Euroopan rautatievirasto	
Esimerkkikokoelma riskien arvioinneista ja YTM-asetusta tukevista mahdollisista välineistä	
Euroopan rautatieviraston viite:	ERA/GUI/02-2008/SAF
Versio:	1.1
Päiväys:	6.1.2009

Asiakirjan laatija	European Railway Agency Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Ranska
Asiakirjatyyppi:	Opas
Asiakirjan status:	Julkinen

	Nimi	Tehtävä
Julkistaja	Marcel VERSLYPE	Rautatieviraston pääjohtaja
Tarkastaja	Anders LUNDSTRÖM Thierry BREYNE	Turvallisuusyksikön päällikkö Turvallisuusarviointialan päällikkö
Kirjoittaja (laatija)	Dragan JOVICIC	Turvallisuusyksikkö - hankevirkamies

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

ASIAKIRJAN TIEDOT

Muutosasiakirja

Taulukko 1: Asiakirjan tila

Versio Päiväys	Laatija(t)	Kohta	Muutoksen kuvaus
Vanhan asiakirjan otsikko ja rakenne: *”Yhteisten turvallisuusmenetelmien ensimmäistä erää koskevan suosituksen käyttöopas”*			
Ohjeversio 0.1 15.2.2007	Dragan JOVICIC	Kaikki	”Yhteisiä turvallisuusmenetelmiä koskevien suositusten ensimmäisen erän” version 1.0 ”käyttöoppaan” ensimmäinen versio. Tämä on myös ensimmäinen versio YTM-työryhmälle muodollista tarkistusta varten toimitetusta asiakirjasta.
Ohjeversio 0.2 7.6.2007	Dragan JOVICIC	Kaikki	Asiakirjan jäsentäminen uudelleen siten, että se vastaa YTM-suosituksen version 4.0 rakennetta. Suosituksen version 1.0 päivittäminen/muodollinen tarkistusmenettely YTM-työryhmässä.
		Kaikki	Asiakirjan päivittäminen ja täydentäminen Euroopan rautatieviraston sisäisissä kokouksissa kerätyillä tiedoilla ottaen huomioon YTM-erityisryhmän ja työryhmän esittämät uusien kohtien laatimista koskevat pyynnöt.
		Kaavio 1	”Yhteisten turvallisuusmenetelmien ensimmäisen erän riskinhallintakehystä” kuvaavan kaavion muuttaminen tarkistuksen tuloksena esitettyjen huomautusten ja ISO:n terminologian mukaisesti.
Ohjeversio 0.3 20.7.2007	Dragan JOVICIC	Lisäykset	Lisäysten uudelleen järjestäminen ja uusien lisäysten laatiminen. Uusi lisäys, johon on kerätty kaikki kaaviot, joilla havainnollistetaan ja helpotetaan oppaan lukemista ja ymmärtämistä.
		Kaikki kohdat	Asiakirjan päivittäminen siten, että • kehitetään mahdollisimman pitkälle voimassa olevia x kohtia, • kehitetään edelleen näkökohtia, joihin viitataan ”järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisella”, • luodaan linkki CENELECin V-sykliin (eli standardin EN 50 126 kaavioon 8 ja 10), • kehitetään edelleen yhteistyötä ja yhteensovittamista sellaisten rautatiealan eri toimijoiden välillä, joiden toimilla voi olla vaikutusta rautatiejärjestelmän turvallisuuteen, • selvennetään todisteita (esim. vaaraloki ja turvallisuusarvio), joilla on määrä osoittaa arviointielimille, että YTM:n riskinarviointimenettelyä sovelletaan oikein. Asiakirjaa päivitetään myös viraston ensimmäisen sisäisen tarkistuksen perusteella.
Ohjeversio 0.4 16.11.2007	Dragan JOVICIC	Kaikki kohdat	Asiakirjan päivittäminen muodollisen tarkistusmenettelyn jälkeen jäljempänä mainituilta YTM-työryhmän jäseniltä tai organisaatioilta saatujen versiota 0.3 koskevien huomautusten mukaisesti ja siten kuin niiden kanssa on sovittu puhelinkeskusteluissa: • Belgian, Espanjan, Suomen, Norjan, Ranskan ja Tanskan kansalliset turvallisuusviranomaiset, • SIEMENS (UNIFEn jäsen), • Norjalainen infrastruktuurin haltija (Jernbaneverket – EIM:n jäsen).
Ohjeversio 0.5 27.2.2008	Dragan JOVICIC	Kaikki kohdat	Asiakirjan päivittäminen jäljempänä mainituilta YTM-työryhmän jäseniltä tai organisaatioilta saatujen versiota 0.3 koskevien huomautusten mukaisesti ja siten kuin niiden kanssa on sovittu puhelinkeskusteluissa: • Euroopan rautatieyhteisö (CER), • Alankomaiden kansallinen turvallisuusviranomainen.
		Kaikki kohdat	Asiakirjan päivittäminen YTM-suosituksen allekirjoitetun version mukaisesti. Asiakirjan päivittäminen Christophe Cassirin ja Marcus Anderssonin viraston sisäisen tarkistuksen tuloksena esittämien huomautusten

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

Taulukko 1: Asiakirjan tila

Versio Päiväys	Laatija(t)	Kohta	Muutoksen kuvaus
			perusteella.
		Kaikki kohdat Lisäykset	Asiakirjan tai suosituksen kohtien uudelleennumeroinnin loppuunsaattaminen. YTM-suosituksen soveltamisesimerkkien sisällyttäminen asiakirjaan.
Uuden asiakirjan otsikko ja rakenne: ”Esimerkkikokoelma riskien arvioinneista ja YTM-asetusta tukevista mahdollisista välineistä”			
Ohjeversio 0.1 23.5.2008	Dragan JOVICIC	Kaikki	”Käyttöoppaan” version 0.5 kahteen täydentävään asiakirjaan jakamisen tuloksena laaditun asiakirjan ensimmäinen versio.
Ohjeversio 02 3.9.2008	Dragan JOVICIC	Kaikki	Asiakirjan päivittäminen: • Euroopan komission yhteisiä turvallisuusmenetelmiä koskevan asetuksen mukaisesti {Ref. 3}, • 1. heinäkuuta 2008 yhdessä rauteteiden yhteenliitettävyyttä ja turvallisuutta käsittelevän komitean (RISC) jäsenten kanssa järjestetyn työpajan tuloksena saatujen huomautusten mukaisesti, • YTM-työryhmän jäseniltä (Norjan, Suomen, Yhdistyneen kuningaskunnan ja Ranskan kansalliset turvallisuusviranomaiset, CER, EIM, Jens BRABAND (UNIFE) ja Stéphane ROMEI (UNIFE)) saatujen huomautusten mukaisesti.
Ohjeversio 1.0 10.12.2008	Dragan JOVICIC	Kaikki	Asiakirjan päivittäminen rautateiden yhteenliitettävyyttä ja turvallisuutta käsittelevän komitean (RISC) 25. marraskuuta 2008 järjestämässä kokouksessa hyväksymän riskien arvioinnista annettavan Euroopan komission YTM-asetuksen {Ref. 3} mukaisesti.
Ohjeversio 1.1 6.1.2009	Dragan JOVICIC	Kaikki	Asiakirjan päivittäminen Euroopan komission oikeudellisen ja lingvistisen yksikön YTM-asetuksesta esittämien huomautusten perusteella.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Sisällysluettelo

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

Luettelo kaavioista

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Luettelo taulukoista

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

0. JOHDANTO

0.1. Soveltamisala

0.1.1. Tämän asiakirjan tarkoituksena on selventää edelleen ”komission asetusta Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymisestä” {Ref. 3}. Asetukseen viitataan nyt esillä olevassa asiakirjassa ilmaisulla yhteistä turvallisuusmenetelmää koskeva asetus (YTM-asetus).

0.1.2. Tämä asiakirja ei ole oikeudellisesti sitova, eikä sen sisältöä pidä tulkita siten, että se on ainoa keino täyttää YTM-asetuksen vaatimukset. Asiakirjalla pyritään täydentämään YTM-asetuksen soveltamisopasta {Ref. 4}, jossa selvennetään, miten YTM-asetuksessa säädettyä menettelyä on käytettävä ja sovellettava. Asiakirjassa annetaan käytännöllistä lisätietoa, mutta siinä ei määrätä noudatettavista pakollisista menettelyistä eikä vahvisteta oikeudellisesti sitovia menettelytapoja. Tästä tiedosta voi olla hyötyä kaikille toimijoille[(1)], joiden toimilla voi olla vaikutusta rautatiejärjestelmien turvallisuuteen ja joiden on sovellettava suoraan tai välillisesti YTM-asetusta. Asiakirjassa esitetään esimerkkejä riskien arvioinneista ja kuvataan muutamia mahdollisia työvälineitä YTM-asetuksen soveltamisen tueksi. Nämä esimerkit on tarkoitettu ainoastaan ohjeeksi ja tueksi. Toimijat voivat käyttää vaihtoehtoisia menetelmiä tai jatkaa omien menetelmiensä ja työvälineidensä käyttöä YTM-asetuksen vaatimusten täyttämiseksi, jos ne ovat toimijoiden mielestä soveltuvampia.
Tässä asiakirjassa esitetyt esimerkit ja lisätiedot eivät ole tyhjentäviä, eivätkä ne kata kaikkia mahdollisia tilanteita, joissa merkittävät muutokset ovat mahdollisia, ja tästä syystä asiakirjaa on pidettävä pelkästään informatiivisena.

0.1.3. Tätä informatiivista asiakirjaa on käytettävä ainoastaan YTM-asetuksen soveltamisen tukena. Asiakirjaa on luettava yhdessä YTM-asetuksen {Ref. 3} ja sitä koskevan soveltamisoppaan {Ref. 4} kanssa, mutta sillä ei korvata YTM-asetusta.

0.1.4. Asiakirjan on laatinut Euroopan rautatievirasto (ERA), jota on avustanut YTM-työryhmään osallistuneet rautatieyhdistys ja kansallisia turvallisuusviranomaisia edustavat asiantuntijat. Asiakirjassa esitetään kokoelma pitkälle kehitettyjä ideoita ja tietoja, jotka virasto on koonnut sisäisissä kokouksissa ja YTM-työryhmän ja -erityisryhmän kanssa järjestetyissä kokouksissa. Euroopan rautatievirasto tarkastelee opasta uudelleen tarpeen mukaan ja päivittää sitä siten, että otetaan huomioon eurooppalaisten standardien kehittyminen, riskien arviointia koskevaan YTM-asetukseen tehdyt muutokset ja YTM-asetuksen käytöstä saadusta kokemuksesta annettu mahdollinen palaute. Koska tätä opasta kirjoitettaessa tarkistusmenettelyn aikataulu ei ole vielä selvillä, lukijaa kehotetaan ottamaan yhteyttä Euroopan rautatievirastoon saadakseen tiedot oppaan uusimmasta saatavana olevasta painoksesta.

---

(1) Tällaisia toimijoita ovat rautatiejärjestelmän yhteentoimivuudesta yhteisössä annetun direktiivin 2008/57/EY 2 artiklan r kohdassa määritetyt hankintayksiköt tai valmistajat, jotka ovat asetuksen mukaan ”hakijoita”, tai niiden toimittajat ja palveluntarjoajat.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

0.2. Soveltamisalan ulkopuolelle jäävät asiat

0.2.1. Tässä asiakirjassa ei anneta ohjeita rautatiejärjestelmän tai sen osien organisoimista, käyttöä tai suunnittelua (valmistusta) varten. Asiakirjassa ei myöskään vahvisteta toimijoiden välisiä riskinhallintamenettelyn soveltamiseen liittyviä mahdollisia sopimusehtoja tai järjestelyjä. Hankekohtaiset sopimusjärjestelyt ovat YTM-asetuksen, sen soveltamisoppaan ja tämän asiakirjan soveltamisalan ulkopuolella.

0.2.2. Vaikka asianomaisten toimijoiden väliset järjestelyt eivät kuulu tämän asiakirjan soveltamisalaan, ne voidaan kirjata asiaa koskeviin sopimuksiin hankkeen alussa, sanotun kuitenkaan rajoittamatta YTM-asetuksen säännösten soveltamista. Tällaiset järjestelyt voivat kattaa esimerkiksi seuraavat näkökohdat:

(a) toimijoiden välisiin rajapintoihin liittyvien turvallisuusriskien hallinnasta aiheutuvat kustannukset,
(b) sellaisten vaarojen ja niihin liittyvien turvallisuustoimenpiteiden siirrosta toimijoiden kesken aiheutuvat kustannukset, jotka eivät ole vielä tiedossa hankkeen alussa,
(c) hankkeen aikana mahdollisesti ilmenevien ristiriitojen hallinnointi,
(d) muut näkökohdat.

Jos hakijan ja hänen alihankkijoidensa kesken syntyy erimielisyyksiä tai ristiriitoja hankkeen kehittämisen aikana, mahdollisten riitojen sopimiseksi voidaan nojautua asiaa koskeviin sopimuksiin.

