



Eiropas Dzelzceļa aģentūra

Rokasgrāmata, kā piemērot Komisijas regulu par kopīgas drošības metodes ieviešanu riska noteikšanai un novērtēšanai atbilstoši Dzelzceļa drošības direktīvas 6. panta 3. punkta a) apakšpunktam

Atsauce ERA:	ERA/GUI/01-2008/SAF
Versija ERA:	1.1.
Datums:	06.01.2009.

Dokumentu izstrādāja:	Eiropas Dzelzceļa aģentūra Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Francija
Dokumenta veids:	Rokasgrāmata
Dokumenta statuss:	Publisks

	Vārds	Amats
Atļāva publicēt	<i>Marcel VERSLYPE</i>	Izpilddirektors
Pārskatīja	<i>Anders LUNDSTRÖM</i> <i>Thierry BREYNE</i>	Drošības nodaļas vadītājs Drošības novērtēšanas sektora vadītājs
Autors	<i>Dragan JOVICIC</i>	Drošības nodaļa – projekta amatpersona

INFORMĀCIJA PAR DOKUMENTU

Grozījumu uzskaitē

1. tabula: Dokumenta statuss.

Versija Datums	Autors(i)	Iedaļas numurs	Grozījuma apraksts
Vecā dokumenta nosaukums un struktūra: „Norādījumi, kā izmantot ieteikumu attiecībā uz CSM pirmo kopumu”			
Norādījums u 0.1. versija 15.02.2007	<i>Dragan JOVICIC</i>	Visas	„Izmantošanas norādījumu” pirmā versija, kas saistīta ar “CSM ieteikumu pirmā kopuma” 1.0. versiju. Šī ir arī dokumenta pirmā versija, kas nodota CSM darba grupai oficiālai pārskatīšanai.
Norādījums u 0.2. versija 07.06.2007	<i>Dragan JOVICIC</i>	Visas	Reorganizē dokumentu, lai tas saskanētu ar CSM ieteikuma 4.0. versijas struktūru. Atjaunina, ņemot vērā CSM darba grupas veikto <u>oficiālo pārskatīšanas procesu</u> attiecībā uz ieteikuma 1.0. versiju.
		Visas	Atjaunina dokumentu ar papildu informāciju, kas savākta ERA iekšējo sanāksmju laikā, kā arī ar pieprasījumiem, kas saņemti no CSM darba grupas, par jauno punktu izstrādi.
		3. shēma	Groza shēmu, kas pārstāv „risku pārvaldības sistēmu pirmajam kopīgo drošības metožu kopumam” – gan saskaņā ar pārskata atsauksmēm, gan ISO terminoloģiju.
Norādījums u 0.3. versija 20.07.2007	<i>Dragan JOVICIC</i>	Papildinājumi	Reorganizē papildinājumus un izveido jaunus papildinājumus. Jauns papildinājums, kurā apkopotas visas diagrammas, kas ar piemēriem ilustrē rokasgrāmatu un ļauj vieglāk to lasīt un saprast.
		Visas iedaļas	Dokuments atjaunināts, lai: <ul style="list-style-type: none"> pēc iespējas izstrādātu esošās x iedaļas, turpmāk izstrādātu to, uz ko attiecas „sistēmas atbilstības pierādīšana saskaņā ar noteiktajām drošības prasībām”, izveidotu saiti ar CENELEC V-Cycle (t.i., EN 50 126 8. un 10. shēmu), turpmāk izstrādātu sadarbības un saskaņošanas vajadzību starp dažādajiem dzelzceļa nozares dalībniekiem, kuru darbības var ietekmēt dzelzceļa sistēmas drošību, paskaidrotu pierādījumus (piemēram, apdraudējumu žurnālu un apliecinājuma dokumentāciju), ar ko plānots pierādīt novērtēšanas iestādēm, ka CSM riska novērtēšanas process tiek piemērots pareizi. Dokuments atjaunināts arī atbilstīgi Aģentūras pirmajam iekšējam pārskatam.
Norādījums u 0.4. versija 16.11.2007	<i>Dragan JOVICIC</i>	Visas iedaļas	Dokuments atjaunināts pēc <u>oficiāla pārskatīšanas procesa</u> atbilstīgi atsauksmēm, kas par 0.3. versiju saņemtas no šādiem CSM darba grupas locekļiem vai organizācijām un saskaņotas ar tiem telefona sarunu laikā: <ul style="list-style-type: none"> Beļģijas, Spānijas, Somijas, Norvēģijas, Francijas un Dānijas valsts drošības iestādes, SIEMENS (UNIFE loceklis), Norvēģijas infrastruktūras pārvaldītājs (<i>Jernbaneverket – EIM</i> loceklis)
Norādījums u 0.5. versija	<i>Dragan JOVICIC</i>	Visas iedaļas	Dokuments atjaunināts atbilstīgi atsauksmēm, kas par 0.3. versiju saņemtas no šādiem CSM darba grupas locekļiem vai organizācijām un saskaņotas ar tiem telefona sarunu laikā:



1. tabula: Dokumenta statuss.

Versija Datums	Autors(i)	Iedaļas numurs	Grozījuma apraksts
27.02.2008			<ul style="list-style-type: none"> Eiropas dzelzceļu un infrastruktūras uzņēmumu kopienas (CER), Nīderlandes valsts drošības iestādes
		Visas iedaļas	Dokuments atjaunināts saskaņā ar CSM ieteikuma parakstīto versiju. Dokuments atjaunināts atbilstīgi Aģentūras iekšējās pārskatīšanas atsauksmēm, kas saņemtas no <i>Christophe CASSIR</i> un <i>Marcus ANDERSSON</i>
		Visas iedaļas Papildinājumi	Daļu pilnīgā pārnumerācija dokumentā, ņemot vērā ieteikumu. Iekļauti piemēri par CSM ieteikuma piemērošanu.
Jaunā dokumenta nosaukums un struktūra: „Rokasgrāmata, kā piemērot CSM regulu”			
Rokasgrāmatas 0.1. versija 23.05.2008	<i>Dragan JOVICIC</i>	Visas	Dokumenta pirmā versija, kas iegūta, sadalot „izmantošanas norādījumu” 0.5. versiju divos papildu dokumentos.
Rokasgrāmatas 0.2. versija 03.09.2008	<i>Dragan JOVICIC</i>	Visas	Dokumenta atjauninājums saskaņā ar: <ul style="list-style-type: none"> Eiropas Komisijas CSM regulu {Ref. 2}, atsauksmes, kas izteiktas 2008. gada 1. jūlija darbseminārā ar Dzelzceļa savstarpējās izmantojamības un drošības komitejas (RISC) locekļiem, atsauksmes no CSM darba grupas locekļiem (Norvēģijas NSA, Somijas NSA, Apvienotās Karalistes NSA, Francijas NSA, CER, EIM, Jens BRABAND [UNIFE] un Stéphane ROMEI [UNIFE]).
Rokasgrāmatas 1.0 versija 10.12.2008	<i>Dragan JOVICIC</i>	Visas	Dokumenta atjauninājums saskaņā ar Eiropas Komisijas CSM regulu par riska noteikšanu un novērtēšanu {Ref. 2}, ko pieņēmusi Dzelzceļa savstarpējās izmantojamības un drošības komiteja (RISC) savā pilnsapulcē 2008. gada 25. novembrī
Rokasgrāmatas 1.1. versija 06.01.2009.	<i>Dragan JOVICIC</i>	Visas	Dokumenta atjauninājums atbilstīgi tām atsauksmēm par CSM regulu, ko iesniedzis Eiropas Komisijas juridiskais un valodu dienests.

Saturs

INFORMĀCIJA PAR DOKUMENTU	2
Grozījumu uzskaitē	2
Saturs 4	
Shēmu saraksts	5
Tabulu saraksts	5
0. IEVADS	6
0.1. Tvērums	6
0.2. Ārpus tvēruma	6
0.3. Šīs rokasgrāmatas princips	6
0.4. Dokumenta apraksts	7
0.5. Atsauces dokumenti	7
0.6. Standarta definīcijas, termini un saīsinājumi	7
0.7. Specifiskas definīcijas	8
0.8. Specifiski termini un saīsinājumi	8
CSM REGULAS PANTU PASKAIDROJUMS	9
1. pants. Nolūks	9
2. pants. Tvērums	10
3. pants. Definīcijas	13
4. pants. Būtiskas izmaiņas	15
4. panta 1. punkts	15
4. panta 2. punkts	16
5. pants. Riska pārvaldības process	18
6. pants. Neatkarīgs novērtējums	19
7. pants. Drošības novērtējuma ziņojumi	21
8. pants. Riska kontroles pārvaldība/iekšējās un ārējās revīzijas	22
9. pants. Atsauksmes un tehniskais progress	23
10. pants. Stāšanās spēkā	24
I PIELIKUMS – PASKAIDROJUMS PAR PROCESU CSM REGULĀ	25
1. VISPĀRĪGIE PRINCIPI, KAS PIEMĒROJAMI RISKA PĀRVALDĪBAS PROCESAM	25
1.1. Vispārīgie principi un saistības	25
1.2. Saskaņo pārvaldība	29
2. RISKA NOVĒRTĒŠANAS PROCESA APRAKSTS	32
2.1. Vispārīgs apraksts	32
2.2. Apdraudējuma noteikšana	35
2.3. Prakses kodeksu izmantošana un riska noteikšana	38
2.4. Atsauces sistēmas izmantošana un riska noteikšana	41
2.5. Precīza riska prognoze un noteikšana	42
3. PIERĀDĪJUMS PAR ATBILSTĪBU DROŠĪBAS PRASĪBĀM	46
4. APDRAUDĒJUMU PĀRVALDĪBA	48
4.1. Apdraudējumu pārvaldības process	48
4.2. Informācijas apmaiņa	51
5. RISKA PĀRVALDĪBAS PROCESA PIEMĒROŠANAS DOKUMENTĀCIJA	52

CSM REGULAS II PIELIKUMS	54
Kritēriji, kas jāievēro novērtēšanas iestādēm	54

Shēmu saraksts

1. shēma: 4. pantā minēto kritēriju izmantošana, lai novērtētu izmaiņas būtiskumu	16
2. shēma: Ar drošību saistītas izmaiņas un CSM stāšanās spēkā.	18
3. shēma: Riska pārvaldības sistēma CSM regulā {Ref. 2}.	26

Tabulu saraksts

1. tabula: Dokumenta statuss.	2
2. tabula: Atsauces dokumentu tabula.	7
3. tabula: Terminu tabula.	8
4. tabula: Saīsinājumu tabula.	8

0. IEVADS

0.1. Tvērums

- 0.1.1. Šajā rokasgrāmatā ir sniegta informācija par to, kā piemērot Komisijas Regulu par kopīgas drošības metodes ieviešanu riska noteikšanai un novērtēšanai atbilstoši Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK 6. panta 3. punkta a) apakšpunktam. {Ref. 2}. Šajā dokumentā minētā regula tiks saukta par „CSM regulu”.
- 0.1.2. Šajā rokasgrāmatā nav tiesiski saistošu padomu. Tajā ir paskaidrojoša informācija par iespējamo izmantošanu visiem dalībniekiem¹, kuru darbībām var būt ietekme uz dzelzceļa sistēmu drošību un kuriem tieši vai netieši jāpiemēro CSM regula. Tā var noderēt kā paskaidrojuma instruments, tomēr nekādā veidā nediktējot obligāti ievērojamas procedūras un nenosakot nekādu tiesiski saistošu praksi. Šajā rokasgrāmatā ir paskaidroti noteikumi, kas ietverti CSM regulā, lai būtu vieglāk saprast tajā aprakstītās pieejas un normas. Dalībnieki var turpināt izmantot esošās metodes, lai panāktu atbilstību CSM regulai.
- 0.1.3. Rokasgrāmata jālasa un jāizmanto tikai kā nesaistošs informatīvs dokuments, kas palīdz piemērot CSM regulu. Rokasgrāmata jāizmanto kopā ar CSM regulu, lai atvieglotu tās piemērošanu, bet tā neaizstāj minēto regulu.
- 0.1.4. Šo rokasgrāmatu ir sagatavojusi Eiropas Dzelzceļa aģentūra (ERA) ar atbalstu no dzelzceļu asociācijas un valsts drošības iestāžu ekspertiem no CSM darba grupas puses. Tajā apkopotas idejas un informācija, ko Aģentūra savākusi iekšējo sanāksmju laikā, kā arī, tiekoties ar CSM darba grupu un CSM darba grupām atsevišķos jautājumos. Vajadzības gadījumā ERA pārskatīs un atjauninās rokasgrāmatu, lai atspoguļotu Eiropas standartu attīstību, izmaiņas kopīgajās drošības metodēs attiecībā uz riska novērtēšanu un iespējamam atsauksmēm no pieredzes, kas gūta CSM regulas izmantošanas laikā. Tā kā šā dokumenta sastādīšanas laikā nav iespējams paredzēt tāda pārskatīšanas procesa grafiku, lasītājam jāvērsas pie Eiropas Dzelzceļa aģentūras, lai saņemtu informāciju par rokasgrāmatas jaunāko pieejamo izdevumu.

0.2. Ārpus tvēruma

- 0.2.1. Šī rokasgrāmata nesniedz norādījumus par to, kā organizēt, ekspluatēt vai projektēt (un ražot) dzelzceļa sistēmu vai tās daļas. Tajā arī nav noteikti līgumi un vienošanās, kas var būt noslēgti starp dalībniekiem, lai piemērotu riska pārvaldības procesu. Projektam specifiskie līgumi ir ārpus CSM regulas un saistītās rokasgrāmatas tvēruma.

0.3. Šīs rokasgrāmatas princips

- 0.3.1. Lai gan šī rokasgrāmata var šķist kā atsevišķi lasāms dokuments, tā neaizstāj CSM regulu {Ref. 2}. Lai būtu ērtāk lasīt atsauces, šajā rokasgrāmatā ir apkopēti katrs CSM regulas pants. Tad nākamajos punktos ir sniegti norādījumi, lai tur, kur to uzskata par vajadzīgu, palīdzētu labāk saprast minētos pantus.

¹ Attiecīgie dalībnieki ir līgumslēdzēji subjekti, kas noteikti Direktīvas 2008/57/EK par dzelzceļa sistēmas savstarpēju izmantojamību Kopienā 2. panta r) apakšpunktā, vai ražotāji, kas regulā minēti kā „priekšlikuma iesniedzēji”, vai viņu piegādātāji un pakalpojumu sniedzēji.

0.3.2. CSM regulas panti ar punktiem un apakšpunktiem ir pārkopēti esošajā dokumentā tekstlodziņā, izmantojot „Bookman Old Style” slīprakstu tā, kā šis teksts. Šāda rakstīšana dod iespēju viegli atšķirt CSM regulas oriģinālo tekstu no šajā dokumentā esošajiem papildu paskaidrojumiem.

0.3.3. Lai palīdzētu lasītājam, šā dokumenta struktūra ir veidota, ievērojot CSM regulas struktūru.

0.4. Dokumenta apraksts

0.4.1. Dokuments ir sadalīts šādās daļās:

- (a) 0. nodaļā ir noteikts rokasgrāmatas tvērums un sniegts atsaucēs dokumentu saraksts,
- (b) CSM regulas pantu paskaidrojums,
- (c) I pielikums: procesa paskaidrojums CSM regulā,
- (d) II pielikums: kritēriji, kas jāizpilda novērtēšanas iestādēm.

0.5. Atsauces dokumenti

2. tabula: Atsauces dokumentu tabula.

{Ref. N°}	Nosaukums	Atsauce	Versija
{Ref. 1}	Eiropas Parlamenta un Padomes 2004. gada 29. aprīļa Direktīva 2004/49/EK par drošību Kopienas dzelzceļos, un par Padomes Direktīvas 95/18/EK par dzelzceļa pārvadājumu uzņēmumu licencēšanu un Direktīvas 2001/14/EK par dzelzceļa infrastruktūras jaudas sadali un maksas iekasēšanu par dzelzceļa infrastruktūras izmantošanu un drošības sertifikāciju grozījumiem (Dzelzceļu drošības direktīva)	2004/49/EK OV L 164, 30.4.2004., 44. lpp., kurā labojums izdarīts ar OV L 220, 21.6.2004., 16. lpp.	-
{Ref. 2}	Komisijas [...] Regula (EK) Nr. .../.. par kopīgas drošības metodes ieviešanu riska noteikšanai un novērtēšanai atbilstoši Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK 6. panta 3. punkta a) apakšpunktam	xxxx/yy/EK	balsojusi RISC 25.11.2008.
{Ref. 3}	Eiropas Parlamenta un Padomes 2008. gada 17. jūnija Direktīva 2008/57/EK par dzelzceļa sistēmas savstarpēju izmantojamību Kopienā	2008/57/EK OV L 191, 18.7.2008., 1. lpp.	-
{Ref. 4}	Drošības pārvaldības sistēma – novērtēšanas kritēriji dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem	SMS novērtēšanas kritēriji A daļa. Drošības sertifikāti un atļaujas	31.05.2007.
{Ref. 5}	Komisijas Lēmums par kopīgas drošības metodes pieņemšanu, lai novērtētu drošības mērķu sasniegšanu, kā minēts Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK 6. pantā	xxxx/yy/EK	balsojusi RISC 25.11.2008.
{Ref. 6}	/		

0.6. Standarta definīcijas, termini un saīsinājumi

0.6.1. Vispārīgās definīcijas, terminus un saīsinājumus, kas izmantoti šajā dokumentā, var atrast standarta vārdnīcā.

0.6.2. Šajā rokasgrāmatā izmantotās jaunās definīcijas, termini un saīsinājumi ir definēti turpmākajās iedaļās.

