der direkte medfører ulykker med potentielt katastrofale følger. For at anvende kriteriet på farer med ikkekatastrofale følger og fastslå målraten for svigt, er det derfor muligt at udføre afvejninger (f.eks. ved at kalibrere en risikomatrix ved hjælp af dette kriterium) mellem forskellige parametre, f.eks. alvorlighed vs. hyppighed.

A.3.6.2. Eksempel 1: Direkte risikoafvejninger

- (a) RAC-TS kan let anvendes på scenarier, som kun adskiller sig ved nogle få uafhængige parametre fra referenceforholdene, der er defineret i RAC-TS i afsnit 2.5.4. i CSM-forordningen {Ref. 3}.
- (b) Lad os antage, at forholdet til risiko er multiplikativt for en bestemt parameter p. Lad os antage, at p* er til stede i referencetilstanden, mens p' er gældende i det alternative scenario. I dette tilfælde er kun parameterforholdet p*/p' relevant, og hyppigheden kan reduceres. Denne procedure kan gentages, hvis parametrene er uafhængige.
- (c) Eksempel:
- (1) Lad os antage, at det faktiske potentiale for katastrofale følger er blevet vurderet i en ekspertafgørelse til at være ti gange mindre end potentialet i referencetilstanden i afsnit 2.5.4 i CSM-forordningen {Ref. 3}. Så ville kravet være $10^{-8} h^{-1}$ i stedet for $10^{-9} h^{-1}$.
 - (2) Lad os antage, at der identificeres en yderligere sikkerhedsbarriere i et andet teknisk system (uafhængigt af følgerne), som er effektiv i 50 % af tilfældene.
 - (3) Så ville sikkerhedskravet være $5 \cdot 10^{-7} h^{-1}$ (dvs. $0.5 \cdot 10^{-8} h^{-1}$) i stedet for $10^{-9} h^{-1}$.

A.3.6.3. Eksempel 2: Risikomatrixkalibrering

- (a) Af hensyn til en korrekt anvendelse af RAC-TS i en risikomatrix skal matricen vedrøre det korrekte systemniveau (sammenligneligt med det, der gives i afsnit A.3.5. i tillæg A).

- (b) RAC-TS definerer ét felt i risikomatrixen som acceptabelt, hvilket svarer til koordinaten (katastrofal alvorlighed, 10^{-9} h^{-1} hyppighed): Se rødt felt i Tabel 5. Alle felter, som vedrører en højere hyppighed, skal mærkes "uacceptabel". Det skal bemærkes, at kun i tilfælde af et muligt direkte potentiale for katastrofale følger er ulykkeshyppigheden den samme som funktionssvighyppigheden.
- (c) Derefter kan resten af matrixen udfyldes, men der skal tages hensyn til virkninger som risikoaversion eller skalering af kategorierne. I det enkleste tilfælde med lineær dekadal skalering (som vist i Tabel 5 med pilen) bliver feltet, der blev mærket "acceptabel" af RAC-TS, ekstrapoleret lineært til resten af matrixen. Dette betyder, at alle felter på samme diagonale (eller under diagonalen) også mærkes "acceptabel". Felterne under kan også mærkes "acceptabel".

Tabel 5: Typisk eksempel på en kalibreret risikomatrix

Ulykkeshyppighed (forårsaget af en fare)	Risikoniveauer			
Hyppig (10^{-4} pr. time)	Uacceptabel	Uacceptabel	Uacceptabel	Uacceptabel
Sandsynlig (10^{-5} pr. time)	Uacceptabel	Uacceptabel	Uacceptabel	Uacceptabel
Lejlighedsvis (10^{-6} pr. time)	Acceptabel	Uacceptabel	Uacceptabel	Uacceptabel
Sjælden (10^{-7} pr. time)	Acceptabel	Acceptabel	Uacceptabel	Uacceptabel
Usandsynlig (10^{-8} pr. time)	Acceptabel	Acceptabel	Acceptabel	Uacceptabel
Utænkelig (10^{-9} pr. time)	Acceptabel	Acceptabel	Acceptabel	Acceptabel
	Ubetydelig	Marginal	Kritisk	Katastrofal
	Alvorlighedsniveauer for farens konsekvenser (dvs. ulykke)			
Risikoevaluering	Risikoreduktion/-kontrol			
Uacceptabel	Risikoen skal fjernes.			
Acceptabel	Risikoen er acceptabel. Uafhængig vurdering er påkrævet.			

- (d) Når matrixen er udfyldt, kan den også anvendes på ikkekatastrofale farer. Hvis f.eks. et andet funktionssvigt har den alvorlighed, der er klassificeret som "kritisk", må den acceptable ulykkeshyppighed ifølge den kalibrerede risikomatrix ikke være mere end "usandsynlig" (eller endnu mindre).
- (e) Det skal bemærkes, at anvendelsen af risikomatrixen kan medføre meget konservative resultater, når den anvendes på funktionssvighyppighed (dvs. for funktionssvigt, som ikke direkte medfører ulykker).

A.3.6.4. Princip for kalibrering af andre risikoanalysemetoder

Andre risikoanalysemetoder, f.eks. den foreslåede ordning med risikoprioriteringsnummer eller risikografen fra VDV 331 eller IEC 61508, kan også kalibreres ved hjælp af en lignende procedure som beskrevet for risikomatrixen:

- (a) Trin 1: Klassificér referencepunktet fra RAC-TS som acceptabelt og punkter med højere hyppigheder eller alvorlighed som en uacceptabel RAC-TS.
- (b) Trin 2: Brug afvejningsmekanismen for den pågældende metode til at ekstrapolere risikotolerancen til ikkekatastrofale farer (ved hjælp af lineær risikoafvejning som udgangspunkt).
- (c) Trin 3: For de ikkekatastrofale farer kan RAC-TS derefter udledes af den kalibrerede risikoanalysemetode ved at sammenligne koordinatet (for hyppighed-alvorlighed) med den således opnåede F-N-kurve.

A.3.7. Konklusioner for RAC-TS

- A.3.7.1. I den generelle risikovurderingsramme, som foreslås af CSM, er risikoacceptkriterierne nødvendige for at fastslå, hvornår den eller de resterende risikoniveauer bliver acceptable, og dermed hvornår den eksplicit risikoestimering skal standses.
- A.3.7.2. RAC-TS er et konstruktionsmål (10^{-9} h^{-1}) for tekniske systemer.
- A.3.7.3. De primære formål med RAC-TS er:
- (a) at specificere en øvre grænse for risikoaccept og dermed et referencepunkt, hvorfra risikoanalysemetoderne for de tekniske systemer kan kalibreres
 - (b) at muliggøre den gensidige anerkendelse af tekniske systemer, siden den tilhørende risiko- og sikkerhedsvurdering vil blive evalueret i forhold til det samme risikoacceptkriterium i alle medlemsstater
 - (c) at spare omkostninger, da det ikke kræver unødvendigt høje kvantitative sikkerhedskrav
 - (d) at lette konkurrencen mellem fabrikanterne. Anvendelsen af forskellige risikoacceptkriterier af initiativtageren eller en medlemsstat ville få branchen til at udføre en mængde forskellige påvisninger på de samme tekniske systemer. Det ville derfor sætte fabrikanternes konkurrenceevne på spil og gøre produkterne unødvendigt dyre.
- A.3.7.4. Det semikvantitative krav indeholdt i RAC-TS skal ikke altid påvises for tekniske systemer. I forbindelse med CSM skal RAC-TS da også kun finde anvendelse på tekniske systemer, hvori de identificerede farer hverken kan kontrolleres tilstrækkeligt ved hjælp af adfærdskodekser eller ved sammenligning med lignende referencesystemer. Dette gør det muligt at fastsætte mildere sikkerhedskrav, forudsat at det overordnede sikkerhedsniveau kan fastholdes.
- A.3.7.5. Kun når der hverken findes en adfærdskodeks og et referencesystem, er det nødvendigt med et harmoniseret semikvantitativt risikoacceptkriterium for tekniske systemer.
- A.3.7.6. Da sikkerhedsintegritetsniveauet for systematiske svigt/fejl er begrænset til SIL 4, skal sikkerhedsintegritetsniveauet for tilfældige hardwaresvigt i tekniske systemer også begrænses til SIL4. Det svarer til en maksimal (acceptabel farerisiko) på 10^{-9} h^{-1} (dvs. den maksimale svigtrate). Ifølge CENELEC 50129-standardens kan det ikke opnås med kun ét system, hvis der stilles skærpede sikkerhedskrav. Arkitekturen i systemet skal ændres, f.eks. ved hjælp af to systemer, som uundgåeligt øger omkostningerne ved det tekniske system drastisk. Se flere detaljer i afsnit A.3.1. i tillæg A.
- A.3.7.7. Endelig er det i afsnit A.3.6. i tillæg A beskrevet, hvordan RAC-TS kan anvendes som et referencepunkt for kalibrering af bestemte risikoanalysemetoder, når tekniske systemer har potentiale for mindre alvorlige konsekvenser end katastrofer.

A.4. Beviser fra sikkerhedsvurdering

- A.4.1. Dette afsnit giver vejledning i beviser, som normalt gives til et vurderingsorgan med henblik på en uafhængig vurdering og tilvejebringelse af en sikkerhedsaccept med forbehold af de nationale krav i en medlemsstat. Det kan bruges som en tjekliste til kontrol af, at alle tilhørende aspekter er blevet dækket og dokumenteret, når det er relevant, i forbindelse med anvendelsen af CSM.

A.4.2. Sikkerhedsplan: CENELEC anbefaler, at der udarbejdes en sikkerhedsplan ved projektstart, eller hvis det ikke er hensigtsmæssigt for projektet, at den tilhørende beskrivelse er inkluderet i et andet relevant dokument. Hvis vurderingsorganerne udpeges ved projektstart, kan sikkerhedsplanen også forelægges dem til udtalelse. I princippet beskriver sikkerhedsplanen:

- (a) den organisation, der er oprettet, og kompetencerne hos de mennesker, der arbejder med projektudvikling og risikovurdering
- (b) alle de sikkerhedsrelaterede aktiviteter, som er planlagt i de forskellige faser af projektet, samt de forventede resultater.

A.4.3. Beviser, der kræves udledt af systemdefinitionsfasen:

- (a) beskrivelse af system:
 - (1) definition af systemafgrænsning
 - (2) beskrivelse af funktioner
 - (3) beskrivelse af systemstruktur
 - (4) beskrivelse af drifts- og miljøforhold
- (b) beskrivelse af eksterne grænseflader
- (c) beskrivelse af interne grænseflader
- (d) beskrivelse af livscyklusfaser
- (e) beskrivelse af sikkerhedsprincipper
- (f) beskrivelse af de antagelser, der definerer grænserne for risikovurdering.

A.4.4. For at muliggøre udførelsen af risikovurderingen tages der i systemdefinitionen hensyn til den sammenhæng, som ændringen tænkes indført i.

- (a) Hvis den planlagte ændring er en ændring af et eksisterende system, beskriver systemdefinitionen både systemet inden ændringen og den planlagte ændring.
- (b) Hvis den planlagte ændring er anlæggelse af et nyt system, er beskrivelsen begrænset til en definition af systemet, da der ikke findes en beskrivelse af et eksisterende system.

A.4.5. Beviser, der kræves udledt af fareidentifikationsfasen:

- (a) beskrivelse af og belæg (herunder begrænsninger) for metoder og værktøjer til fareidentifikation (top-down-metode, bottom-up-metode, HAZOP, osv.)
- (b) resultater:
 - (1) liste over farer:
 - (2) system(grænse)farer
 - (3) delsystemfarer
 - (4) grænsefladefarer
 - (5) sikkerhedsforanstaltninger, som kunne blive identificeret i denne fase.

A.4.6. Følgende beviser skal også udledes af risikoanalysefasen:

- (a) Når der anvendes adfærdskodekser til at kontrollere farer, skal det påvises, at alle relevante krav fra adfærdskodekserne er overholdt for det system, der vurderes. Bl.a. skal det påvises, at de pågældende adfærdskodekser er korrekt anvendt.
- (b) Når der anvendes lignende referencesystemer til at kontrollere farer:
 - (1) definition af sikkerhedskravene til det system, der vurderes, fra de relevante referencesystemer
 - (2) påvisning af, at systemet, der vurderes, anvendes under lignende drifts- og miljøforhold som det relevante referencesystem. Hvis dette ikke kan lade sig gøre, skal det påvises, at afvigelserne fra referencesystemet er korrekt vurderet

- (3) bevis for, at sikkerhedskravene fra referencesystemerne er korrekt indført i det system, der vurderes.
- (c) Når der anvendes eksplicit risikoestimering til at kontrollere farer:
 - (1) beskrivelse af og belæg (herunder begrænsninger) for metoder og værktøjer til risikoanalyse (kvalitative, kvantitative, semikvantitative, ikke-regressionsanalyse osv.)
 - (2) identificering af eksisterende sikkerhedsforanstaltninger og risikoreducerende faktorer for hver fare (herunder den menneskelige faktor)
 - (3) evaluering og rangordning af risiko for hver fare:
 - (i) estimering af følgerne af farer og belæg (med antagelse og betingelser)
 - (ii) estimering af hyppigheden af farer og belæg (med antagelse og betingelser)
 - (iii) rangordning af farer i henhold til deres kritiskhed og hyppighed
 - (4) identifikation af supplerende egnede sikkerhedsforanstaltninger, der sikrer acceptable risici for hver fare (iterativ proces efter risikoevalueringsfasen).

A.4.7. Beviser, der kræves udledt af risikoevalueringen:

- (a) Når der udføres eksplicit risikoestimering:
 - (1) definition af og belæg for risikoevalueringskriterier for hver fare
 - (2) påvisning af/belæg for, at sikkerhedsforanstaltningerne og sikkerhedskravene holder hver fare på et acceptabelt niveau (ifølge ovenstående risikoevalueringskriterium)
 - (b) I henhold til afsnit 2.3.5 og 2.4.3 i CSM-forordningen bliver risici, der er omfattet af anvendelse af adfærdskodekser og sammenligning med referencesystemer, betragtet implicit som acceptable, forudsat henholdsvis (jf. prikket cirkel i Figur 1):
 - (1) at betingelserne for anvendelse af adfærdskodekser i afsnit 2.3.2 er opfyldt
 - (2) at betingelserne for anvendelse af et referencesystem i afsnit 2.4.2 er opfyldt.
- Risikoacceptkriterierne er implicitte for disse to risikoacceptprincipper.