0.3. Asiakirjan käyttöä ohjaava periaate

0.3.1. Tätä asiakirjaa ei ole tarkoitettu luettavaksi itsenäisenä asiakirjana, eikä sillä korvata YTM-asetusta {Ref. 3}. Vertailun helpottamiseksi YTM-asetuksen jokainen artikla on kopioitu tähän asiakirjaan. Kyseistä artiklaa on selvennetty tarvittaessa YTM-asetuksen soveltamisoppaassa {Ref. 4}. Artiklan jälkeen esitetyissä kohdissa annetaan tarvittaessa ohjeita artiklan ymmärtämisen helpottamiseksi.

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

0.3.3. Tämän asiakirjan rakenne vastaa YTM-asetuksen ja sen soveltamisoppaan rakennetta, millä pyritään parantamaan luettavuutta.

0.4. Asiakirjan kuvaus

0.4.1. Asiakirja on jaettu osiin seuraavasti:

(a) Luvussa 0 määritetään asiakirjan soveltamisala ja esitetään viiteasiakirjojen luettelo.
(b) Liitteessä I ja liitteessä II annetaan lisätietoa YTM-asetuksen {Ref. 3} ja sen soveltamisoppaan {Ref. 4} vastaavista kohdista.
(c) Uusissa lisäyksissä työstetään edelleen joitakin erityisnäkökohtia ja annetaan esimerkkejä.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.5. Viiteasiakirjat

Taulukko 2: Viiteasiakirjat

{Ref N:o}	Otsikko	Viite	Versio
{Ref. 1}	Euroopan parlamentin ja neuvoston direktiivi 2004/49/EY, annettu 29 päivänä huhtikuuta 2004, yhteisön rautateiden turvallisuudesta sekä rautatieyritysten toimiluvista annetun neuvoston direktiivin 95/18/EY ja rautateiden infrastruktuurikapasiteetin käyttöoikeuden myöntämisestä ja rautateiden infrastruktuurin käyttömaksujen perimisestä sekä turvallisuustodistusten antamisesta annetun direktiivin 2001/14/EY muuttamisesta (rautatieturvallisuusdirektiivi)	2004/49/EY *EUVL L 164, 30.4.2004, s. 44,* oikaisu *EUVL 220, 21.6.2004, s. 16*.	–
{Ref. 2}	Euroopan parlamentin ja neuvoston direktiivi 2008/57/EY, annettu 17 päivänä kesäkuuta 2008, rautatiejärjestelmän yhteentoimivuudesta yhteisössä	2008/57/EY EUVL L 191, 18.7.2008, s. 1.	–
{Ref. 3}	Komission asetus (EY) N;o°.../.., annettu [...], Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymisestä	xxxx/yy/EY	äänestys toimitettu RISC:n kokouksessa 25.11.2008
{Ref. 4}	Rautatieturvallisuusdirektiivin 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymistä koskevan komission asetuksen soveltamisopas	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Euroopan parlamentin ja neuvoston direktiivi 2008/57/EY, annettu 17 päivänä kesäkuuta 2008, rautatiejärjestelmän yhteentoimivuudesta yhteisössä	2008/57/EY EUVL L 191, 18.7.2008, s. 1.	–
{Ref. 6}	Turvallisuusjohtamisjärjestelmän arviointiperusteet rautatieyritysten ja infrastruktuurin haltijoita varten	Turvallisuusjohtamis-järjestelmän (SMS) arviointiperusteet Osa A: Turvallisuustodistukset ja -luvat	31.5.2007
{Ref. 7}	Rautatiesovellukset – Tietoliikenne, merkinanto- ja tietojenkäsittelyjärjestelmät – Turvallisuuteen liittyvät elektroniset järjestelmät	EN 50129	Helmikuu 2003
{Ref. 8}	Rautatiesovellukset - Toimintavarmuuden, käyttövarmuuden, kunnossapidettävyyden ja turvallisuuden (RAMS) määrittely ja esittäminen (RAMS) – Osa 1: Perusvaatimukset ja yleiset menetelmät	EN 50126-1	Syyskuu 2006
{Ref. 9}	Rautatiesovellukset - Toimintavarmuuden, käyttövarmuuden, kunnossapidettävyyden ja turvallisuuden (RAMS) määrittely ja esittäminen (RAMS) – Osa 2: Standardin EN 50126-1 soveltamisopas	EN 50126-2 (ohje)	Lopullinen ehdotus (Elokuu 2006)
{Ref. 10}	Vaarallisten aineiden rautatiekuljetuksiin liittyvien riskien laskennassa sovellettava yleinen ohje (Generic Guideline for the Calculation of Risk inherent in the Carriage of Dangerous Goods by Rail)	RID-asiantuntijakomitean hyväksymä OTIF:in ohje,	24.11.2005
{Ref. 11}	Teknisten järjestelmien hyväksyttävää riskitasoa koskeva peruste (RAC-TS)	Muistio 01/08	1.1 (25.1.2008)
{Ref. 12}	Euroopan rautatieviraston turvallisuusyksikön laatima toteutettavuustutkimus “Apportionment of safety targets (to TSI sub-systems) and consolidation of TSI from a safety point of view” WP1.1 - Assessment of the feasibility to apportion Common Safety Targets	WP1.1	1.0
{Ref. 13}	”Kiskoliikenne. Kiskokaluston merkintäjärjestelmä. Osa 4: EN 0015380 Osa 4: Toimintaryhmät".	EN 0015380. Osa 4	

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

0.6. Yleiset määritelmät, käsitteet ja lyhenteet

0.6.1. Tässä asiakirjassa käytetyt yleiset määritelmät, käsitteet ja lyhenteet löytyvät tavanomaisesta sanakirjasta.

0.6.2. Tässä oppaassa käytetyt uudet määritelmät, käsitteet ja lyhenteet määritellään jäljempänä olevissa kohdissa.

0.7. Erityiset määritelmät

0.7.1. Katso 3 artikla

0.8. Erityiset käsitteet ja lyhenteet

0.8.1. Tässä kohdassa määritellään nyt tarkasteltavassa asiakirjassa usein toistuvat uudet erityiset käsitteet ja lyhenteet.

Taulukko 3: Käsitteet

Käsite	Määritelmä
Virasto	Euroopan rautatievirasto (ERA)
Opas	”Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymisestä [...] annetun komission asetuksen (EY) N:o …/.. soveltamisopas”
YTM-asetus	”Komission asetus (EY) N:o .../.., annettu [...], Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymisestä” {Ref. 3}

Taulukko 4: Lyhenteet

Lyhenne	Merkitys
CCS	Ohjaus-, hallinta- ja merkinantojärjestelmä (Control Command and Signalling)
CSM (YTM)	Yhteinen turvallisuusmenetelmä
CST (YTT)	Yhteiset turvallisuustavoitteet
EC	Euroopan komissio
ERA	Euroopan rautatievirasto
IM	Infrastruktuurin haltija(t)
ISA	Riippumaton turvallisuuden arvioija
OTIF	Kansainvälisten rautatiekuljetusten hallitustenvälinen järjestö (Intergovernmental Organisation for International Carriage by Rail)
MS	Jäsenvaltio
NOBO	Ilmoitettu laitos
NSA	Kansallinen turvallisuusviranomainen
QMP	Laadunhallintamenettely
QMS	Laadunhallintajärjestelmä
RISC	Rautateiden yhteentoimivuutta ja turvallisuutta käsittelevä komitea
RU	Rautatieyritys
SMP	Turvallisuusjohtamismenettely

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Taulukko 4: Lyhenteet

Lyhenne	Merkitys
SMS	Turvallisuusjohtamisjärjestelmä
SRT	Rautatietunnelien turvallisuus
TBC	Täydennetään myöhemmin
TSI	Yhteentoimivuuden tekniset eritelmät

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

YTM-ASETUKSEN ARTIKLOJA KOSKEVAT SELVENNYKSET

1 artikla Tarkoitus

1 artiklan 1 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

1 artiklan 2 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

2 artikla Soveltamisala

2 artiklan 1 kohta

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] YTM:ää sovelletaan koko rautatiejärjestelmään, ja se kattaa jäljempänä mainitut rautatiejärjestelmiin tehtävät muutokset, jos niiden arvioidaan olevan merkittäviä 4 artiklan perusteella:

(a) uusien ratojen rakentaminen tai vanhojen ratojen muuttaminen,
(b) uusien ja/tai muutettujen teknisten järjestelmien käyttöönotto,
(c) toiminnalliset muutokset (kuten uudet tai mukautetut toimintasäännöt ja kunnossapitomenettelyt),

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(d) rautatieyrityksen/infrastruktuurin haltijan organisaatiossa tehtävät muutokset.

Käsitteellä ”järjestelmä” viitataan YTM-asetuksessa järjestelmän kaikkiin näkökohtiin, kuten järjestelmän kehittämiseen, käyttöön ja kunnossapitoon siihen saakka, kunnes järjestelmä poistetaan käytöstä tai hävitetään.

[G 2] YTM kattaa seuraaviin järjestelmiin tehtävät merkittävät muutokset:

(a) ”pienet ja yksinkertaiset” järjestelmät, jotka muodostuvat muutamasta teknisestä osajärjestelmästä tai osasta, ja
(b) ”suuret ja monimutkaiset” järjestelmät (kuten asemia ja tunneleita käsittävät järjestelmät).

2 artiklan 2 kohta

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

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

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

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

[G 1] Rautatieturvallisuusdirektiivin {Ref. 1} ja rautateiden yhteentoimivuusdirektiivin {Ref. 2} mukaan esimerkiksi suurten nopeuksien rautatiejärjestelmän uudentyyppisen liikkuvan kaluston on oltava yhdenmukainen suurten nopeuksien rautatiejärjestelmän liikkuvaa kalustoa koskevien yhteentoimivuuden teknisten eritelmien kanssa. Vaikka yhteentoimivuuden tekniset eritelmät kattavat valtaosin arvioitavana olevan järjestelmän, ne eivät kata tärkeitä ohjaamoon liittyviä inhimillisiä tekijöitä. Yhteistä turvallisuusmenetelmää on sovellettava sen varmistamiseksi, että kaikki inhimillisiin tekijöihin liittyvät kohtuullisesti ennakoitavat vaarat (toisin sanoen kuljettajan, liikkuvan kaluston ja rautatiejärjestelmän muiden osien välisiin rajapintoihin liittyvät vaarat) tunnistetaan ja niitä valvotaan asianmukaisesti.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

2 artiklan 3 kohta

This Regulation shall not apply to:

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

2 artiklan 4 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

3 artikla Määritelmät

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

The following definitions shall also apply:

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

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

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

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

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

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

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

(8) 'actors' means all parties which are, directly or through contractual arrangements, involved in the application of this Regulation pursuant to 0;

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

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

(4) *EYVL L 235, 17.9.1996, s. 6.*

(5) *EYVL L 110, 20.4.2001, s. 1.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

4 artikla Merkittävät muutokset

4 artiklan 1 kohta

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] Jos kansallista sääntöä ei ole ilmoitettu, päätöksen tekeminen on hakijan vastuulla. Muutoksen merkittävyys määritetään asiantuntija-arvion perusteella. Jos esimerkiksi käytössä olevaan järjestelmään suunniteltu muutos on monimutkainen, sitä voidaan pitää merkittävänä, jos järjestelmän nykyisiin toimintoihin kohdistuvien vaikutusten riski on suuri[(6)], vaikka muutos itsessään ei välttämättä liity olennaisesti turvallisuuteen.

4 artiklan 2 kohta

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] **Esimerkki pienistä muutoksista:** järjestelmän käyttöönoton jälkeen radan enimmäisnopeuden lisääminen kerran 5 km:llä/h ei välttämättä ole merkittävä muutos. Jos radan enimmäisnopeutta lisätään kuitenkin jatkossakin vaiheittain 5 km/h, peräkkäisten muutosten (jotka yksittäin arvioituna ovat vähämerkityksisiä) summa voi muodostaa merkittävän muutoksen järjestelmän alkuperäisiin turvallisuusvaatimuksiin nähden.

(6) *Järjestelmän toiminnot eivät ole aina riippumattomia toisistaan ja joidenkin toimintojen muutoksilla voi olla vaikutusta myös järjestelmän muihin toimintoihin, vaikka näyttäisikin siltä, ettei muutos koske niitä välittömästi.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Arvioitaessa, onko useiden peräkkäisten (vähämerkityksisten) muutosten sarja merkittävä kokonaisuutena tarkasteltuna, on otettava huomioon kaikki muutoksiin liittyvät vaarat ja riskit. Tarkasteltavien muutosten sarjaa voidaan pitää vähämerkityksisenä, jos tuloksena oleva riski on yleisesti hyväksyttävä.

[G 3] Viraston toteuttamat merkittäviä muutoksia koskevat toimet ovat osoittaneet, että:

(a) on mahdotonta määrittää yhdenmukaistettuja raja-arvoja tai sääntöjä, joiden perusteella voitaisiin päättää tietyn muutoksen merkittävyydestä, ja;
(b) on mahdotonta laatia tyhjentävää luetteloa merkittävistä muutoksista;
(c) päätöstä ei voida soveltaa kaikkiin hakijoihin eikä kaikissa teknisissä, toiminnallisissa, organisatorisissa ja ympäristöoloissa.