0.7. Specifiskas definīcijas

0.7.1. Skatīt 3. pantu.

0.8. Specifiski termini un saīsinājumi

0.8.1. Šajā iedaļā ir definēti jaunie specifiskie termini un saīsinājumi, kas bieži izmantoti šajā dokumentā.

3. tabula: Terminu tabula.

Termins	Definīcija
Aģentūra	Eiropas Dzelzceļa aģentūra (ERA)
rokasgrāmata	“rokasgrāmata, kā piemērot Komisijas [...] Regulu (EK) Nr. .../.. par kopīgas drošības metodes ieviešanu riska noteikšanai un novērtēšanai atbilstoši Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK 6. panta 3. punkta a) apakšpunktam”
CSM regula	“Komisijas [...] Regula (EK) Nr. .../.. par kopīgas drošības metodes ieviešanu riska noteikšanai un novērtēšanai atbilstoši Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK 6. panta 3. punkta a) apakšpunktam” {Ref. 2}

4. tabula: Saīsinājumu tabula.

Saīsinājums	Nozīme
CSM	Kopīga(s) drošības metode(s)
CST	Kopīgie drošības mērķi
EK	Eiropas Komisija
ERA	Eiropas Dzelzceļa aģentūra
IM	Infrastrukturā pārvaldītājs(i)
ISA	Neatkarīgs drošības novērtētājs
DV	Dalībvalsts
NOBO	Pilnvarotā iestāde
NSA	Valsts drošības iestāde
ORR	(Apvienotās Karalistes) Dzelzceļa regulēšanas pārvalde
RISC	Dzelzceļa savstarpējās izmantojamības un drošības komiteja
RU	Dzelzceļa pārvadājumu uzņēmums(i)
RAC-TS	Riska pieņemšanas kritērijs attiecībā uz tehniskajām sistēmām
SMS	Drošības pārvaldības sistēma
SITS	Savstarpējās izmantojamības tehniskās specifikācijas



CSM REGULAS PANTU PASKAIDROJUMS

1. pants. Nolūks

1. panta 1. punkts

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] Dzelzceļu drošības direktīvas {Ref. 1} 6. panta 3. punkta a) apakšpunktā ir noteikts, ka: *“Kopīgās drošības metodes apraksta, kā novērtēt drošības līmeni un drošības mērķu sasniegšanu, kā arī citu drošības prasību ievērošanu, izstrādājot un nosakot riska noteikšanas un novērtēšanas metodes”.*
- [G 2] CSM regula apraksta tikai to, kā tiek novērtēti un ievēroti drošības līmeņi un atbilstība citām drošības prasībām. Dzelzceļu drošības direktīvas {Ref. 1} 6. panta 3. punktā ir minēta arī *„drošības mērķu sasniegšana”*. Metodes, kas saistītas ar kopīgo drošības mērķu (CST) sasniegšanas novērtējumu valsts līmenī, ir balstītas uz valstu sistēmu agrāko drošības raksturlielumu statistisku novērtējumu, un līdz ar to tās atšķiras no metodēm, ko izmanto, lai novērtētu drošības līmeņus un atbilstību drošības prasībām. Uz minētajām CST sasniegšanas novērtējuma metodēm attiecas atsevišķs „Komisijas lēmums par kopīgu drošības metožu pieņemšanu, lai novērtētu drošības mērķu sasniegšanu, kā minēts Eiropas Parlamenta un Padomes Direktīvas 2004/49/EK” {Ref. 5} 6. pantā”.
- [G 3] „Riska noteikšanu” gan CSM regulā, gan šajā rokasgrāmatā uzskata par kopēja „riskā novērtēšanas procesa” daļu. Līdz ar to, ja vien tas nav izteikti prasīts (piemēram, vajadzīga kvantitatīva riska noteikšana), frāzi „riskā noteikšana” abos minētajos dokumentos neizmanto.

1. panta 2. punkts

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] CSM regulā un 3. shēmā minētie riska pārvaldības un riska novērtēšanas procesi attiecas uz procesiem, kas īstenoti, lai novērtētu drošības līmeņus un būtiskas izmaiņas atbilstību drošības prasībām. Līdz ar to tie ir tikai daļa no kopēja riska pārvaldības un riska novērtēšanas procesa dzelzceļa pārvaldījumu uzņēmumu un infrastruktūras pārvaldītāju drošības pārvaldības sistēmā. I pielikuma 1.1.1. iedaļā ir paredzēts kopējs riska pārvaldības ietvars, uz ko attiecas CSM regula. CSM regulā ir izklāstīti arī saskaņoti lēmumu pieņemšanas procesi, lai novērtētu izmaiņu būtiskumu: skatīt 4. pantu.



- [G 2] Ievērojot 2. panta 1. punktu, CSM riska pārvaldības un riska novērtēšanas procesi attiecas uz drošības riskiem, kas saistīti ar dzelzceļu sistēmu tehniskajām, ekspluatācijas un organizatoriskajām izmaiņām. Tie nenovērš citus projekta riskus, piemēram, pārvaldības vai finansiālos riskus vai riskus neiekļauties projekta termiņos.

2. pants. Tvērums

2. panta 1. punkts

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 palīdz dalībniekiem ievērot prasības, kas noteiktas Dzelzceļu drošības direktīvas {Ref. 1} III pielikuma 2. punkta d) apakšpunktā un saistītas ar RU un IM drošības pārvaldības sistēmu. Attiecīgie novērtēšanas kritēriji, ko ERA drošības sertifikācijas komanda izstrādājusi dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem saistībā ar minētajām prasībām, ir izklāstīti turpmāk (*fragments no {Ref. 4}*):

FRAGMENTS/APRAKSTS

d.0 Dzelzceļa organizācijas obligāti ir ieviesušas sistēmu, lai kontrolētu izmaiņas/jaunos projektus un pārvaldītu attiecīgos riskus, ņemot vērā arī tos, kuri attiecas uz darba drošību².

Izmaiņas var attiekties uz:

- tehniku/tehnoloģijām,
- ekspluatācijas procedūrām/normām/standartiem,
- organizatorisko struktūru.

SMS jānodrošina, lai attiecīgā gadījumā tiktu piemērotas kopīgas drošības metodes attiecībā uz riska novērtēšanu, kas izstrādātas atbilstīgi Drošības direktīvas 6. panta 3. punkta a) apakšpunktam.

NOVĒRTĒŠANAS KRITĒRIJI

- d.1 RU/IM ir ieviesuši procesus un kritērijus, lai atzītu izmaiņas aprīkojumā, procedūrās, organizācijā, darbinieku sastāvā vai saskarnēs,
- d.2 RU/IM rīcībā ir procesi, lai novērtētu izmaiņu ietekmes līmeni nolūkā nolemt, vai piemērot kopīgās drošības metodes attiecībā uz riska novērtēšanu,
- d.3 RU/IM rīcībā ir procesi, lai nodrošinātu riska novērtēšanu un kontroles pasākumu identificēšanu,
- d.4 RU/IM rīcībā ir procesi, lai pārraudzītu kontroles pasākumu īstenošanu un efektivitāti,
- d.5 ir ieviesti procesi/pasākumi, lai kopā ar citām organizācijām (IM, pārējiem RU, trešām personām utt.) novērtētu izmaiņu ieviestos riskus saskarnēs,
- d.6 riska analīzes rezultāti ir redzami visiem attiecīgajiem darbiniekiem, un ir ieviesti procesi, lai minētos rezultātus ieviestu pārējos organizācijas procesos.

- *****
- [G 2] Kopīgo drošības metožu piemērošana ļauj dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem izpildīt novērtēšanas kritērijus d.2, d.3 un d.5. Tā neizskata un nerisina novērtēšanas kritēriju d.1, d.4 un d.6 izpildi (atbilstība d.1 un d.6 kritērijiem ļauj pierādīt atbilstību drošības pārvaldības sistēmai).
- [G 3] Ja izmaiņu iekļauj kategorijā „būtiska”, tad riska novērtējums jākoncentrē tikai uz tām novērtējamās sistēmas funkcijām un saskarnēm, kas saistītas ar drošību un ko tāda izmaiņa ietekmē vai var ietekmēt. Analizējot un novērtējot ar drošību nesaistītus aspektus, var tikai pierādīt, ka tie neietekmē novērtējamās sistēmas funkcijas un saskarnes, kas saistītas ar drošību. Minēto principu – koncentrēt riska novērtējuma pasākumus uz funkcijām un saskarnēm, kas saistītas ar drošību – var paplašināt un attiecināt arī uz visiem nākamajiem sistēmas izstrādes procesa posmiem.
- [G 4] Būtisku izmaiņu gadījumā riska novērtējums attiecas ne tikai uz izmaiņām, bet arī ietver novērtējumu attiecībā uz visām saskarnēm ar citām apakšsistēmām un/vai komponentiem, ko izmaiņa(s) var ietekmēt. Novērtējums nav jāattiecina uz esošās sistēmas nemainītajām daļām vai funkcijām, jo ir jau pierādīts, ka tās ir drošas izmantošanā. Tomēr kopīgajai drošības metodei jāpierāda, ka tiek pareizi integrēta novērtējamā sistēma ar nemainītajām daļām vai esošās dzelzceļa sistēmas nemainītās funkcijas. Tad riska novērtējums ļauj sniegt pierādījumu, ka izmaiņas nemazina novērtējamās sistēmas drošību.
- [G 5] Riska novērtēšanas procesu, kas aprakstīts CSM regulā, piemēro tikai būtiskām izmaiņām dzelzceļa sistēmā. Atbilstīgi 2. panta 4. punktam CSM regula neattiecas uz sistēmām un izmaiņām, ko īsteno vai kas pakļautas drošības akceptēšanas procesam dienā, kad CSM regula stājas spēkā.
Ja izmaiņu novērtē kā nebūtisku, pamatojoties uz 4. panta kritērijiem, tad CSM regulas riska novērtēšanas process nav jāpiemēro.
- [G 6] Ievērojot CSM regulas 5. panta 2. punktu, Dzelzceļa drošības direktīvas {Ref. 1} 4. pantu un III pielikumu, lai veiktu izmaiņas savā iekšējā organizācijā, nepiemēro kopīgās drošības metodes dalībvalsts līmenī. Dalībvalstu politiskos lēmumus saistībā ar dzelzceļa sistēmu īsteno infrastruktūras pārvaldītāji un dzelzceļa pārvadājumu uzņēmumi. *IM* un *RU* atbild par CSM regulas piemērošanu un par to vajadzīgo riska kontroles pasākumu īstenošanu, attiecīgā gadījumā sadarbojoties, kas vajadzīgi dalībvalsts lēmuma izpildei.

2. panta 2. punkts

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] levērojot Dzelzceļu drošības direktīvas {Ref. 1} 4. panta 2. punktu un Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} 15. panta 1. punktu, attiecībā uz būtisku izmaiņu ir vajadzīga sistēmiska pieeja un riska novērtējums, lai nodrošinātu strukturālo apakšsistēmu, uz ko attiecas SITS, drošu integrāciju un ekspluatāciju sistēmā.
- [G 2] SITS ~~specifikācijās~~ ir izklāstītas tehniskās prasības apakšsistēmas(u) savstarpējai izmantojamībai, bet ne obligāti visas drošības prasības (skatīt 7. apsvērumu Dzelzceļu drošības direktīvā {Ref. 1}), kas vajadzīgas apakšsistēmu vai komponentu drošai integrācijai visā dzelzceļa sistēmā. Sistēmiska pieeja, ko atbalsta saskaņots riska novērtējums, ļauj pareizi noteikt visas papildu (drošības) prasības, kas vajadzīgas drošai integrācijai.
- [G 3] Ja kopīgās drošības metodes piemērošana noved pie prasības, kas neatbilst SITS, tad priekšlikuma iesniedzējs vispirms var analizēt iespēju mainīt sistēmas definīciju, lai panāktu atbilstību SITS. Tad un tikai tad, ja to nevar izdarīt, lai ļautu dalībvalstīm nepiemērot SITS, var izmantot noteikumus, kas paredzēti Dzelzceļa savstarpējās izmantojamības direktīvas ā {Ref. 3}.6. panta 2. punktā vai 7. un 9. pantā³. Tad priekšlikuma iesniedzējs informē attiecīgo dalībvalsti, kura var nolemt:
- lūgt attiecīgo SITS pārskatīšanu saskaņā ar Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} 6. panta 2. punktu vai 7. pantu, vai
 - lūgt atkāpšanos no prasības saskaņā ar Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} 9. pantu.

2. panta 3. punkts

This Regulation shall not apply to:

- metros, trams and other light rail systems;*
- 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;*
- privately owned railway infrastructure that exists solely for use by the infrastructure owner for its own freight operations;*
- 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;*
- heritage, museum and tourist railways that operate on their own network, including workshops, vehicles and staff.*

- [G 1] CSM ir piemērojamas dalībvalstī, kā noteikts Dzelzceļu drošības direktīvas {Ref. 1} transpozīcijā valsts tiesību aktos.
- [G 2] Lai gan tīklus vai infrastruktūras, kas uzskaitītas 2. panta 3. punktā, var atbrīvot no prasības par atbilstību CSM, CSM jāpiemēro **ritošajam sastāvam** ~~ritošajiem sastāviem~~, kuri kursē gan minētajos tīklos, gan pa tām pašām sliedēm, pa kurām parastie vilcieni.

³ Teksta fragments no Dzelzceļa savstarpējās izmantojamības direktīvas 9. panta {Ref. 3}: „jebkurai jau esošas apakšsistēmas iecerētai atjaunošanai, paplašināšanai vai modernizācijai, ja „šo vai vairāku SITS” piemērošana”, tostarp to, kas attiecas uz ritošo sastāvu, „var apdraudēt projekta ekonomisko dzīvotspēju un/vai dalībvalsts dzelzceļu sistēmas saderību”, tad „dalībvalstij nav jāpiemēro” „minētās SITS”.

2. panta 4. punkts

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] CSM nav piemērojamas sistēmām un izmaiņām, kas CSM regulas spēkā stāšanās dienā ir jau sāktas un ir izstrādes beigu posmā: skatīt 3. GADĪJUMU 3. shēmā. Pieņem, ka priekšlikuma iesniedzējs turpina piemērot savas ieviestās metodes riska novērtēšanai, līdz tās tiek aizstātas ar CSM regulu (skatīt 2. shēmu).
- [G 2] Jebkura izmaiņa, kas veikta pēc CSM stāšanās spēkā, jānovērtē saskaņā ar CSM regulu (skatīt 4. panta 2. punktu, tostarp 4. panta 2. punkta f) apakšpunktu).

3. pants. Definīcijas

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 5. panta 2. punkts;*
- (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] Ja definīcija CSM regulā attiecas uz esošu standartu, tad definīcijā šajā rokasgrāmatā ir norādīta arī saite ar attiecīgo standartu.
- [G 2] Papildus minētajām definīcijām no CSM regulas šādas definīcijas var palīdzēt labāk saprast rokasgrāmatu:
- (a) „Ilgumslēdzējs subjekts” Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} 2. panta r) punktā „ir jebkurš valsts vai privātā sektora subjekts, kas ir apakšsistēmas projektēšanas un/vai būves darbu, atjaunināšanas vai modernizēšanas pasūtītājs. Šis

(4) OJL 235, 17.9.1996, p. 6.