A.4.8. Beviser fra farehåndtering:

- (a) registrering af alle farer i en faredegørelse med følgende elementer:
 - (1) identificeret fare
 - (2) sikkerhedsforanstaltninger, der forebygger farens opståen eller afbøder dens konsekvenser
 - (3) sikkerhedskrav til foranstaltningerne
 - (4) relevant del af systemet
 - (5) aktør, der er ansvarlig for sikkerhedsforanstaltningerne
 - (6) farestatus (f.eks. åben, løst, slettet, overført, kontrolleret)
 - (7) dato for registrering, gennemgang og kontrol af hver fare
- (b) beskrivelse af, hvordan farer skal styres effektivt i hele livscyklussen
- (c) beskrivelse af udvekslingen af oplysninger mellem parterne om farer ved grænseflader og ansvarsfordeling.

A.4.9. Beviser vedrørende kvaliteten af risikoevaluerings- og -vurderingsprocessen:

- (a) beskrivelse af personer, der er involveret i processen, og deres kompetencer
- (b) med hensyn til eksplicitte risikoestimeringer, beskrivelse af information, data og andre statistikker, der er anvendt i processen, og belæg for deres tilstrækkelighed (f.eks. følsomhedsundersøgelser af de anvendte data).

A.4.10. Beviser for overensstemmelse med sikkerhedskrav:

- (a) liste over anvendte standarder
- (b) beskrivelse af konstruktions- og driftsprincipper
- (c) beviser for anvendelse af et godt kvalitets- og sikkerhedsledelsessystem for projektet:
Se punkt [G 3] i afsnit 1.1.2
- (d) sammendrag af sikkerhedsanalyserapporter (f.eks. fareårsagsanalyse) til påvisning af opfyldelsen af sikkerhedskravene
- (e) beskrivelse af og belæg for metoder og værktøjer (FMECA, FTA osv.), som anvendes til fareårsagsanalysen
- (f) sammendrag af sikkerhedsverificerings- og -valideringstester.

A.4.11. Sikkerhedscase: CENELEC anbefaler, at alle tidligere nævnte beviser samles og resumeres i ét dokument, som forelægges vurderingsorganet: Se punkt [G 4] og [G 5] i afsnit 5.1.

TILLÆG B: EKSEMPLER PÅ TEKNIKKER OG VÆRKTØJER, DER STØTTER RISIKOVURDERINGSPROCESSEN

- B.1. Der gives eksempler på teknikker og værktøjer til udførelse af risikovurderingsaktiviteter, der er omfattet af CSM, i bilag E til vejledningen EN 50126-2 {Ref. 9}. Der gives et sammendrag af teknikker og værktøjer i tabel E.1. Hver teknik er beskrevet, og om nødvendigt angives en henvisning til andre standarder til oplysning.

TILLÆG C: EKSEMPLER

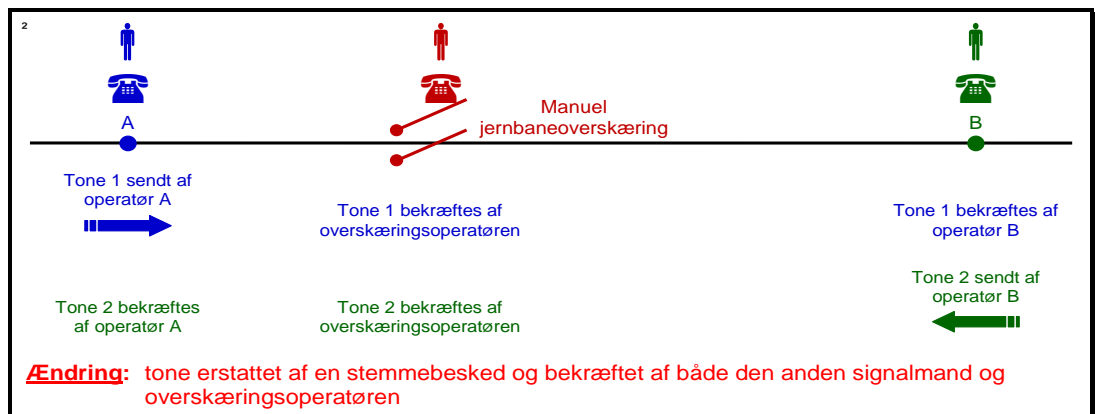
C.1. Indledning

- C.1.1. Formålet med dette tillæg er at lette læsningen af nærværende dokument. Her er alle de indsamlede eksempler, der skal lette anvendelsen af CSM, samlet.
- C.1.2. Eksemplerne på risiko- eller sikkerhedsvurderinger, som er anført i dette tillæg, hidrører ikke fra anvendelsen af CSM-processen, idet de blev udført før indførelsen af CSM-forordningen. Eksemplerne kan klassificeres i:
- eksempler, med henvisning til deres oprindelse, givet af eksperter i CSM-arbejdsgruppen
 - eksempler, bevidst uden henvisning til deres oprindelse, også givet af eksperter i CSM-arbejdsgruppen. Eksperter anmodede om, at oprindelsen forblev fortrolig
 - eksempler, hvis oprindelse ikke nævnes, og som blev fremlagt af medlemmer af agenturets personale baseret på deres tidligere personlige faglige erfaring.

For hvert eksempel stilles den anvendte proces over for den, der kræves af CSM, og endvidere anføres argumenterne for at gennemføre de eventuelle supplerende skridt, som CSM kræver, og den deraf følgende merværdi.

C.2. Eksempler på anvendelse af væsentlige ændringskriterier i Artikel 4 (2)

- C.2.1. Agenturet arbejder på definitionen af, hvad der kan anses for en "væsentlig ændring". Fra dette arbejde gives i dette afsnit et eksempel på, hvordan kriterierne i Artikel 4 (2) skal anvendes.
- C.2.2. Ændringen består i ved en manuelt betjent jernbaneoverskæring at ændre den måde, signalfolkene kommunikerer oplysningerne om et ankomende togs retning til operatøren ved jernbaneoverskæringen. Ændringen er vist i Figur 15.



**Figur 15: Eksempel på en ubetydelig ændring
Telefonbesked til kontrol ved jernbaneoverskæring**

- C.2.3. Eksisterende system: Før indførelsen af den planlagte ændring blev oplysningen om et ankomende togs retning automatisk givet til operatøren ved jernbaneoverskæringen ved hjælp af en ringetone i telefonen. Tonen var forskellig, alt efter hvor opkaldet kom fra.

C.2.4. Planlagt ændring: Da det gamle telefonsystem bliver forældet og skal erstattes af et nyt digitalt system, kan den relevante information rent teknisk ikke længere indgå i tonen. Tonen er nøjagtig den samme, uanset hvilken signalmand den kommer fra. Det beslutes derfor at opnå samme funktion gennem en driftsprocedure:

- (a) Ved togafgang informerer signalmanden verbalt operatøren ved jernbaneoverskæringen om det ankomende togs retning.
- (b) Informationen tjekkes i forhold til køreplanen, og både operatøren ved jernbaneoverskæringen og den anden signalmand kvitterer for at undgå misforståelser hos operatøren.

Den planlagte ændring og tilhørende driftsprocedure er illustreret i Figur 15.

C.2.5. Selv om ændringen ser ud til at have en potentiel sikkerhedsvirkning (risiko for ikke at sænke bommen ved jernbaneoverskæringen i tide), kan andre kriterier i Artikel 4 (2) som f.eks.:

- (a) lav kompleksitet
- (b) manglende innovation og
- (c) let overvågning

tyde på, at den planlagte ændring ikke er væsentlig.

C.2.6. I dette eksempel er det alligevel nødvendigt med nogle sikkerhedsanalyser eller argumenter for at vise, at udskiftningen af et gammelt teknisk system med en driftsprocedure (med personale, der krydstjekker hinanden) for denne sikkerhedskritiske opgaves vedkommende ville munde ud i et lignende sikkerhedsniveau. Spørgsmålet er, om dette ville kræve anvendelse af den fulde CSM-proces med fareredegørelse, uafhængig vurdering af et vurderingsorgan osv. I så fald er det tvivlsomt, om det ville medføre en merværdi, fordi en sådan ændring så ikke kunne kaldes væsentlig.

C.3. Eksempler på grænseflader mellem jernbaneaktører

C.3.1. Her er nogle eksempler på grænseflader og grunde til samarbejde mellem aktører i jernbanesektoren:

- (a) IF– IF: f.eks. skal begge infrastrukturer tage højde for sikkerhedsforanstaltninger med henblik på en sikker overgang for togene mellem infrastrukturerne
- (b) IF– JV: f.eks. kunne der være specifikke driftsregler alt efter infrastrukturen, som lokoføreren skal overholde
- (c) IF– fabrikant: f.eks. kunne fabrikantens delsystemer være belagt med anvendelsesrestriktioner, som skal overholdes af IF
- (d) IF– tjenesteydere: f.eks. kunne der være specifikke vedligeholdelseskrav til infrastrukturen, som skal opfyldes af underleverandøren af vedligeholdelsen
- (e) JV – fabrikant: f.eks. kunne fabrikantens delsystemer være belagt med anvendelsesrestriktioner, som skal overholdes af JV
- (f) JV – tjenesteydere: f.eks. kunne der være specifikke vedligeholdelseskrav til infrastrukturen, som skal opfyldes af underleverandøren af vedligeholdelsen
- (g) JV – materielforvaltere: f.eks. kunne der være vognspecifikke anvendelsesrestriktioner, som skal overholdes af jernbanevirksomheden, der driver disse vogne
- (h) Fabrikant – fabrikant: f.eks. styring af sikkerhedsrelaterede tekniske grænseflader mellem delsystemer fra to forskellige fabrikanter

- (i) Fabrikant – tjenesteyder: f.eks. fabrikantens forvaltning af fareredegørelsen, når fabrikanten udliciterer en opgave til et selskab, hvis størrelse er for beskeden til, at det har en sikkerhedsorganisation for det pågældende projekt
 - (j) Tjenesteyder – tjenesteyder: lignende eksempler som i punkt (i) ovenfor.
- C.3.2. Tjenesteydere dækker alle aktiviteter, der udliciteres af enten IF eller JV eller fabrikanten, såsom vedligeholdelse, billetter, ingeniørydelser osv.
- C.3.3. For at illustrere grænsefladestyringen og den tilhørende fareidentifikation gives følgende eksempler. Eksemplet gælder en grænseflade mellem en togfabrikant og en initiativtager (RU). Det beskrives herefter, hvordan de primære kriterier, der kræves i punkt [G 3] i afsnit 1.2.1 kunne opfyldes:
- (a) Lederskab: initiativtageren (JV)
 - (b) Input:
 - (1) liste over relevante farer fra lignende projekter
 - (2) beskrivelse af alle input og output (I/O) fra grænsefladen, herunder ydelsesegenskaber
 - (c) Metoder: Se tillæg A.2 til vejledningen EN 50126-2 {Ref. 9}
 - (d) Påkrævede deltagere:
 - (1) initiativtagerens (JV) sikkerhedskontrolchef
 - (1) togfabrikantens sikkerhedskontrolchef
 - (2) initiativtagerens konstruktionsmyndighed
 - (3) togfabrikantens konstruktionsmyndighed
 - (4) initiativtagerens vedligeholdelsespersonale (delvis afhængigt af de analyserede I/O)
 - (5) lokoførere (delvis afhængigt af de analyserede I/O)
 - (e) Output:
 - (1) fælles aftalt fareidentifikationsrapport
 - (2) sikkerhedsforanstaltninger til fareredegørelsen med en klar beskrivelse af ansvaret.

C.4. Eksempler på metoder til bestemmelse af bredt acceptable risici

C.4.1. Indledning

- C.4.1.1. Bredt acceptable risici defineres i CSM-forordningen som risici, der er så små, at det ikke er rimeligt at gennemføre nogen yderligere sikkerhedsforanstaltning (for at reducere risikoen yderligere) ("*so small that it is not reasonable to implement any additional safety measure (to reduce the risk further)*"). Ved fareidentifikationen giver en klassificering af visse farer, som er forbundet med bredt acceptable risici, ikke mulighed for at analysere disse farer yderligere i risikovurderingsprocessen. Den ovennævnte definition af bredt acceptable risici giver en vis mulighed for fortolkning. Derfor er det angivet i forordningen, at beslutningen om klassificering af farer med bredt acceptable risici overlades til ekspertafgørelser.
- C.4.1.2. Det er faktisk vanskeligt at definere et gængs og mere eksplicit kriterium for bredt acceptable risici, som kunne anvendes på alle de forskellige mulige systemniveauer, hvor der kunne identificeres sådanne farer, og som også er baggrunden for de forskellige risikoaversionsfaktorer, som kan være fremherskende for forskellige anvendelser. Da det imidlertid er vigtigt at sikre, at ekspertafgørelserne er letforståelige og sporbare, er det nyttigt med vejledning i, hvordan man definerer risici som bredt acceptable. Kriterierne for definition

af bredt acceptable risici kan være kvantitative, kvalitative eller semikvalitative. Nedenfor anføres nogle eksempler på, hvordan man udleder kriterier med henblik på at evaluere bredt acceptable risici på en kvantitativ eller semikvantitativ måde.

- C.4.1.3. Eksemplerne nedenfor illustrerer dette princip. De er taget fra dokumentet: *"Die Gefährdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal + Draht (100) 9/2008.*

C.4.2. Udledning af kvantitativt kriterium

- C.4.2.1. Man kan definere bredt acceptable risici som risici, der er meget mindre end den acceptable risiko for en given fareklasse. Ved hjælp af statistiske data er det måske muligt at beregne, hvad det aktuelle risikoniveau er for jernbanesystemer, og dermed erklære, at det beregnede er acceptabelt. Ved at dividere dette risikoniveau med antallet (N) af farer (f.eks. kan man skønsomt antage, at der er ca. $N = 100$ hovedkategorier af farer i jernbanesystemet) får man et acceptabelt risikoniveau pr. farekategori. Man kunne dernæst anføre, at en fare med en risiko, som ligger to størrelsesordner lavere end det acceptable risikoniveau pr. fare (dette er parameteren $x\%$ i punkt [G 1] i afsnit 2.2.3), vil blive betragtet som en bredt acceptabel risiko.

- C.4.2.2. Det skal dog tjekkes, at bidraget fra alle farer, der er forbundet med bredt acceptable risici, ikke overstiger en given andel (f.eks. $y\%$) af den samlede risiko på systemplan: Se afsnit 2.2.3 og forklaringen i punkt [G 2] i afsnit 2.2.3.

C.4.3. Evaluering af bredt acceptable risici

- C.4.3.1. Grænseværdierne for bredt acceptable risici, som de udledes i ovenstående eksempler, kan derefter bruges til at kalibrere kvalitative værktøjer med, f.eks. en risikomatrix, en risikograf eller risikoprioriteringsnumre, for at hjælpe eksperten med at træffe sin afgørelse om at klassificere risikoen som bredt acceptabel. Det er vigtigt at understrege, at kvantitative værdier som kriterier for bredt acceptable risici ikke indebærer, at det er nødvendigt at foretage en præcis risikoestimering eller -analyse for at træffe beslutning om, hvorvidt en risiko er bredt acceptabel. Det er her, eksperten skal bruge sin dømmekraft til at foretage en løselig estimering i fareidentifikationsfasen.