Siksi on ehdottoman tärkeää jättää päätös hakijan vastuulle, sillä hakija vastaa rautatieturvallisuusdirektiivin {Ref. 1} 4 artiklan 3 kohdan mukaan sille kuuluvan järjestelmän osan turvallisesta käytöstä ja siihen liittyvien riskien hallinnasta.

[G 4] Liitteessä LISÄYS C olevassa C.2. kohdassa on esitetty hakijan avuksi esimerkki ”perusteiden arvioinnista ja käytöstä”.

[G 5] YTM:ää ei pidä soveltaa, jos turvallisuuteen liittyvä muutos on vähämerkityksinen, mutta se ei kuitenkaan merkitse kaikista toimista luopumista. Hakija toteuttaa tällöin jonkinlaisen (alustavan) riskianalyysin sen toteamiseksi, onko muutos merkittävä. Tällaiset riskianalyysit ja kaikki asiaa koskeva perustelu ja väitteet on dokumentoitava, jotta kansallinen turvallisuusviranomainen voi toteuttaa tarkastukset. Muutoksen merkittävyyden arviointi ja muutoksen luokittelemista vähämerkityksiseksi koskeva päätös ei edellytä arviointielimen toteuttamaa riippumatonta arviota.

5 artikla Riskinhallintamenettely

5 artiklan 1 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

5 artiklan 2 kohta

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5 artiklan 3 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

6 artikla Riippumaton arviointi

6 artiklan 1 kohta

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] Arviointielimeltä vaadittu riippumattomuuden taso määräytyy arvioitavalta järjestelmältä vaaditun turvallisuustason perusteella. Koska alan toimien yhdenmukaistaminen on edelleen kesken, paras käytäntö on esitetty standardin IEC 61508-1:2001 kohdassa 8 tai standardin EN 50 kohdassa 5.3.9 {Ref. 7}. Riippumattomuuden taso määräytyy sekä laitteisiin liittyvän vaaran seurauksien vakavuuden että laitteiden uutuuden perusteella. Standardin EN 50 126-2 kohdassa 9.7.2 ja standardissa EN 50129 määritetään opastinjärjestelmien riippumattomuuden taso. Sitä voidaan soveltaa periaatteessa myös muihin järjestelmiin.

[G 2] Eri arviointielinten (NSA, NOBO ja ISA) tehtävien ja vastuiden sekä niiden välisten välttämättömien rajapintojen määrittämistä koskevat viraston toimet ovat edelleen kesken. Tarkoituksena on määrittää mahdollisuuksien mukaan, mitä kukin arviointielin tekee ja miten se hoitaa tehtävän. Tämän perusteella voidaan lopulta määrittää, miten:

(a) tarkastetaan todisteiden pohjalta, että YTM:n riskinhallinta- ja riskinarviointimenettelyjä sovelletaan oikein, ja
(b) tuetaan hakijaa arvioitavaan järjestelmään tehtävän merkittävän muutoksen hyväksymistä koskevassa päätöksenteossa.

6 artiklan 2 kohta

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] Viraston toteuttamilla arviointielinten tehtävien ja vastuiden määrittämistä koskevilla toimilla tuotetaan lisätietoa.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

6 artiklan 3 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

6 artiklan 4 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

7 artikla Turvallisuusarviointikertomukset

7 artiklan 1 kohta

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

7 artiklan 2 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

7 artiklan 3 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

7 artiklan 4 kohta

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] Tämä vastavuoroisen tunnistamisen periaate on jo hyväksytty CENELEC-standardeissa: katso standardin EN 50 129 kohta 5.5.2 ja standardin EN 50 126-2 kohta 5.9. CENELEC-standardeissa hakijat tai riippumattomat turvallisuuden arvioijat soveltavat ristiinhyväksynnän tai vastavuoroisen tunnustamisen periaatetta yleisiin tuotteisiin ja yleisiin sovelluksiin[(7)] edellyttäen, että turvallisuusarviointi ja turvallisuusvaatimusten mukaisuuden osoittaminen toteutetaan CENELEC-standardien vaatimusten mukaisesti.

[G 2] Vastavuoroista tunnustamista on sovellettava myös uusien tai mukautettujen järjestelmien hyväksynnässä, jos niiden riskinarviointi ja järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen toteutetaan YTM-asetuksen {Ref. 3} säännösten mukaisesti.

8 artikla Riskinhallinta / sisäiset ja ulkoiset tarkastukset

8 artiklan 1 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

(7) *Ks. lisätietoa käsitteistä ”yleinen tuote” ja ”yleinen sovellus” ja niihin liittyvistä periaatteista 1.1.5 kohtaa koskevasta G 5 kohdasta ja sivun 24 alaviitteistä [9] ja [10] sekä tämän asiakirjan kaaviosta 3.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

8 artiklan 2 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

9 artikla Palaute ja tekninen kehitys

9 artiklan 1 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

9 artiklan 2 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

9 artiklan 3 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

9 artiklan 4 kohta

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;

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(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] Lisäselvennystä ei pidetä tarpeellisena.

10 artikla Voimaantulo

10 artiklan 1 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

10 artiklan 2 kohta

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

LIITE I - YTM-ASETUKSESSA SÄÄDETTYÄ MENETTELYÄ KOSKEVAT SELVENNYKSET

1. RISKINHALLINTAMENETTELYYN SOVELLETTAVAT YLEISET PERIAATTEET

1.1. Yleiset periaatteet ja velvoitteet

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] Kaaviossa 1 esitetään YTM-asetuksen riskinhallintakehys ja siihen liittyvä riskinarviointimenettely. Kaavion kutakin laatikkoa/toimea kuvataan tarvittaessa yksityiskohtaisemmin tämän asiakirjan erillisessä kohdassa.

[G 2] CENELECin ohjeen mukaan riskinhallinta- ja riskinarviointimenettelyt on kuvattava turvallisuussuunnitelmassa. Jos se ei kuitenkaan ole asianmukaista hankkeen kannalta, kyseinen kuvaus voidaan sisällyttää toiseen asiaa koskevaan asiakirjaan. Katso 1.1.6 kohta.

[G 3] Riskinarviointimenettely käynnistetään alustavalla järjestelmämäärittelyllä. Hanketta kehitettäessä alustavaa järjestelmämäärittelyä päivitetään vaiheittain, ja alustava määrittely korvataan lopullisella järjestelmämäärittelyllä. Jos alustavaa järjestelmämäärittelyä ei ole tehty, riskiarvioinnin toteuttamiseen käytetään lopullista järjestelmämäärittelyä. On kuitenkin järkevää, että kaikki toimijat, joita merkittävä muutos koskee, tapaavat hankkeen alussa sopiakseen

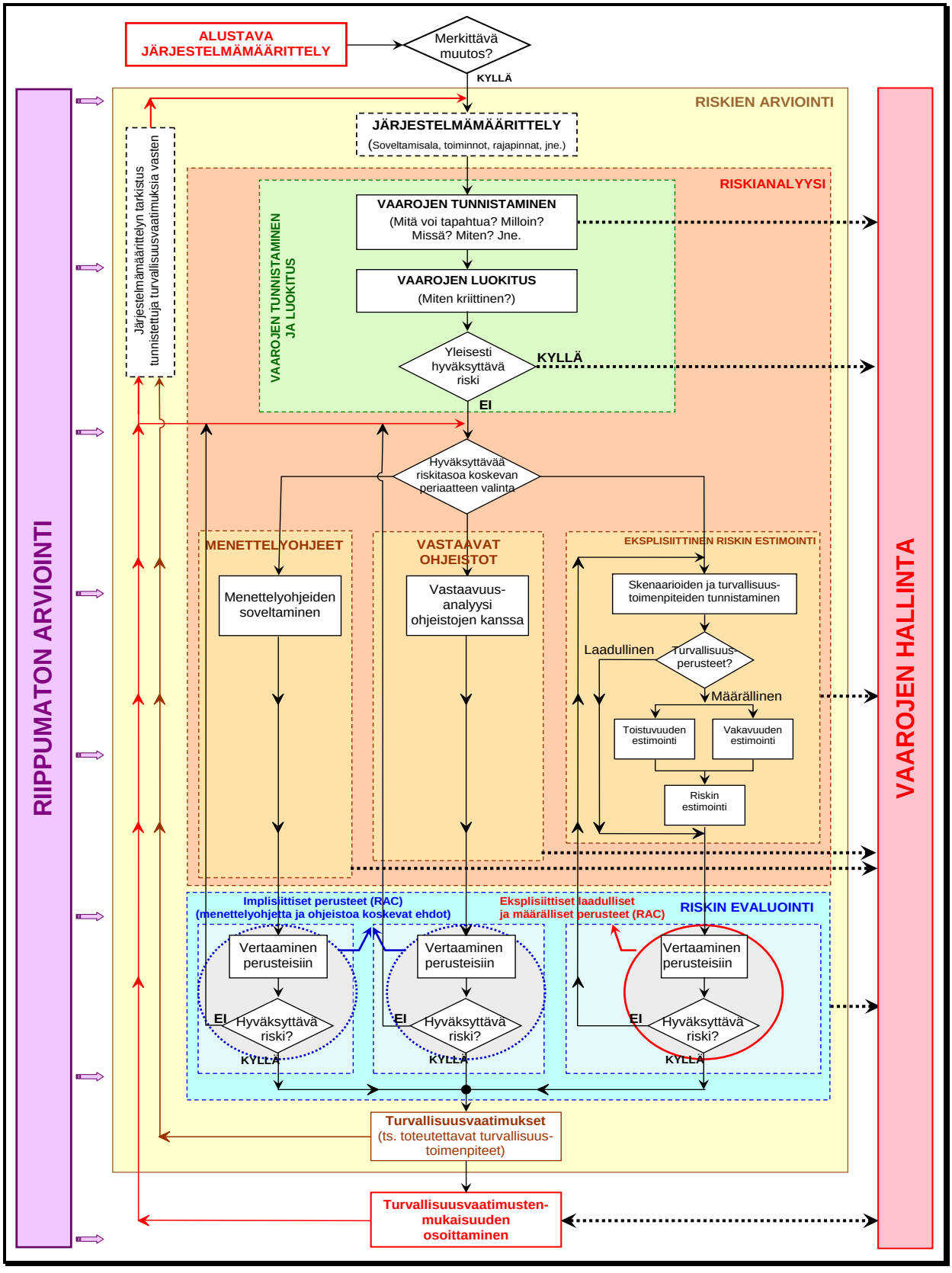
(a) järjestelmän yleisperiaatteista, järjestelmän toiminnoista jne. Nämä voidaan kuvata periaatteessa alustavassa järjestelmämäärittelyssä;
(b) hankeorganisaatiosta;
(c) tehtävien ja vastuiden jaosta jo mukana olevien eri toimijoiden, kuten kansallisen turvallisuusviranomaisen, ilmoitetun laitoksen ja riippumattoman turvallisuuden arvioijan kesken.

Tällaiset koordinointitoimet, jotka voidaan toteuttaa esimerkiksi alustavan järjestelmämäärittelyn yhteydessä, mahdollistavat sen, että hakija, alihankkijat, kansallinen turvallisuusviranomainen, ilmoitettu laitos ja riippumaton turvallisuuden arvioija voivat

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

tarvittaessa sopia jo varhaisessa vaiheessa hankkeessa sovellettavista menettelyohjeista tai vastaavista ohjeistoista.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu



Kaavio 1: YTM-asetuksen riskinhallintakehys

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

1.1.2. This iterative risk management process:

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

[G 1] Rautatieyrityksen ja infrastruktuurin haltijan turvallisuusjohtamisjärjestelmässä (SMS) määritetään prosessi ja menettelyt, joilla

(a) valvotaan, että järjestelmä pysyy turvallisena sen koko elinkaaren ajan (eli järjestelmän käytön ja kunnossapidon ajan);
(b) varmistetaan järjestelmän turvallinen purkaminen tai korvaaminen.

Tämä prosessi ei kuulu YTM:n mukaiseen riskinarviointiin.

[G 2] YTM:n toteuttamiseksi on välttämätöntä, että kaikki menettelyyn osallistuvat osapuolet ovat päteviä (eli heillä on asianmukaiset taidot, tiedot ja kokemusta). Rautatiealan toimijoiden organisaatiossa on jatkuva pätevyyden hallinnan tarve:

(a) infrastruktuurin haltijoiden ja rautatieyritysten osalta rautatieturvallisuusdirektiivin {Ref. 1} liitteessä III olevan 2 kohdan e alakohdan turvallisuusjohtamisjärjestelmä kattaa pätevyyden hallinnan;
(b) vaikka turvallisuusjohtamisjärjestelmä ei olekaan pakollinen, muilla toimijoilla, joiden toimilla voi olla vaikutusta rautatiejärjestelmän turvallisuuteen, on yleensä käytössä vähintään hanketasolla (katso 5.1 kohtaa koskeva G 1 kohta) laadunhallintamenettely ja/tai turvallisuusjohtamismenettely, jolla täytetään tämä vaatimus.