(5) OJL 110, 20.4.2001, p. 1.

subjekts var būt dzelzceļa pārvadājumu uzņēmums, infrastruktūras pārvaldītājs vai turētājs, vai koncesionārs, kurš ir atbildīgs par projekta nodošanu ekspluatācijā”;

- (b) „darbinieku kompetenci” var raksturot kā zināšanu, prasmju un praktiskās pieredzes apvienojumu, ar ko jābūt apveltītai personai, lai tā spētu pienācīgi veikt konkrētu uzdevumu. Tas ietver ne tikai regulāros uzdevumus, bet attiecas arī uz negaidītām situācijām un izmaiņām:

CSM regulas tvērumā šī definīcija attiecas uz „personas spēju” vai, ja runa ir par darbinieku vai komandas kompetenci, par „personu komandas spēju” attiecībā uz novērtējamo sistēmu pareizi veikt dažādos uzdevumus, kas prasīti CSM riska novērtēšanas un riska pārvaldības procesā. Tas nozīmē, ka, lai pienācīgi veiktu konkrētu uzdevumu, persona vai personu komanda ir kompetenta abās šādās jomās:

- (1) tehniskajā, ekspluatācijas vai organizatoriskajā jomā, ko persona novērtē, un
- (2) riska novērtēšanas procesā, metodēs un mehānismos, ko persona izmanto (piemēram, procesa briesmu analīzes metodes (PHA), briesmu un operatīvās darbības izpētes metode (HAZOP), „notikumu koki” (Event Trees), „kļūdu koki” (Fault Trees), kļūdu iespējamo cēloņu, seku un bīstamības analīze (FMECA) utt.). Skatīt arī 1.1.4. iedaļu I pielikumā.

Dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem, uz kompetences pārvaldības sistēmu, lai darbinieki pareizi izpildītu savus uzdevumus, attiecas atbilstība Dzelzceļu drošības direktīvas {Ref. 1} III pielikuma 2. punkta e) apakšpunkta prasībām.

Kompetences pārvaldības sistēmu, kā arī visus pārējos RU un IM drošības pārvaldības sistēmas (SMS) pamatelementus pieņems valsts drošības iestāde saskaņā ar Dzelzceļu drošības direktīvas {Ref. 1} 10. panta 2. punkta a) apakšpunktu un 11. panta 1. punkta a) apakšpunktu. Tāpēc CSM pareizas piemērošanas pārbaudes tvērumā novērtēšanas iestāde ņems to vērā.

Citiem dalībniekiem SMS nav obligāta. Tāpēc tiem jāpierāda novērtēšanas iestādei savu darbinieku kompetence veikt drošības novērtēšanas uzdevumus attiecībā uz to novērtējamās sistēmas daļu, par kuru tie atbild;

- (c) „eksperta atzinums” ir tad, kad konkrētā eksperta kompetencē ir pieņemti lēmumi, kas ir derīgi un pietiekami tai situācijai vai uzdevumam, ko eksperts veic. Ekspertiem, kuri sniedz atzinumus, jābūt pilnībā kompetentiem tajā vidē, kurā viņi darbojas, kas nozīmē, ka viņi var sniegt atbildīgus un saprātīgus atzinumus, pamatojoties uz sniegto informāciju un pieejamajiem avotiem, pieredzi un zināšanām;
- (d) „apakšsistēma” neattiecas uz strukturālajām un funkcionālajām apakšsistēmām, kas uzskaitītas Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} II pielikumā. Pēc analogijas ar 3.1.61. definīciju CENELEC EN 50129 standartā termins „apakšsistēma” šajā rokasgrāmatā apzīmē „daļu no novērtējamās sistēmas, kas izpilda specializētu funkciju”.

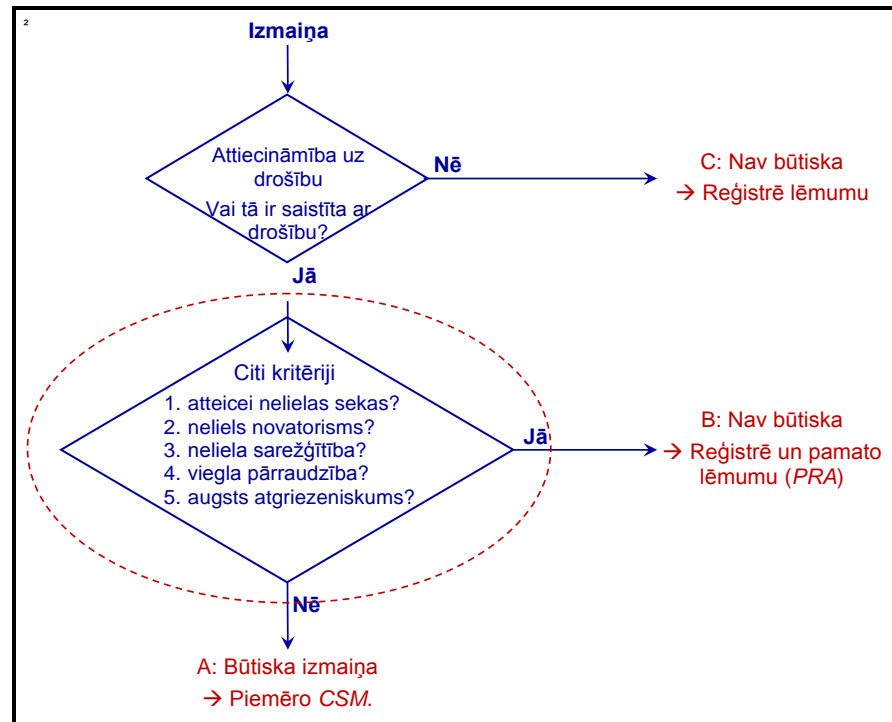
4. pants. Būtiskas izmaiņas

4. panta 1. punkts

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

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

[G 1] Pirmajā pārbaudē jānovērtē, vai izmaiņa ir, vai nav saistīta ar drošību. Ja izmaiņa ir saistīta ar drošību, tad, lai noteiktu, vai izmaiņa ir būtiska vai nebūtiska, var izmantot pārējos 4. panta 2. punktā minētos kritērijus. Tas ir atspoguļots plūsmkartē 1. shēmā. Atteices seku kritēriju var izmantot, piemēram, lai pārbaudītu, vai esošie drošības pasākumi, kas neietilpst novērtējamajā sistēmā, mazina jebkuras tādas novērtējamā sistēmā veiktas izmaiņas atteices sekas, kas būtiska drošībai. Minētais kritērijs kopā ar pārējiem tad var ļaut spriest, ka ar drošību saistītu izmaiņu joprojām var droši pārvaldīt, neizmantojot kopīgo drošības metodi. Priekšlikuma iesniedzējam jānosaka, kāds nozīmīgums jāpiešķir katram no minētajiem kritērijiem attiecībā uz novērtēto izmaiņu.



1. shēma: 4. pantā minēto kritēriju izmantošana, lai novērtētu izmaiņas būtiskumu

4. panta 2. punkts

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



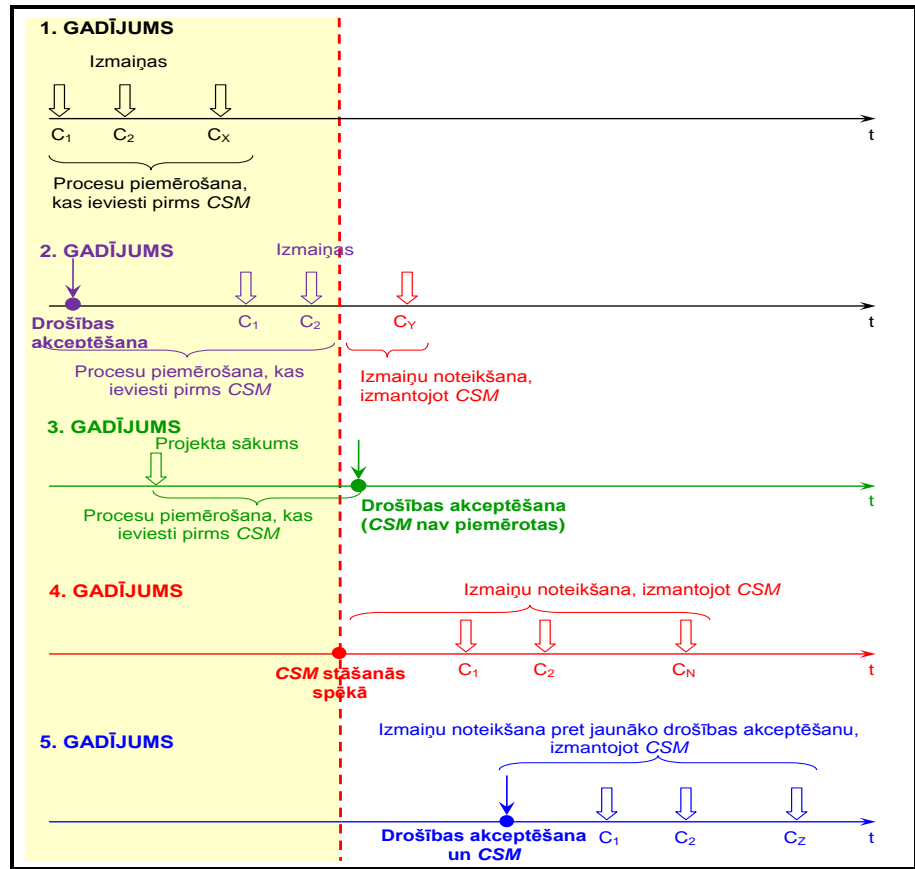
significant.

The proposer shall keep adequate documentation to justify his decision.

- [G 1] Lai novērtētu izmaiņas būtiskumu, priekšlikuma iesniedzējam jāizanalizē visi 4. panta 2. punktā minētie kritēriji, bet priekšlikuma iesniedzējs varētu pieņemt lēmumu, pamatojoties tikai uz vienu vai dažiem no minētajiem kritērijiem.
- [G 2] Tik tiešām, daudzas ar drošību saistītas izmaiņas, kas novērtētas uz minēto kritēriju pamata, vistīcāmāk iekļaus nebūtisko izmaiņu kategorijā. Tomēr, apsverot katru izmaiņu, ir svarīgi, lai visas secīgās, nebūtiskās izmaiņas, „kopā ņemot”, nekļūtu par būtisku izmaiņu, kam jāpiemēro CSM process.
- [G 3] Nosakot vairāku secīgu (nebūtisku) izmaiņu kopumu, jāapsver visa veida izmaiņu apvienojums, kas veiktas kopš pēdējās drošības akceptēšanas. Jāņem vērā tikai tās ar drošību saistītās izmaiņas, kas veicina zināmu apdraudējumu riska analīzē.
- [G 4] Atskaites punkts, lai noteiktu jau izmantotā sistēmā veikto „nebūtisko izmaiņu summu”, ir šādi jaunākie dati (skatīt arī 4. un 5. GADĪJUMU 2. shēmā):
- (a) vai nu CSM stāšanās spēkā,
 - (b) vai attiecīgās sistēmas pēdējā drošības akceptēšana atbilstīgi 7. pantam.

ievērojot 2. panta 4. punktu, CSM nav retrospektīvas: skatīt 1. un 2. GADĪJUMU 2. shēmā. Tās neprasa vēlāk novērtēt izmaiņas, kas veiktas pirms CSM pieņemšanas. Pieņem, ka priekšlikuma iesniedzējs turpina piemērot jau ieviestās metodes riska novērtēšanai, līdz tās tiek aizstātas ar kopīgo drošības metodi.





2. shēma: Ar drošību saistītas izmaiņas un CSM stāšanās spēkā.

[G 5] CSM neprasa, lai novērtēšanas iestāde pārbaudītu izmaiņas būtiskuma noteikšanu: skatīt arī [G 1] un [G 2] punktu 1.1.7. iedaļā. Tomēr CSM pieprasa dokumentēt lēmumus par visu izmaiņu būtiskumu, lai dotu valsts drošības iestādei iespēju izpildīt savu pienākumu – pārraudzīt CSM regulas piemērošanu: skatīt 8. panta 2. punktu.

5. pants. Riska pārvaldības process

5. panta 1. punkts

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] Šajā daļā ir apkopoti dažādie gadījumi, kuros piemēro CSM procesu. Panti, kas minēti 5. panta 1. punktā, prasa, lai priekšlikuma iesniedzējs piemērotu CSM procesu būtiskām izmaiņām un uzturētu pienācīgu dokumentāciju, lai pamatotu savu lēmumu: skatīt arī 4. panta 2. punkta paskaidrojumus iepriekš.

5. panta 2. punkts

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

- [G 1] Papildu paskaidrojumu neuzskata par vajadzīgu. IPriekšlikuma iesniedzēja definīcija 3. panta 11. punktā paskaidro, kas var būt priekšlikuma iesniedzējs.

5. panta 3. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

6. pants. Neatkarīgs novērtējums

6. panta 1. punkts

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] 1.1.2. iedaļas b) apakšpunkts un 1.1.7. iedaļa I pielikumā prasa, lai CSM pareizu piemērošanu neatkarīgi novērtētu novērtēšanas iestāde, pirms priekšlikuma iesniedzējs pieņem būtisku izmaiņu. Novērtēšanas iestādes darbības CSM ir noteiktas attiecīgajās CSM regulas iedaļās.
- [G 2] Neskarot līgumsaistības (skatīt iedaļu § 0.2.) vai tiesiskās prasības⁶ dalībvalstī, priekšlikuma iesniedzējs var brīvi iecelt savu novērtēšanas iestādi. Novērtēšanas iestādes var būt valsts drošības iestādes (NSA), pilnvarotās iestādes (NOBO), kā arī neatkarīgi ārējie vai paša uzņēmuma iekšējie drošības novērtētāji (ISA), ja tie atbilst II pielikumā noteiktajiem kritērijiem.

⁶ Dažās dalībvalstīs daži novērtējumi tiesiski jau jāveic noteiktiem dalībniekiem, piemēram, valsts drošības iestādēm. Tādā gadījumā attiecīgās personas nevar brīvi iecelt novērtēšanas iestādi. Jāpiemēro valsts tiesību normas.

6. panta 2. punkts

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] Novērtēšanas iestādes darbību pārvaldības tvērumā priekšlikuma iesniedzējam vai viņa līgumslēdzējiem jāparūpējas, lai līdz minimumam samazinātu iespējamu pārklāšanos starp pārbaudēm, ko var veikt dažādas novērtēšanas iestādes, kā arī, lai vajadzības gadījumā nodrošinātu informācijas apmaiņu starp attiecīgajām novērtēšanas iestādēm.

6. panta 3. punkts

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] Šajā daļā ir apkopoti dažādie gadījumi no Dzelzceļu drošības direktīvas {Ref. 1} un Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3}, kuros NSA atbild par vajadzīgās atļaujas vai sertifikāta izdošanu.

- [G 2] Lai pārbaudītu CSM procesa pareizu piemērošanu novērtējamai sistēmai, 6. panta 1. punktā priekšlikuma iesniedzējam ir atļauts iecelt jebkuru novērtēšanas iestādi, kas atbilst II pielikumā noteiktajiem kritērijiem. Tas neskar līgumsaistības vai jebkuras attiecīgās tiesiskās prasības dalībvalstī. Lai samazinātu pārbaudi un izmaksu dubultošanu, ja priekšlikuma iesniedzējs vēlas, viņš var nolemt lūgt NSA, lai tā piekrīt darboties kā neatkarīga novērtēšanas iestāde. Tas papildinātu minētās iestādes uzdevumus atbilstīgi CSM 6. panta 3. punktam. NSA var brīvi pieņemt vai noraidīt uzdevumu darboties novērtēšanas iestādes statusā, ja vien to neprasa Kopienas vai valsts tiesību akti. Ja tās atsakās, tad priekšlikuma iesniedzējam jāieceļ cita neatkarīga novērtēšanas iestāde. NSA ir atbildīga par uzdevumiem, kas prasīti atbilstīgi Dzelzceļu drošības direktīvai un Dzelzceļa savstarpējās izmantojamības direktīvai.

6. panta 4. punkts

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] Papildus atļaujai, kas vajadzīga, lai sāktu ekspluatēt strukturālās apakšsistēmas, NSA var arī pārbaudīt, vai CSM process tiek pareizi piemērots strukturālajai apakšsistēmai. Pēc analogijas ar 6. panta 3. punktu iepriekš tas pats paskaidrojuma veids, kāds sniegts minētajā pantā, ir derīgs arī 6. panta 4. punktam.

7. pants. Drošības novērtējuma ziņojumi

7. panta 1. punkts

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

- [G 1] Drošības novērtējuma ziņojuma nolūks ir atbalstīt priekšlikuma iesniedzēju būtiskās izmaiņas pieņemšanā. Neskarot tiesiskās prasības dalībvalstī, priekšlikuma iesniedzējs tomēr paliek atbildīgs par to, lai pieņemtu izmaiņu novērtējamā sistēmā.