- C.4.3.2. Det er også vigtigt at tjekke, at bidraget fra alle farer, der er forbundet med bredt acceptable risici, ikke overstiger en given andel (f.eks. $y\%$) af den samlede risiko på systemplan: Se afsnit 2.2.3 og forklaringen i punkt [G 2] i afsnit 2.2.3.

C.5. Risikovurderingseksempel på en væsentlig organisatorisk ændring

- C.5.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

- C.5.2. Eksemplet vedrører en organisatorisk ændring. Den blev betragtet som væsentlig af den pågældende initiativtager. Der blev anvendt en risikovurderingsbaseret tilgang til evaluering af ændringen.
- C.5.3. En afdeling i infrastrukturforvalterens organisation, som indtil ændringen udførte vedligeholdelse (ud over signaler og telematik), skulle skilles ud og sendes i konkurrence med andre selskaber på samme område. Den direkte virkning var et behov for nedskæring og flytning af personale og opgaver i den afdeling af IM-organisationen, der skulle udskilles og sendes i direkte konkurrence.
- C.5.4. Bekymringer for den påvirkede infrastrukturforvalter:
- (a) IF-personalet, der blev berørt af ændringen, var ansvarligt for nødvedligeholdelse og reparationer, der var nødvendiggjort af pludselige fejl i infrastrukturen. Personalet udførte også visse planlagte eller projektbaserede vedligeholdelsesaktiviteter som ballaststopning, ballastrensning, beplantningsbeskæring.
 - (b) Disse opgaver blev anset for kritiske for sikkerheden og togdriftens præcision. De skulle derfor analyseres for at finde de rette foranstaltninger, som sikrer, at situationen ikke forringes, efterhånden som mange af de sikkerhedsansvarlige forlader IF's organisation.
 - (c) Samme sikkerheds- og togpræcisionsniveau skal opretholdes under og efter ændringen i organisationen.
- C.5.5. Sammenlignet med CSM-processen blev følgende trin anvendt (jf. også Figur 1):
- (a) systembeskrivelse [afsnit 2.1.2]:
 - (1) beskrivelse af de opgaver, der udføres af den eksisterende organisation (dvs. af IF-organisationen før ændringen)
 - (2) beskrivelse af de planlagte ændringer i IF-organisationen
 - (3) "den udskilte afdelings" grænseflader til andre omgivende organisationer eller det fysiske miljø kunne kun beskrives kortfattet. Grænserne kunne ikke fremlægges 100 % tydeligt
 - (b) fareidentifikation [afsnit 2.2]:
 - (1) brainstorming i en ekspertgruppe:
 - (i) for at finde frem til alle de farer med en relevant indflydelse på risikoen, som skabes af den planlagte organisatoriske ændring
 - (ii) for at identificere mulige tiltag til kontrol med risikoen
 - (2) fareklassificering:
 - (i) alt efter alvorligheden af den tilhørende risiko: høj, middelhøj, lav risiko
 - (ii) alt efter ændringens indvirkning: øget, uændret, mindsket risiko
 - (c) anvendelse af et referencesystem [afsnit 2.4]:

Systemet før ændringen blev vurderet til at have et acceptabelt risikoniveau. Det blev brugt som "referencesystem" til at udlede risikoacceptkriterierne (RAC) for ændringen af organisationen.
 - (d) eksplicit risikoestimering og -evaluering [afsnit 2.5]:

For hver fare med øget risiko som følge af ændringen af organisationen er der identificeret risikoreduktionsforanstaltninger. Den resterende risiko sammenholdes med RAC fra referencesystemet for at tjekke, om der skal identificeres yderligere foranstaltninger.

(e) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

- (1) Risikoanalysen og fareredegørelsen viser, at farer ikke kan kontrolleres, førend de er verificeret, og førend det er påvist, at sikkerhedskravene (dvs. udvalgte sikkerhedsforanstaltninger) er gennemført.
- (2) Risikoanalysen og fareredegørelsen var levende dokumenter. Effektiviteten af de besluttede tiltag blev overvåget med jævne mellemrum for at tjekke, om forholdene ændrede sig, og om risikoanalysen og risikoevalueringen skulle opdateres.
- (3) Hvis de gennemførte foranstaltninger ikke var effektive nok, blev risikoanalysen, risikoevalueringen og fareredegørelsen opdateret og overvåget igen.

(f) farehåndtering [afsnit 4.1]:

De identificerede farer og sikkerhedsforanstaltninger blev registreret og styret i en fareredegørelse. En af konklusionerne i eksemplet var, at der løbende skulle ske opdatering af risikoanalysen og fareredegørelsen, efterhånden som beslutninger og tiltag blev truffet under omlægningen af organisationen. Risikoen ved grænseflader til f.eks. underleverandører og entreprenører blev også omfattet af risikoanalysen.

Strukturen og de felter, som anvendes i fareredegørelsen samt et uddrag på nogle linjer findes i afsnit C.16.2. i tillæg C.

(g) uafhængig vurdering [Artikel 6]:

En tredjepart gennemførte også en uafhængig vurdering med henblik på:

- (1) at kontrollere, at risikostyringen og risikovurderingen blev korrekt udført
- (2) at kontrollere, at organisationsændringen er velegnet og vil gøre det muligt at opretholde det samme sikkerhedsniveau som før ændringen.

C.5.6. Eksemplet viser, at de principper, der kræves ifølge den fælles sikkerhedsmetode (CSM), er eksisterende metoder i jernbanesektoren, som allerede finder anvendelse ved vurdering af risici ved organisatoriske ændringer. Risikovurderingen i eksemplet opfylder alle krav fra CSM. Der er anvendt to ud af tre risikoacceptprincipper, som er muliggjort af den harmoniserede CSM-tilgang:

- (a) Der er anvendt et "referencesystem" til at bestemme de risikoacceptkriterier, der er nødvendige for at evaluere risikoaccepten af den organisatoriske ændring.
- (b) Der er anvendt "eksplicit risikoestimering og -evaluering":
 - (1) for at analysere ændringens afvigelser fra referencesystemet
 - (2) for at identificere risikoreduktionsforanstaltninger med henblik på den øgede risiko som følge af ændringen
 - (3) for at evaluere, om et acceptabelt risikoniveau er nået.

C.6. Risikovurderingseksempel på en væsentlig driftsændring – Ændring af køretider

C.6.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.6.2. Eksemplet er en driftsændring, hvor jernbanevirksomheden ønskede at tildele lokoførerne nye ruter og potentielt nye arbejdstider (herunder rotation og skiftehold).

C.6.3. Sammenlignet med CSM-processen blev følgende trin anvendt (jf. også Figur 1):

- (a) betydningen af ændringen [Artikel 4]:

Jernbanevirksomheden udførte en foreløbig risikovurdering, hvoraf konklusionen blev, at driftsændringen var væsentlig. Da lokoførerne skulle køre ad nye ruter og muligvis uden for deres sædvanlige arbejdstider, kunne man ikke se bort fra, at de kunne komme til at passere faresignaler, køre for hurtigt eller ignorere midlertidige hastighedsbegrænsninger.

Når man sammenligner denne foreløbige risikovurdering med kriterierne i Artikel 4 (2) i CSM-forordningen, kunne ændringen også kategoriseres som væsentlig baseret på følgende kriterier:

- (1) sikkerhedsrelevans: ændringen er sikkerhedsrelateret, da virkningen af at ændre en lokoførers arbejdsmåde kunne være katastrofal
- (2) følger af svigt: lokoførernes førnævnte fejl har potentiale for katastrofale følger
- (3) nyhed: JV kunne potentielt være i færd med at introducere nye måder at arbejde på for lokoførerne
- (4) ændringens kompleksitet: en ændring af køretiderne kunne være kompleks, da den kunne kræve en komplet vurdering og ændring af eksisterende arbejdsvilkår.

- (b) systemdefinition [afsnit 2.1.2]:

oprindeligt beskrevne systemdefinition:

- (1) eksisterende arbejdsvilkår: arbejdstider, skiftehold osv.
- (2) ændringerne i arbejdstiderne
- (3) grænsefladespørgsmål (f.eks. til infrastrukturforvalteren).

Under de forskellige gentagelser blev systemdefinitionen opdateret med sikkerhedskravene, der hidrørte fra risikovurderingsprocessen. Nøglemedarbejdere var inddraget i denne iterative proces med fareidentifikation og opdatering af systemdefinition.

- (c) fareidentifikation [afsnit 2.2]:

Farerne og de eventuelle sikkerhedsforanstaltninger for de nye ruter og skiftehold blev identificeret ved en brainstorming i en ekspertgruppe, bl.a. repræsentanter for lokoførerne. Lokoførernes opgaver under de nye vilkår blev gennemgået for at vurdere, om de påvirkede lokoførerne, deres arbejdsbyrde, det geografiske omfang og tiderne i skifteholdssystemet.

JV rådførte sig også med fagforeningen for at finde ud af, om de kunne levere yderligere oplysninger, og gennemgik risikoen for træthed og sygdom, som kunne være følgen af en eventuel forøgelse af overtid på grund af længere rejsetider ad ukendte ruter.

Hver af farerne fik tildelt et niveau for alvorligheden af risiko og konsekvenser (høj, middelhøj, lav) og virkningen af den foreslåede ændring holdt op imod dem (øget, uændret, mindsket risiko).

(d) anvendelse af adfærdskodekser [afsnit 2.3]:

Adfærdskodekser i forbindelse med arbejdstider og risici ved menneskelig træthed blev brugt til at revidere de eksisterende arbejdsvilkår og fastlægge de nye sikkerhedskrav. De nødvendige driftsregler blev skrevet i henhold til adfærdskodekserne for det nye skifteholdssystem. Alle nødvendige parter var inddraget i den reviderede driftsprocedure og i aftalen om at gå videre med ændringen.

(e) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

De reviderede driftsprocedurer blev indført i JV's sikkerhedsledelsessystem. De blev overvåget, og en gennemgang blev iværksat for at sikre, at de identificerede farer fortsat kontrolleres korrekt under driften af jernbanesystemet.

(f) farehåndtering [afsnit 4.1]:

Se punktet herover, da jernbanevirksomheders farehåndteringsproces kan være led i deres sikkerhedsledelsessystem for registrering og styring af risici. De identificerede farer blev registreret i en faredegørelse med sikkerhedskravene (dvs. henvisning til de reviderede driftsprocedurer), der kontrollerer den tilhørende risiko.

De reviderede procedurer blev overvåget og gennemgået, når det var nødvendigt, for at sikre, at de identificerede farer fortsat blev kontrolleret korrekt under driften af jernbanesystemet.

(g) uafhængig vurdering [Artikel 6]:

Risikovurderings- og risikostyringsprocessen blev vurderet af en kompetent person hos JV, som var uafhængig af vurderingsprocessen. Den kompetente person vurderede både processen og resultaterne, dvs. de identificerede sikkerhedskrav.

JV har baseret sin beslutning om at sætte det nye system i drift på den uafhængige vurderingsrapport, der er udfærdiget af den kompetente person.

C.6.4. Eksemplet viser, at principperne og processen, der blev anvendt af JV, er i overensstemmelse med den fælles sikkerhedsmetode. Risikostyrings- og risikovurderingsprocessen opfyldte alle kravene fra CSM.

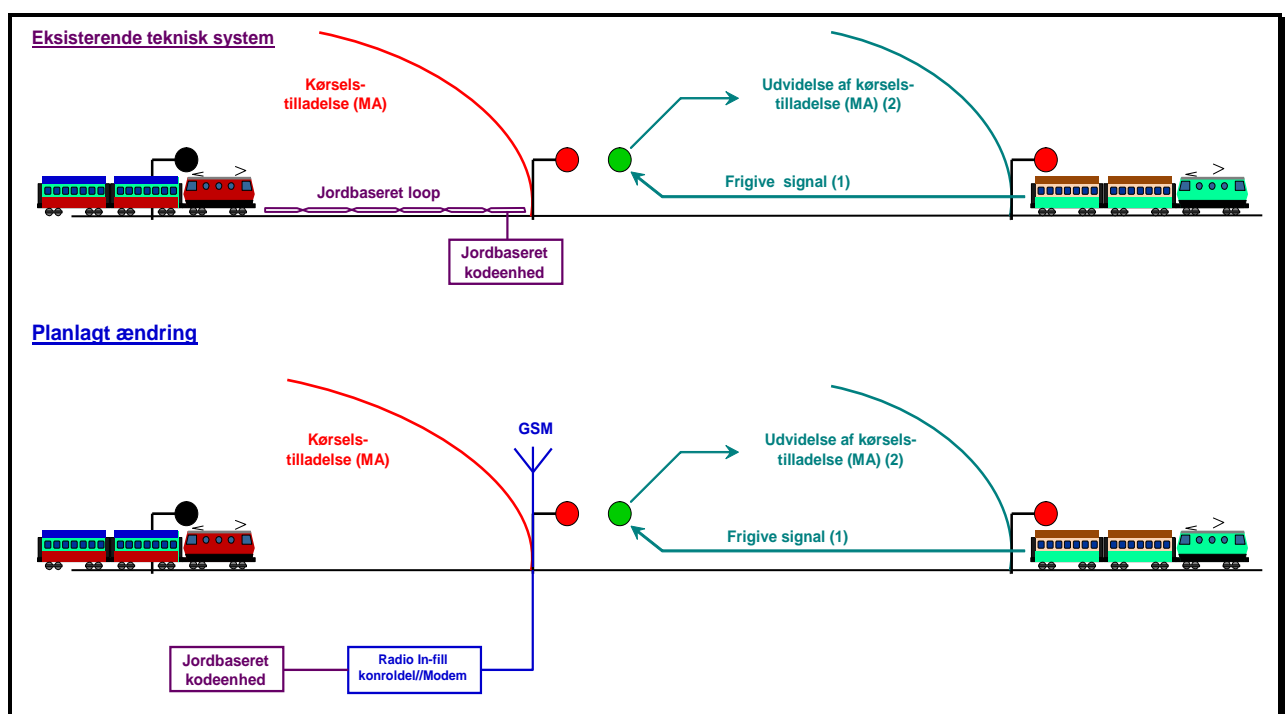
C.7. Risikovurderingseksempel på en væsentlig teknisk ændring (CCS)

C.7.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

- C.7.2. Eksemplet vedrører en teknisk ændring af styringskontrollsystemet (CCS). Den blev betragtet som væsentlig af den pågældende fabrikant. Der blev anvendt en risikovurderingsbaseret tilgang til evaluering af ændringen.
- C.7.3. Beskrivelse af ændringen: ændringen består i at erstatte et jordbaseret (fast anlæg) loop placeret før et signal med et delsystem med "radio infill + GSM" (jf. Figur 16).
- C.7.4. Bekymring: opretholde systemets sikkerhedsniveau efter ændringen.