[G 3] CENELEC-standardin EN 50 126-1 {Ref. 8} seuraavissa kohdissa esitetään pätevyyttä koskevat ohjeet:

(a) kohdan 5.3.5 b alakohdan mukaan *”kaikkien henkilöstön jäsenten, joilla on riskinhallintamenettelyyn liittyviä tehtäviä, on oltava päteviä hoitamaan kyseisiä tehtäviä”*;
(b) kohdan 5.3.5 d alakohdan mukaan riskinhallinnan ja riskinarvioinnin vaatimukset on ”*täytettävä liiketoiminnan menettelyillä, joita tuetaan arvioitavana olevan järjestelmän kannalta sopivalla standardien EN ISO 9001, EN ISO 9002 tai EN ISO 9003 vaatimusten mukaisella laadunhallintajärjestelmällä”*. Standardin EN 50 129 {Ref. 7} kohdassa 5.2 esitetään esimerkki laadunhallintajärjestelmän avulla valvottavista näkökohdista.

Nämä kattavat laadunvarmistustoimet sekä henkilöstön/henkilöiden pätevyyden ja koulutuksen YTM:ään sisältyvän menettelyn tukemiseksi.

[G 4] On hyvin yleistä, että arviointielin seuraa riskinarviointimenettelyä hankkeen alusta lähtien, mutta jollei jäsenvaltion kansallisessa lainsäädännössä toisin vaadita, tällainen arviointielimen varhainen osallistuminen ei ole pakollista, vaikka se on suositeltavaa. Riippumattoman arviointielimen lausunnosta voi olla hyötyä ennen seuraavaan riskinarviointivaiheeseen siirtymistä. Lisätietoa riippumattomasta arvioinnista on esitetty 6 artiklassa.

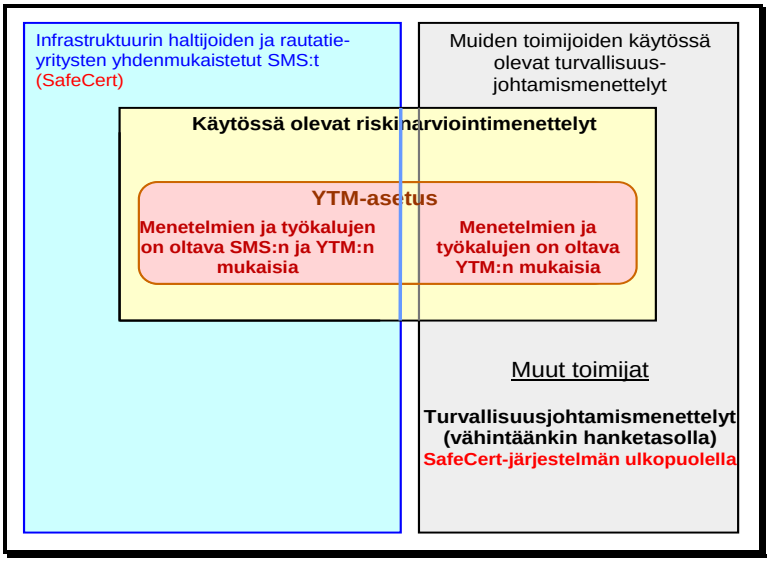
Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

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] Kaaviossa 2 esitetään YTM:n ja ”turvallisuusjohtamisjärjestelmien ja riskinarviointimenettelyjen” välinen suhde.



Kaavio 2: Yhdenmukaistettu turvallisuusjohtamisjärjestelmä (SMS) ja YTM.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

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

[G 1] Jos hakija on infrastruktuurin haltija tai rautatieyritys, menettelyyn voi olla välttämätöntä ottaa mukaan myös muita toimijoita[8] (katso 1.2.1 kohta). Joissakin tapauksissa infrastruktuurin haltija tai rautatieyritys voi teettää riskinarviointitoimet joko osittain tai kokonaan alihankintana. Kunkin toimijan tehtävistä ja vastuista sovitaan yleensä asianomaisten toimijoiden kesken jo hankkeen varhaisessa vaiheessa.

[G 2] On tärkeää panna merkille, että hakija on aina vastuussa YTM:n soveltamisesta, riskien hyväksymisestä ja siten koko järjestelmän turvallisuudesta. Tässä yhteydessä on varmistettava, että

(a) asianomaiset toimijat tekevät kattavaa yhteistyötä kaikkien välttämättömien tietojen saamiseksi, ja
(b) on selvää, kenen vastuulla erityisten YTM-vaatimusten täyttäminen on (esimerkiksi riskianalyysin toteuttaminen tai vaaroja koskevan asiakirjan hallinnointi).

Jos toimijat eivät pääse sopimukseen niille asetettavista vaatimuksista, kansalliselta turvallisuusviranomaiselta voidaan pyytää asiasta lausunto. Vastuu ratkaisun löytämisestä on kuitenkin hakijalla, eikä sitä voida siirtää kansalliselle turvallisuusviranomaiselle: katso myös 0.2.2. kohta

[G 3] Jos tehtävä annetaan toimeksi alihankkijalle, alihankkijalla ei ole velvollisuutta pitää yllä omaa turvallisuusorganisaatiota, jos se ei ole infrastruktuurin haltija tai rautatieyritys tai varsinkaan jos alihankkijan rakenne/koko tai sen osuus kokonaisjärjestelmästä on pieni. Vastuu riskinhallinnasta, riskien arviointi ja vaarojen hallinta mukaan luettuina, voidaan säilyttää ylemmällä organisaatiotasolla (eli alihankkijan asiakkaalla). Alihankkija on kuitenkin aina vastuussa sellaisten toimintoihinsa liittyvien oikeiden tietojen toimittamisesta, jotka ovat välttämättömiä ylemmälle organisaatiotasolle riskinhallintaan liittyvien asiakirjojen laatimiseksi.
Yhteistyöorganisaatiot voivat myös sopia yhteisen turvallisuusorganisaation perustamisesta esimerkiksi kustannusten optimoimiseksi. Tällöin ainoastaan yksi organisaatio hallinnoi kaikkien osallistujaorganisaatioiden turvallisuustoimia. Vastuu tietojen (eli vaarojen, riskien ja turvallisuustoimenpiteiden) tarkkuudesta ja turvallisuustoimenpiteiden täytäntöönpanon hallinnoinnista säilyy sillä organisaatiolla, joka on vastuussa näihin turvallisuustoimenpiteisiin liittyvien vaarojen valvonnasta.

[G 4] Yleensä hakija määrittää hankkeeseen osallistuvien toimijoiden ja näiden toimijoiden eri osajärjestelmien ja laitteiden ”turvallisuustasot” ja ”turvallisuusvaatimukset”:

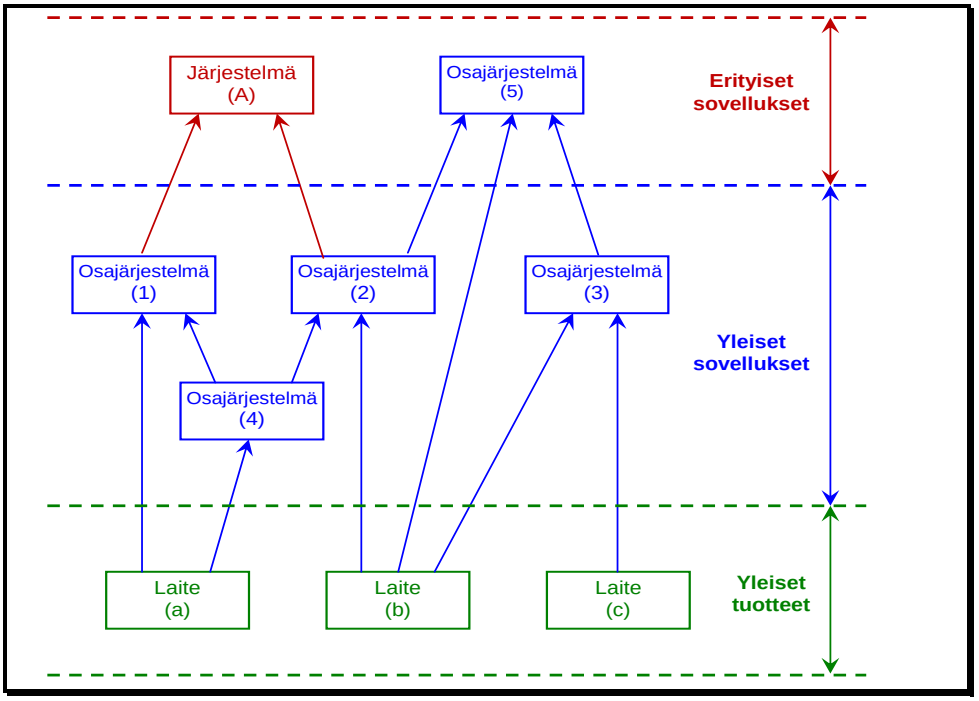
(a) hakijan ja asianomaisten toimijoiden (alihankkijoiden) välisissä sopimuksissa;
(b) turvallisuussuunnitelmassa tai muussa samaa tarkoitusta varten laaditussa asiakirjassa, jossa kuvataan koko hankkeen organisaatio ja kunkin toimijan vastuut, hakijan vastuut mukaan luettuina: katso 1.1.6 kohta;
(c) hakijan vaaroja koskevassa asiakirjassa: katso 4.1.1 kohta.

(8) *Tämä vastaa CENELEC-standardin 50 129 {Ref. 7} lisäyksessä A.4 esitettyä käytäntöä.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

Järjestelmän ”turvallisuustasojen” ja ”turvallisuusvaatimusten” jaottelua osajärjestelmien ja laitteiden ja siten asianomaisten toimijoiden mukaan, itse hakija mukaan luettuna, voidaan tarkentaa/laajentaa kattamaan ”järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisen”: katso kaavio 1. CENELECin V-sykliin (katso 2.1.1 kohta ja kaavio 5 sivulla 35) verrattuna tämä toiminto vastaa vaihetta 5, joka koskee ”järjestelmävaatimusten jaottelemista” eri osajärjestelmien ja osien mukaan.

[G 5] Asetuksen 2 artiklan 2 kohdassa sallitaan myös muiden toimijoiden kuin rautatieyrityksen ja infrastruktuurin haltijan ottaa yleinen vastuu YTM:n vaatimusten täyttymisestä niiden tarpeiden mukaan. Valmistaja voi esimerkiksi toteuttaa yleisten tuotteiden tai yleisten sovellusten(9) riskinarvioinnin ”yleisen järjestelmämäärittelyn” pohjalta määrittääkseen turvallisuustasot ja turvallisuusvaatimukset, jotka yleisten tuotteiden ja yleisten sovellusten on täytettävä.



Kaavio 3: Esimerkkejä turvallisuusarvioiden välisistä riippuvuussuhteista (laadittu standardin EN 50 129 kaavion 9 pohjalta).

[G 6] CENELECin mukaan valmistajan on annettava riskinarvioinnista dokumentoitu näyttö yleistä tuotetta (tai yleistä sovellusta(9)) koskevissa turvallisuusarvioinneissa ja vaaroja koskevissa

---

(9) *Käsite ”yleistä sovellusta ja yleistä tuotetta koskevat turvallisuusarviot” on lainattu CENELEC-standardeista, joissa turvallisuusarvioita on kolmenlaisia (ks. Kaavio 3):*

(a) ***Yleistä tuotetta koskeva turvallisuusarvio*** *(sovelluksesta riippumaton). Yleistä tuotetta voidaan käyttää uudelleen erilaisissa riippumattomissa sovelluksissa;*

(b) ***Yleistä sovellusta koskeva turvallisuusarvio*** *(sovellusluokka). Yleistä sovellusta voidaan käyttää uudelleen tiettyyn luokkaan/lajiin kuuluvissa sovelluksissa, joilla on yhteisiä toimintoja;*

(c) ***Erityistä sovellusta koskeva turvallisuusarvio*** *(erityinen sovellus). Erityistä sovellusta käytetään ainoastaan yhtä tiettyä asennusta varten.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

asiakirjoissa. Tällaiset turvallisuusarviot ja vaaroja koskevat asiakirjat sisältävät kaikki oletukset(10) ja yksilöidyt ”käyttörajoitukset” (ts. turvallisuuteen liittyvät sovellusehdot), joita sovelletaan asiaan liittyviin yleisiin tuotteisiin (tai yleisiin sovelluksiin). Näin ollen kun yleistä tuotetta ja yleistä sovellusta käytetään erityisen sovelluksen yhteydessä, on osoitettava, että nämä oletuksia(10) ja ”käyttörajoituksia” (tai turvallisuuteen liittyviä sovellusehtoja) koskevat vaatimukset täyttyvät kussakin erityisessä sovelluksessa.

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] Jollei toisin sovita hankkeen alussa tehtävässä sopimuksessa, jokaista hanketta varten laaditaan tavallisesti asiakirja, jossa kuvataan riskinhallintatoimet. Kyseinen asiakirja päivitetään ja tarkistetaan aina, kun alkuperäiseen järjestelmään tehdään merkittäviä muutoksia.