7. panta 2. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

7. panta 3. punkts

*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] Ievērojot 5. panta 1. punktu, SITS var pieprasīt veikt riska novērtējumus. Pilnvaroto iestāžu atbildība ir novērtēt novērtējamās sistēmas atbilstību piemērojamo SITS prasībām. Ja pilnvarotās iestādes neizpilda CSM regulas II pielikumā noteiktos kritērijus, lai neatkarīgi novērtētu CSM pareizu piemērošanu, tad tās slēdz apakšlīgumu par novērtēšanas darbu ar citu novērtēšanas iestādi, kura atbilst minētajiem kritērijiem. Tādā gadījumā:
- (a) pilnvarotajām iestādēm jāpārbauda, lai citas novērtēšanas iestādes uzdevumi tiktu pienācīgi izpildīti,
 - (b) novērtēšanas iestādei, kas veic novērtēšanas darbu, jāsniedz savi secinājumi pilnvarotajai iestādei vai līgumslēdzējam subjektam neatkarīgā drošības novērtējuma ziņojumā. Tāds ziņojums būs pamatojums pilnvarotajai iestādei iesniegt savus secinājumus par atbilstību attiecīgajām SITS.
- [G 2] Ievērojot 6. panta 2. punktu, neatkarīgi no tā, vai pilnvarotā iestāde pati veiks darbu, vai slēgs par to apakšlīgumu ar kādu novērtēšanas iestādi, jānovērš darba dubultošanās.

7. panta 4. punkts

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] Dalībvalstīm un novērtēšanas iestādēm jāpiemēro savstarpējas atzīšanas princips riska novērtējumiem, kas noteikti saskaņā ar CSM. Tāda savstarpēja atzīšana jāpamato ar saskaņotiem pierādījumiem, kas iegūti to riska pārvaldības un riska novērtēšanas pasākumu laikā, uz ko attiecas CSM.

[G 2] Ja attiecībā uz dzelzceļa sistēmu kādā dalībvalstī:

- (a) sistēmas riska novērtējums atbilst CSM,
- (b) CSM piemērošanu ir novērtējusi novērtēšanas iestāde, un
- (c) sistēmu ir pieņēmis priekšlikuma iesniedzējs (skatīt 7. panta 1. punktu),

tad novērtēšanas iestādēm citās dalībvalstīs jāpiemēro minētajam riska novērtējumam savstarpējas atzīšanas princips. Tādējādi sistēmu var izmantot citās dalībvalstīs bez papildu riska novērtējumiem un pārbaudēm, ja saistītais priekšlikuma iesniedzējs pierāda, ka:

- (d) sistēmu izmantos tādos pašos funkcionālajos, ekspluatācijas un vides apstākļos, kā jau pieņemto sistēmu sākotnējā dalībvalstī, un
- (e) lai kontrolētu noteikto(s) apdraudējumu(s), piemēro tos pašus riska pieņemšanas kritērijus, ko attiecīgajā dalībvalstī piemēro tāda(u) paša(u) apdraudējuma(u) kontrolei vai ko uzskata par pieņemamu(iem) tajā dalībvalstī.

[G 3] Ja 7. panta 4. punkta [G 2] punktā minētais nosacījums nav izpildīts, tad savstarpējas atzīšanas principu nevar piemērot automātiski, tāpēc ir vajadzīgi priekšlikuma iesniedzēja papildu novērtējumi. Atšķirīgums jāuzskata par novirzi no jau pieņemtas sistēmas. Ja 4. panta 2. punkta piemērošana parāda, ka minēto novirzi var uzskatīt par būtisku izmaiņu salīdzinājumā ar pieņemto sistēmu, tad atšķirīgo elementu novērtē saskaņā ar CSM.

[G 4] Tad novērtēšanas iestādei attiecīgajā dalībvalstī:

- (a) jāveic neatkarīgs novērtējums par to, vai CSM tiek pareizi piemērota attiecībā uz noteiktajām atšķirībām, salīdzinot ar jau pieņemto sistēmu,
- (b) jāpiemēro savstarpējas atzīšanas princips tai sistēmas daļai un tās riska novērtējumam, kas atbilst 7. panta 4. punkta [G 2] punktā minētos nosacījumiem.

8. pants. Riska kontroles pārvaldība/iekšējās un ārējās revīzijas

8. panta 1. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

8. panta 2. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

9. pants. Atsauksmes un tehniskais progress

9. panta 1. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

9. panta 2. punkts

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] Lai atbalstītu NSA tās uzdevumā un sniegtu padomus par to, kā ziņot par pieredzi saistībā ar CSM regulu, Aģentūra pārskata ikgadējā ziņojuma formu. Šo formu nosūtīs valstu drošības iestādēm.

9. panta 3. punkts

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] Aģentūra saistībā ar minēto jautājumu savāc informāciju par grūtībām, ar kurām saskārušies dažādi dalībnieki, kuri piemēro CSM. Lai to izdarītu, Aģentūra ar NSA atbalstu apspriežas ar personām, kas tieši atbild par CSM piemērošanu. Tā nolūks ir, nākotnē pārskatot CSM, ņemt vērā grūtības, kas var būt radušās CSM pirmās piemērošanas laikā.

9. panta 4. punkts

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] CSM regulas kopējās efektivitātes analīze, cita starpā, ietvers to gadījumu pārbaudi, kuros ir piemērots riska pieņemšanas kritērijs tehniskajām sistēmām (RAC-TS), un atsauksmes, kas saņemtas no neatkarīgiem drošības novērtējumiem.

10. pants. Stāšanās spēkā

10. panta 1. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

10. panta 2. punkts

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] Papildu paskaidrojumu neuzskata par vajadzīgu.



I PIELIKUMS – PASKAIDROJUMS PAR PROCESU CSM REGULĀ

1. VISPĀRĪGIE PRINCIPI, KAS PIEMĒROJAMI RISKĀ PĀRVALDĪBAS PROCESAM

1.1. Vispārīgie principi un saistības

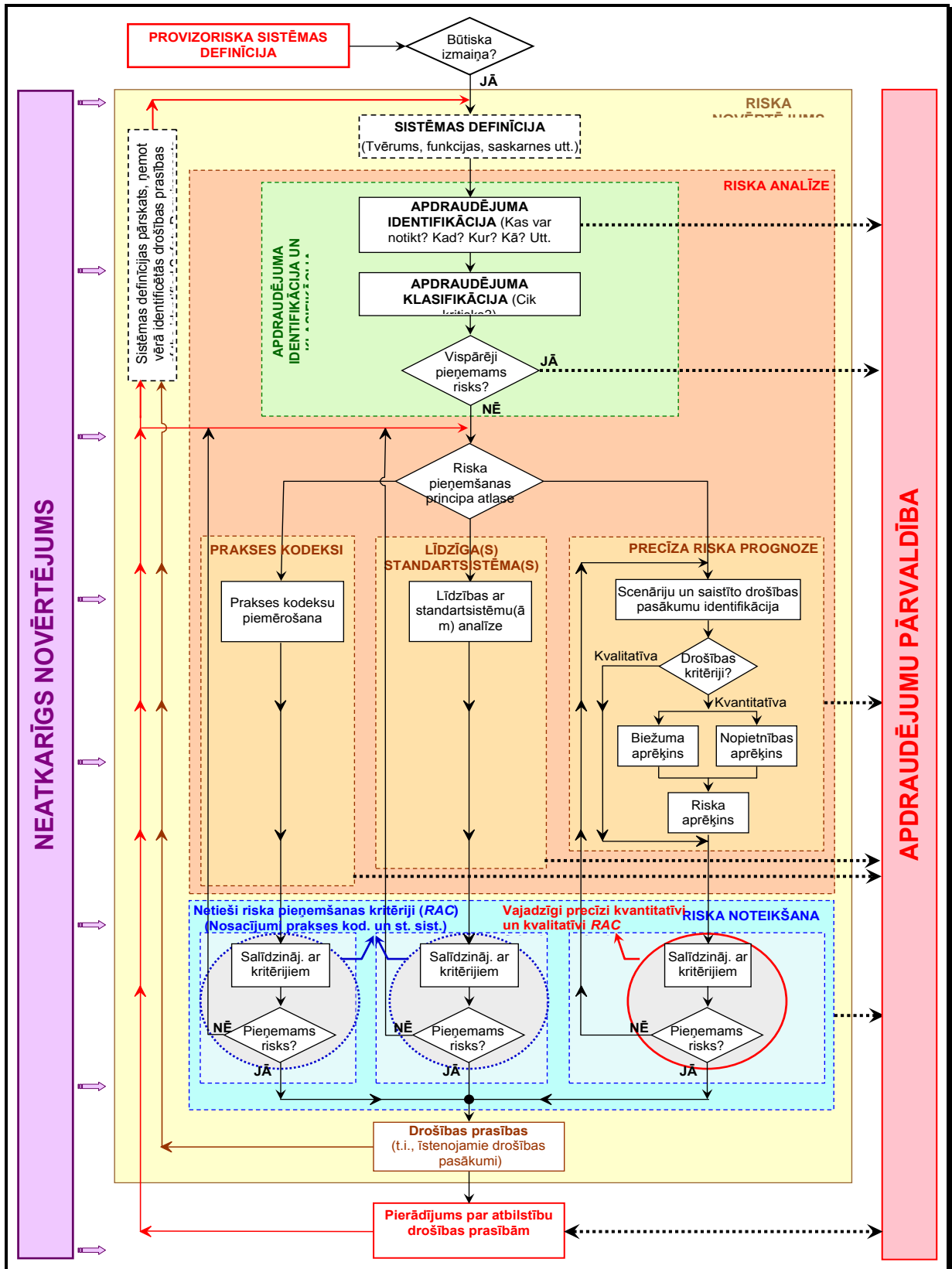
1.1.1. *The risk management process covered by this Regulation shall start from a definition of the system under assessment and comprise the following activities:*

- (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] Kopīgo drošības metodi piemēro projekta sākumā, lai nodrošinātu, ka ir noteikti un pārvaldīti visi piemērojami apdraudējumi, izmantojot apdraudējumu reģistru (skatīt 4. iedaļu).
- [G 2] Riska pārvaldības sistēma kopīgai drošības metodei un saistītais riska novērtēšanas process ir atspoguļoti 3. shēmā. Katra šīs shēmas aile/darbība ir aprakstīta konkrētā šīs rokasgrāmatas iedaļā.
- [G 3] Atkārtotais riska pārvaldības process, uz ko attiecas CSM, ir pabeigts, kad ir pierādīts (skatīt 3. iedaļu) un apdraudējumu reģistrā dokumentēts, ka novērtējamā sistēma atbilst:
- (a) drošības prasībām, kas iegūtas riska novērtējuma rezultātā,
 - (b) drošības prasībām, ko var noteikt, pierādot sistēmas atbilstību iepriekšējā a) apakšpunkta prasībām.





3. shēma: Riska pārvaldības sistēma CSM regulā {Ref. 2}.

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] Riska novērtēšanas procesu sāk piemērot izmaiņas dēļ, kurai piešķir kategoriju „būtiska” (skatīt 3. shēmu). Atkārtotais riska pārvaldības process beidzas, kad priekšlikuma iesniedzējs pieņem būtisko izmaiņu, pamatojoties uz drošības novērtējuma ziņojumu, ko novērtēšanas iestāde iesniegusi par novērtējamo sistēmu (skatīt 7. panta 1. punktu). Pēc tam, ja sistēmas ekspluatācijas un apkopes laikā izrādās, ka vajadzīga vēl cita izmaiņa, tad jāapsver tādas izmaiņas būtiskums. Ja izmaiņu uzskata par būtisku, tad tādai jaunai izmaiņai jāpiemēro CSM.

[G 2] „Darbinieku kompetences” definīcija ir dota [G 2] punkta (b) apakšpunktā 3. panta paskaidrojumā.

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Atbilstīgi 4. apsvērumam Dzelzceļu drošības direktīvā {Ref. 1} „Kopienas dzelzceļu sistēmas drošības līmenis ir visumā augsts ... Ir svarīgi drošību saglabāt arī pašreiz notiekošajā restrukturizācijas posmā ...”. Dalībnieki, kas jau ir ieviesuši metodes riska novērtēšanai, var turpināt tās piemērot tiktāl, cik tās ir saderīgas ar CSM regulā paredzētajiem noteikumiem. Jebkurš riska novērtēšanas process, kas jau ir īstenots un neatbilst CSM, būs jāpārskata, lai nodrošinātu, ka tas atbilst CSM prasībām.

[G 2] Termini „metodes vai mehānismi” attiecas uz „procesiem, paņēmieniem vai mehānismiem” (piemēram, HAZOP, PHA, Event Trees, Fault Trees, FMECA utt.), ko var piemērot, lai ievērotu prasības, kas noteiktas CSM kopīgajā procesā. Tāpēc, kamēr tādi jau ieviesti procesi, paņēmieni un mehānismi ir saderīgi ar CSM noteikumiem, tos var turpināt izmantot. Tādā pašā veidā jāapsver arī cilvēka faktora analīzes vai cilvēka uzticamības analīzes tehnikas un mehānismi.

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] Atbilstīgi 5. panta 2. punktam priekšlikuma iesniedzējam jāpiemēro CSM aprakstītais riska pārvaldības process. Priekšlikuma iesniedzēja definīcija 3. panta 11. punktā paskaidro, kas var būt priekšlikuma iesniedzējs. Ievērojot 5. panta 3. punktu, priekšlikuma iesniedzējs var pieprasīt piegādātājiem, pakalpojumu sniedzējiem, tostarp viņu apakšlīgumu slēdzējiem, piedalīties tādā riska pārvaldības procesā, jo viņu darbības var ietekmēt dzelzceļa sistēmas drošību. Priekšlikuma iesniedzēji parasti ir infrastruktūras pārvaldītāji un dzelzceļa pārvaldījumu uzņēmumi, jo tiem ir galvenā atbildība par dzelzceļa sistēmas ekspluatāciju un saistīto risku kontroli. Bet līgumslēdzējus un ražotājus arī var uzskatīt par priekšlikuma iesniedzējiem:

- (a) ražotāji var veikt riska novērtējumu, ja viņiem vajag atļauju vispārēja pielietojuma ekspluatācijai vai kas būtiski groza jau atļautu ritošo sastāvu,
- (b) apkopes materiālu piegādātāji, mainot savas organizācijas vai uzturēšanas darbības, var veikt riska novērtējumu. Tas var ietvert darbseminārus, kuros uzturēšanas sertifikātu var pieprasīt uz brīvprātības principa pamata,
- (c) turētājiem, iespējams, jāveic riska novērtējums, ja viņi piesakās uz sertifikātu par jaunu ritošo sastāvu vai ja viņi būtiski groza jau atļautu ritošo sastāvu.

[G 2] Uz pārējiem dzelzceļa nozares dalībniekiem arī var attiekties CSM, jo katrs no dalībniekiem, kas minēti 1.1.5. iedaļas [G 1] punktā, var nodrošināt (ar līgumu starpniecību), ka piegādātāji un pakalpojumu sniedzēji, tostarp viņu apakšlīgumu slēdzēji, piedalās CSM aprakstītajā procesā.

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] Drošības pasākumu saskaņošana saskarnēs starp sadarbības dalībniekiem ir galvenais uzdevums, lai uzturētu dzelzceļa sistēmas drošības līmeni.

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] Attiecībā uz būtisku izmaiņu 1.1.2. iedaļas b) punktā ir prasība, lai riska pārvaldības procesu neatkarīgi novērtētu novērtēšanas iestāde, nodrošinot atbilstību CSM noteiktajam procesam. CSM neprasa, lai novērtēšanas iestāde pārbaudītu izmaiņas būtiskuma noteikšanu.

[G 2] Ja izmaiņu novērtē kā nebūtisku, pamatojoties uz 4. pantā minētajiem kritērijiem, tad:

- (a) CSM regulas riska novērtēšanas process nav jāpiemēro,



(b) novērtēšanas iestādei nav neatkarīgi jānovērtē, vai CSM aprakstītais process tiek piemērots pareizi.

[G 3] Neskarot līgumsaistības (skatīt 0.2. iedaļu) vai tiesiskās prasības⁷ dalībvalstī, katrs dalībnieks var brīvi iecelt savu novērtēšanas iestādi attiecībā uz to novērtējamās sistēmas daļu, par kuru viņš atbild. Vienā projektā var iesaistīt vairāk nekā vienu novērtēšanas iestādi. Atkarībā no projekta var būt nepieciešama koordinācija starp dažādām novērtēšanas iestādēm. Parasti par to atbild priekšlikuma iesniedzējs ar savas novērtēšanas iestādes atbalstu.

[G 4] Par dažādo novērtēšanas iestāžu lomām un atbildību, kā arī saskarnēm starp tām skatīt 5. iedaļu un 6. panta 1. punktu.