Figur 16: Ændring af jordbaseret loop til et delsystem med radio infill

- C.7.5. Sammenlignet med CSM-processen blev følgende trin anvendt (jf. også Figur 1):
- vurdering af betydningen af ændringen [Artikel 4]:
Kriterierne i Artikel 4 (2) bruges til at vurdere betydningen af en ændring. Primært kompleksiteten og nyhedsværdien blev brugt til at afgøre, om ændringen var væsentlig.
 - systembeskrivelse [afsnit 2.1.2]:
 - beskrivelse af det eksisterende system: loop og dets funktioner i styringskontrollsystemet
 - beskrivelse af ændringen, der er planlagt af initiativtager og fabrikant
 - beskrivelse af de funktionelle og fysiske grænseflader i loopet til resten af systemet.

"Loop+kodeenhed" i det eksisterende system har den funktion at aktivere signalet, når et tog nærmer sig, i det øjeblik strækningen bag signalet (dvs. foran det ankomende tog) bliver ledig: Se Figur 16.

(c) fareidentifikation [afsnit 2.2]:

Den iterative risikovurderingsproces og fareidentifikation (jf. afsnit 2.1.1) anvendes på grundlag af en brainstorming i en ekspertgruppe for:

- (1) at finde frem til de farer med en relevant indflydelse på risikoen, der skabes af den planlagte organisatoriske ændring
- (2) at identificere mulige tiltag til kontrol med risikoen.

Da loopet og dermed radio infill aktiverer signalet, er der risiko for at afgive en usikker kørselstilladelse til det tog, der nærmer sig, mens det foregående tog stadig optager strækningen foran signalet. Risikoen skal holdes på et acceptabelt niveau.

(d) anvendelse af et referencesystem [afsnit 2.4]:

Systemet før ændringen (loop) blev vurderet til at have et acceptabelt risikoniveau. Det bruges dermed som "referencesystem" til at udlede sikkerhedskravene til delsystemet med "radio infill".

(e) eksplicit risikoestimering og -evaluering [afsnit 2.5]:

- (1) forskellene mellem delsystemerne "loop" og "radio infill+GSM" analyseres ved hjælp af eksplicit risikoestimering og -evaluering. Følgende nye farer er blevet identificeret for delsystemet "radio infill + GSM":
 - (i) hackers overførsel af usikker information i luftspalten, eftersom "radio infill+GSM" er et delsystem med åben transmission
 - (ii) forsinket transmission eller transmission af lagrede datapakker i luftspalten
- (2) eksplicit risikoestimering og brug af RAC-TS kontroldelen til "radio infill".

(f) anvendelse af adfærdskodekser [afsnit 2.3]:

- (1) EN 50159-2-standarden ("Jernbaneanvendelser : Del 2: Sikkerhedsrelateret kommunikation i åbne transmissionssystemer") rummer sikkerhedskravene for at holde nye farer på et acceptabelt niveau, f.eks.:
 - (i) datakryptering og -beskyttelse
 - (ii) sekvensering af beskeder og tidsstempling
- (2) brug af f.eks. EN 50128 standarden til softwareudvikling af kontrolenheden til "Radio Infill".

(g) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

- (1) opfølgning på gennemførelsen af sikkerhedskravene gennem udvikling af delsystemet "radio infill+GSM"
- (2) verificering af, at systemet, som det er konstrueret og installeret, stemmer overens med sikkerhedskravene.

(h) farehåndtering [afsnit 4.1]:

De identificerede farer, sikkerhedsforanstaltningerne og de sikkerhedskrav, der er udledt af risikovurderingen og anvendelsen af de tre risikoacceptprincipper registreres og forvaltes i en faredegørelse.

(i) uafhængig vurdering [Artikel 6]:

En uafhængig vurdering af en tredjepart udføres også med henblik på:

- *****
- (1) at kontrollere, at risikostyringen og risikovurderingen er korrekt udført
 - (2) at kontrollere, at den tekniske ændring er velegnet og vil sikre opretholdelse af det samme sikkerhedsniveau som før ændringen.

C.7.6. Eksemplet viser, at de tre risikoacceptprincipper, der kræves af den fælles sikkerhedsmetode, anvendes på en komplementær måde til at definere sikkerhedskravene til det system, der vurderes. Risikovurderingen i eksemplet opfylder alle krav fra CSM resumeret i Figur 1, herunder forvaltningen af fareredegørelsen og den uafhængige sikkerhedsvurdering ved tredjepart.

C.8. Eksempel på svensk BVH 585.30 vejledning i risikovurdering af jernbanetunneler

C.8.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.8.2. Formålet med eksemplet er at sammenligne processen i CSM med BVH 585.30-vejledningen, som anvendes af den svenske infrastrukturforvalter Banverket til at fastlægge og verificere opnåelsen af et tilstrækkeligt sikkerhedsniveau i planlægningen og opførelsen af nye jernbanetunneler. Ligheder og forskelle i forhold til CSM er anført nedenfor. De detaljerede risikovurderingskrav findes i vejledningen til BVH 585.30.

C.8.3. Sammenlignet med CSM-processen i Figur 1:

- (a) er der følgende ligheder i vejledningen BVH 585.30:

- (1) systembeskrivelse [afsnit 2.1.2]:

Vejledningen kræver en detaljeret systembeskrivelse indeholdende:

- (i) en beskrivelse af tunnelen
- (ii) en beskrivelse af sporet
- (iii) en beskrivelse af typen af rullende materiel (herunder mobilt personale)
- (iv) en beskrivelse af trafik og planlagt drift
- (v) en beskrivelse af den eksterne bistand (herunder redningstjenester).

- (2) fareidentifikation [afsnit 2.2]:

I vejledningen forlanges der ikke eksplicit fareidentifikation. Der forlanges risikoidentifikation og et "ulykkeskatalog", der indeholder typerne af identificerede potentielle ulykker, som vurderes at have en betydelig virkning på tunnelens risikoniveau, og som skal være omfattet af den efterfølgende vurdering. Eksempler på ulykker:

- (i) "afsporing af passagertog"
 - (ii) "afsporing af godstog"
 - (iii) "ulykke, hvori der indgår farligt gods"
 - (iv) "ild i vogn"
 - (v) "kollision mellem passagertog og let/tung genstand"
 - (vi) osv.
- (3) Der findes ingen bestemmelse om anvendelsen af adfærdskodekser eller lignende referencesystemer. Det vurderes, at der under alle omstændigheder skal udføres en risikoanalyse.
- (4) eksplicit risikoestimering og -evaluering [afsnit 2.5]:
- (i) Generelt anbefales det i vejledningen, at der for hver type ulykke udarbejdes et fuldt hændelsestræ baseret på kvantitativ risikoanalyse. Men da formålet med risikoanalysen er at analysere tunnelens samlede risikoniveau frem for at analysere sikkerheden på de enkelte niveauer mere detaljeret, opsummeres konsekvenserne af alle scenarier for at få tunnelens samlede risikoniveau.
 - (ii) Om dette samlede risikoniveau for tunnelen kan accepteres, skal sammenlignes med følgende eksplicite kvantitative acceptkriterium: *"Jernbanetrafikken pr. km i tunneler skal være lige så sikker som jernbanetrafikken pr. km på spor under åben himmel, dog ikke ved overskæringer"*. Dette kriterium omsættes i en F-N-kurve baseret på historiske data over jernbaneulykker i Sverige og ekstrapoleres for også at dække konsekvenser, der ikke findes i statistikkerne.
 - (iii) Ud over dette kriterium vedrørende tunnelens samlede risiko skal der opfyldes yderligere krav specifikt for evakuering i tunneler og muligheder for redningstjenester:
 - ☞ verificering af, at selvredning er mulig i tilfælde af brand i et tog for et "værest tænkeligt tilfælde" (kriterier for denne vurdering gives også)
 - ☞ tunnelen skal planlægges, så det er muligt at foretage redningsindsats i et givet antal scenarier.
- (5) output fra risikovurderingen [afsnit 2.1.6]:
- Outputtene fra risikovurderingen er:
- (i) en liste over sikkerhedsforanstaltninger fra minimumstandarden baseret på TSI-SRT og nationale regler, der skal bruges til konstruktion af tunnelen, og
 - (ii) alle yderligere sikkerhedsforanstaltninger, der er identificeret som nødvendige i risikoanalysen, med angivelse af deres formål. Det anføres, at foranstaltningerne skal træffes efter aftale i følgende prioriterede orden:
 - ☞ forebygge ulykker
 - ☞ reducere konsekvenser af ulykker
 - ☞ lette evakuering
 - ☞ lette redningsindsats.
- (6) farehåndtering [afsnit 4.1]:
- I vejledningen forlanges det ikke eksplicit, at der føres en liste over farer. Det skyldes, at vurderingsniveauet er overordnet, og derfor evalueres og kontrolleres farerne ikke enkeltvis. Acceptabiliteten af tunnelens samlede risiko evalueres uden fordeling af det samlede risikoacceptkriterium ned til de forskellige typer ulykker eller underliggende farer.

Der er dog en liste over alle sikkerhedsforanstaltninger, både dem, der hidrører fra "minimumstandarden", og dem, der er blevet identificeret som nødvendige i risikoenalysen: Se ovenstående punkt (a)(5)(ii). Det bør være angivet i listen over sikkerhedsforanstaltninger, om de vedrører tunnelens infrastruktur, sporet, driften eller det rullende materiel, og også hvad deres tilsigtede virkning er i henhold til den nummererede liste i punkt (a)(5)(ii). Men i vejledningen forlanges det ikke, at det udtrykkeligt anføres, hvilke farer sikkerhedsforanstaltningerne kontrollerer, og hvem der er ansvarlig for hvilke sikkerhedsforanstaltninger.

(7) uafhængig vurdering [Artikel 6]:

En uafhængig vurdering foretaget af en tredjepart er obligatorisk med henblik på:

- (i) at kontrollere, at risikovurderingen, der anbefales af BVH 585.30-vejledningen, er korrekt udført
- (ii) at anse risikoanalysen for acceptabel
- (iii) at kontrollere, at det er tydeligt angivet, hvordan den fremtidige sikkerhedsledelse skal varetages i projektet.

Det afsluttende risikoanalysedokument underskrives af det uafhængige vurderingsorgan og af projektets sikkerhedskoordinator.

(b) adskiller BVH 585.30-vejledningen sig på følgende punkter:

(1) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

Ifølge BVH 585.30-vejledningen forlanges det hverken, at det spores, hvordan de identificerede sikkerhedskrav er gennemført, eller at det verificeres, at den endelige tunnelkonstruktion opfylder de anførte sikkerhedskrav. Det beskrives kun, hvordan disse krav bør overføres for at sikre, at de er blevet gennemført i anlægsfasen.

Vejledningen angiver de sikkerhedskrav, der skal bruges til at verificere, at risikoanalysen er blevet udført på en hensigtsmæssig og gennemskelig måde, og at den kan accepteres af projektet.

C.8.4. Samlet set viser sammenligningen med CSM:

- (a) at BVH 585.30-vejledningen opfylder de relevante dele af CSM, selv om deres afgrænsning og formål ikke er nøjagtig sammenfaldende
- (b) at BVH 585.30-vejledningen vurderer jernbanetunnelens samlede risikoniveau
- (c) at farer ikke kontrolleres enkeltvis, og at der således er mindre fokus på farehåndtering
- (d) at påvisningen af overensstemmelse og verifikation af den korrekte gennemførelse af alle sikkerhedsforanstaltninger ikke er udtrykkeligt anført. Vejledningen angiver imidlertid, at sikkerhedskoordinatorens rolle i projektet (en rolle og en kompetence, som kræves af BVH 585.30) er at verificere, at risikoanalysens konklusioner er gennemført i konstruktionsdokumenterne og -tegningerne, og desuden at kontrollere, at de bliver korrekt gennemført i anlægsfasen.

C.8.5. De fælles sikkerhedsmetoder er mere generelle end BVH 585.30-vejledningen, i og med at de giver mulighed for at anvende tre forskellige risikoacceptprincipper. Imidlertid giver anvendelsen af BVH 585.30-vejledningen inden for CSM ikke problemer, da det vil være foreneligt med at anvende det tredje princip om eksplicit risikoestimering.

C.9. Eksempel på risikovurdering på systemniveau for Københavns Metro

C.9.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.9.2. Eksemplet vedrører et komplet og komplekst førerløst metrosystem, inklusive de underliggende tekniske delsystemer (f.eks. automatisk togdækning og rullende materiel) samt drift og vedligeholdelse af systemet. Der blev anvendt en risikovurderingsbaseret tilgang til evaluering af systemet og de underliggende delsystemer. Projektet dækkede også certificering af SMS hos det selskab, der skulle drive systemet. Dette vedrører JV's og IF's evne til at drive og vedligeholde det samlede system i hele dets livscyklus på sikker vis.