[G 2] Tällaisessa asiakirjassa määritetään organisaation rakenne, henkilöstölle osoitetut vastuut, prosessit, menettelyt ja toimet, joilla varmistetaan yhdessä, että arvioitava järjestelmä on määritettyjen turvallisuustasojen ja turvallisuusvaatimusten mukainen. Asiakirjan on oltava YTM:n mukainen, sillä asiakirjaa käytetään arviointielimen tukena ja ohjeena. CENELEC-standardien mukaan tällaiset tiedot on sisällytettävä turvallisuussuunnitelmaan tai muuhun asiakirjaan, jossa on näitä aiheita käsittelevä erityinen osa.

[G 3] Hakijan turvallisuussuunnitelma tai muu asiaa koskeva asiakirja edustaa koko hankkeen organisaatiota. Siinä kuvataan, miten tehtävät ja vastuut jaetaan asianomaisten toimijoiden kesken. Yksityiskohtaisten tietojen osalta voidaan viitata kyseisten toimijoiden

---

Continuation of the footnote

Lisätietoa riippuvuussuhteista annetaan CENELEC-ohjeen 50 126-2 {Ref. 9} kohdassa 9.4. ja kaaviossa 9.1.

(10) *Yleisen tuotteen ja yleisen sovelluksen turvallisuusarvioon liittyvien ”turvallisuusarviointien” ja ”turvallisuusanalyysien” rajat ja voimassaolo määräytyvät tällaisten oletusten ja käyttörajoitusten perusteella. Jos tarkasteltava erityinen sovellus ei täytä näitä vaatimuksia, vastaavat ”turvallisuusarvioinnit” ja ”turvallisuusanalyysit” (esim. kausaalianalyysit) on päivitettävä tai korvattava uusilla.*

> *Tämä käytäntö on yhdenmukainen seuraavan yleisen turvallisuusperiaatteen kanssa: ”Jos erityisen (osa-)järjestelmän suunnitelma perustuu yleisiin sovelluksiin tai yleisiin tuotteisiin, on osoitettava, että erityinen (osa-)järjestelmä on kaikkien niiden oletusten ja käyttörajoitusten mukainen (joita kutsutaan CENELECissä turvallisuuteen liittyviksi sovellusehdoiksi), jotka viedään yleisen sovelluksen tai yleisen tuotteen vastaaviin turvallisuusarvioihin (ks. kaavio 3)”.*

Jos erityinen sovellus ei ole yhdenmukainen joidenkin oletusten tai käyttörajoitusten kanssa osajärjestelmän tasolla (esim. toiminnallisten turvallisuusvaatimusten osalta), vastaavat oletukset ja käyttörajoitukset voidaan siirtää korkeammalle tasolle (ts. yleensä järjestelmätasolle). Nämä oletukset ja käyttörajoitukset yksilöidään selkeästi kyseisen osajärjestelmän ”erityisen sovelluksen turvallisuusarviossa”. Tämä on ehdottoman tärkeää, jotta tällaisissa riippuvuustapauksissa voidaan varmistaa, että kunkin turvallisuusarvion turvallisuuteen liittyvät sovellusehdot täyttyvät korkeamman tason turvallisuusarviossa tai että ne siirretään osaksi kaikkein korkeimman tason turvallisuusarvion (ts. järjestelmän turvallisuusarvion) turvallisuuteen liittyviä sovellusehtoja.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

turvallisuussuunnitelmiin tai turvallisuusorganisaatioihin. Vastuiden jakamisesta eri toimijoiden kesken neuvotellaan ja siitä sovitaan tavallisesti alustavan järjestelmämäärittelyn yhteydessä (ts. hankkeen alussa), jos sellainen laaditaan.

[G 4] Turvallisuussuunnitelma on muuttuva asiakirja, jota päivitetään tarvittaessa hankkeen aikana.

[G 5] Lisätietoja esitetään standardissa EN 50 126-1 {Ref. 8} ja siihen liittyvässä ohjeessa 50 126-2 {Ref. 9}, joissa tarkastellaan turvallisuussuunnitelman sisältöä.

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] Lisäselvennystä ei pidetä tarpeellisena.

1.2. Rajapintojen hallinta

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] Jos rautatieyritys tarvitsee toiminnallisista syistä infrastruktuurin haltijaa toteuttamaan määritetyt muutokset infrastruktuuriin, rautatieturvallisuusdirektiivin {Ref. 1} liitteen III 2 kohdan g alakohdan vaatimusten nojalla rautatieyritys valvoo myös yleisiä toimia sen varmistamiseksi, että kaikki tarvittavat muutokset tehdään oikein. Vaikka vastuu säilyykin rautatieyrityksellä, kyseisen infrastruktuurin haltijan velvollisuutena on silti antaa tietoa muille rautatieyrityksille, jos infrastruktuurin muutoksella on vaikutusta myös niihin. Infrastruktuurin haltijan on mahdollisesti toteutettava riskinarviointi YTM:n mukaisesti, jos asiaa koskeva muutos on sen kannalta merkittävä.

[G 2] Vastuiden siirto eri toimijoiden kesken on mahdollista ja joissakin olosuhteissa jopa välttämätöntä. Jos järjestelmässä on osallisena useita toimijoita, on kuitenkin hyvin yleistä, että yksi toimija nimitetään vastaamaan koko järjestelmästä. Osajärjestelmien ja toimintojen välillä on aina riippuvuussuhteita, joiden yksilöiminen edellyttää erityisiä toimia. Siksi on välttämätöntä, että jokin toimijoista ottaa yleisen vastuun turvallisuusanalyyseista ja saa rajoittamattoman pääsyn asiaa koskeviin asiakirjoihin. Hakijalla, joka aikoo toteuttaa merkittävän muutoksen, on luonnollisestikin yleinen vastuu siitä, että riskinarviointi toteutetaan järjestelmällisesti ja kattavasti.

[G 3] Asianomaisten toimijoiden välisten rajapintojen hallinnan osalta on sovittava seuraavista keskeisistä perusteista:

(a) toimien johtaminen; yleensä toimien johtamisesta vastaa hakija, joka aikoo toteuttaa merkittävän muutoksen;
(b) vaaditut panokset;
(c) vaarojen tunnistamisessa ja riskien arvioinnissa sovellettavat menetelmät;
(d) osallistujat ja vaadittu pätevyys (eli tietojen, taitojen ja käytännön kokemusten yhdistelmä – katso myös ”henkilöstön pätevyyden” määritelmä 3 artiklaa {Ref. 4} koskevassa G 2 kohdan b alakohdassa);

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(e) odotetut tuotokset.

Nämä perusteet määritetään niiden yritysten turvallisuussuunnitelmissa (tai muissa asiaa koskevissa asiakirjoissa), joita kyseiset rajapinnat koskevat.

[G 4] Liitteessä LISÄYS C olevassa C.3. kohdassa esitetään esimerkkejä rajapinnoista ja havainnollistetaan, miten tällaisia keskeisiä perusteita sovelletaan junavalmistajan ja infrastruktuurin haltijan tai rautatieyrityksen välisen rajapinnan hallinnassa.

[G 5] Rajapintojen hallinnassa on tarkasteltava myös riskejä, jotka voivat syntyä rajapinnoissa ihmisoperaattoreiden kanssa (käytön ja kunnossapidon aikana), tällaisten rajapintojen suunnittelua varten.

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] Vaarojen ja niihin liittyvien turvallisuustoimenpiteiden siirtämisessä toimijoiden kesken sovellettavaa menettelyä voidaan soveltaa myös sivulla 35 olevassa kaaviossa 5 esitetyn CENELECin V-syklin alemmilla tasoilla. Menettelyä voidaan soveltaa aina, kun on tarpeen vaihtaa tällaista tietoa esimerkiksi toimijan ja sen alihankkijoiden kesken. Järjestelmätasolla tämä menettely eroaa siten, että hakijalle ei tarvitse antaa tietoa kaikista osajärjestelmän tasolla tehdyistä vaarojen ja niihin liittyvien turvallisuustoimenpiteiden siirroista. Hakijalle tiedotetaan asiasta vain, jos siirretyt vaarat ja niihin liittyvät turvallisuustoimenpiteet koskevat korkean tason rajapintoja (toisin sanoen jos niillä on vaikutusta rajapintaan hakijan kanssa).

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] Rautatieyrityksen ja infrastruktuurin haltijan turvallisuusjohtamisjärjestelmä (SMS) kattaa järjestelyt ja menettelyt, joilla varmistetaan, että vaatimustenvastaisia tai riittämättömiä turvallisuustoimenpiteitä hallinnoidaan oikein. Siksi tällaiset järjestelyt ja menettelyt eivät ole osa YTM:ää.

[G 2] Järjestelyistä ja menettelyistä[(11)], jotka muiden toimijoiden[(12)] on määrä ottaa käyttöön sen varmistamiseksi, että vaatimustenvastaisia tai riittämättömiä turvallisuustoimenpiteitä hallinnoidaan oikein ja että turvallisuustoimenpiteet siirretään tarvittaessa kaikille asianomaisille toimijoille, sovitaan asianomaisten toimijoiden kesken hankkeen alussa, ja ne esitetään yksityiskohtaisesti niiden turvallisuussuunnitelmassa: katso 0.2. kohta.

(11) *Periaatteessa kyseisten toimijoiden laadunhallinta- ja/tai turvallisuusjohtamismenettelyt, jotka on määritetty vähintäänkin hanketasolla, kattavat tällaiset järjestelyt ja menettelyt (ks. myös kaavio 2).*

(12) *Käsitteellä ”muut toimijat” tarkoitetaan kaikkia muita asianomaisia toimijoita kuin infrastruktuurin haltijoita ja rautatieyrityksiä.*

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

[G 1] Tällä mahdollistetaan mahdollisen vaatimustenvastaisen tai riittämättömän turvallisuustoimenpiteen hallinta arvioitavassa järjestelmässä tai muissa samankaltaisissa järjestelmissä, joissa sovelletaan samaa toimenpidettä.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

2. RISKINARVIOINTIMENETTELYN KUVAUS

2.1. Yleinen kuvaus – YTM:n riskinarviointimenettelyn ja CENELECin V-syklin vastaavuus

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

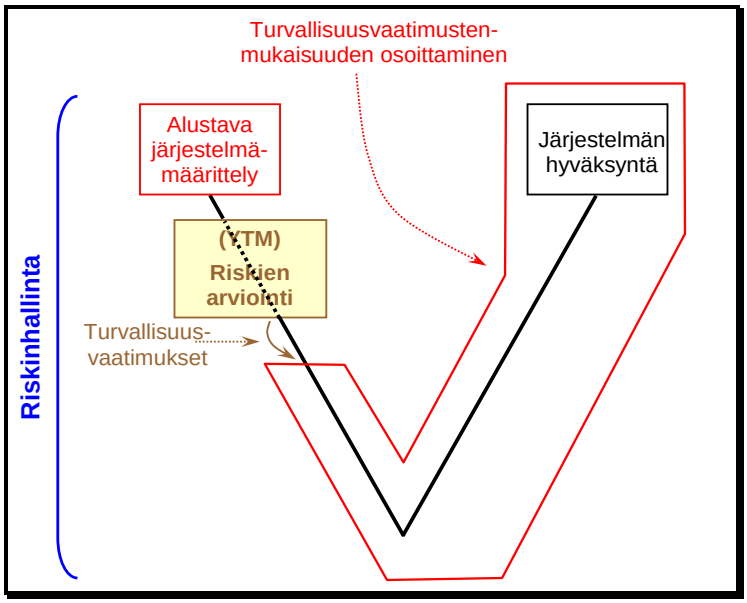
(a) the system definition;
(b) the risk analysis including the hazard identification;
(c) the risk evaluation.