1.2. Saskarņu pārvaldība

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] Darbību un/vai funkciju sadalījums starp dažādajiem dalībniekiem, kuri iesaistīti dzelzceļa sistēmu attīstībā un ekspluatācijā (*IM, RU, līgumslēdzējiem* utt.), var radīt atlikumriskus saskarnēs. Minētie riski kopīgi jāpārvalda visiem dalībniekiem, kuri iesaistīti attiecīgajās saskarnēs. Tas ir vajadzīgs, jo saskarnes atlikumriski atšķiras no tā veida riskiem, kuri rodas no atsevišķi veiktām darbībām, ko veic *IM, RU* vai citi dalībnieki (*līgumslēdzēji* utt.), kad tie tieši atbild par to pārvaldību un kontroli.

[G 2] Visiem iesaistītajiem dalībniekiem jāsadarbjas, lai nodrošinātu, ka atlikumriskus saskarnēs novērš saskaņotā veidā. Tas nozīmē, ka visi konkrētie dalībnieki nosaka apdraudējumus un vienojas par saistītajiem drošības pasākumiem un rezultātā izteiktajām drošības prasībām. Dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem minētajā procesā ir galvenā nozīme, jo tiem ir sistēmisks skatījums un tie atbild par vilcienu ekspluatācijas vides pārvaldību. Tie atbild par sistēmas riska kopējo kontroli. Tomēr, lai arī *RU* un *IM* var pārraudzīt un sniegt atbalstu pārējiem dalībniekiem, kuri iesaistīti saskarņu pārvaldīšanā, katrs dalībnieks tomēr atbild par to, lai pareizi veiktu darbības un uzdevumus, kas paredzēti kopīgajā drošības metodē, kura piemērojama konkrētā dalībnieka pārziņā esošajai(ām) apakšsistēmai(ām).

[G 3] Priekšlikuma iesniedzējam, kurš nodomājis ieviest būtisku izmaiņu dzelzceļa sistēmā, jāsaņem kopīgo risku pārvaldība saskarnēs. Jo īpaši priekšlikuma iesniedzēja pārziņā būs sadalīt atbildību par kopīgo risku pārvaldību starp dažādajiem dalībniekiem, uz kuriem attiecas attiecīgās saskarnes.

⁷ *Dažās dalībvalstīs daži novērtējumi tiesiski jau jāveic noteiktiem dalībniekiem, piemēram, valsts drošības iestādei. Tādā gadījumā attiecīgās personas nevar brīvi iecelt novērtēšanas iestādi. Jāpiemēro valsts tiesību normas.*



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] Apdraudējumu un saistīto drošības pasākumu deleģēšanas process starp dalībniekiem ir aprakstīts 4., 4.1. un 4.2. iedaļā.

[G 2] Atbilstīgi 4.2. iedaļai par apdraudējumu un saistīto drošības pasākumu deleģēšanu starp minētajiem iesaistītajiem dalībniekiem jāvienojas ar attiecīgo dalībnieku – saņēmēju. Sistēmas līmenī priekšlikuma iesniedzējs atbild par kopīgo risku kopējo saskaņošanu un pārvaldību, priekšlikuma iesniedzējam pastāvīgi jābūt informētam par riska deleģēšanu dažādo dalībnieku starpā, pat ja priekšlikuma iesniedzējs nav obligāti tieši iesaistīts attiecīgo risku kontrolē. Tas ļauj priekšlikuma iesniedzējam paziņot informāciju pārējiem dalībniekiem, kurus attiecīgie riski var ietekmēt caur saskarnēm.

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] Sistēmas novērtēšanas laikā var konstatēt novirzes no drošības pasākumiem vai pat drošības pasākumu nepiemērotību. Tas nozīmē, ka attiecīgie drošības pasākumi (ko atlasījis priekšlikuma iesniedzējs atbilstīgi 2.1.6. iedaļai, lai kontrolētu saistītos apdraudējumus un riskus) nav piemēroti saistīto risku kontrolei. 3.4. iedaļā ir paskaidrots, ka tādas novirzes vai neatbilstības jāuzskata par jauniem datiem jaunā 2. iedaļā aprakstītā atkārtota riska novērtēšanas procesa ciklā.

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] Šis punkts attiecas uz situāciju, kad nosaka drošības pasākuma neatbilstību vai nepiemērotību saistītā apdraudējuma kontrolei (skatīt 1.2.3. iedaļu). Dalībniekam, kurš atbild par attiecīgā drošības pasākuma īstenošanu, būs jāinformē visi pārējie dalībnieki, uz kuriem tas attiecas vai nu:

- (a) novērtējamā sistēmā. Tas dod iespēju izmantot citu drošības pasākumu, lai pienācīgi kontrolētu saistīto apdraudējumu, vai
- (b) esošās (standarta) sistēmās, ja dalībnieks zina, ka tāda paša apdraudējuma kontrolei tiek izmantots tāds pats drošības pasākums. Ir ļoti svarīgi, lai *RU* un *IM* darītu ražotājiem zināmas ar drošību saistītās problēmas, ar ko tie saskaras pat pēc tehniskā aprīkojuma garantijas perioda. Tāda informācija ļautu ražotājiem novērtēt attiecīgo nepiemērotību visās pārējās līdzīgās sistēmās, kurās izmanto to pašu drošības pasākumu, kā arī veikt atbilstošu rīcību attiecībā uz visiem pārējiem klientiem, ko tāda ar drošību saistīta problēma var ietekmēt.



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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Priekšlikuma iesniedzējs, kurš nodomājis ieviest dzelzceļa sistēmā būtisku izmaiņu, atbild par piemērota risinājuma rašanu, ja dalībnieki nevar vienoties par risku sadali saskarnēs vai par apdraudējumu un drošības pasākumu deleģēšanu.

[G 2] Pēc analogijas ar 2. panta 2. punkta pēdējo daļu, ja kāds dalībnieks nevar izpildīt paziņotā valsts tiesību normā noteiktu prasību, tad priekšlikuma iesniedzējs var lūgt dalībvalstij atkāpi.

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] Papildu paskaidrojumu neuzskata par vajadzīgu.



2. RISKĀ NOVĒRTĒŠANAS PROCESA APRAKSTS

2.1. Vispārīgs apraksts

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

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

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

[G 1] Skatīt arī 2.2.5. iedaļu.

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] Šajā pantā ir uzskaitītas minimālās prasības, kam jābūt sistēmas definīcijā. Pieņēmumiem, kas nosaka sistēmas robežas, jābūt izsmejoši uzskaitītiem (skatīt g) punktu). Tos reģistrē apdraudējumu reģistrā tāpat kā drošības prasības, kas izklāstītas riska novērtējumā. Tā kā sistēmas pieņēmumi nosaka riska novērtējuma robežas un derīgumu, tad riska novērtējumu atjaunina vai aizstāj ar jaunu, ja minētos pieņēmumus maina vai pārskata.

[G 2] Lai dotu iespēju veikt riska novērtējumu, sistēmas definīcijai jāņem vērā arī paredzētās izmaiņas konteksts:

- (a) ja paredzētā izmaiņa ir esošas sistēmas grozījums, tad sistēmas definīcijā jāapraksta gan sistēma pirms izmaiņas, gan paredzētā izmaiņa,*
- (b) ja paredzētā izmaiņa ir jaunas sistēmas izveide, tad apraksts ir tikai sistēmas definīcija, un nav jāapraksta neviena esoša sistēma.*

[G 3] Sistēmas definēšana ir svarīgs posms riska novērtēšanas procesā. Sākotnēji tas precīzē sistēmas nolūku, funkcijas, saskarnes un visus jau esošos drošības pasākumus, kas raksturīgi sistēmai. Riska pārvaldības un riska novērtēšanas procesu dažādo atkārtojumu laikā to pārskata un atjaunina ar papildu drošības prasībām, kas noteiktas riska analizēs.

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

[G 1] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Minētie trīs riska pieņemšanas principi jau ir atzīti kā pašreizējas iespējamās prakses, lai kontrolētu apdraudējumus un saistītos riskus dzelzceļa sistēmās.

[G 2] Iespēja izmantot trīs minētos riska pieņemšanas principus dod priekšlikuma iesniedzējam iespēju elastīgi novērtēt, kurš princips ir vispiemērotākais atkarībā no projekta īpašajām prasībām. Ievērojot 5. panta 1. punktu un 1.1.5. iedaļu I pielikumā un neskarot dalībvalsts tiesību aktus, priekšlikuma iesniedzējs var brīvi izmantot jebkuru no minētajiem trīs principiem, ja tos pienācīgi piemēro, lai kontrolētu ar noteiktajiem apdraudējumiem saistītos riskus. Novērtēšanas iestāde var apšaubīt priekšlikuma iesniedzēja rīcību un novērtēt, vai viņš pareizi ir izvēlējis riska pieņemšanas principu, lai kontrolētu noteikto apdraudējumu (un saistīto risku), un novērtēt, vai atlasītais princips tiek pareizi piemērots. Tomēr novērtēšanas iestāde nevar apšaubīt minēto izvēli, ja risks tiek kontrolēts līdz pieņemamam līmenim.

[G 3] Novērtēšanas iestādei jānovērtē izmantotie riska pieņemšanas principi.

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] To var veikt priekšlikuma iesniedzējs riska novērtēšanas procesa beigās. Konsekvences pārbaudē var verificēt, vai:

- (a) riska pieņemšanas principi ir pareizi atlasīti, t.i., ka tos var izmantot to attiecīgo apdraudējumu kontrolei, kuri saistīti ar riskiem, ko neuzskata par vispārēji pieņemamiem,
- (b) atlasītos riska pieņemšanas principus pareizi piemēro apdraudējumiem, kas saistīti ar riskiem, kurus neuzskata par vispārēji pieņemamiem. Piemēram, ja standartu piemēro kā prakses kodeksu apdraudējumu kontrolei, tad jāpārbauda atbilstība īpašām standarta prasībām,
- (c) nav pretrunu starp drošības pasākumiem, ko īsteno katrs atsevišķais dalībnieks, kurš iesaistīts dažādos būtiskās izmaiņas aspektos,
- (d) ja dažādi dalībnieki, kuri iesaistīti tajā pašā projektā, piemēro vienu un to pašu riska pieņemšanas principu (piemēram, to pašu prakses kodeksu), tad tādu principu izmanto vienos un tajos pašos apstākļos.

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] Riska novērtēšanas procesā identificēs dažādus iespējamus drošības pasākumus, ko var ieviest, vai nu, lai likvidētu risku(s), vai, lai kontrolētu risku(s) līdz pieņemamam līmenim (t.i., samazinātu tā gadījumu biežumu vai mazinātu apdraudējuma sekas). Tādi drošības pasākumi var būt tehniski, operatīvi vai organizatoriski. Drošības pasākumu efektivitāti var novērtēt kvantitatīvi, attiecīgā gadījumā puskvantitatīvi vai kvalitatīvi (piemēram, izmantot apmācītus vadītājus, lai kontrolētu cilvēka faktora kļūdas). Priekšlikuma iesniedzējam jāizvēlas piemērotākie īstenojamie pasākumi. Atlasītie drošības pasākumi, lai kontrolētu noteiktos apdraudējumus, kļūst par „drošības prasībām” un jāiekļauj atjauninātā „sistēmas definīcijas” versijā: skatīt 2.1.2. iedaļu un 2. shēmu.
- [G 2] Skaidri jāizklāsta noteikto apdraudējumu kontrolei izvēlēto drošības pasākumu segums, derīguma termiņi un efektivitāte. To formulējumam jābūt skaidram un pietiekamam, lai saprastu apdraudējumus un saistītos riskus, ko tie novērš/mazina, lai nav jāatgriežas pie attiecīgās drošības analīzes.
- [G 3] Pierādījums, ka sistēma atbilst „drošības prasībām”, kas iegūtas riska novērtēšanas procesā, ir aprakstīts 3. iedaļā.

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] Riska novērtējumu var uzskatīt par pabeigtu, kad ir izpildīti šādi nosacījumi:
- (a) ir novērtēti visi noteiktie apdraudējumi un saistītie riski,
 - (b) ir veikta konsekvences pārbaude, lai nodrošinātu, ka trīs riska pieņemšanas principi ir piemēroti pareizi (skatīt 2.1.5. iedaļu),
 - (c) ir verificēts, ka veiktie drošības pasākumi, lai kontrolētu noteiktos riskus, ir pienācīgi un nerada konfliktus, kuri var novest pie jauniem apdraudējumiem, kas jānovērtē atkārtoti,
 - (d) ir pierādīts, ka novērtējamā sistēma atbilst drošības prasībām: skatīt arī 3. iedaļu,
 - (e) nav drošībai būtisku papildu apdraudējumu, kas jāapsver.
- [G 2] Ja pierādījums liecina, ka sistēma neatbilst visām drošības prasībām, t.i., daži drošības pasākumi, kas atlasīti apdraudējumu kontrolei, nav īstēnoti pilnībā vai pareizi (skatīt 2.1.6. iedaļu), tad:
- (a) ja attiecībā uz konkrēto apdraudējumu tika noteikts cits drošības pasākums, tad to var atlasīt kā jauno „drošības prasību” apdraudējuma kontrolei, vai
 - (b) ja ir izmantošanas ierobežojums, tad tas ir reģistrēts apdraudējumu reģistrā, vai
 - (c) ja nebija neviena cita noteikta izmantošanas ierobežojuma vai drošības pasākuma, tad jāidentificē jauni drošības pasākumi, lai kontrolētu saistīto risku līdz pieņemamam līmenim.
- Jāpierāda arī sistēmas atbilstība minētajām jaunajām drošības prasībām, kā aprakstīts 3. iedaļā.

2.2. Apdraudējuma noteikšana

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] Ir ļoti svarīgi, lai apsvērtajā detalizācijas pakāpē⁸ apdraudējumu noteikšana būtu pabeigta un lai apdraudējumi nebūtu ne aizmirsti, ne nepareizi klasificēti kā saistīti ar plaši pieņemamu(iem) risku(iem)⁹. Attiecīgās detalizācijas pakāpes iegūšanai apdraudējuma noteikšanai var apsvērt sekojošo:

- (a) visus sistēmas ekspluatācijas režīmus (t.i., nominālo un pazemināto),
- (b) sistēmas ekspluatācijas dažādos apstākļus (galvenā līnija, tunelis, tilts utt.),
- (c) cilvēka faktoros,
- (d) vides apstākļus,
- (e) visus būtiskos un paredzamos sistēmas atteices veidus,
- (f) visus potenciālos faktoros, kas ir būtiski novērtējamās sistēmas drošībai.

Tas ir ļoti svarīgi, jo, ja apdraudējumus nenosaka, tos nemazina un turpmāk neizskata riska pārvaldības, riska novērtēšanas un apdraudējumu pārvaldības procesā.

[G 2] “Darbinieku kompetences” definīcija ir dota 3. panta [G 2] punkta b) apakšpunktā.

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] Noteikto apdraudējumu klasifikācija – vismaz apdraudējumos, kas saistīti ar „vispārēji pieņemamu(iem) risku(iem)”, un apdraudējumos, kas saistīti ar riskiem, ko neuzskata par vispārēji pieņemamiem – ļauj prioritāri attiecināt riska novērtējumu uz tiem apdraudējumiem, kas prasa riska pārvaldību un riska kontroles pasākumus.

[G 2] Apdraudējumu klasifikāciju abās minētajās kategorijās pamato ar eksperta atzinumu, un to veic atbilstīgi 2.2.3. iedaļai.

[G 3] “Ekspertu atzinuma” definīcija ir dota 3. panta [G 2] punkta c) apakšpunktā.

⁸ Kā aprakstīts [G 2] punktā 2.2.5. iedaļā, riska novērtējumu atkārto tik reizi, cik vajadzīgs, līdz (individuālais(ie) un/vai vispārējais(ie)) risks(i), kas saistīts(i) ar visiem pēdējā apsvērtajā detalizācijas pakāpē noteiktajiem (apakš)apdraudējumiem, ir pieņemams(i) attiecībā pret saistītajiem riska pieņemšanas kritērijiem.

⁹ Skatīt 2.2.3. iedaļā „vispārēji pieņemama riska” definīciju.

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] Priekšlikuma iesniedzējam jānosaka, vai ar katru noteikto apdraudējumu saistītais risks ir vispārēji pieņemams, kā arī jānodrošina, lai novērtējumu veiktu kompetenti eksperti (skatīt definīcijas 3. panta [G 2] punkta b) un c) apakšpunktā).

[G 2] Ņemot vērā to, ka riska detalizēta kvantifikācija apdraudējuma noteikšanas posmā ne vienmēr ir iespējama, praksē ekspertu atzinums šādos gadījumos var dot iespēju nolemt, vai konkrēto apdraudējumu var saistīt ar vispārēji pieņemamu risku:

- (a) vai nu, ja apdraudējuma gadījumu biežumu uzskata par pietiekami nelielu, piemēram, fiziskā fenomena dēļ¹⁰ (kā meteorītu nokrišana uz sliedēm), neatkarīgi no potenciālās nopietnības,
- (b) vai/un, ja apdraudējuma seku potenciālo nopietnību uzskata par pietiekami nelielu neatkarīgi no apdraudējuma gadījumu biežuma.