C.9.3. Sammenlignet med CSM-processen blev følgende trin anvendt (jf. også Figur 1):

- (a) systembeskrivelse [afsnit 2.1.2]:
 - (1) beskrivelse af systemydelseskrav
 - (2) beskrivelse af driftsregler
 - (3) klar beskrivelse af grænseflader og ansvarsfordeling mellem de forskellige aktører, særlig mellem de tekniske delsystemer
 - (4) definition af systemkrav på højere niveau (med hensyn til acceptabel ulykkeshyppighed og definition af et ALARP-område)
- (b) fareidentifikation [afsnit 2.2]:
 - (1) en foreløbig fareanalyse på systemniveau
 - (2) funktionsanalyse på systemniveau med fokus på alle delsystemer og ikke kun dem, der er indlysende sikkerhedskritiske (f.eks. automatisk togdækning og rullende materiel), som indgår i sikkerhedsfunktioner og har en aktiv rolle i beskyttelsen af passagerers og personalets sikkerhed
 - (3) intensiv koordinering mellem aktørerne (entreprenører, delsystemleverandører af de tekniske delsystemer og anlægsarbejde):
 - (i) for systematisk at identificere alle med rimelighed forudsigelige farer
 - (ii) for at identificere mulige tiltag til at holde alle risici forbundet med de identificerede farer på et acceptabelt niveau
- (c) anvendelse af adfærdskodekser [afsnit 2.3]:

Der blev brugt forskellige adfærdskodekser, standarder og forordninger, f.eks.:

- (1) BOStrab-reglerne for bygning og drift af sporvogne (tysk regelsæt gældende for lukkede banesystemer) og om førerløs drift

- (2) VDV-dokumenter (tyske adfærdskodekser) om krav til udstyr vedrørende passagerers sikkerhed på stationer med førerløs drift
- (3) CENELEC's standarder for jernbanesystemer (EN50126, 50128 og 50129). Disse standarder omhandler navnlig tekniske jernbanesystemer. Men da de indeholder en metodisk tilgang, som har generel gyldighed, er de i vidt omfang blevet anvendt til Københavns Metro:
 - (i) EN 50126 blev brugt til sikkerhedsledelse og risikovurdering for det fulde jernbanesystem
 - (ii) EN 50129 blev brugt til det fulde signalsystem
 - (iii) EN 50128 blev brugt til softwareudvikling (herunder verificering og validering) af de tekniske delsystemer
- (4) brandbeskyttelsesstandarder for tunneler (NEPA 130)
- (5) standarder for konstruktions- og anlægsarbejde (Eurocodes).
- (d) anvendelse af et referencesystem [afsnit 2.4]:

Metroen skulle nå sikkerhedsniveauet for et tilsvarende moderne anlæg i Tyskland, Frankrig eller Det Forenede Kongerige. Disse eksisterende systemer blev brugt som lignende referencesystemer til at udlæse risikoacceptkriterierne for acceptable ulykkehypotheter for Københavns Metro.
- (e) eksplicit risikoestimering og -evaluering [afsnit 2.5]:
 - (1) til estimering af risici forbundet med specifikke farer
 - (2) til kontrol af nødventilation i tunnelen (herunder menneskelige faktorer, f.eks. brandvæsenet)
 - (3) til identificering af risikoreducerende foranstaltninger
 - (4) til evaluering af, om der er nået et acceptabelt risikoniveau for det fulde system
- (f) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:
 - (1) ledelsesmæssig og teknisk indsats i overensstemmelse med kompleksiteten i systemet med henblik på at påvise systemets sikkerhed
 - (2) fordeling af systemets sikkerhedskrav ned til tekniske delsystemer og anlægsarbejde samt til alle sikkerhedsrelaterede metrofunktioner
 - (3) påvisning af, at hvert delsystem, sådan som det er opført, opfylder sikkerhedskravene til det
 - (4) for så vidt angår sikkerhedsfunktioner udført af mere end ét delsystem, kunne påvisningen af overholdelsen af sikkerhedskravene ikke udføres på delsystemniveau. Den blev udført på systemniveau ved at integre de forskellige delsystemer, værktøjer og procedurer
 - (5) påvisning af, at det samlede system overholder sikkerhedskravene på højt niveau
- (g) farehåndtering [afsnit 4.1]:

De identificerede farer, de tilknyttede sikkerhedsforanstaltninger og de afledte sikkerhedskrav blev registreret og styret i en central faredegørelse. Projektets overordnede sikkerhedschef var ansvarlig for denne faredegørelse. De driftsmæssige farer påpeget under konstruktion og installation samt farer forbundet med drift og vedligeholdelse blev indskrevet i faredegørelsen.
- (h) beviser fra risikostyring og risikovurdering [afsnit 5]:

Risikovurderingsresultaterne blev formelt dokumenteret og understøttet af en sikkerhedscase i overensstemmelse med kravene i CENELEC-standarderne:

 - (1) samlet systemsikkerhedscase

- (2) sikkerhedscase for hvert tekniske delsystem (herunder signaldelsystemer og anlægsarbejde)
- (3) sikkerhedscase for anlægsarbejde (stationer, tunneler, viadukter, dæmninger)
- (4) installationssikkerhedscase
- (5) vognsikkerhedscase
- (6) operatørsikkerhedscase (understøtter JV's og IF's SMS-certificering, dvs. påvisning af initiativtagerens evne til at drive og vedligeholde systemet på sikker vis)

(i) uafhængig vurdering [Artikel 6]:

Den overordnede proces blev fulgt og vurderet af et uafhængigt sikkerhedsvurderingsorgan, der optrådte på vegne af den tekniske tilsynsmyndighed (i dette tilfælde det danske transportministerium). De opgaver, som det uafhængige sikkerhedsvurderingsorgan har, er beskrevet i en relevant adfærdskodeks. Det er bl.a.:

- (1) kontrol af, om der er udført korrekt risikostyring og risikovurdering,
- (2) kontrol af, at systemet er egnet til formålet, og at det vil blive drevet og vedligeholdt på sikker vis i hele sin livscyklus
- (3) anbefaling af godkendelse til den tekniske tilsynsmyndighed.

C.9.4. Det fulde projekt blev understøttet af en egnet kvalitetsledelsesproces.

C.9.5. I projektet blev leverandørernes beviser (dvs. sikkerhedscases og detaljeret støttedokumentation for de tekniske delsystemer og anlægsarbejdet) viderebragt til initiativtagerens sikkerhedschef. Disse beviser blev dernæst gennemgået af sikkerhedsledelsesorganisationen samt af det uafhængige sikkerhedsvurderingsorgan, hvis konklusioner blev nedfældet i en vurderingsrapport. Det uafhængige sikkerhedsvurderingsorgan blev gennemgået af initiativtagerens sikkerhedschef og overbragt initiativtageren, som videresendte alle papirer til den tekniske tilsynsmyndighed (dvs. det danske transportministerium) til endelig godkendelse.

C.9.6. Eksemplet viser, at de principper, der kræves i henhold til den fælles sikkerhedsmetode, allerede findes i jernbanesektoren. Risikovurderingen i eksemplet opfylder alle krav fra CSM. Der er navnlig gjort brug af alle tre risikoacceptprincipper, som er mulige ifølge den harmoniserede CSM-tilgang.

C.10. Eksempel på OTIF-vejledning i beregning af risiko som følge af jernbanetransport af farligt gods

C.10.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.10.2. Den overordnede filosofi i OTIF-vejledningen er i overensstemmelse med formålet med CSM, men vejledningen har et mindre anvendelsesområde. Formålet med OTIF-vejledningen er at opnå en mere ensartet tilgang til risikovurdering af transport af farligt gods i COTIF-medlemsstaterne og dermed gøre de enkelte risikovurderinger sammenlignelige (*"guideline is to obtain a more uniform approach for the risk assessment of transport of dangerous goods in the COTIF Member States and consequently make individual risk assessments comparable"*). Hermed støttes den gensidige accept mellem COTIF-medlemsstaterne af risikovurderinger af transport af farligt gods ad jernbane.

C.10.3. Sammenlignet med CSM og flowskemaet i Figur 1:

(a) er der følgende ligheder i OTIF-vejledningen:

- (1) De har en fælles tilgang til risikovurdering, dog kun baseret på eksplicit risikoestimering (dvs. det tredje CSM-risikoacceptprincip).
- (2) OTIF-risikovurderingen består af:
 - (i) en risikoanalysefase, som omfatter:
 - ↳ en fareidentifikationsfase
 - ↳ en risikoestimeringsfase
 - (ii) en risikoevalueringsfase baseret på risiko(accept)kriterier, som endnu ikke er harmoniserede. Der er da også en mængde nationale særtræk, der kan påvirke disse kriterier.

(b) adskiller OTIF-vejledningen sig på følgende punkter:

- (1) Anvendelsesområdet er anderledes. Mens CSM kun skal anvendes til ændringer i jernbanesystemet, bør OTIF-vejledningen anvendes til vurdering af risici ved transport af farligt gods ad jernbane, uanset om der her er tale om en væsentlig ændring eller ikke i jernbanesystemet.
- (2) Der er ingen mulighed for at vælge mellem tre risikoacceptprincipper til kontrol med risiciene. Det tredje princip, dvs. eksplicit risikoestimering, er det eneste tilladte. Ydermere skal det bygge udelukkende på en kvantitativ frem for en kvalitativ estimering. Den kvalitative risikoanalyse er måske kun egnet til sammenligning af alternative (sikkerheds)foranstaltninger til risikoreduktion.
- (3) Der kræves anvendelse af ALARP-princippet for at fastslå, om ekstra sikkerhedsforanstaltninger kunne reducere den vurderede risiko yderligere til en rimelig omkostning.
- (4) Begrebet "farer forbundet med bredt acceptable risici", der gør det muligt at fokusere risikovurderingsindsatsen på de farer, der bidrager mest, findes ikke. Men det anbefales at reducere antallet af potentielle ulykkesscenerier til et rimeligt antal basisscenerier (jf. afsnit 3.2 i {Ref. 10}).
- (5) Processen er koncentreret om risikovurdering, men rummer ikke:
 - (i) processen for udvælgelse og gennemførelse af (sikkerheds)foranstaltninger til ændring af risikoen
 - (ii) processen for risikoaccept
 - (iii) processen for påvisning af systemets overensstemmelse med sikkerhedskravene
 - (iv) processen for kommunikering af risikoen til andre berørte aktører (jf. punktet herefter).
- (6) Den giver ikke forskrifter om beviser, der skal tilvejebringes ved hjælp af risikovurderingsprocessen.
- (7) Der stilles ikke krav om farehåndtering.

- *****
- (8) Der stilles ikke krav om uafhængig vurdering ved tredjepart af den korrekte anvendelse af den fælles tilgang.
- C.10.4. Sammenligningen mellem OTIF-vejledningen og CSM viser, at de er forenelige, selv om deres afgrænsning og formål ikke er nøjagtig sammenfaldende. CSM er mere generel end OTIF-vejledningen og således mere fleksibel. På den anden side dækker CSM også flere risikostyringsaktiviteter:
- (a) Den tillader brug af tre risikoacceptprincipper, som bygger på eksisterende praksis i jernbanesektoren: Se afsnit 2.1.4.
 - (b) Den kræves kun anvendt til væsentlige ændringer, og der kræves kun yderligere risikoanalyse for farer, som ikke er forbundet med en bredt acceptabel risiko.
 - (c) Den rummer udvælgelse og gennemførelse af sikkerhedsforanstaltninger, som forventes at kontrollere de identificerede farer og tilhørende risici.
 - (d) Den harmoniserer risikostyringsprocessen, herunder:
 - (1) harmonisering af risikoacceptkriterier, som behandles i forbindelse med agenturets arbejde med bredt acceptable risici og risikoacceptkriterier
 - (2) påvisning af systemets overensstemmelse med sikkerhedskravene
 - (3) resultater og beviser fra risikovurderingsprocessen
 - (4) udvekslingen af sikkerhedsrelateret information mellem aktørerne ved grænsefladerne
 - (5) styring i en fareredegørelse af alle identificerede farer og tilknyttede sikkerhedsforanstaltninger
 - (6) uafhængig vurdering ved tredjepart af den korrekte anvendelse af CSM.
- C.10.5. Anvendelse af OTIF-vejledningen i CSM (i tilfælde af at transport af farligt gods udgør en væsentlig ændring for en IF eller JV) giver imidlertid ingen problemer, da den er forenelig med anvendelsen af det tredje princip om eksplicit risikoestimering.

C.11. Risikovurderingseksempel på en ansøgning om godkendelse af nyt rullende materiel

- C.11.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:
- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
 - (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
 - (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

- C.11.2. Dette eksempel på risikovurdering vedrører en ansøgning om godkendelse af en ny type rullende materiel. Der blev udført en risikoanalyse for at evaluere risikoen ved indførelse af en ny godsvogn.

C.11.3. Formålet med ændringen var at øge effektiviteten, kapaciteten, ydeevnen og pålideligheden af bulktransporten af gods på en specifik fragtlinje. Da vognene var beregnet til grænseoverskridende trafik, skulle der også indhentes godkendelse af to forskellige NSA'er. Initiativtageren var banegodsoperatøren, som igen er ejet af det selskab, der producerer de varer, der skal transporteres.

C.11.4. Projekteringen omfattede konstruktion, fremstilling, samling, idriftsættelse og verificering af det nye rullende materiel. Risikoanalysen blev udført for at verificere, at den nye konstruktion opfyldte sikkerhedskravene for hvert af delsystemerne samt for det samlede system.

C.11.5. I risikoanalysen henvises der til CENELEC's EN 50126-standards procedurer og definitioner, og risikoevalueringen udføres i henhold til denne standard.

C.11.6. Sammenlignet med CSM-processen blev følgende trin anvendt:

(a) systembeskrivelse [afsnit 2.1.2]:

For hver af konstruktionsfaserne var der krav til sikkerhedsverifikationsdokumentationen og beskrivelsen af systemkonstruktionen:

- (1) konceptfasen: foreløbig beskrivelse af operatørens driftskrav
- (2) specifikationsfase: funktionel specifikation, gældende tekniske standarder, plan for prøvning og verifikation. Krav fra operatøren vedrørende brug og vedligeholdelse af vognen indgik også
- (3) fremstillingsfase: fabrikantens tekniske dokumentation, herunder tegninger, standarder, beregninger, analyse osv. Tilbundsgående risikoanalyse for nye eller innovative konstruktioner eller nye anvendelsesområder
- (4) verifikationsfase:
 - (i) fabrikantens verifikation af vognens tekniske ydeevne (testrapporter, beregninger, verifikationer i overensstemmelse med standarder og funktionskrav)
 - (ii) dokumentation for risikoreducerende foranstaltninger og testrapporter for at bevise vognens forenelighed med jernbaneinfrastrukturen
 - (iii) vedligeholdelses- og uddannelsesdokumenter, brugermanualer osv.

(5) acceptfase:

- (i) fabrikantens sikkerhedserklæring og sikkerhedsbevis (sikkerhedscase)
- (ii) operatørens accept af både godsvognen og dokumentationen.

(b) fareidentifikation [afsnit 2.2]:

Dette blev udført løbende i alle konstruktionsfaser. Først blev der brugt en bottom-up-metode, hvor de forskellige fabrikanter evaluerede risikosekvenser, der opstod som følge af svigt i komponenter i deres delsystemer. Opdelingen i delsystemer var følgende:

- (1) karosseri
- (2) bremsesystem
- (3) centralkobling
- (4) osv.

Dernæst blev der brugt en supplerende top-down-metode for at finde mangler eller manglende oplysninger. Risici, som ikke umiddelbart kunne accepteres, blev overført til fareredegørelsen til viderebehandling og klassificering.

(c) anvendelse af risikoacceptprincipper [afsnit 2.1.4]:

Der blev udført eksplicit risikoestimering på systemet som helhed. Imidlertid kunne adfærdskodekser eller lignende referencesystemer bruges til at vurdere enkelte farer. Princippet er, at hvert nyt delsystem skal være mindst lige så sikkert som det delsystem, det erstatter, og dermed sikre et nyt komplet system med et højere sikkerhedsniveau end det tidligere. Risikomatrixen for EN 50126 blev brugt til at plote de identificerede farer. Der blev også anvendt forskellige andre risikoacceptkriterier. Bl.a.:

- (1) Et enkelt svigt bør ikke medføre en situation, hvor mennesker, materiale eller miljø kan påvirkes i alvorlig grad.
- (2) Hvis dette ikke kan undgås ved hjælp af anlægsteknikker, bør det forebygges gennem driftsregler eller vedligeholdelseskrav. Dette var kun gældende for farer, hvor det var muligt at identificere det opståede svigt, før det skabte en farlig situation.
- (3) For komponenter med en høj svigtsandsynlighed, eller hvor svigt ikke kan detekteres på forhånd eller forhindres gennem vedligeholdelses- eller driftsregler, bør man overveje ekstra sikkerhedsfunktioner og -barrierer.
- (4) Redundante systemer med komponenter, som kan udvikle ikke detekterbare svigt under drift, bør beskyttes gennem vedligeholdelsesforanstaltninger for at hindre reduceret redundans.
- (5) Det deraf følgende endelige sikkerhedsniveau var en ledelsesbeslutning baseret på kvantitativ og kvalitativ risikoanalyse.