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

[G 1] YTM:n kattama riskinhallintamenettely voidaan esittää V-syklinä, joka alkaa (alustavalla) järjestelmämäärittelyllä ja päättyy järjestelmän hyväksymiseen: katso kaavio 4. Tällainen yksinkertaistettu V-sykli voidaan esittää standardin EN 50 126–1 {Ref. 8} kaavion 10 mukaisen perinteisen V-syklin muodossa. Kaaviossa 1 esitetyn YTM:n riskinhallintamenettelyn ja CENELECin standardin kaaviossa 10 esitetyn V-syklin vastaavuuden osoittamiseksi CENELECin V-sykli toistetaan kaaviossa 5:

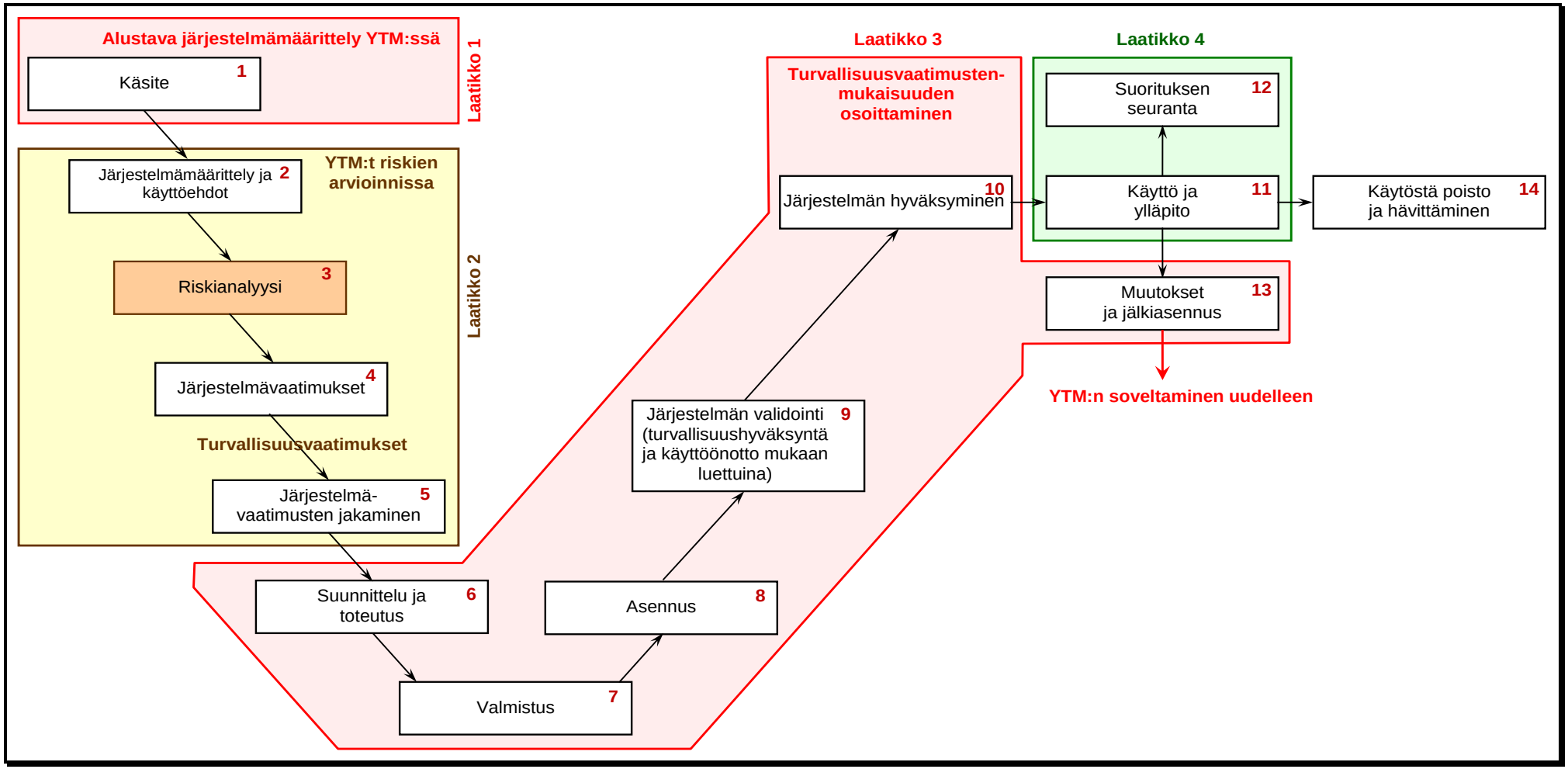
(a) Kaaviossa 1 esitetty YTM:n ”alustava järjestelmämäärittely” vastaa CENELECin V-syklin vaihetta 1, ts. järjestelmäkäsitteen määritelmää (katso kaaviossa 5 esitetty laatikko 1);
(b) Kaaviossa 1 esitetty YTM:n ”riskinarviointi” kattaa seuraavat CENELECin V-syklin vaiheet (katso kaavion 5 laatikko 2):

(1) Kaavion 5 vaihe 2: ”järjestelmämäärittely ja sovellusehdot”
(2) Kaavion 5 vaihe 3: ”riskianalyysi”
(3) Kaavion 5 vaihe 4: ”järjestelmävaatimukset”
(4) Kaavion 5 vaihe 5: ”järjestelmävaatimusten jakaminen” eri osajärjestelmien ja osien mukaan



Kaavio 4: Standardin EN 50 126 kaavion 10 mukainen yksinkertaistettu V-sykli

Euroopan Rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu



Kaavio 5: Standardin EN 50 126 kaaviossa 10 kuvattu V-sykli (CENELECin järjestelmän elinkaari)

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

[G 2] YTM:n riskinarviointimenettelyn tuotoksia ovat (toistojen jälkeen – katso kaavio 1):

(a) “järjestelmämäärittely” päivitettynä ”riskianalyysin” ja ”riskinarvioinnin” tuloksena määritetyillä “turvallisuusvaatimuksilla” (katso 2.1.6 kohta);
(b) ”järjestelmävaatimusten jakaminen” eri osajärjestelmien ja osien mukaan (kaavion 5 vaihe 5);
(c) ”vaaroja koskeva asiakirja”, johon merkitään:

(1) kaikki tunnistetut vaarat ja niihin liittyvät turvallisuustoimenpiteet
(2) johdetut turvallisuusvaatimukset
(3) järjestelmässä huomioon otettavat oletukset, joiden perusteella määritetään riskiarvioinnin rajat ja voimassaolo (katso 2.1.2 kohtaa koskeva g kohta)

(d) yleisesti kaikki YMT:n soveltamisen tuloksena saadut todisteet: katso 5 kohta.

Nämä YTM:n riskinarvioinnin tuotokset vastaavat CENELECin V-syklin vaiheen 4 turvallisuuteen liittyviä tuotoksia, ts. kaaviossa 5 eriteltyjä järjestelmävaatimuksia.

[G 3] Järjestelmämäärittelyä, jota on päivitetty riskinarvioinnin tuloksilla, ja vaaroja koskevaa asiakirjaa käytetään panoksina järjestelmän suunnittelussa ja hyväksynnässä. YTM:ssä ”järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen” vastaa CENELECin V-syklin seuraavia vaiheita (katso kaavion 5 laatikko 3):

(a) kaavion 5 vaihe 6: ”suunnittelu ja toteutus”,
(b) kaavion 5 vaihe 7: ”valmistus”,
(c) kaavion 5 vaihe 8: ”asennus”,
(d) kaavion 5 vaihe 9: ”järjestelmän validointi (turvallisuushyväksyntä ja käyttöönotto mukaan luettuina)”,
(e) kaavion 5 vaihe 10: ”järjestelmän hyväksyntä”.

[G 4] Järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisessa on otettava huomioon, onko merkittävä muutos luonteeltaan tekninen, toiminnallinen vai organisatorinen. Kaaviossa 5 esitetyn CENELECin V-syklin eri vaiheet eivät siten välttämättä sovellu yhteen kaikkien merkittävien muutosten kanssa. Tämä on otettava huomioon kaaviossa 5 esitetyn V-syklin osalta, ja sitä sovellettaessa on arvioitava, mikä sopii yhteen tietyn sovelluksen kanssa (esimerkiksi toiminnallisissa ja organisatorisissa muutoksissa valmistusvaihetta ei oteta huomioon).

[G 5] YTM:ssä ”järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen” ei kata siten yksistään testien tai simuloinnin avulla tapahtuvaa ”varmennusta ja validoimista”. Siihen sisältyy käytännössä CENELECin V-syklin vaiheet 6–10 (katos edellä esitetty luettelo ja kaavio 5). Nämä vaiheet kattavat suunnittelun, valmistuksen, asentamisen, varmennus- ja validointitoimet, asiaan liittyvät RAMS-toimet ja järjestelmän hyväksynnän.

[G 6] ”Järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisessa” yleisperiaatteena on, että riskinarvioinnissa keskitytään ainoastaan järjestelmän turvallisuuteen liittyviin toimintoihin ja rajapintoihin. Jos kaaviossa 5 esitetyn CENELECin V-syklin jokin vaihe edellyttää riskin- ja turvallisuudenarviointitoimia, niissä on keskityttävä:

(a) turvallisuuteen liittyviin toimintoihin ja rajapintoihin;
(b) osajärjestelmiin ja/tai osiin, jotka ovat merkityksellisiä korkean tason riskinarvioinnissa arvioitavien turvallisuuteen liittyvien toimintojen ja/tai rajapintojen kannalta.

[G 7] Kaaviossa 5 esitetyn perinteisen CENELECin V-syklin vertailun tuloksena voidaan siten todeta, että:

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) YTM kattaa tämän V-syklin vaiheet 1–10 ja vaiheen 13. Nämä vaiheet sisältävät arvioitavan järjestelmän hyväksymisen edellyttämät toimet;

(b) YTM ei kata järjestelmän elinkaaren vaiheita 11, 12 ja 14:

(1) vaihe 11 liittyy järjestelmän ”käyttöön ja kunnossapitoon” ja vaihe 12 järjestelmän ”suorituksen seurantaan” YTM:ään pohjautuvan järjestelmän hyväksymisen jälkeen. Nämä kaksi vaihetta sisältyvät rautatieyrityksen ja infrastruktuurin haltijan turvallisuusjohtamisjärjestelmään – (katso kaavion 5 laatikko 4). Jos järjestelmän käytön, kunnossapidon tai suorituksen seurannan aikana ilmenee, että järjestelmää on muutettava tai siihen on tehtävä jälkiasennuksia (kaavion 5 vaihe 13), kun järjestelmä on jo käytössä, YTM:ää sovelletaan uudelleen uusiin välttämättömiin muutoksiin 2 artiklan mukaisesti. Jos muutos on merkittävä:

(i) YTM:n riskinhallinta- ja riskinarviointimenettelyjä sovelletaan näihin uusiin muutoksiin;
(ii) nämä uudet muutokset edellyttävät 6 artiklan mukaista hyväksyntää;

(2) jo käytössä olevan järjestelmän ”käytöstäpoistoa ja hävittämistä” (vaihe 14) voidaan myös pitää merkittävänä muutoksena, ja siksi kaavion 5 vaiheeseen 14 voidaan soveltaa uudelleen YTM:ää 2 artiklan mukaisesti.

Lisätietoa kaaviossa 5 esitetyn CENELECin V-syklin kunkin vaiheen tai toimen soveltamisalasta esitetään standardin EN 50 126-1 {Ref. 8} kohdassa 6.

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] Lisäselvennystä ei pidetä tarpeellisena.

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

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).

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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] Yleensä hakija päättää hankkeen erityisvaatimusten ja kyseisten kolmen periaatteen soveltamisesta saamansa kokemuksen perusteella, mikä hyväksyttävää riskitasoa koskeva periaate on asianmukaisin tunnistettujen vaarojen hallitsemiseksi.

[G 2] Järjestelmän hyväksyttävää riskitasoa ei voida aina arvioida soveltamalla vain yhtä näistä kolmesta hyväksyttävää riskitasoa koskevasta periaatteesta. Riskitason hyväksyminen perustuu usein näiden periaatteiden yhdistelmään. Jos merkittävään muutokseen on sovellettava asiaan liittyvien riskien hallitsemiseksi useampaa kuin yhtä hyväksyttävää riskitasoa koskevaa periaatetta, asiaan liittyvät vaarat on jaettava osavaaroihin, jotta jokaista yksittäistä osavaaraa voidaan valvoa riittävästi ainoastaan yhden hyväksyttävää riskitasoa koskevan periaatteen avulla.

[G 3] Päätettäessä, mitä hyväksyttävää riskitasoa koskevaa periaatetta sovelletaan vaaran hallitsemiseksi, on otettava huomioon vaarojen tunnistamisvaiheessa jo tunnistetut vaarat ja niiden syyt. Jos samaan vaaraan liittyy kaksi erillistä ja toisistaan riippumatonta syytä, vaara on jaettava kahteen erilliseen osavaaraan. Kutakin osavaaraa valvotaan siten yhdellä ainoalla hyväksyttävää riskitasoa koskevalla periaatteella. Nämä kaksi osavaaraa on kirjattava vaaroja koskevaan asiakirjaan, ja niitä on hallittava sen avulla. Jos vaara aiheutuu esimerkiksi suunnitteluvirheestä, sitä voidaan hallita soveltamalla menettelyohjetta, kun taas kunnossapitovirheestä johtuvan vaaran hallitsemiseksi menettelyohje ei yksinään ole välttämättä riittävä, vaan tällöin on sovellettava toista hyväksyttävää riskitasoa koskevaa periaatetta.

[G 4] Riskin vähentäminen hyväksyttävälle tasolle voi edellyttää riskianalyysi- ja riskinarviointivaiheiden toistamista useita kertoja, kunnes asianmukaiset turvallisuustoimenpiteet saadaan yksilöityä.