[G 3] Ja tiek noteikti apdraudējumi ar dažādām detalizācijas pakāpēm (t.i., augsta līmeņa apdraudējumi, no vienas puses, un detalizēti apakšapdraudējumi, no otras puses), tad priekšlikuma iesniedzējam jānodrošina, ka tos pareizi klasificē vismaz apdraudējumos, kas saistīti ar vispārēji pieņemamu risku, un apdraudējumos, kas saistīti ar riskiem, kurus neuzskata par vispārēji pieņemamiem. Tas iekļaus pasākumus, lai nodrošinātu, ka ar vispārēji pieņemama(u) riska(u) saistīto apdraudējumu ieguldījums nepārsniedz kopējā riska noteiktu daļu sistēmas līmenī.

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Detalizācijas pakāpe, kas prasīta apdraudējuma noteikšanai, ir atkarīga no novērtējamās sistēmas.

[G 2] Kā izklāstīts 3. shēmā, atkārtotais riska novērtēšanas process sākas ar sistēmas definēšanu (skatīt 2.1.2. iedaļu), ko izmanto kā pamatu apdraudējuma noteikšanas posmam. Vispirms apsver „augsta līmeņa apdraudējumus”, kas saistīti ar „augsta līmeņa funkcijām”. Tad:

¹⁰ Ja gadījumu retuma iemesls ir tas, ka apdraudējums ir neticams fizikas likumu dēļ, tad apdraudējums un pamatojums gadījumu retumam jāreģistrē apdraudējumu reģistrā.



- (a) ja riskus, kas saistīti ar tādiem „augsta līmeņa apdraudējumiem”, līdz pieņemamam līmenim kontrolē ar drošības pasākumiem, uz ko attiecas sistēmas definīcija, vai ar jauniem noteiktiem pasākumiem¹¹, tad apdraudējuma noteikšana nav jāturpina ārpus minētā līmeņa, vai
- (b) ja dažus tādu „augsta līmeņa apdraudējumu” aspektus nekontrolē ne drošības pasākumi, kas pastāv sistēmas definīcijas ietvaros, ne kāds jauns noteikts pasākums, tad attiecībā uz nekontrolētajiem aspektiem apdraudējuma noteikšana jāpaplašina līdz sīkākai detalizācijas pakāpei¹².

[G 3] Tāpēc riska novērtēšanas procesu atkārtoti tik daudz reizi, cik vajadzīgs, līdz kopējais sistēmas risks tiek kontrolēts līdz pieņemamam līmenim un/vai risks, kas saistīts ar katru noteikto pēdējās apsvērtās detalizācijas pakāpes apdraudējumu¹², ir pieņemams attiecībā pret piemērotajiem riska pieņemšanas kritērijiem vai riska pieņemšanas principiem. Katru reizi, kad riska novērtēšanas procesu atkārtoti, tajā var noteikt

- (a) vai nu detalizētākus apakšapdraudējumus un saistītos drošības pasākumus, kas jāievieš, lai pieņemtu saistīto(s) risku(s),
- (b) vai jaunus drošības pasākumus, ja riska pieņemšanas kritēriji netiek ievēroti ar jau noteiktajiem drošības pasākumiem.

[G 4] Drošības prasības, kas noteiktas riska analizēs, iekļauj sistēmas definīcijā kā papildu (drošības prasības) specifikāciju: skatīt 2.1.2(f) punktu un 2.1.6. iedaļu.

[G 5] Apdraudējuma noteikšanas posms ir nepieciešams arī sistēmām, kur (visus) apdraudējumus var kontrolēt vai nu, piemērojot prakses kodeksus, vai, salīdzinot ar līdzīgām standartsistēmām. Tas ļauj:

- (a) pārbaudīt, vai noteiktos apdraudējumus var faktiski kontrolēt ar attiecīgajiem prakses kodeksiem vai līdzīgām standartsistēmām,
- (b) atbalstīt riska novērtējumu savstarpēju atzīšanu, jo drošības prasības, kas atvasinātas no minētajiem trīs riska pieņemšanas principiem, ir sasaistītas ar apdraudējumiem, ko tās kontrolē,
- (c) iegūt pārredzamību, izmantojot prakses kodeksus un novērtējot to spēju kontrolēt noteiktos apdraudējumus.

Apdraudējuma noteikšanu var ierobežot ar augsta līmeņa apdraudējumiem, ja attiecīgie prakses kodeksi vai standartsistēmas pilnībā kontrolē saistītos apdraudējumus.

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.*

¹¹ Ja apsvērtos apdraudējumus var pilnībā kontrolēt, piemērojot prakses kodeksus vai līdzīgas standartsistēmas, tad turpmāka apdraudējuma noteikšana nav vajadzīga. Lai pieņemtu risku(s), pietiek ar pierādījumu par atbilstību tādiem no jauna noteiktiem noteikt drošības pasākumiem (t.i., prakses kodeksiem vai no standartsistēmas atvasinātajām drošības prasībām).

Dziļāku apdraudējuma noteikšanu parasti veic tikai attiecībā uz tādiem apdraudējumiem, ko nevar pilnībā novērst ar abiem minētajiem riska pieņemšanas principiem: skatīt [G 5] punktu 2.2.5. iedaļā.

¹² Dažos avotos terminu „detalizācijas līmenis” izmanto, lai apzīmētu detalizācijas pakāpi, kas tiek apsvērta strukturālā pieejā. Piemēram, detalizācijas līmeņu skaits agregātā attiecas uz to, cik detalizēti var sadalīt minēto agregātu.





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

- [G 1] Šī prasība jāapsver vispārējā 2.2. iedaļas kontekstā saistībā ar apdraudējuma noteikšanas posmu. Tajā ir teikts, ka, izmantojot prakses kodeksus un standartsistēmas, ievērojot 2.2.1. un 2.2.5. iedaļu, apdraudējuma noteikšana ir vajadzīga, bet to var uzskatīt par pabeigtu, un tādējādi apdraudējuma noteikšana nav jāpadziļina līdz sīkākai detalizācijas pakāpei, ja atlasītie prakses kodeksi vai standartsistēmas kontrolē visus noteiktos apdraudējumus līdz pieņemamam līmenim.
- [G 2] Izmantojot prakses kodeksus un standartsistēmas, riska novērtējums sastāv no šādām darbībām:
- (a) verificēt izvēlēta prakses kodeksa vai standartsistēmas attiecināmību, lai pienācīgi kontrolētu noteiktos apdraudējumus,
 - (b) noteikt iespējamās novirzes no izvēlēta prakses kodeksa vai standartsistēmas. Tikai tad, ja tiek noteiktas novirzes, apdraudējuma identifikācija jāpadziļina līdz sīkākai detalizācijas pakāpei, kā paskaidrots 2.2.5. iedaļā. Tad nepieciešams papildu cikls(i) daudzkārtējā riska novērtēšanas procesā, lai kontrolētu ar minētajām novirzēm saistītos apdraudējumus un riskus.
- [G 3] Prasība 2.2.6. iedaļā neļauj izlaist ne apdraudējuma noteikšanas posmu, ne nākamos posmus riska novērtēšanas procesā pēc apdraudējuma noteikšanas posma. Joprojām jāpierāda atbilstība visam CSM procesam, tādējādi arī 2.3.8. un 2.4.3. iedaļā noteikto prasību izpilde.

2.3. Prakses kodeksu izmantošana un riska noteikšana

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] Nosakot, vai prakses kodekss kontrolē vai nekontrolē vienu vai vairākus apdraudējumus, var ietvert šādas darbības:
- (a) pārbaude, lai novērtējamās sistēmas definīcijas attiecīgā daļa atrastos attiecīgā prakses kodeksa¹³ tvērumā,
 - (b) rūpīga pārbaude attiecībā uz atšķirībām starp novērtējamās sistēmas definīciju un attiecīgā prakses kodeksa tvērumu, izmantojot citus prakses kodeksus vai vienu no abiem pārējiem riska pieņemšanas principiem,
 - (c) novērtējamās sistēmas konstrukcijas parametru salīdzinājums ar konkrētā prakses kodeksa prasībām. Ja konstrukcijas parametri atbilst attiecīgā prakses kodeksa prasībām, saistīto(s) risku(s) var uzskatīt par pieņemamu(iem),
 - (d) apdraudējuma kontrolei piemērojamā prakses kodeksa reģistrācija apdraudējumu reģistrā, nosakot to par drošības prasību attiecīgajam apdraudējumam.

¹³ Piemēram, prakses kodeksi, ko izmanto maģistrālē noteikto apdraudējumu kontrolei, var atšķirties no prakses kodeksiem, ko izmanto attiecībā uz „tuneļu drošību” vai „bīstamo preču pārvadājumu drošību”.



- *****
- [G 2] Attiecībā uz jebkuru sistēmas konstrukcijas parametru, kas neatbilst prakses kodeksa prasībām:
- (a) ja konstrukcijas parametru var mainīt, lai tas atbilstu prakses kodeksa prasībām, sistēmas definīcija jāpārskata un projekta parametrs jānovērtē saskaņā ar CSM,
 - (b) ja projekta parametru nevar mainīt, tad tas jāuzskata par novirzi, ko novērsīs atbilstīgi 2.3.6. iedaļai.

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] Ir svarīgi, lai „prakses kodeksos” būtu dokumenti, kas pieņemami attiecīgajai novērtēšanas iestādei.

- [G 2] Zināmiem tehniskiem pielietojumiem dzelzceļa sistēmās var piemērot arī prakses kodeksus no citām nozarēm (piemēram, kodolenerģijas, militārās un aviācijas nozares), ja konkrētais dalībnieks pierāda, ka saistītie prakses kodeksi ir efektīvi saistīto dzelzceļa apdraudējumu kontrolei.

- [G 3] Dzelzceļu drošības direktīvas {Ref. 1} un CSM regulas ietvaros par prakses kodeksiem var uzskatīt šādus:

- (a) S/TS un obligātos Eiropas standartus,
- (b) paziņotie valsts drošības **noteikumi** ~~normas~~,
- (c) paziņotie valsts tehniskie **noteikumi** ~~normas~~ (tehniskos standartus vai ar likumu noteiktos dokumentus) un attiecīgā gadījumā fakultatīvus Eiropas standartus,
- (d) ja ir izpildīti 2.3.2. iedaļā minētie nosacījumi, tad iekšējos noteikumus vai standartus, ko izdevis dzelzceļa nozares dalībnieks.

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] Ja attiecībā uz novērtējamo sistēmu var pierādīt, ka piemērojamās S/TS arī ļauj pienācīgi kontrolēt vienu vai vairākus noteiktos apdraudējumus, tad turpmāka riska analīze un drošības pasākumi attiecībā uz tādiem apdraudējumiem nav vajadzīgi.

- [G 2] Ja attiecīgās S/TS nevar pilnībā kontrolēt noteiktos apdraudējumus, tad, lai kontrolētu minētos apdraudējumus, jāpiemēro citi prakses kodeksi vai cits riska pieņemšanas princips.

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Apdraudējumus un saistītos riskus, uz ko attiecas prakses kodeksu piemērošana, netieši uzskata par pieņemamiem, ja ir izpildīti prakses kodeksu piemērošanas nosacījumi, kas minēti 2.3.2. iedaļā. Tas nozīmē, ka attiecībā uz apdraudējumiem, ko kontrolē ar minēto principu, nav jānosaka precīzi riska pieņemšanas kritēriji.

[G 2] Pierādījumu, ka novērtējamā sistēma atbilst attiecīgajiem prakses kodeksiem, veic atbilstīgi 3. iedaļai.

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] Ja novērtējamā sistēma neatbilst vienam vai vairākiem prakses kodeksa nosacījumiem, attiecīgo prakses kodeksu joprojām var izmantot apdraudējumu kontrolei, ja priekšlikuma iesniedzējs pierāda, ka tiek sasniegts vismaz tāds pats drošības līmenis.

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] Tas var arī gadīties, ja tiek konstatēts, ka attiecīgais prakses kodekss pietiekami neaptver noteiktos apdraudējumus, piemēram, ka prakses kodekss nav piemērojams visam apdraudējumu klāstam. Tad, lai kontrolētu saistītos riskus, attiecībā uz minētajiem apdraudējumiem jāizmanto vai nu citi prakses kodeksi, vai viens no abiem pārējiem riska pieņemšanas principiem (skatīt arī [G 1] punktu 2.3.1. iedaļā).

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] Šajā tekstā vienā iedaļā ir apkopotas dažādās CSM regulas prasības, kas jāizpilda, ja visus novērtējamās sistēmas apdraudējumus kontrolē prakses kodeksi.

2.4. Atsauces sistēmas izmantošana un riska noteikšana

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] Dzelzceļu drošības direktīvas {Ref. 1} 4. apsvērumā ir arī ierosināts piemērot līdzīgas atsaucē sistēmas, lai uzturētu Kopienas dzelzceļu sistēmas drošības līmeņus.

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] Tajā ir izklāstīti vajadzīgie nosacījumi, lai dotu iespēju kontrolēt vienu vai vairākus novērtējamās sistēmas apdraudējumus, salīdzinot ar līdzīgām atsaucē sistēmām.

[G 2] Apdraudējumus var noteikt, ja pastāv „līdzīgas atsaucē sistēmas”, bet īpašos apstākļos salīdzinājums ar tām var nebūt pietiekams, lai nodrošinātu novērtējamās sistēmas drošību. Tāpēc ir ļoti svarīgi nodrošināt, lai novērtējamo sistēmu izmantotu līdzīgos funkcionālos, ekspluatācijas un vides apstākļos kā līdzīgo atsaucē sistēmu. Ja tā nav, var izmantot citu „līdzīgu atsaucē sistēmu” vai vienu no abiem pārējiem riska pieņemšanas principiem, lai kontrolētu risku līdz pieņemamam līmenim.

[G 3] Ja novērtējamai sistēmai izmanto drošības prasības no atsaucē sistēmas, jāpārbauda arī tas, vai atsaucē sistēma joprojām „pretendē uz pieņemšanu” dalībvalstī, kurā ievieš plānoto izmaiņu. Var gadīties, piemēram, ka aplūkotās atsaucē sistēmas drošības raksturlielumi nav piemēroti novērtējamai sistēmai, jo tās pamatā ir novecojusi tehnoloģija (t.i., vecmodīga tehnoloģija).

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] Apdraudējumus un saistītos riskus, uz ko attiecas atsaucē sistēmas, netieši uzskata par pieņemamiem, ja ir izpildīti atsaucē sistēmu piemērošanas nosacījumi, kas minēti 2.4.2. iedaļā. Tas nozīmē, ka attiecībā uz apdraudējumiem, kurus kontrolē minētais princips, nav jādefinē precīzi riska pieņemšanas kritēriji.

[G 2] Attiecībā uz konkrētajiem apdraudējumiem nav vajadzīga turpmāka riska analīze un riska noteikšana.

[G 3] Pierādījumu, ka novērtējamā sistēma atbilst drošības prasībām, kuras atvasinātas no atsaucēs sistēmas, veic atbilstīgi 3. iedaļai.

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] Ja ir novirze no atsaucēs sistēmas, var joprojām izmantot drošības prasības attiecībā uz apdraudējumiem, uz kuriem attiecas atsaucēs sistēma. Bet ir jāpierāda, ka novērtējamā sistēma sasniedz vismaz tādus pašus drošības raksturlielumus kā atsaucēs sistēma. Var būt nepieciešama arī precīza riska prognoze, lai pierādītu, ka riska līmenis ir vismaz tāds pats kā atsaucēs sistēmas riska līmenis.

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] Ja nevar pierādīt tādu pašu drošības līmeni, vai ja nav izpildītas 2.4.2. iedaļā minētās prasības, tad atvasinātie drošības pasākumi novērtējamajai sistēmai būs nepietiekami. Attiecīgie apdraudējumi tad jāuzskata par novirzēm no atsaucēs sistēmas. Tie kļūst par jauniem datiem jaunā atkārtotā riska novērtēšanas procesa ciklā, kas aprakstīts 2.1.1. un 2.2.5. iedaļā. Papildu drošības pasākumus var noteikt, piemērojot vienu no abiem pārējiem riska pieņemšanas principiem.