(d) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

Alle identificerede risici og farer blev registreret, og listen blev løbende konsulteret og ført ajour. De resterende farer blev registreret i fareredegørelsen sammen med den tilsvarende liste over risikoreducerende foranstaltninger, der skulle træffes inden for anlæg, drift og vedligeholdelse. På baggrund heraf blev der udarbejdet en endelig sikkerhedsrapport med bekræftelse af, at sikkerhedskravene var gennemført.

(e) farehåndtering [afsnit 4.1]:

Som ovenfor nævnt blev farerne og de tilknyttede sikkerhedsforanstaltninger registreret i fareredegørelsen, så alle identificerede farer og sikkerhedsforanstaltninger kunne spores. Farer forbundet med risici, som var acceptable uden foranstaltninger, blev imidlertid ikke registreret i fareredegørelsen.

(f) uafhængig vurdering [Artikel 6]:

Der blev ikke nævnt noget om en uafhængig vurdering i de dokumenter, der blev fremsendt vedrørende denne væsentlige ændring.

C.11.7. Risikovurderingseksemplet er baseret på CENELEC's EN 50126-standard og passer dermed godt ind i CSM-processen. Risikovurderingen i eksemplet opfylder alle krav fra CSM med undtagelse af kravet om uafhængig vurdering, som ikke var udtrykkeligt præciseret i de fremsendte dokumenter. Der blev anvendt eksplicitte risikoacceptkriterier, hvilket også blev tydeligt angivet.

C.12. Risikovurderingseksempel på en væsentlig driftsændring – ren lokoførerdrift

C.12.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.12.2. Eksemplet er en driftsændring, hvor jernbanevirksomheden besluttede, at toget skulle føres udelukkende af lokoføreren (Driver Only Operated – DOO) på en strækning, hvor der tidligere var en togbetjent med om bord til at hjælpe lokoføreren med togafsendelse.

C.12.3. Sammenlignet med CSM-processen blev følgende trin anvendt (jf. også Figur 1):

- (a) betydningen af ændringen [Artikel 4]:

Jernbanevirksomheden udførte en foreløbig risikovurdering, hvoraf konklusionen blev, at driftsændringen var væsentlig. Da lokoføreren skulle føre toget alene og uden assistance, kunne risikoen for, at passagererne kunne blive fanget mellem dørene eller falde ned på sporet (f.eks. hvis dørene åbnes til den forkerte side) ikke tilsidesættes.

Når man sammenligner denne foreløbige risikovurdering med kriterierne i Artikel 4 i CSM-forordningen, kunne ændringen også kategoriseres som væsentlig baseret på følgende kriterier:

- (1) sikkerhedsrelevans: ændringen er sikkerhedsrelateret, da virkningen af at kræve en helt anderledes måde at varetage driften af togtjenesten på kunne blive katastrofal,
- (2) følger af svigt: den potentielle virkning af lokoførerens præstation kunne få katastrofale følger, hvis driften ikke kontrolleres effektivt,
- (3) nyhedsværdi: drift kun med lokofører kunne kræve nye metoder for togdrift, hvis risici skulle vurderes.

- (b) systemdefinition [afsnit 2.1.2]:

Systemdefinitionen beskrev:

- (1) det eksisterende system, der klart forklarede, hvilke opgaver der blev udført af lokoføreren, og hvilke andre opgaver der blev varetaget af det kørende personale (eller togbetjenten) for at assistere lokoføreren
- (2) ændringen i lokoførerens ansvarsområder som følge af fjernelse af det kørende assisterende personale
- (3) systemets tekniske krav vedrørende driftsændringer
- (4) de eksisterende grænseflader mellem det kørende assisterende personale, lokoføreren og det fast baserede personale hos infrastrukturforvalteren.

Under de forskellige gentagelser blev systemdefinitionen opdateret med sikkerhedskravene, der hidrørte fra risikovurderingsprocessen. Nøglemedarbejdere (herunder lokoførere, personalerepræsentanter og infrastrukturforvalteren) var inddraget i denne iterative proces med fareidentifikation og opdatering af systemdefinition.

(c) fareidentifikation [afsnit 2.2]:

Farerne og de eventuelle sikkerhedsforanstaltninger blev identificeret ved en brainstorming i en ekspertgruppe, bl.a.:

- (1) repræsentanter for lokoførere og personalet med deres driftserfaring
- (2) IF-repræsentanter, idet infrastrukturen også kunne blive påvirket af ændringen og f.eks. betyde ændringer på stationerne (f.eks. opsætning af spejle/overvågningskameraer (CCTV) på perronerne).

De yderligere opgaver, der skulle varetages af lokoføreren, blev gennemgået for at finde alle forudsigelige farer, som måske kunne opstå efter fjernelse af det kørende assisterende personale. Navnlig så man ved fareidentifikationen på, hvilke centrale driftsfarer der kunne være på stationerne, på de eksisterende ruter, hvor der var assistance fra kørende eller fast baseret personale, bl.a. til sikker togafsendelse, specifikke spørgsmål vedrørende lokoføreren, det rullende materiel (f.eks. kontrol af åbning/lukning af døre), vedligeholdelseskrav osv.

Hver af farerne fik tildelt et niveau for alvorligheden af risiko og konsekvenser (høj, middelhøj, lav) og virkningen af den foreslåede ændring holdt op imod dem (øget, uændret, mindsket risiko).

(d) anvendelse af adfærdskodekser [afsnit 2.3] og brug af lignende referencesystemer [afsnit 2.4]:

Både adfærdskodekser (dvs. en serie standarder for drift kun med lokofører) og lignende referencesystemer blev anvendt til at definere sikkerhedskravene vedrørende de identificerede farer. Der var bl.a. tale om følgende sikkerhedskrav:

- (1) de reviderede driftsprocedurer for lokoføreren, som kræves af hensyn til sikker drift af togene uden kørende assistance
- (2) eventuelt supplerende udstyr, der er nødvendigt om bord eller langs sporet af hensyn til sikre og pålidelige metoder til togafsendelse
- (3) en tjekliste til sikring af, at førerrummet var egnet under hensyntagen til grænsefladen mellem jernbanesystemet (både om bord og langs sporet) og føreren.

De nødvendige driftsregler blev revideret i overensstemmelse med kravene fra de gældende adfærdskodekser og de relevante referencesystemer. Alle nødvendige parter var inddraget i den reviderede driftsprocedure og i aftalen om at gå videre med ændringen.

(e) påvisning af systemets overensstemmelse med sikkerhedskravene [afsnit 3]:

Systemet blev gennemført i overensstemmelse med de identificerede sikkerhedskrav (yderligere udstyr og reviderede procedurer). Disse blev verificeret som egnede midler til at sikre et tilstrækkeligt sikkerhedsniveau for det system, der blev vurderet.

De reviderede driftsprocedurer blev indført i JV's sikkerhedsledelsessystem. De blev overvåget og gennemgået, når det var nødvendigt, for at sikre, at de identificerede farer fortsat blev kontrolleret korrekt under driften af jernbanesystemet.

(f) farehåndtering [afsnit 4.1]:

Se punktet herover, da jernbanevirksomheders farehåndteringsproces kan indgå i deres sikkerhedsledelsessystem for registrering og styring af risici. De identificerede farer blev registreret i en faredegegørelse sammen med de sikkerhedskrav, der kontrollerede de tilhørende risici, dvs. henvisning til supplerende udstyr om bord og langs sporet samt til de reviderede driftsprocedurer.

De reviderede procedurer blev overvåget og gennemgået, når det var nødvendigt, for at sikre, at de identificerede farer fortsat blev kontrolleret korrekt under driften af jernbanesystemet.

(g) uafhængig vurdering [Artikel 6]:

Risikovurderings- og risikostyringsprocessen blev vurderet af en kompetent person hos JV, som var uafhængig af vurderingsprocessen. Den kompetente person vurderede både processen og resultaterne, dvs. de identificerede sikkerhedskrav.

JV har baseret sin beslutning om at sætte det nye system i drift på den uafhængige vurderingsrapport, der er udfærdiget af den kompetente person.

- C.12.4. Eksemplet viser, at principperne og processen, der blev anvendt af RU, er i overensstemmelse med den fælles sikkerhedsmetode. Risikostyrings- og risikovurderingsprocessen opfyldte alle kravene fra CSM.

C.13. Eksempel på brug af et referencesystem til udledning af sikkerhedskrav til nye elektroniske sammenkoblingssystemer i Tyskland

- C.13.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

- C.13.2. For at udlede standardsikkerhedskrav til fremtidige elektroniske sammenkoblingssystemer havde Deutsche Bahn udført en risikoanalyse af et allerede godkendt elektronisk system. Sidstnævnte system var i forvejen blevet godkendt i henhold til tyske adfærdskodekser (Mü 8004).
- C.13.3. Risikoanalysen blev udført i overensstemmelse med CENELEC-standarderne (EN 50126 og EN 50129) og omfattede følgende trin:
- (a) systemdefinition
 - (b) fareidentifikation
 - (c) fareanalyse og kvantificering.

- *****
- C.13.4. For systemdefinitionens vedkommende var der sørget for at definere systemets afgrænsning, funktioner og grænseflader. Den primære udfordring var her at definere systemet på en sådan måde, at det er uafhængigt af den interne arkitektur i et sammenkoblingssystem og samtidig stadig foreneligt med eksisterende sammenkoblingssystemer. Der blev derfor gjort ekstra meget ud af at definere meget klart, hvilke grænseflader til systemer udenfor der kom i samspil med sammenkoblingen, uden at gå i detaljer med sammenkoblingens indre funktioner.
- C.13.5. Farerne blev derefter kun identificeret ved grænsefladerne, for at de kunne forblive generiske (dvs. undgå afhængighed af specifik arkitektur). Kun farer som følge af tekniske fejl blev taget i betragtning. For hver grænseflade blev der således identificeret to generiske fejl:
- (a) transmission af forkert output fra sammenkobling til grænsefladen
 - (b) (korrekt) input ødelagt ved grænsefladen.
- C.13.6. Der blev herefter sat mere specifikke egenskaber på disse generiske farer for hver grænseflade.
- C.13.7. I følgende fase blev bidragene fra det eksisterende systems komponenter til hver identificeret fare analyseret og samlet i et fejltræ. Dette gjorde det muligt på basis af komponenternes estimerede svigtprocenter at beregne en hyppighedsprocent for hver fare og anvende disse procenter som acceptabel farerisiko for kommende generationer af elektronisk sammenkobling.
- C.13.8. Risikoanalysen blev fulgt op og vurderet af den nationale sikkerhedsmyndighed (EBA).
- C.13.9. Som led i risikoanalysen blev der også udført en analyse af kontrol- og displayfunktioner i det elektroniske system. Igen blev et eksisterende elektronisk sammenkoblingssystem valgt som reference for at udlede sikkerhedskravene til menneske-maskine-grænsefladefunktioner (MMI, Man-Machine-Interface)) for både at kontrollere tilfældige svigt og fejl og kontrollere systematiske fejl. Som et resultat heraf blev der fastlagt sikkerhedsintegritetsniveauer (SIL'er, Safety Integrity Level) for følgende funktioner: MMI-funktioner i standarddrift, MMI-funktioner i Command-Release-drift (forringede driftsvilkår) og displayfunktionalitet.
- C.13.10. Risikoanalysen blev fulgt op og vurderet af den nationale sikkerhedsmyndighed (EBA).
- C.13.11. Disse risikovurderingseksempler illustrerer, hvordan det andet risikoacceptprincip (referencesystem) i CSM kan anvendes til at udlede sikkerhedskrav til nye systemer. Yderligere blev de baseret på CENELEC-standarderne og passer dermed godt ind i CSM-processen. Risikovurderingen i eksemplerne opfylder kravene fra CSM vedrørende de faser, som er omfattet. Men da der ikke indgår konstruktionsvirksomhed, er der hverken henvisning til håndtering af fareredegørelse eller påvisning af overensstemmelse mellem det system, der vurderes, og de identificerede sikkerhedskrav.
- C.13.12. Yderligere information om disse risikoanalyser findes i:
- (a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15, og
 - (b) Bock, H., Braband, J., and Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

C.14. Eksempel på et eksplicit risikoacceptkriterium for radiobaseret togdrift med FFB (FunkFahrBetrieb) i Tyskland

C.14.1. **Bemærkning:** Dette eksempel på risikovurdering blev ikke fremlagt som resultat af anvendelsen af CSM-processen. Det blev udført før indførelsen af CSM. Formålet med eksemplet er:

- (a) at identificere lighederne mellem de eksisterende risikovurderingsmetoder og CSM-processen
- (b) at sikre sporbarhed mellem den eksisterende proces og den, der kræves af CSM
- (c) at tilvejebringe belæg for merværdien af at gennemføre de eventuelle supplerende skridt, som CSM kræver.

Det skal understreges, at dette eksempel alene gives til information. Formålet er at hjælpe læseren med at forstå CSM-processen. Men eksemplet skal ikke i sig selv omsættes i eller anvendes som et referencesystem for en anden væsentlig ændring. Risikovurderingen skal udføres for hver væsentlig ændring i overensstemmelse med CSM-forordningen.

C.14.2. Der blev udført en risikoanalyse i overensstemmelse med CENELEC-standarderne for en helt ny driftsprocedure, som var planlagt (men aldrig indført) i Tyskland for konventionelle jernbanelinjer. Konceptet bestod i sikker drift af tog ved hjælp af radiobaseret styring (rute og tog). Da der ikke fandtes eksisterende adfærdskodekser (anerkendte anlægsforskrifter) og referencesystemer for sådan et nyt system, blev der foretaget en eksplicit risikoestimering for at påvise sikkerheden i den nye procedure. Det var nødvendigt at vise, at risikoniveauet for en passager ved det nye system ikke ville overstige en acceptabel risikoværdi (eksplicit risikoacceptkriterium).

C.14.3. Dette eksplicitte risikoacceptkriterium blev estimeret på grundlag af statistikker over ulykker i Tyskland, som kunne tilskrives signal- og kontrolsystemer, og sandsynligheden herfor blev også holdt op imod MEM-kriteriet. Denne påvisning af sikkerhed er i overensstemmelse med de tyske EBO-krav til "samme sikkerhedsniveau" i tilfælde af afvigelser fra anlægsforskrifterne. Risikoanalysen blev også fulgt op og vurderet af den nationale sikkerhedsmyndighed (EBA).