[G 5] Käytössä olevien järjestelmien ja menettelyohjeiden soveltamiseen perustuvien järjestelmien nykyisten jäännösriskien katsotaan olevan hyväksyttäviä käytännöstä saatujen kokemusten perusteella. Eksplisiittisen riskin estimoinnin tuloksena saatu jäännösriski perustuu asiantuntija-arvioon ja asiantuntijoiden analyyseissa tekemiin oletuksiin tai onnettomuuksia tai käyttökokemuksia koskeviin tietokantoihin. Eksplisiittisen riskin estimoinnin jäännösriskiä ei voida siten vahvistaa välittömästi käytännössä. Jäännösriskin osoittaminen edellyttää järjestelmän pitkäaikaista käyttöä, seurantaa ja vastaavista järjestelmistä saatuja kokemuksia. Yleensä menettelyohjeiden soveltamisella ja muihin vastaaviin ohjeistoihin vertaamisella on se etu, että näin vältetään sellaisten tarpeettoman tiukkojen turvallisuusvaatimusten määrittely, jotka voivat perustua eksplisiittisessä riskin estimoinnissa käytettyihin kohtuuttoman varovaisiin (turvallisuus)oletuksiin. Arvioitavan järjestelmän ei kuitenkaan välttämättä tarvitse täyttää kaikkia menettelyohjeiden tai vastaavien ohjeistojen turvallisuusvaatimuksia. Tällöin eksplisiittisen riskin estimoinnin soveltamisella on se etu, että sillä vältetään arvioitavan järjestelmän liian tarkka suunnittelu ja mahdollistetaan kustannustehokkaampi suunnittelu, jota ei ole kokeiltu aiemmin.

[G 6] Jos arvioitavan järjestelmän tunnistettuja vaaroja ja niihin liittyviä riskejä ei voida hallita menettelyohjeita tai vastaavia ohjeistoja soveltamalla, on toteutettava eksplisiittinen riskin estimointi vaarallisten tilanteiden määrällisten tai laadullisten analyysien pohjalta. Tällainen tilanne syntyy, kun arvioitava järjestelmä on täysin uusi (tai suunnitelma on innovatiivinen) tai kun järjestelmä poikkeaa menettelyohjeesta tai ohjeistosta. Eksplisiittisessä riskin

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

estimoinnissa arvioidaan tällöin, onko riski hyväksyttävällä tasolla (jolloin lisäanalyyseja ei tarvita) tai tarvitaanko täydentäviä turvallisuustoimenpiteitä riskin pienentämiseksi edelleen.

[G 7] Ohjeen EN 50 126-2 {Ref. 9} kohdassa 8 esitetään riskien pienentämiseen ja riskitason hyväksymiseen liittyviä ohjeita.

[G 8] Arviointielimen on arvioitava käyttöönotettua hyväksyttävää riskitasoa koskevaa periaatetta ja sen soveltamista.

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] Jos esimerkiksi jonkin komponenttiohjelmiston turvallisuusvaatimukseksi on määritetty standardin EN 50 128 turvallisuustason SIL 4 soveltaminen, vaatimustenmukaisuuden osoittamisessa on todistettava, että standardissa suositeltua menettelyä noudatetaan. Tähän sisältyy esimerkiksi seuraavien vaatimusten täyttymisen osoittaminen:

(a) ohjelmiston suunnittelun, varmennuksen ja validoinnin riippumattomuutta koskevat vaatimukset täyttyvät;
(b) standardin EN 50 128 turvallisuustasoa SIL 4 koskevia oikeita menetelmiä sovelletaan;
(c) muut näkökohdat.

[G 2] Jos esimerkiksi hätäjarrujen sähköventtiilien valmistamisessa on sovellettava tiettyä menettelyohjetta, on osoitettava, että valmistusprosessissa täytetään kaikki menettelyohjeessa esitetyt vaatimukset.

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] Turvallisuustoimenpiteitä on kahdenlaisia:

(a) ”ehkäisevillä turvallisuustoimenpiteillä” torjutaan vaarojen tai niiden syiden esiintymistä, ja;
(b) ”lieventävillä turvallisuustoimenpiteillä” estetään vaaroja kehittymästä onnettomuuksiksi tai lievennetään tapahtuneiden onnettomuuksien seurauksia (suojatoimenpiteet).

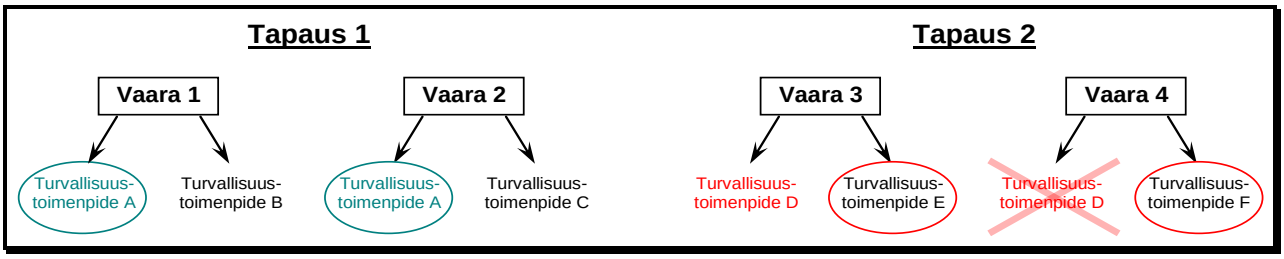
Toiminnan kannalta syiden torjuminen on yleensä tehokkaampi keino.

[G 2] Hakijan on asetettava etusijalle ne turvallisuustoimenpiteet, joilla saavutetaan paras kompromissi riskien vähentämisen edellyttämien kustannusten ja jäännösriskien välillä. Valitut turvallisuustoimenpiteet määritetään arvioitavan järjestelmän turvallisuusvaatimuksiksi.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] On tärkeää tarkastaa, että jonkin vaaran hallitsemiseksi valitut turvallisuustoimenpiteet eivät ole ristiriidassa muiden vaarojen kanssa. Kuten kaaviossa 6 esitetään, esimerkiksi seuraavat kaksi tapausta ovat mahdollisia[13]:

(a) Tapaus 1: Jos samalla turvallisuustoimenpiteellä (kaavion 6 toimenpide A) voidaan hallita eri vaaroja aiheuttamatta niiden välille ristiriitaa ja jos se on taloudellisesti perusteltua, kyseinen turvallisuustoimenpide voidaan valita yksin ”turvallisvaatimukseksi”. Täytettävien turvallisuusvaatimusten määrä on tällöin pienempi kuin toteutettaessa molemmat toimenpiteet B ja C.



Kaavio 6: Asianmukaisten turvallisuustoimenpiteiden valinta riskien hallitsemiseksi

(b) Tapaus 2: Vastaavasti jos yhdellä turvallisuustoimenpiteellä voidaan hallita yhtä vaaraa mutta samalla luodaan ristiriita toisen vaaran kanssa (kaavion 6 toimenpide D), sitä ei voida valita ”turvallisuusvaatimukseksi”. Tarkasteltavan vaaran hallitsemiseksi on käytettävä muita turvallisuustoimenpiteitä (kaavion 6 toimenpiteet E ja F):

(1) Yksi tyypillinen ohjaus- ja valvontajärjestelmään liittyvä esimerkki on käyttää junan sijaintia radalla apuna joko jarrun käytön valvomiseksi tai junan kiihdyttämisen sallimiseksi. Junan etupäädyn (tai junan takapäädyn) käyttö junan sijainnin osoittamiseen ei ole turvallista kaikissa tilanteissa:

(i) kun eurooppalaisessa liikenteenvalvontajärjestelmässä (ETCS) on käytettävä turvallisuuden vuoksi hätäjarruja, järjestelmä käyttää niin sanottua MAXIMUM SAFE FRONT END -toimintoa varmistaakseen, että juna todella pysähtyy ennen vaarapisteen saavuttamista;

(ii) vastaavasti, kun junalle on annettu lupa kiihdyttää esimerkiksi nopeusrajoituksen jälkeen, ETCS-järjestelmä käyttää niin sanottua MINIMUM SAFE REAR END -toimintoa.

(2) Toinen esimerkki liittyy turvallisuustoimenpiteeseen, jota voidaan käyttää junan pysäyttämiseksi lähes kaikissa olosuhteissa, siten että saavutetaan vikaturvallinen tila, tunneleita tai siltoja lukuun ottamatta. Viimeksi mainitussa tapauksessa ei pidä soveltaa kaaviossa 6 esitettyä tapauksen 2 toimenpidettä D.

(13) *Huomautettakoon, että asiakirjassa ei luetella kaikkia tilanteita, joissa turvallisuustoimenpiteet voivat olla ristiriidassa muiden tunnistettujen vaarojen kanssa. Asiakirjassa esitetään vain muutama havainnollistava esimerkki.*

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

[G 1] Esimerkiksi järjestelmän, sen osajärjestelmien ja laitteiden suunnittelun teknisten vaihtoehtojen mukaan uusia vaaroja voidaan tunnistaa ”turvallisuusvaatimusten mukaisuuden osoittamisen” yhteydessä (esimerkiksi tietyn maalin käyttö voi aiheuttaa myrkyllisiä kaasuja palon syttyessä). Tällaisia uusia vaaroja ja niihin liittyviä riskejä on pidettävä uusina panoksina toistuvan riskinarviointimenettelyn uudessa silmukassa. Standardin EN 50 129 liitteessä A.4.3 esitetään muita esimerkkejä tapauksista, joissa uusia vaaroja voidaan tunnistaa ja hallita.

2.2. Vaarojen tunnistaminen

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] Vaarat ilmaistaan mahdollisuuksien mukaan samalla tarkkuudella. Tarkkuudeltaan erilaiset vaarat voidaan tunnistaa alustavissa vaara-analyyseissa (muun muassa siksi että HAZOP-analyyseissa kootaan yhteen kokemustaustaltaan erilaisia ihmisiä).
Tarkkuusaste määräytymiseen vaikuttaa myös vaarojen hallitsemiseksi valittu hyväksyttävää riskitasoa koskevan periaate. Jos esimerkiksi vaaraa hallitaan täysin menettelyohjeen tai vastaavan ohjeiston avulla, tarkempi vaaran tunnistaminen ei ole tarpeen.

[G 2] Kaikki riskinarviointimenettelyssä tunnistetut vaarat (yleisesti hyväksyttäviin riskeihin liittyvät vaarat mukaan luettuina), asiaan liittyvät turvallisuustoimenpiteet ja riskit on merkittävä vaaroja koskevaan asiakirjaan.

[G 3] Analysoitavan järjestelmän luonteen mukaan vaarojen tunnistamiseen voidaan käyttää erilaisia menetelmiä:

(a) empiirisessä vaarojen tunnistamisessa voidaan hyödyntää jo saatuja kokemuksia (esimerkiksi tarkastusluetteloiden tai yleisiä vaaroja koskevien luetteloiden käyttö);
(b) luovaa vaarojen tunnistamista voidaan käyttää uusilla tarkasteltavilla aloilla (proaktiivinen ennustaminen, esimerkiksi jäsennellyt ”mitä jos” -tutkimukset, kuten FMEA tai HAZOP).

[G 4] Empiirisiä ja luovia vaarojen tunnistamismenetelmiä voidaan käyttää yhdessä toistensa täydentämiseksi, millä varmistetaan, että potentiaalisten vaarojen luettelo ja turvallisuustoimenpiteet ovat kattavia.

[G 5] Vaarojen tunnistaminen voidaan käynnistää alustavasti ideointiryhmässä, jossa on mukana eri alan asiantuntijoita, joilla on tietämystä merkittävän muutoksen kaikista asiaa koskevista näkökohdista. Empiirisiä menetelmiä voidaan käyttää tietyn toiminnon tai toimintatilan analysoimiseen, jos asiantuntijaryhmä pitää sitä tarpeellisena.

[G 6] Vaarojen tunnistamisessa käytettävät menetelmät ovat riippuvaisia järjestelmämäärittelystä. Liitteessä LISÄYS B esitetään muutamia esimerkkejä.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

[G 7] Lisätietoa vaarojen tunnistamistekniikoista ja -menetelmistä esitetään standardin EN 50 126-2 {Ref. 9} liitteissä A.2 ja E.

[G 8] Liitteessä LISÄYS C olevassa C.17. kohdassa esitetään esimerkki yleisten vaarojen luettelosta.

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] Riskinarviointimenettelyn helpottamiseksi merkittävät vaarat voidaan luokitella edelleen eri alaluokkiin. Merkittävät vaarat voidaan luokitella tai ryhmitellä esimerkiksi niiden odotetun riskin vakavuuden ja esiintymistiheyden mukaan. CENELEC-standardeissa annetaan tätä koskevia ohjeita: katso liitteessä LISÄYS A oleva A.2. kohta.

[G 2] 2.1.4 kohdassa kuvattua riskianalyysia ja riskinarviointia sovelletaan tärkeysjärjestyksen mukaisesti alkaen merkittävimmistä vaaroista.