2.5. Precīza riska prognoze un noteikšana

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] Precīzu riska prognozi un noteikšanu parasti izmanto (skatīt arī 2.1.4. iedaļas [G 2] punktu):

- (a) ja prakses kodeksus vai atsaucēs sistēmas nevar piemērot, lai pilnībā kontrolētu risku līdz pieņemamam līmenim. Tāda situācija parasti rodas, ja novērtējamā sistēma ir pilnīgi jauna vai ja ir novirzes no prakses kodeksa vai no līdzīgas atsaucēs sistēmas,
- (b) vai ja ir izvēlēta tāda projektēšanas stratēģija, kas neļauj izmantot prakses kodeksus vai līdzīgas atsaucēs sistēmas, jo, piemēram, ir vēlme izstrādāt rentablāku projektu, kas iepriekš nav izmēģināts.

[G 2] Precīzā riska prognoze ne vienmēr obligāti ir kvantitatīva. Riska prognoze var būt kvantitatīva (ja ir pieejama pietiekama kvantitatīvā informācija to gadījumu biežuma un nopietnības izteiksmē), puskvantitatīva (ja tāda kvantitatīvā informācija nav pietiekami



pieejama) vai pat kvalitatīva (piemēram, sistemātisku kļūdu/atteices pārvaldības procesa izteiksmē, ja kvantifikācija nav iespējama).

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] [G 1] punkts 2.3.5. iedaļā un [G 1] punkts 2.4.3. iedaļā paskaidro, ka riska pieņemšanas kritēriji attiecībā uz riskiem, uz ko attiecas prakses kodeksu piemērošana un salīdzinājums ar līdzīgām atsaucēs sistēmām, ir netieši.

[G 2] Tāpēc precīzi riska pieņemšanas kritēriji būs vajadzīgi tikai tam, lai noteiktu riska pieņemamību, piemērojot precīzo riska prognozi.

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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Šis ir riska pieņemšanas kritērijs tehniskajām sistēmām (RAC-TS), ko var izmantot precīzai riska prognozei. CSM regula neprasa izmantot 10^{-9} h^{-1} vērtību RAC-TS kritērijā attiecībā uz ekspluatācijas un organizatoriskajām izmaiņām.

[G 2] **RAC-TS terminoloģijas paskaidrojums 2.5.4. iedaļā:**

(a) *"ja apdraudējumi rodas no tehnisko sistēmu atteices"* nozīmē, ka no visa scenāriju kopuma, kas noteikti precīzajā riska prognozē, RAC-TS piemēro tikai tehnisko sistēmu nepareizās puses atteicēm, kas potenciāli var novest pie katastrofālām sekām;

(b) *„ko neaptver prakses kodeksi vai atsaucēs sistēmas izmantošana"* nozīmē, ka tas nav atsevišķs kritērijs, bet ir integrēts CSM riska novērtējuma sistēmā. RAC-TS piemēro tehniskajām sistēmām, attiecībā uz kurām noteiktos apdraudējumus nevar pienācīgi kontrolēt ne, izmantojot prakses kodeksus, ne, salīdzinot ar līdzīgām standartsistēmām. Piemēram, RAC-TS parasti nebūs jāpiemēro attiecībā uz mehāniskajām daļām vai ķēdes veida apakšsistēmu, kur atbilstoši prakses kodeksi ļauj kontrolēt apdraudējumus;





- (c) „tehniskās sistēmas projektēšanai tiek piemēroti šādi riska pieņemšanas kritēriji” nozīmē, ka šis kritērijs būs projekta mērķis. Tas nenozīmē, ka tie būs attiecīgās tehniskās sistēmas faktiskie drošības raksturlielumi dabā;
- (d) *”tehniskajās sistēmās, kurās funkcionāla atteice var radīt ticamu tiešu nopietnu seku iespējamību”* nozīmē, ka ir jābūt ļoti ticamam, ka tehniskās sistēmas konkrētās atteices gadījumā var notikt negadījums ar katastrofālām sekām;
- (e) *”tiešs”* šajā kontekstā nozīmē, ka nav efektīvu barjeru, kas var novērst nelaimes gadījumu tehniskās sistēmas atteices dēļ. Ja sekas nerodas tieši no tehniskās sistēmas atteices, tad drošības analizē var ņemt vērā mazinošo seku vai drošības barjeru ietekmi (piemēram, cilvēka rīcība vai cita tehniska sistēma, kas novērš nelaimes gadījumu);
- (f) *”iespējamība”* nozīmē, ka gadījumā, ja notiek tehniskās sistēmas atteice, tā ticami var izraisīt nopietnas sekas. Tas ir konservatīvs pieņēmums. Praksē, ja notiek tehniskās sistēmas atteice, tad sekas (piemēram, vilciena noskriešana no sliedēm) nav noteikti nopietnas;
- (g) *”nopietnas sekas”* ir nelaimes gadījums, kas rada vairāk nekā vienu upuri;
- (h) *”saistītais risks nav papildus jāsamazina, ja atteices iespējamība katrā darbības stundā nepārsniedz 10^{-9} .”* Ja ir izpildīti visi iepriekš minētie nosacījumi un tehniskās sistēmas atteices gadījumu biežums, kas pierādīts projektēšanas laikā, nepārsniedz 10^{-9} darbības stundā, tad saistītais risks ir pieņemams. Līdz ar to risks nav papildus jāsamazina.
Darbības stunda attiecas tieši uz funkciju, kas izraisa atteices režīmu. Tas attiecas uz konkrētās tehniskās sistēmas kopējo darbības laiku.

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] Dalībvalsts, kas vēlas piemērot stingrākus riska pieņemšanas kritērijus nekā 2.5.4. iedaļā minētos, paziņo valsts drošības noteikumu saskaņā ar Dzelzceļu drošības direktīvas {Ref. 1} 8. pantā minētajiem noteikumiem. Atbilstīgi minētās direktīvas 8. panta 7. punktam *„dalībvalsts iesniedz Komisijai izskatīšanai drošības noteikuma projektu, pamatojot tā ieviešanas nepieciešamību”*.
- [G 2] Dzelzceļu drošības direktīvas {Ref. 1} 8. pantā ir paredzēts, ka Komisija (kas var lūgt Aģentūrai tehnisku padomu) analizē, cik pamatoti ir cēloņi prasībai ieviest stingrākus riska pieņemšanas kritērijus, un analizē drošības noteikuma projektu, lai pārbaudītu, vai *„drošības noteikuma projekts”* nav *„līdzeklis tīšai diskriminācijai vai slēptu ierobežojumu noteikšanai dzelzceļa pārvadājumiem starp dalībvalstīm”*. Tad *„saskaņā ar Dzelzceļu drošības direktīvas {Ref. 1} 27. panta 2. punktā minēto procedūru pieņem attiecīgajai dalībvalstij adresētu lēmumu”*.
- [G 3] Papildu kritērijiem, ko NSA var pieprasīt, ja vajadzīgas papildu atļaujas laist transportlīdzekļus ekspluatācijā, jāatbilst Dzelzceļa savstarpējās izmantojamības direktīvas {Ref. 3} 23. un 25. pantam. Līdz ar to, ja transportlīdzeklis ir jau atļauts kādā dalībvalstī, pamatojoties uz 2.5.4. iedaļā minēto riska pieņemšanas kritēriju, tad to pašu transportlīdzekli nenoraida citā dalībvalstī, ja tas neatbilst stingrākiem valsts drošības noteikumiem, kas minēti 2.5.5. iedaļā: skatīt arī 2.5.6. iedaļu.



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] Papildu paskaidrojumu neuzskata par vajadzīgu.

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] Lai izpildītu minētās prasības, var apsvērt šādus aspektus:

- (a) precīzajā riska prognozē apsver visus attiecīgos novērtējamās sistēmas ekspluatācijas režīmus (gan nominālo, gan pazemināto režīmu),
- (b) rezultātus noformē formātā, kas saderīgs ar riska pieņemšanas kritērijiem, lai varētu salīdzināt novērtēto risku ar kritērijiem,
- (c) iesniedz pierādījumu tam, ka ir ņemti vērā visi būtiskie riska modeļa parametri, kuri attiecas uz apsvērtajiem riskiem,
- (d) „metodi”, kas „spēj” veikt kompromisa (*trade-off*) / ietekmes analīzi, pamatojoties uz ekspertu atzinumu un pārskatīšanu, attiecībā uz dažādajiem „būtiskajiem riska modeļa parametriem” izmanto precīzajai riska prognozei un noteikšanai,
- (e) visas parametru izvēles un rezultāti ir „saprotami” dokumentēti un pamatoti,
- (f) rezultātus iesniedz kopā ar jutības analīzi attiecībā uz galvenajiem riska „ieguldītājiem”, lai pierādītu, ka ievaddatu parametru mērens grozījums nerada būtiski atšķirīgas drošības prasības,
- (g) rezultātus dokumentē pietiekami detalizētā pakāpē, lai būtu iespējams veikt kontrolpārbaudes,
- (h) ja izmanto kvantitatīvos kritērijus, tad kopējo rezultātu pieļaujamā precizitāte ir vienā kārtā, vai arī visi kvantifikācijai izmantotie parametri ir piesardzīgi.

[G 2] Veids, kādā nosaka novērtējamās sistēmas kvantitatīvos parametrus, jāatbalsta ar labi dokumentētu pamatojumu un atbilstošiem argumentiem.

3. PIERĀDĪJUMS PAR ATBILSTĪBU DROŠĪBAS PRASĪBĀM

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] CSM piemērošanā ir precizēts, ar kādām drošības prasībām plāno kontrolēt apdraudējumus un saistītos riskus, kas noteikti riska analīzes posmā 2. shēmā. Sistēmu tad projektē, validē un pieņem, ņemot vērā tādas drošības prasības.
- [G 2] Pirms sistēmas drošību var pieņemt (skatīt 7. panta 1. punktu), priekšlikuma iesniedzējam jāpierāda, ka:
- (a) trīs riska pieņemšanas principus pareizi piemēro, lai kontrolētu noteiktos apdraudējumus un saistītos riskus līdz pieņemamam līmenim: skatīt 2.1.5. iedaļu,
 - (b) sistēma faktiski atbilst visām precizētajām drošības prasībām.

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] Priekšlikuma iesniedzējam ir vispārēja atbildība par to, lai saskaņotu un pārvaldītu pierādījumu tam, ka sistēma atbilst drošības prasībām, Tomēr priekšlikuma iesniedzējs ne obligāti veic visas pierādīšanas darbības. Praksē katrs dalībnieks, tostarp attiecīgā gadījumā priekšlikuma iesniedzējs, pierāda tās apakšsistēmas¹⁴, par ko viņš atbild, atbilstību šādām attiecīgajām drošības prasībām:
- (a) drošības prasībām, ko apakšsistēmai piešķīris priekšlikuma iesniedzējs, kā aprakstīts 1.1.5. iedaļā,
 - (b) drošības prasībām, kas saistītas ar drošības pasākumiem, kuri attiecas uz saskarnēm un ko attiecīgajam dalībniekam nodevuši citi dalībnieki saskaņā ar 1.2.2. iedaļu,
 - (c) papildu iekšējām drošības prasībām, kas noteiktas apakšsistēmas līmenī veikto drošības novērtējumu un drošības analīzes tvērumā: skatīt [G 2] punktu 3.2. iedaļā.
- [G 2] Lai izpildītu drošības prasības, kas katrai apakšsistēmai noteiktas iepriekš minētajā a) un b) apakšpunktā, katrs attiecīgais dalībnieks veic drošības novērtējumus un drošības analīzes, lai:
- (a) sistemātiski noteiktu visus saprātīgi paredzamos cēloņus, kuri veicina apdraudējumus novērtējamās sistēmas līmenī, kas saistīti ar drošības prasībām attiecībā uz attiecīgo apakšsistēmu.
Minētos apdraudējumu cēloņus novērtējamās sistēmas līmenī tad var uzskatīt par apdraudējumiem apakšsistēmas līmenī (ievērojot apakšsistēmas robežu).
 - (b) noteiktu drošības pasākumus apakšsistēmas līmenī un no tiem izrietošās drošības prasības, ar kurām plāno kontrolēt minētos apakšsistēmas līmeņa apdraudējumus un saistītos riskus līdz pieņemamam līmenim. Praksē konkrētais dalībnieks var arī izmantot prakses kodeksus, līdzīgas standartsistēmas vai precīzo prognozi un noteikšanu apakšsistēmas līmenī. Attiecīgais dalībnieks arī pierādīs savas apakšsistēmas atbilstību

¹⁴ *Sistēmas līmenī izmaiņš atbild par to, lai pierādītu sistēmas atbilstību drošības prasībām, kas rodas no riska novērtējuma.*

minētajām papildu drošības prasībām, kas noteiktas apakšsistēmas līmenī (skatīt 3.2. iedaļu).

- [G 3] Tāpēc katrs dalībnieks atbild gan par apakšsistēmas drošības prasību īstenošanu, gan par to, lai pierādītu apakšsistēmas atbilstību minētajām drošības prasībām.

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] 1.1.2. iedaļas b) punktā un 1.1.7. iedaļā ir prasīts, lai riska pārvaldības un riska novērtēšanas procesus neatkarīgi novērtētu novērtēšanas iestādes. Tādā procesā jāiekļauj arī neatkarīgais novērtējums attiecībā uz pierādījumu par sistēmas atbilstību drošības prasībām. Novērtēšanas iestāde iesniedz attiecīgajam dalībniekam neatkarīgā novērtējuma rezultātus kopā ar novērtējuma ziņojumu: skatīt 7. panta 1. punktu.

- [G 2] Neskarot [G 3] punktu 1.1.7. iedaļā, katrs dalībnieks ieceļ novērtēšanas iestādi tai sistēmas daļai, par ko tas atbild. Šī novērtēšanas iestāde neatkarīgi novērtē pierādījumu par apakšsistēmas atbilstību drošības prasībām, kas izklāstītas 3.2. iedaļā, kā arī pieeju, ko dalībnieks izvēlējis tādā pierādījumam. Atkarībā no projekta var būt nepieciešamība koordinēt dažādas novērtēšanas iestādes. Parasti par to atbild priekšlikuma iesniedzējs ar novērtēšanas iestādes atbalstu.

- [G 3] Attiecīgie dalībnieki iesniedz novērtēšanas iestādēm pierādījumus, kas izklāstīti 5. iedaļā.

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] Ja konstatē, ka drošības pasākumi ir neefektīvi vai nepiemēroti, tad saistītais risks netiek pietiekami kontrolēts (t.i., netiek kontrolēts pieņemamā līmenī). Tādā gadījumā ne vienmēr rodas jauns apdraudējums, bet jāpiemēro prasības, kas minētas [G 3] punktā 3.4. iedaļā.

- [G 2] Jauni apdraudējumi var rasties, īstenojot drošības pasākumus, ar kuriem plāno izpildīt drošības prasības. Tas var notikt, piemēram, tehniskā risinājuma izvēles dēļ, kas nav paredzēts drošības prasībās, attiecībā uz sistēmas vai tās pamatā esošo apakšsistēmu projektēšanu.

- [G 3] Minētās novirzes un/vai jauni apdraudējumi ar saistītajiem riskiem jāuzskata par jauniem datiem jaunā atkārtotas riska novērtēšanas procesa ciklā, kas aprakstīts 2. iedaļā.

4. APDRAUDĒJUMU PĀRVALDĪBA

4.1. Apdraudējumu pārvaldības process

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] 4.1.1. iedaļā minētajā prasībā ir noteikti divi apdraudējumu pārvaldības procesa posmi:

- (a) līdz novērtējamās sistēmas pieņemšanai apdraudējumu reģistrs jāpārvalda priekšlikuma iesniedzējam vai citiem dalībniekiem, ja tas paredzēts līgumā (skatīt „dalībnieku” definīciju 3. panta 8. punktā, kā arī [G 2] punktā 4.1.1. iedaļā),
- (b) kad sistēma ir pieņemta, apdraudējumu reģistru turpmāk uztur un pārvalda infrastruktūras pārvaldītājs vai dzelzceļa pārvadājumu uzņēmums, kura pārziņā ir novērtējamās sistēmas darbība. Kā paskaidrots turpmāk, *IM* un *RU* apdraudējumu pārvaldības process ir to drošības pārvaldības sistēmas integrēta daļa.

[G 2] Atbilstīgi 5. panta 2. un 3. punktam un „priekšlikuma iesniedzēja” definīcijai 3. panta 11. punktā piegādātāji un pakalpojumu sniedzēji, tostarp viņu apakšlīgumu slēdzēji, arī var nodrošināt apdraudējumu reģistru, ja tas prasīts līgumos, kas noslēgti starp viņiem un priekšlikuma iesniedzēju. Tādā gadījumā minētie dalībnieki ievieš un pārvalda paši savu apdraudējumu reģistru attiecībā uz to novērtējamās sistēmas daļu, par ko viņi atbild. Neatkarīgi no tā, vai viņi, vai priekšlikuma iesniedzējs pārvalda apdraudējumu reģistru, par apdraudējumu reģistrā iekļaujamās informācijas pareizību atbild tas dalībnieks, kurš kontrolē apsvērto apdraudējumu.