C.14.4. Risikovurderingseksemplet viser, hvordan et overordnet eksplicit kriterium (for det tredje risikoacceptprincip i CSM) kan udledes for nye systemer uden anvendelige adfærdskodekser eller referencesystemer. Risikoanalysen, som siden blev udført for det nye system, bygger på CENELEC-standarderne og passer dermed godt ind i CSM-processen. Risikovurderingen i eksemplet opfylder kravene fra CSM, men der er ingen henvisning til håndtering af fareredegørelse eller til påvisning af overensstemmelse mellem det system, der vurderes, og de identificerede sikkerhedskrav.

C.14.5. Yderligere information om denne risikoanalyse findes i: Braband, J., Günther, J., Lennartz, K., Reuter, D.: "Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)", Signal + Draht, Nr.5, 2001, 10-15.

C.15. Eksempel på anvendelighedstest af RAC-TS

C.15.1. Formålet med dette tillæg er ved hjælp af et eksempel på det mobile delsystem ETCS's funktion at vise, hvordan man anvender kriteriet i afsnit 2.5.4, og hvordan man fastslår, om RAC-TS er anvendelig.

C.15.2. Det mobile delsystem ETCS er et teknisk system. Følgende funktion tages i betragtning: "Giv lokoføreren information, der sætter ham i stand til at føre toget sikkert, og igangsæt en bremsefunktion i tilfælde af for høj hastighed".

Beskrivelse af funktionen: På basis af information modtaget fra jordbaserede anordninger (tilladt hastighed) og togets hastighedscomputer i det mobile ETCS:

- (a) styrer lokoføreren toget og sikrer, at togets hastighed ikke overstiger den tilladte, og
- (b) samtidig overvåger det mobile delsystem ETCS, at toget aldrig overstiger den tilladte hastighedsgrænse. I tilfælde af for høj hastighed udløser det automatisk bremsene.

Både lokoføreren og det mobile delsystem ETCS anvender evaluering af togets hastighed, som bliver computerbehandlet af det mobile delsystem ETCS.

C.15.3. Spørgsmål: "Finder RAC-TS anvendelse på det mobile delsystems evaluering af toghastigheden?"

C.15.4. Anvendelse af flowskemaet i Figur 14 og svar på de forskellige spørgsmål:

- (a) Omhandlet fare vedrørende det tekniske system:

"overtrædelse af den sikre hastighed jf. anbefalingen i ETCS" (jf. UNISIG SUBSET 091).

- (b) Kan faren kontrolleres af en adfærdskodeks eller et referencesystem?

NEJ. Det antages, at ETCS-systemet er en ny og innovativ konstruktion. Der er derfor ingen adfærdskodekser eller referencesystemer, som kan gøre det muligt at holde faren på et acceptabelt risikoniveau.

- (c) Er det sandsynligt, at faren kan få katastrofale følger?

JA, eftersom en overtrædelse af den sikre hastighed, *"overtrædelse af den sikre hastighed jf. anbefalingen i ETCS"*, kan medføre afsporing af toget, hvilket eventuelt kan medføre dødsfald og/eller alvorlige kvæstelser og/eller store skader på miljøet".

- (d) Er de katastrofale følger et direkte resultat af svigtet i det tekniske system?

JA, hvis der ikke findes yderligere sikkerhedsbarrierer. Den samme evaluering af toghastigheden, som computerbehandles af det mobile delsystem ETCS, sendes både til lokoføreren og bremsestyringsfunktionen i det mobile delsystem ETCS. Hvis det derfor antages, at lokoføreren (af ydelsesrelaterede årsager) fører toget ved den maksimale hastighed, der er tilladt af de faste anlæg, vil hverken lokoføreren eller det mobile delsystem ETCS detektere, at toget kører for stærkt i tilfælde af underestimering af togets hastighed. Det kan potentielt medføre en togafsporing med katastrofale følger.

- (e) Konklusioner:

- (1) for de kvantitative krav: Der bør anvendes en THR på 10^{-9} h^{-1} for de tilfældige hardwaresvigt i det mobile delsystem ETCS, og det bør sikres:

- (i) at evalueringen af dette kvantitative mål tager hensyn til de fælles komponenter i redundante systemer (f.eks. enkelt eller fælles input til alle kanaler, fælles strømforsyning, komparatorer, overvågningsudstyr osv.)
- (ii) at den tid, der skal til for at detektere hvilende eller latente svigt, er dækket
- (iii) at der udføres en analyse af Common Cause/Mode Failure (CCF/CMF)
- (iv) at der udføres en uafhængig vurdering

- (2) for proceskravene: Der bør anvendes en SIL 4-proces til styring af de systematiske svigt/fejl i det mobile delsystem ETCS. Dette kræver anvendelse af:

- (i) en kvalitetsledelsesproces, der er i overensstemmelse med SIL 4

- (ii) en sikkerhedsledelsesproces, der er i overensstemmelse med SIL 4
- (iii) de relevante standarder, f.eks.:

- ✎ til softwareudvikling bruges EN 50128-standarden
- ✎ til hardwareudvikling bruges standarderne 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 osv.,

- (3) en uafhængig vurdering af processen(erne).

C.16. Eksempler på mulige strukturer for fareredegørelsen

C.16.1. Indledning

C.16.1.1. Mindstekravene for registrering i fareredegørelsen er angivet i afsnit 4.1.2 i CSM-forordningen. De er angivet på rasterbaggrund i nedenstående eksempler på fareredegørelser.

C.16.1.2. Der kan være forskellige måder at strukturere en fareredegørelse på sammen med de yderligere oplysninger, som kunne karakterisere farerne og de tilknyttede sikkerhedsforanstaltninger. F.eks. kan farerne og tilhørende sikkerhedsforanstaltninger få ét felt pr. oplysning. Imidlertid er det vigtigt uanset valg af struktur, at fareredegørelsen tydeligt viser forbindelsen mellem farerne og de tilhørende sikkerhedsforanstaltninger. En mulig løsning er, at fareredegørelsen for hver fare og for hver sikkerhedsforanstaltning indeholder mindst ét felt med:

- (a) en klar beskrivelse, herunder henvisninger til dens oprindelse og det risikoacceptprincip, der er valgt til at kontrollere den tilhørende fare. Dette felt gør det muligt at forstå faren og de tilknyttede sikkerhedsforanstaltninger samt vide, i hvilken sikkerhedsanalyse de er blevet identificeret.

Da fareredegørelsen bruges og vedligeholdes i hele systemets livscyklus (dvs. drift og vedligeholdelse) er det nyttigt med tydelig sporbarhed eller forbindelser mellem hver fare og:

- (1) den tilhørende risiko
- (2) farens årsager, når den er identificeret
- (3) de tilknyttede sikkerhedsforanstaltninger samt de antagelser, der definerer grænserne for det system, der vurderes
- (4) de tilknyttede sikkerhedsanalyser, hvori faren blev identificeret.

Yderligere skal formuleringen af sikkerhedsforanstaltningerne (særligt dem, der skal overføres til andre aktører, f.eks. initiativtageren) og formuleringen af de tilhørende farer og risici være klar og fyldestgørende. "Klar og fyldestgørende" betyder, at det er forståeligt, hvilke risici sikkerhedsforanstaltningerne og de tilhørende farer forventes at kontrollere, uden at det er nødvendigt at gå tilbage til den pågældende sikkerhedsanalyse.

- (b) det risikoacceptprincip, der er brugt til at kontrollere faren, for at støtte den gensidige anerkendelse og hjælpe vurderingsorganet med at vurdere den korrekte anvendelse af CSM
- (c) klar oplysning om dens status: Dette felt angiver, om den tilknyttede fare/sikkerhedsforanstaltning stadig er åben eller kontrolleret/valideret.

- (1) En åben fare/sikkerhedsforanstaltning spores, indtil den er kontrolleret/valideret.

(2) Omvendt spores de kontrollerede/validerede farer/sikkerhedsforanstaltninger ikke længere, medmindre der sker væsentlige ændringer i drift eller vedligeholdelse af systemet: Se punkt [G 6](b) i afsnit 2.1.1. Hvis det sker:

- (i) anvendes CSM igen på de fornødne ændringer i overensstemmelse med Artikel 2. Se også punkt [G 6](b)(1) i afsnit 2.1.1
- (ii) genbehandles alle kontrollerede farer og sikkerhedsforanstaltninger for at kontrollere, at de ikke påvirkes af ændringerne. Hvis de påvirkes, genåbnes de pågældende farer og sikkerhedsforanstaltninger og styres igen i fareredegørelsen.

Det kunne ske, at der er gennemført andre sikkerhedsforanstaltninger end dem, der er registreret i fareredegørelsen (f.eks. til omkostningsformål). De gennemførte sikkerhedsforanstaltninger registreres derefter i fareredegørelsen med bevis/belæg for, hvorfor de er egnede, og påvisning af, at systemet med disse sikkerhedsforanstaltninger opfylder sikkerhedskravene.

- (d) henvisning til det tilhørende bevis, der kontrollerer en fare eller validerer en sikkerhedsforanstaltning. Dette felt gør, at man senere kan finde det bevis, der har gjort det muligt at kontrollere faren og validere de(n) tilknyttede sikkerhedsforanstaltning(er).

En fare kunne kun kontrolleres i fareredegørelsen, når alle de tilknyttede sikkerhedsforanstaltninger, forbundet med faren, er valideret på forhånd.

- (e) den/de organisationer eller enheder, der er ansvarlige for at håndtere fareredegørelsen.

C.16.1.3. Der gives et andet eksempel på det mulige indhold af en fareredegørelse i tillæg A.3. til vejledningen EN 50126-2 {Ref. 9}.

C.16.2. Eksempel på faredegørelsen for den organisatoriske ændring i afsnit C.5. i tillæg C

Tabel 6: Eksempel på faredegørelsen for den organisatoriske ændring i afsnit C.5. i tillæg C

Farebeskrivelse	Sikkerhedsforanstaltninger	Prioritering / Sikkerhed Præcision	Gennemførelse ⁽¹⁸⁾	Noter	Ansvar ⁽¹⁸⁾	Oprindelse	Anvendt risikoaccept-princip	Ansvar for verificering	Verificeringsmetode	Status xx.xx.xx
Mindsket motivation hos tilbageværende medarbejdere i selskabet. Derfor forsvinder der konstant personale. Demotiverede/udbrændte ledere	Ny omgang motiverende arbejde til personalet; skal udføres i mindre grupper. Omfordeling af midler, så selskabet får meningsfyldte opgaver at udføre. Hyppigere inspektion foretaget af sporchefen. Tildeling af midler for at sikre, at nøglemedarbejdere bliver processen ud. Særlig opmærksomhed på at sikre, at information og viden overføres mellem afgående medarbejdere og dem, som overtager opgaverne. Osv.	Høj / høj	Koordineret af XYZ. Regionerne skal se på foranstaltninger til øget kontrol med sporene, overlappende medarbejdere og opfølgning fra linjefestens side	Flere inspektioner skal indgå i kontrakterne. Osv.	Selskabets leder	Brainstorming HAZID rapport R _x	Ikke relevant			Ændring af forholdene har reduceret denne risiko betydeligt Arbejdsmiljøanalyse udført og uddannelse af personale.
Underleverandører til entreprenørerne mangler færdigheder, kompetence og kvalitetskontrol	Øgede krav om dokumenteret kompetence. Systematisk kontrol af udførte opgaver	Høj / middelhøj	IF skal koordinere. Regionerne skal gennemføre foranstaltninger til krav om kompetence og kontrol af arbejdet	Gennemført ved opfølgning på kontrakt. Input til revisionsplanlægning.	Infrastrukturforvalter	Brainstorming HAZID rapport R _x	Ikke relevant	Sikkerhedschef		Øget fokus på rutiner til kontrol (to driftskontroller pr. måned og pr. driftsområde)
Uvished med hensyn til roller og ansvar ved grænsefladen mellem selskabet og IM (sporchef)	Definere roller og ansvar. Kortlægge alle grænseflader og definere, hvem der er ansvarlig for grænsefladerne	Middelhøj / middelhøj	I hver region for sig	Gennemført ved hjælp af vedligeholdelseskontrakt og strategiplan for reorganisering	Regionale direktører	Brainstorming HAZID rapport R _x	Ikke relevant	Sikkerhedschef		Regionerne har præsenteret deres strategi.

⁽¹⁸⁾ Disse to kolonner vedrører informationen/feltet om de aktører, der har ansvaret for at kontrollere de identificerede farer.

C.16.3. Eksempel på en komplet fareredegørelse for delsystemet mobil styringskontrol

C.16.3.1. Dette afsnit giver et eksempel på en enkelt fareredegørelse (jf. punkt [G 3] i afsnit 4.1.1) til styring af både:

- alle de interne sikkerhedskrav, der gælder for delsystemet, som aktøren er ansvarlig for, og
- alle identificerede farer og tilknyttede sikkerhedsforanstaltninger, som aktøren ikke kan gennemføre, og som skal overføres til andre aktører.

Tabel 7: Eksempel på en fabrikants fareredegørelse for delsystemet mobil styringskontrol.

Fare nr.	Oprindelse	Farebeskrivelse	Yderligere oplysninger	Ansvarlig aktør	Sikkerhedsforanstaltning	Anvendt risikoaccept princip	Ekspor-teret	Status
1	HAZOP rapport R _x	Maksimal toghastighed sat for højt (V _{max})	Forkert specifik konfiguration af det mobile delsystem (vedligeholdelsespersonale). Forkert dataindførsel om bord (lokoførere)	Jernbane-virksomhed	<ul style="list-style-type: none"> Definere en procedure for godkendelse af konfigurationsdata til det mobile delsystem Definere en driftsprocedure for lokoførers indførsel af data 	EksPLICIT risiko-estimering	Ja	Kontrolleret (eksporteret til JV) Se også afsnit i tillæg C
2	HAZOP rapport R _x	Bremsekurver (dvs. kørselstilladelse) i konfigurationsdata til det mobile delsystem er for lemfældige	Proceduren for den specifikke konfiguration af det mobile delsystem afhænger af: <ul style="list-style-type: none"> sikkerhedsmarginer for togets bremsesystem, reaktionsforsinkelse i togets bremsesystem (dette er direkte afhængigt af togets længde, særligt for godstog) 	Jernbane-virksomhed	<ul style="list-style-type: none"> Specificere systemkrav korrekt i systemdefinition Fastlægge tilstrækkelige sikkerhedsmarginer for bremsesystemet i det specifikke tog 	EksPLICIT risiko-estimering	Ja	Kontrolleret (eksporteret til JV) Se også afsnit Error! Reference source not found. i tillæg C
3	HAZOP rapport R _x	<ul style="list-style-type: none"> Maksimal toghastighed sat for højt (V_{max}) Bremsekurver (dvs. kørselstilladelse) i konfigurationsdata til det mobile delsystem er for lemfældige 	Mangel på opdatering af togets hjul diameter i den specifikke konfiguration af det mobile delsystem (vedligeholdelsespersonale)	Jernbane-virksomhed	<ul style="list-style-type: none"> Definere en procedure for vedligeholdelsespersonalets måling af togets hjul diameter Definere en procedure for regelmæssig opdatering af togets hjul diameter i det mobile delsystem 	EksPLICIT risiko-estimering	Ja	Kontrolleret (eksporteret til JV) Se også afsnit Error! Reference source not found. i tillæg C
			Mangel i fabrikantens procedure vedrørende forberedelse og indlæsning af konfigurationsdata i det mobile delsystem	Fabrikant	Definere en procedure for opdatering af togets hjul diameter i de mobile konfigurationsdata	EksPLICIT risiko-estimering	Ja	Kontrolleret ved procedure P _x

Tabel 7: Eksempel på en fabrikants fareredegørelse for delsystemet mobil styringskontrol.