[G 3] Dzelzceļu drošības direktīvas {Ref. 1} III pielikuma 2. punkta g) apakšpunktā ir butiska prasība, lai *RU* un *IM* drošības pārvaldības sistēmā ietilptu „procedūras un paraugi, kā dokumentējama drošības informācija un procedūras noteikšana svarīgas drošības informācijas kontrolei”. Novērtēšanas kritēriji, ko izstrādājusi *ERA* drošības sertifikācijas darba grupa attiecībā uz minēto jautājumu, ir izklāstīti turpmāk (fragments no {Ref. 4}):

FRAGMENTS/APRAKSTS

g.0 Organizācijām jānosaka dokumentu un datu kontroles procedūras, pamatojoties uz esošām pārvaldības sistēmām; dokumentiem un uzskaitē jābūt ātri pieejamiem konsultācijai un/vai verificācijai.

Vitālas drošības informācijas kontroles pasākumi ir svarīgi, lai uzturētu un uzlabotu drošības raksturlielumus organizācijā, kā arī lai dotu iespēju ātri un efektīvi veikt koriģējošu rīcību.

RU un IM, darbojoties vienā tīklā sistēmā, ir jābūt ieviestiem pasākumiem, lai nodrošinātu visas drošībai būtiskās informācijas pareizu apmaiņu, kas tiek pienācīgi dokumentēta. Tiem jāizstrādā un jāatbalsta standartizētu protokolu izmantošana formālai saziņai attiecībā uz ekspluatāciju (vilcienu žurnāli, satiksmes/ekspluatācijas ierobežojumi utt.) kā noderīgs saskaņošanas mehānisms.

NOVĒRTĒŠANAS KRITĒRIJI

g.1 SMS rīcībā ir piemēroti procesi, lai nodrošinātu, ka visa attiecīgā drošības informācija ir precīza, pilnīga, pienācīgi atjaunināta un pienācīgi dokumentēta;

g.2 SMS rīcībā ir piemēroti procesi, lai:

- formatētu, izveidotu, izplatītu un pārvaldītu izmaiņu kontroli visā attiecīgajā drošības dokumentācijā,
- saņemt, savāktu un glabātu/arhivētu visu attiecīgo dokumentāciju/informāciju papīra formātā vai ar citiem mehānismiem/citās reģistrācijas sistēmās,
- nodrošinātu, lai darbiniekiem iepriekš tiktu sniegta visa attiecīgā un atjauninātā informācija, un viņi to attiecīgi izmanto;

g.3 SMS rīcībā ir piemēroti procesi, lai nodrošinātu, ka valoda/saturs ir konsekventi, saskanīgi un saprotami.

g.4 RU un IM ir ieviesuši pasākumus, lai nodrošinātu, ka nerodas saziņas barjeras vai ka tās tiek mazinātas; jāiesniedz pierādījums tam, ka tiek izmantoti standartizēti protokoli/formāti attiecībā uz informāciju, kas saistīta ar drošību, kā arī, lai dokumentētu visus attiecīgos datus.

- [G 4] Attiecībā uz prasībām, kas noteiktas Dzelzceļu drošības direktīvas {Ref. 1} III pielikuma 2. panta g) apakšpunktā, CSM regula nosaka, kāda informācija no riska novērtēšanas procesa jāuzskata par saistītu ar drošību un tāpēc jāreģistrē apdraudējumu reģistrā. CSM apdraudējumu pārvaldības process tad dod iespēju RU un IM izpildīt to SMS prasības attiecībā uz informāciju, kas saistīta ar drošību, kā noteikts CSM riska novērtēšanas procesā. Uz citas ar drošību saistītas informācijas reģistrēšanu, pārvaldību un kontroli attiecas citi RU un IM SMS procesi vai procedūras.
- [G 5] Ievērojot 2. panta 1. punktu, apdraudējumu pārvaldība CSM regulā ir prasīta attiecībā uz būtiskām tehniskām, ekspluatācijas un organizatoriskām izmaiņām. Ja izmaiņa nav būtiska, apdraudējumu pārvaldības process netiek prasīts.
- [G 6] Tādējādi apdraudējumu pārvaldības process, kura pamatā ir apdraudējumu reģistrs, dod iespēju:
- (a) kontrolēt drošības prasību apmaiņu starp dažādajiem dalībniekiem, kuri iesaistīti būtiskajā izmaiņā, kā arī
 - (b) pārvaldīt to apdraudējumu statusu, par ko dalībnieks atbild.
- [G 7] Attiecībā uz būtisku izmaiņu jau esošā sistēmā, kas ir jau pieņemta, bet kurai vēl nav apdraudējumu reģistra, apdraudējumu reģistrs jāizveido, jāatjaunina un jāuztur attiecībā uz to sistēmas daļu, kuru maina.
- [G 8] Parasti, ja par novērtējamo sistēmu atbildīgā organizācija noslēdz par kādu darbību apakšlīgumu ar citu organizāciju, prasība, lai tāda organizācija uzturētu apdraudējumu reģistru, var būt pārmērīga, jo īpaši, ja apakšlīguma slēdzējas struktūra/izmērs ir neliels vai ja tā ieguldījums kopējā sistēmā ir ierobežots. Tādos gadījumos attiecīgie dalībnieki var projekta sākumā vienoties par vispiemērotāko dalībnieku, kurš uzņemsies atbildību par apdraudējumu reģistra kopējo pārvaldību. Ja izmanto vienotu apdraudējumu reģistru, sadarbības organizācijas var rīkoties elastīgāk, jo vismaz viena no tām atbild par kopējā apdraudējumu reģistra pārvaldību visām iesaistītajām organizācijām. Par informācijas (t.i., apdraudējumu, risku un drošības pasākumu) precizitāti, kā arī par drošības pasākumu īstenošanas pārvaldību joprojām atbild tā organizācija, kuras pārziņā ir kontrolēt ar minētajiem drošības pasākumiem saistītos apdraudējumus.

[G 9] Apdraudējumu pārvaldības process dzelzceļa pārvadājumu uzņēmumiem un infrastruktūras pārvaldītājiem var būt daļa no to drošības pārvaldības sistēmas, lai reģistrētu un pārvaldītu riskus, kas gadās tehniskā aprīkojuma darbībā, dzelzceļa sistēmas darbības un organizācijas laikā. Tam nav jābūt papildu un atsevišķam procesam.

[G 10] Attiecībā uz pārējiem dalībniekiem, ievērojot Dzelzceļu drošības direktīvas {Ref. 1} III pielikuma 2. punkta g) apakšpunktā minētās prasības, *RU* un *IM* nodrošina, lai viņu apakšlīgumu slēdzēji uzturētu savu ar drošību saistīto informāciju, vai lai *RU* un *IM* darītu to paši. Tāpēc minēto dalībnieku prasības attiecībā uz apdraudējumu pārvaldību var būt atspoguļotas līgumos starp *RU/IM* un tādiem citiem dalībniekiem. Ja minētajiem dalībniekiem jau ir esoša apdraudējumu pārvaldības sistēma, to var pielāgot, lai būtu ievērotas *CSM* regulas prasības.

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] Apdraudējumu reģistrā ietver vismaz šādu informāciju:

- visus apdraudējumus, par ko konkrētais dalībnieks atbild, saistītos drošības pasākumus un rezultātā iegūtās drošības prasības, kas iegūtas riska novērtēšanas procesā (skatīt 2.1.6. iedaļu),
- visus pieņēmumus, kas ņemti vērā novērtējamās sistēmas definīcijā (skatīt [G 1] punktu 2.1.2. iedaļā). Minētie pieņēmumi nosaka riska novērtējuma robežas un derīgumu. Ja tos groza vai pārskata, riska novērtējums jāatjaunina vai jāaizstāj ar jaunu riska novērtējumu,
- visus apdraudējumus un saistītos drošības pasākumus, kas saņemti no citiem dalībniekiem saskaņā ar [G 1] punktu 2.1.2. iedaļā. Te ietilpst visi tie pieņēmumi un izmantošanas ierobežojumi (saukti arī par „ar drošību saistīta pielietojuma nosacījumiem”), kas piemērojami pamatā esošajām apakšsistēmām, tipveida pielietojumam un tipveida izstrādājumu drošību apliecināšanai dokumentācijai, ko sagatavojuši ražotāji,
- apdraudējumu statusu (t.i., kontrolēti vai atvērti) un saistīto drošības pasākumu statusu (t.i., validēti vai atvērti).

Visa minētā informācija skaidri jāreģistrē apdraudējumu reģistrā pietiekamā precizitātes pakāpē, lai varētu pārvaldīt apdraudējumu reģistru.

[G 2] *CSM* regula nenosaka apdraudējumu reģistra mehānismus un formātu. Priekšlikuma iesniedzēja ziņā ir nolemt, kā izpildīt *CSM* regulas 4. iedaļā noteiktās prasības.

[G 3] Apdraudējumu reģistrs nav vienkārši izstrādes mehānisms. *IM/RU* tas jāatjaunina un jāuztur, kad vien tas vajadzīgs visā sistēmas darbībā, jo īpaši:

- kad vien tiek veikta būtiska izmaiņa,
- kad vien tiek konstatēts jauns apdraudējums vai noteikts jauns drošības pasākums,
- kad vien sistēmas ekspluatācijas un uzturēšanas laikā pēc tās nodošanas ekspluatācijā tiek konstatēts jauns apdraudējums, lai apdraudējumu varētu novērtēt saskaņā ar *CSM*, vai tas veido būtisku izmaiņu,
- kad vien tas var būt vajadzīgs, lai ņemtu vērā datus par negadījumiem un starpgadījumiem,
- kad vien tiek grozītas drošības prasības vai pieņēmumi par sistēmu.

- *****
- [G 4] Apdraudējumu reģistrā ievadītās informācijas derīgums arī jāpārbauda, kad vien sistēmas darbības un uzturēšanas laikā tiek veiktas izmaiņas. Atsaucoties uz [G 1] punktu 4.1.2. iedaļā, ja drošības prasība vai pieņēmums, vai izmantošanas ierobežojums vairs netiek ievēroti, tad tā jāuzskata par izmaiņu. Lai noteiktu, vai izmaiņa ir būtiska, tā jānovērtē atbilstīgi 4. pantam. Ja izmaiņa ir būtiska, tad attiecībā uz to rīkojas saskaņā ar CSM.

4.2. Informācijas apmaiņa

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] Apdraudējumu pārvaldības laikā iespējams, ka kontrolēt dažus apdraudējumus un validēt saistītos drošības pasākumus apdraudējumu reģistrā nevar tikai viens dalībnieks. Tādos gadījumos var būt nepieciešams process vai procedūra, lai noteiktu, kā projektā iesaistītie dalībnieki var kontrolēt minētos apdraudējumus. Tas var ietvert vai nu:

- situāciju, ka dažādie dalībnieki apspriežas un vienojas par rezultātu, lai kontrolētu attiecīgos apdraudējumus un validētu saistītos drošības pasākumus apdraudējumu reģistrā, vai
- attiecināmo apdraudējumu un saistīto drošības pasākumu deleģēšanu tā dalībnieka apdraudējumu reģistrā, kurš atbild par to īstenošanu, verificēšanu un validēšanu. Piemēram, var būt vajadzīga operatīva procedūra, lai mazinātu risku, ja nav iespējams tehnisks/projektēšanas pasākums. Šī drošības informācijas apmaiņa atbilst prasībai, kas noteikta pēdējā 4.1.1. iedaļas [G 2] punktā izklāstīto novērtēšanas kritēriju g.0 apraksta rindkopā.

- [G 2] Ja drošības pasākums nav pilnībā validēts, tad:

- apdraudējumu reģistrā jāizstrādā un jāreģistrē skaidrs izmantošanas ierobežojums (piemēram, operatīvie mazināšanas pasākumi),
- tā kā tāds izmantošanas ierobežojums ir papildu vai alternatīvs drošības pasākums, tad jāpamato tā piemērotība pienācīgai riska kontrolei,
- izmantošanas ierobežojums, kā arī saistītais apdraudējums un risks jāeksportē vai jānodod dalībniekam, kurš atbild par tāda izmantošanas ierobežojuma īstenošanu, verificēšanu un validēšanu (piemēram, dzelzceļa pārvadājumu uzņēmumam, ja tas ir ekspluatācijas ierobežojums).

5. RISKĀ PĀRVALDĪBAS PROCESA PIEMĒROŠANAS DOKUMENTĀCIJA

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] CSM nenosaka dokumentu skaitu, ko priekšlikuma iesniedzējs var noformēt, lai dokumentētu riska pārvaldības procesu. Priekšlikuma iesniedzēja ziņā ir nolemt, kā strukturēt šo dokumentāciju: skatīt [G 1] punktu 5.2. iedaļā. Riska pārvaldības un riska novērtēšanas darbību dokumentācijas nolūks ir dot iespēju:

- (a) izstrādāt novērtējamo izmaiņu,
- (b) novērtēšanas iestādēm veikt neatkarīgu novērtējumu,
- (c) ja sistēmas darbmūžā rodas kāda problēma, atgriezties pie saistītajām drošības analīzēm un drošības uzskaites, lai saprastu cēloņus, kuru dēļ pieņēma lēmumus: skatīt [G 4] punktu 5.2. iedaļā,
- (d) atkārtoti izmantot novērtējamo sistēmu kā atsauces sistēmu citiem pielietojumiem.

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] Termins „dokuments” CSM 5.2. iedaļā drīzāk jālasa kā dokumentārs pierādījums, kas iegūts, piemērojot riska pārvaldības procesu CSM, nevis kā „atsevišķs fizisks dokuments”. 5.2. iedaļā ir pastāstīts, kāds dokumentārā pierādījuma minimums ir vajadzīgs, lai dotu novērtēšanas iestādei(ēm) iespēju pārbaudīt CSM pareizu piemērošanu. Nav noteikts, kā izpildīt minēto prasību. Katrs novērtējamā sistēmā iesaistītais dalībnieks var dokumentēšanai brīvi izmantot pats savu struktūru, kas precizēta tā iekšējās kvalitātes pārvaldības un drošības pārvaldības sistēmā/procesā (attiecīgā gadījumā), ja:

- (a) organizācija, kas ieviesta, lai veiktu riska novērtēšanas procesu, ir skaidri noteikta iepriekš,
- (b) ekspertiem, kas iesaistīti riska novērtēšanas procesā, ir pienācīga kompetence. „Darbinieku kompetences” un „ekspertu atzinuma” definīcijas ir dotas [G 2] punkta b) un c) apakšpunktā 3. pantā,
- (c) riska novērtēšanas procesa dažādo posmu rezultāti ir skaidri dokumentēti,
- (d) ir izveidots visu piemērojamo drošības prasību saraksts, lai kontrolētu risku pieņemamā līmenī.

[G 2] Ja dokumentācija nav pieejama, attaisnojums jāiesniedz izvērtējumam novērtēšanas iestādē.

[G 3] Kad projekts ir pabeigts, riska pārvaldības un riska novērtēšanas procesa rezultātus iekļauj vai nu sistēmā, vai vajadzības gadījumā tie kļūst par riska kontroles sistēmas daļu dzelzceļa pārvaldījumu uzņēmumiem un infrastruktūras pārvaldītājiem atbilstīgi to drošības pārvaldības sistēmai.

- *****
- [G 4] Sistēmas darbmuža vai sistēmas darbības laikā var notikt vairākas būtiskas izmaiņas, kuru dēļ dažādiem dalībniekiem un organizācijām, kas izmanto apdraudējumu reģistru, nepieciešams pārskatīt, papildināt un/vai nodot pavaddokumentus. Tādējādi tiek ieteikts turēt un vajadzības gadījumā atjaunināt dokumentāciju (skatīt [G 1] punktu 5.2. iedaļā), kas iegūta, piemērojot CSM procesu, lai dotu iespēju veikt turpmākus riska novērtējumus attiecībā uz dzelzceļa sistēmām un to saskarnēm.
- Attiecīgā gadījumā katras sistēmas konfigurācijas, ko izmanto ekspluatācijā, rezultāti jāievieto priekšlikuma iesniedzēja arhīvos vismaz sistēmas darbmužā. Ja vien līgumos, kas noslēgti projekta sākumā, nav noteikts citādi, pārējiem iesaistītajiem dalībniekiem arī var rasties nepieciešamība arhivēt savus attiecīgos riska un drošības analīzes rezultātus.

CSM REGULAS II PIELIKUMS

Kritēriji, kas jāievēro novērtēšanas iestādēm

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] Papildu paskaidrojumu neuzskata par vajadzīgu.