Fare nr.	Oprindelse	Farebeskrivelse	Yderligere oplysninger	Ansvarlig aktør	Sikkerhedsforanstaltning	Anvendt risikoaccept princip	Eksporteret	Status
4	HAZOP rapport R _x	Indsættelse af toget ved en høj hastighed (160 km/h, hvis optisk signal om fri bane) på sporet, uden at det mobile delsystem er aktivt og uden optiske signaler	Kunne kun kontrolleres ved hjælp af lokoførerens agtpågivenhed. Indkørsel på et område med ATP afhænger af, at lokoføreren udfører en bekræftelsesprocedure, inden han passerer overgangsstedet. Hvis der ikke bekræftes, aktiveres togets bremses automatisk af det mobile styringskontroldelsystem	Infrastrukturforvalter	Infrastrukturforvalteren skal sikre, at tog, der ikke er udstyret med et aktivt mobilt styringskontroldelsystem, ikke kører ind på det givne spor. Definere en procedure for trafikstyring	EksPLICIT risikoestimering	Ja	Kontrolleret (eksporteret til IF) Se også afsnit Error! Reference source not found. i tillæg C
				Jernbanevirksomhed	Sikre lokoførerens uddannelse i at køre ind på et område med ATP	EksPLICIT risikoestimering	Ja	Kontrolleret (eksporteret til JV) Se også afsnit i tillæg C
5	HAZOP rapport R _x	Maksimal toghastighed som vist for lokoføreren sat for højt (V _{max})	Informationen, der vises på lokoførerens grænseflade, overvåges af det mobile SIL 4 styringskontroldelsystem, som aktiverer nødbremsene, hvis der opstår en uoverensstemmelse mellem vist hastighed og forventet værdi. I tilfælde af manglende overholdelse af kørselstilladelsen aktiverer det mobile styringskontroldelsystem nødbremsene	Fabrikant	Udvikle et mobilt SIL 4 styringskontroldelsystem	EksPLICIT risikoestimering	Ja	Sikkerhedscase, der påviser et SIL 4 delsystem vurderet af et uafhængigt vurderingsorgan
6	HAZOP rapport R _x	Toget afgår uden grænseflade mellem lokomotivfører og førerrumsudrustning	Tab af redundant arkitektur i det mobile delsystem	Fabrikant	Udvikle et mobilt SIL 4 styringskontroldelsystem	EksPLICIT risikoestimering	Ja	Sikkerhedscase, der påviser et SIL 4 delsystem vurderet af et uafhængigt vurderingsorgan
Osv.								

C.16.4. Eksempel på en fareredegørelse for overførsel af information til andre aktører

C.16.4.1 Dette afsnit giver et eksempel på en fareredegørelse for overførsel til andre aktører af identificerede farer og tilknyttede sikkerhedsforanstaltninger, som en given aktør ikke kan gennemføre. Se punkt [G 1] i afsnit 4.1.1.

Dette eksempel er det samme som eksemplet i afsnit C.16.3. i tillæg C. Den eneste forskel er, at alle de interne farer og sikkerhedsforanstaltninger, som kunne kontrolleres af den givne aktør, er fjernet.

C.16.4.2. Sidste kolonne bruges til at opfylde kravet i afsnit 4.2 i CSM-forordningen. Der er forskellige måder at løse dette på. En af dem kan være at henvise til det bevis, som den aktør, der modtager den eksporterede sikkerhedsinformation, har gjort brug af. En anden måde kunne være at holde et møde mellem de to aktører for i fællesskab at finde frem til en tilstrækkelig løsning på kontrol med de tilhørende risici. Resultaterne af et sådant møde kunne rapporteres i et aftalt dokument (f.eks. et mødereferat), som aktøren, der eksporterer den sikkerhedsrelaterede information, kan henvise til med henblik på at lukke de tilhørende farer i sin fareredegørelse.

Tabel 8: Eksempel på en fareredegørelse for overførsel af sikkerhedsrelateret information til andre aktører

Fare nr.	Farens oprindelse		Farebeskrivelse	Yderligere oplysninger	Ansvarlig aktør	Sikkerhedsforanstaltning	Kommentar fra modtager
	Nr. i Tabel 7	Andet					
1	Nr. 1	HAZOP rapport R _x	Maksimal toghastighed sat for højt (V _{max})	Forkert specifik konfiguration af det mobile delsystem (vedligeholdelsespersonale). Forkert dataindførsel om bord (lokofører)	Jernbane-virksomhed	<ul style="list-style-type: none"> Definere en procedure for godkendelse af konfigurationsdata til det mobile delsystem Definere en driftsprocedure for lokoførerens indførsel af data 	<ul style="list-style-type: none"> Konfigurationsdata for det mobile styringskontrollsystem afhænger af det rullende materiels fysiske karakteristika. Derefter anvendes sikkerhedsmarginer på disse data i et samarbejde mellem infrastrukturforvalteren og jernbanevirksomheden. Disse data indlæses derefter i det mobile delsystem i overensstemmelse med fabrikantens relevante procedure under installationen, integrationen i det rullende materiel og accepten af styringskontrollsystemet. Lokoførerne uddannes og bedømmes efter procedure D_p. Lokoførerne bedømmes også af IF efter de regler, der gælder for IF's infrastruktur.
2	Nr. 2	HAZOP rapport R _x	Bremsekurver (dvs. kørselstilladelse) i konfigurationsdata til det mobile delsystem er for lemfældige	Proceduren for den specifikke konfiguration af det mobile delsystem afhænger af: <ul style="list-style-type: none"> sikkerhedsmarginer for togets bremsesystem reaktionsforsinkelse i togets 	Jernbane-virksomhed	<ul style="list-style-type: none"> Specificere systemkrav korrekt i systemdefinition Fastlægge tilstrækkelige sikkerhedsmarginer for bremsesystemet i det specifikke tog 	Se kommentar til linje 1 ovenfor.

Tabel 8: Eksempel på en fareredegørelse for overførsel af sikkerhedsrelateret information til andre aktører

Fare nr.	Farens oprindelse		Farebeskrivelse	Yderligere oplysninger	Ansvarlig aktør	Sikkerhedsforanstaltning	Kommentar fra modtager
	Nr. i Tabel 7	Andet					
				bremsesystem (dette er direkte afhængigt af togets længde, særligt for godstog)			
3	Nr. 3	HAZOP rapport R _x	<ul style="list-style-type: none"> Maksimal toghastighed sat for højt (V_{max}) Bremsekurver (dvs. kørselstilladelse) i konfigurationsdata til det mobile delsystem er for lemfældige 	Mangel på opdatering af togets hjul diameter i den specifikke konfiguration af det mobile delsystem (vedligeholdelsespersonale)	Jernbane-virksomhed	<ul style="list-style-type: none"> Definere en procedure for vedligeholdelsespersonalets måling af togets hjul diameter Definere en procedure for regelmæssig opdatering af togets hjul diameter i det mobile delsystem 	<ul style="list-style-type: none"> Vedligeholdelse af det mobile styringskontroldelsystem foregår i overensstemmelse med vedligeholdelsesprocedure MP "Maintenance Procedure MP_z". Togets hjul diameter opdateres med fastlagte mellemrum efter procedure P_w. Med hensyn til dataindførselsprocessen uddannes og bedømmes lokoførerne efter "Procedure P_{DE}".
4	Nr. 4	HAZOP rapport R _x	Indsættelse af toget ved en høj hastighed (160 km/h, hvis optisk signal om fri bane) på sporet, uden at det mobile delsystem er aktivt og uden optiske signaler	Kunne kun kontrolleres ved hjælp af lokoførerens agtpågivenhed. Indkørsel på et område med ATP afhænger af, at lokoføreren udfører en bekræftelsesprocedure, inden han passerer overgangsstedet. Hvis der ikke bekræftes, aktiveres togets brems automatisk af det mobile styringskontroldelsystem	Infrastruktur-forvalter	<p>Infrastrukturforvalteren skal sikre, at tog, der ikke er udstyret med et aktivt mobilt styringskontroldelsystem, ikke kører ind på det givne spor.</p> <p>Definere en procedure for trafikstyring</p>	Trafikstyringen på IM's infrastruktur reguleres af regelsættet R _{TM}
					Jernbane-virksomhed	Sikre lokoførerens uddannelse i at køre ind på et område med ATP	<ul style="list-style-type: none"> Lokoførerne uddannes med jævne mellemrum efter IM's procedure P_{IM_DP} Lokoførerne bedømmes også af IM efter det regelsæt (S_R), der gælder for IM's infrastruktur.
Osv.							

C.17. Eksempel på en generisk fareliste for jernbanedrift

C.17.1. Med ROSA (Rail Optimisation Safety Analysis), et projekt i DEUFRAKO (fransk-tysk samarbejde), blev der gjort forsøg på at opstille en generisk og udtømmende fareliste, der dækker normal jernbanedrift. Målet og udfordringen var at definere disse farer på et maksimalt detaljeniveau uden skelen til særtræk ved henholdsvis franske og tyske jernbaner. Listen blev opstillet ved hjælp af bestående farelister fra begge lande (SNCF og DB) samt krydstjekket med farelister fra andre lande. Til trods for det erklærede mål om, at listen skulle være udtømmende og generisk, gives listen her kun som vejledende eksempel, der kan tjene som hjælp for aktørerne, når de skal identificere farer ved et givet projekt. Det forventes, at farerne i listen sandsynligvis skal finpudses eller suppleres for at afspejle projektets særlige forhold.

C.17.2. Farerne i udkastet til liste nedenfor kaldes "starting point hazards" (SPH), dvs. farer, der danner udgangspunkt for såvel en konsekvensanalyse som en årsagsanalyse med henblik på at fastslå sikkerhedsforanstaltninger/barrierer og sikkerhedskrav til kontrol med farerne.

C.17.3. ROSA-projektets fareliste:

SPH 01	Oprindelig forkert fastlæggelse af hastighedsgrænse (relateret til infrastruktur)
SPH 02	Forkert fastlæggelse af hastighedsgrænse (togrelateret)
SPH 03	Forkert bremselængde fastlagt/forkert hastighedsprofil/forkerte bremsekurver
SPH 04	Utilstrækkelig deceleration (fysiske årsager)
SPH 05	Forkert/uegnet hastigheds-/bremsekommando
SPH 06	Forkert hastighed registreret (forkert toghastighed)
SPH 07	Svigt i kommunikation af hastighedsgrænse
SPH 08	Toget ruller af sted
SPH 09	Forkert køreretning/forsætlig baglænskørsel - (kombination af SPH 08 og SPH 14)
SPH 10	Forkert absolut/relativ position registreret
SPH 11	Togdetektionssvigt
SPH 12	Tab af togintegritet
SPH 13	Eventuelt forkert rute for toget
SPH 14	Svigt i transmission/kommunikation af køreplan/kørselstilladelse
SPH 15	Struktursvigt i ledeskinne
SPH 16	Afbryderkomponent ødelagt
SPH 17	Forkert afbryderkommando
SPH 18	Forkert afbryderstatus
SPH 19	Systemgenstand på ledeskinne / inden for fritrumsprofilen (ekskl. ballast)
SPH 20	Fremmedlegeme på ledeskinne / inden for fritrumsprofilen
SPH 21	Vejtrafikant på overskæring
SPH 22	Slipstrømsvirkninger på ballast
SPH 23	Aerodynamiske kræfters indvirkning på toget
SPH 24	Togets udstyr/element/last overskrider togets fritrumsprofil
SPH 25	Ukorrekt fritrumsprofil for toget (sporkanten)
SPH 26	Forkert lastfordeling
SPH 27	Knækket hjul, knækket aksel
SPH 28	Overophedet aksel/hjul/leje
SPH 29	Svigt i bogie/ophæng, dæmpning
SPH 30	Svigt i chassis/vognkasse
SPH 31	Uvedkommende på sporet (sikkerhedsaspekt)
SPH 32	Personer med tilladelse krydser sporet

SPH 33	Arbejdende personale på sporet
SPH 34	Person uden tilladelse trænger ind på sporet (forsømmelighed)
SPH 35	Person falder fra perronkanten ned på sporet
SPH 36	Slipstrøm/person for tæt på perronkant
SPH 37	Arbejdende personale nær sporet, f.eks. nabospor
SPH 38	Person forlader toget forsætligt (ekskl. passagerudveksling)
SPH 39	Person falder ud ad (side-) dør
SPH 40	Person falder ud ad døren i endevæggen
SPH 41	Toget afgår/ruller af sted med åbne døre (fritrumsprofil ikke overskredet)
SPH 42	Person falder i mellemgangen mellem to vogne
SPH 43	Passager læner sig ud ad dør
SPH 44	Passager læner sig ud ad vindue
SPH 45	Personale/togbetjent læner sig ud ad dør
SPH 46	Personale/togbetjent læner sig ud ad vindue
SPH 47	Rangerpersonale på toget læner sig ud fra trin
SPH 48	Person falder/kravler fra perron ned i mellemrummet mellem tog og perron
SPH 49	Person falder ud af/forlader toget, hvor der ikke er en perron
SPH 50	Person falder i dørrådet ved passagerudveksling
SPH 51	Togets døre lukker sig, mens en person befinder sig i dørrådet
SPH 52	Toget bevæger sig under passagerudveksling
SPH 53	Risiko for, at en person bliver kvæstet i toget
SPH 54	Brand-/eksplosionsfare (i/ved toget) - ulykkeskategori, konsekvens af SPH 55, SPH56)
SPH 55	Ukorrekt temperatur (i toget)
SPH 56	Forgiftning/iltmangel (i/ved toget)
SPH 57	Elektrisk stød (i/ved toget)
SPH 58	Person falder (ned) på perron (ekskl. passagerudveksling)
SPH 59	Ukorrekt temperatur (på perron)
SPH 60	Forgiftning/iltmangel (på perron)
SPH 61	Elektrisk stød (på perron)