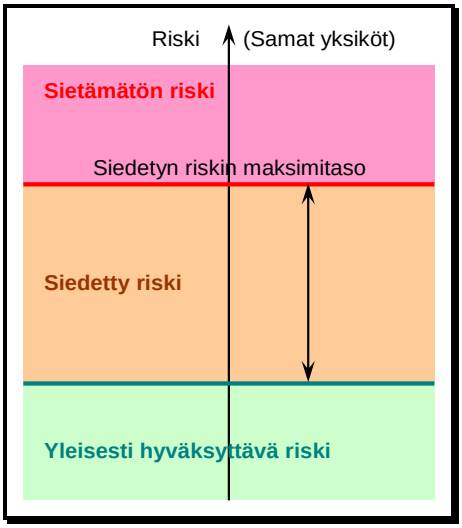
2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed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

[G 1] Johonkin vaaraan liittyvää riskiä voidaan pitää yleisesti hyväksyttävänä,

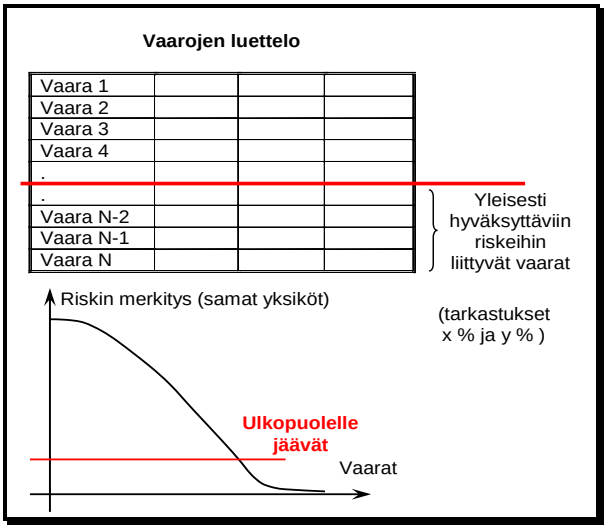
(a) jos riskin todennäköisyysprosentti on pienempi kuin tämäntyyppisen vaaran suurin siedetty riskiprosentti (esimerkiksi x prosenttia). X prosentin arvo voi perustua parhaaseen käytäntöön ja useista riskianalyysimenetelmistä saatuun kokemukseen, kuten yleisesti hyväksyttävän riskin ja sietämättömien riskiluokitusten väliseen suhteeseen FN-käyrissä tai riskimatriisessa. Kaaviossa 7 esitetään tätä koskeva esimerkki;

(b) tai jos riskiin liittyvä vahinko on niin pieni, ettei sen torjumiseksi ole järkevää toteuttaa turvallisuustoimenpiteitä.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Kaavio 7: Yleisesti hyväksyttävät riskit



Kaavio 8: Yleisesti hyväksyttäviin riskeihin liittyvien vaarojen suodattaminen

[G 2] Lisäksi jos tunnistetaan tarkkuudeltaan erilaisia vaaroja (toisin sanoen yhtäältä korkean tason vaaroja ja toisaalta tarkasti määriteltyjä osavaaroja), on ryhdyttävä varotoimiin, jotta niitä ei luokitella väärin yleisesti hyväksyttäviin riskeihin liittyviksi vaaroiksi. Yleisesti hyväksyttäviin riskeihin liittyvien vaarojen osuus ei saa ylittää tiettyä prosenttiosuutta (esimerkiksi y prosenttia) järjestelmän kokonaisriskistä. Osuuden tarkastaminen on välttämätöntä, jottei osuutta pienennetä jakamalla vaaroja useisiin alhaisen tason osavaaroihin. Jos vaara ilmaistaan useina erilaisina ”pienempinä” osavaaroina, niistä jokainen voidaan luokitella helposti yleisesti hyväksyttäviin riskeihin liittyviksi vaaroiksi arvioitaessa niitä itsenäisesti, kun taas yhdessä arvioituna ne luokitellaan vaaraksi, jolla on merkittävä riski (toisin sanoen yhdeksi korkean tason vaaraksi). Osuuden arvo (esimerkiksi y prosenttia) määräytyy järjestelmätasolla sovellettavien hyväksyttävää riskitasoa koskevien perusteiden mukaan. Osuuden arvon perustaksi ja arvioinnin pohjaksi voidaan ottaa samankaltaisista ohjeistoista saatu toiminnallinen kokemus.

[G 3] Edellä käsitellyt kaksi tarkastusta (x ja y prosentteina ilmaistu osuus) mahdollistavat sen, että riskinarvioinnissa voidaan keskittyä kaikkein tärkeimpiin vaaroihin ja että kaikkia merkittäviä riskejä valvotaan (katso kaavio 8).
Hakija on vastuussa arvojen x prosenttia ja y prosenttia määrittämisestä asiantuntija-arvion pohjalta ja siitä, että arviointielin suorittaa niiden riippumattoman arvioinnin, sanotun kuitenkaan rajoittamatta jäsenvaltion lainsäädännöllisiä vaatimuksia. Suuruusluokka voi olla esimerkiksi x = 1 prosenttia ja y = 10 prosenttia, jos arvoa voidaan pitää hyväksyttävänä asiantuntija-arvion pohjalta.

[G 4] 2.2.2 kohdan mukaan luokitus ”yleisesti hyväksyttyihin riskeihin” edellyttää arviointielimen toteuttamaa riippumatonta arviointia.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

2.2.4. During the hazard identification, safety measures may be identified. They shall be registered in the hazard record according to section 4.

[G 1] Tällä toimella on tarkoitus tunnistaa muutokseen liittyvät vaarat. Jos turvallisuustoimenpiteet on jo tunnistettu, ne on merkittävä vaaroja koskevaan asiakirjaan. Turvallisuustoimenpiteiden luonne on riippuvainen muutoksesta. Ne voivat liittyä menettelyihin, tekniikkaan, toimintaan tai organisaatioon.

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] Vaikka riski saataisiinkin hyväksyttävälle tasolle, hakija voi silti päättää, että vaarojen tarkempi tunnistaminen on välttämätöntä. Hakija voi esimerkiksi löytää kustannustehokkaampia turvallisuustoimenpiteitä riskien hallitsemiseksi toteuttamalla yksityiskohtaisemman vaarojen tunnistamisen.

2.2.6. Whenever a code of practices or a reference system is used to control the risk, the hazard identification can be limited to:

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

2.3. Menettelyohjeiden käyttö ja riskinarviointi

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.3.	*Where compliance with TSIs is required by Directive 2008/57/EC and the relevant TSI does not impose the risk management process established by this Regulation, the TSIs may be considered as codes of practice for controlling hazards, provided requirement (c) of point 2.3.2 is fulfilled.*

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

2.4. Ohjeiston käyttö ja riskinarviointi

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] Lisätietoa näistä periaatteista annetaan ohjeen EN 50 126-2 {Ref. 9} kohdassa 8.

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] Esimerkiksi vanha ohjaus- ja hallintajärjestelmä, jonka turvallisuustason on osoitettu käytössä olevan hyväksyttävä, voidaan korvata toisella järjestelmällä, jossa hyödynnetään uudempaa tekniikkaa ja jonka turvallisuustaso on parempi. Siksi on asianmukaista varmistaa aina ohjeistoa sovellettaessa, onko se edelleen voimassa.

[G 2] Koska esimerkiksi tunnelien turvallisuuteen tai vaarallisten aineiden kuljetusten turvallisuuteen liittyvät tietyt näkökohdat voivat vaatia erityistarkastelua ja olla riippuvaisia käyttö- ja ympäristöolosuhteista, on välttämätöntä tarkastaa jokaisen hankkeen yhteydessä, että järjestelmää käytetään samoissa olosuhteissa.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisätietoa vastaavuusanalyyseista annetaan ohjeen EN 50 126-2 {Ref. 9} kohdassa 8.1.3.

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] Lisäselvennystä ei pidetä tarpeellisena.

2.5. Eksplisiittinen riskin estimointi ja evaluointi

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Arvoitaessa, ovatko arvioitavan järjestelmän riskit hyväksyttäviä, on sovellettava hyväksyttävää riskitasoa koskevia perusteita (katso kaaviossa 1 esitetyt

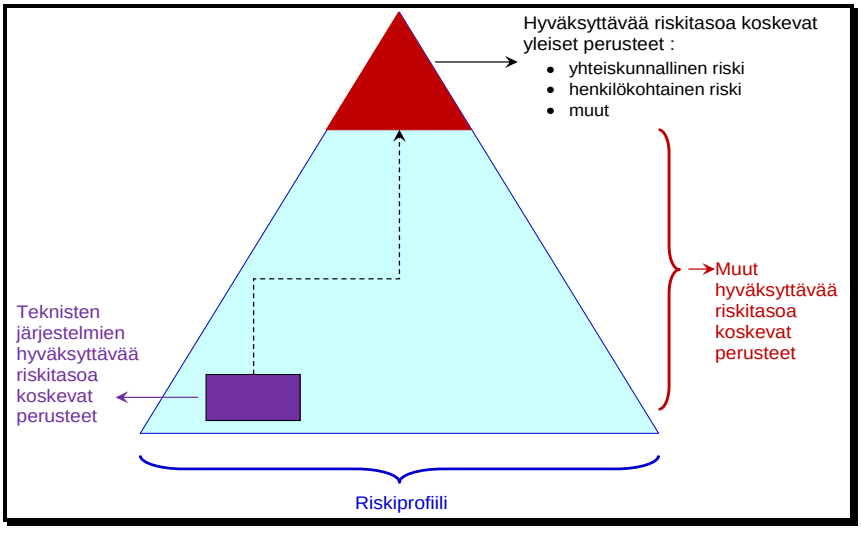
Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

"riskinarviointilaatikot"). Hyväksyttävää riskitasoa koskevat perusteet voivat olla joko implisiittisiä tai eksplisiittisiä:

(a) hyväksyttävää riskitasoa koskevat implisiittiset perusteet: 2.3.5 ja 2.4.3 kohdan mukaan menettelyohjeita tai vastaavia ohjeistoja soveltamalla hallittavia riskejä pidetään implisiittisesti hyväksyttävinä, edellyttäen että (katso kaavion 1 pisteympyrä):

(1) 2.3.2 kohdassa esitetyt menettelyohjeen soveltamisen ehdot täyttyvät;
(2) 2.4.2 kohdassa esitetyt ohjeiston käyttöä koskevat ehdot täyttyvät;

(b) hyväksyttävää riskitasoa koskevia eksplisiittisiä perusteita sovelletaan, kun halutaan arvioida eksplisiittisen riskin estimoinnin avulla hallittavien riskien hyväksyttävyyttä (katso kaaviossa 1 esitetty kolmatta periaatetta koskeva jatkuva ympyrä). Ne voidaan määrittää rautatiejärjestelmän eri tasojen mukaan ja niitä voidaan kuvata "perusteiden pyramidina" (katso kaavio 9), joka alkaa korkean tason hyväksyttävää riskitasoa koskevista perusteista (ilmaistuna esimerkiksi yhteiskunnallisena tai yksilöllisenä riskinä) ja ulottuu osajärjestelmiin ja osiin asti (tekniset järjestelmät), käyttövaiheen ihmisoperaattorit ja järjestelmän ja osajärjestelmien kunnossapitotoimet mukaan luettuina. Vaikka hyväksyttävää riskitasoa koskevien perusteiden tarkoituksena on taata järjestelmän turvallinen toiminta ja vaikka ne liittyvät siten yhteisiin turvallisuustavoitteisiin ja kansallisiin viitearvoihin, niiden välille on hyvin vaikeaa muodostaa matemaattista mallia: katso yksityiskohtaiset tiedot {Ref. 12}.
Hyväksyttävää riskitasoa koskevien eksplisiittisten perusteiden tarkkuuden on vastattava merkittävän muutoksen tärkeyttä ja monimutkaisuutta. Esimerkiksi liikkuvan kaluston jonkin akselityypin muuttamisen yhteydessä ei ole välttämätöntä arvioida koko rautatiejärjestelmää. Hyväksyttävää riskitasoa koskevien perusteiden määrittämisessä voidaan keskittyä liikkuvaan kalustoon. Vastaavasti käytössä olevaan rautatiejärjestelmään tehtäviä suuria muutoksia tai lisäyksiä ei pidä arvioida yksinomaan yksittäisten lisättävien toimintojen tai muutosten turvallisuussuorituksen perusteella. Tällöin on varmistettava rautatiejärjestelmän tasolla, että muutos on kaikilta osin hyväksyttävä.



Kaavio 9: Hyväksyttävää riskitasoa koskevien perusteiden pyramidi

[G 2] Hyväksyttävää riskitasoa koskevia eksplisiittisiä perusteita, joilla tuetaan vastavuoroista tunnustamista jäsenvaltioiden välillä, yhdenmukaistaistetaan viraston käynnissä olevien

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

hyväksyttävää riskitasoa koskeviin perusteisiin liittyvien toimien pohjalta. Kun lisätietoja on saatavana, ne sisällytetään tähän asiakirjaan.

[G 3] Siihen asti riskit voidaan arvioida käyttämällä esimerkiksi standardin EN 50 126-1 {Ref. 8} kohdassa 4.6 esitettyä riskimatriisia. Myös muuntyyppisiä soveltuvia perusteita voidaan käyttää, mikäli näiden perusteiden katsotaan johtavan hyväksyttävään turvallisuustasoon kyseisessä tapauksessa.

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] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisätietoa teknisten järjestelmien hyväksyttävää riskitasoa koskevista perusteista ja siitä, mihin teknisen järjestelmän näkökohtiin ja toimintoihin perustetta sovelletaan, esitetään tähän asiakirjaan liittyvässä viraston laatimassa erillisessä muistiossa: katso liitteessä LISÄYS A oleva A.3. kohta ja viiteasiakirja {Ref. 11}.

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

[G 1] Lisäselvennystä ei pidetä tarpeellisena.

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. TURVALLISUUSVAATIMUSTEN MUKAISUUDEN OSOITTAMINEN

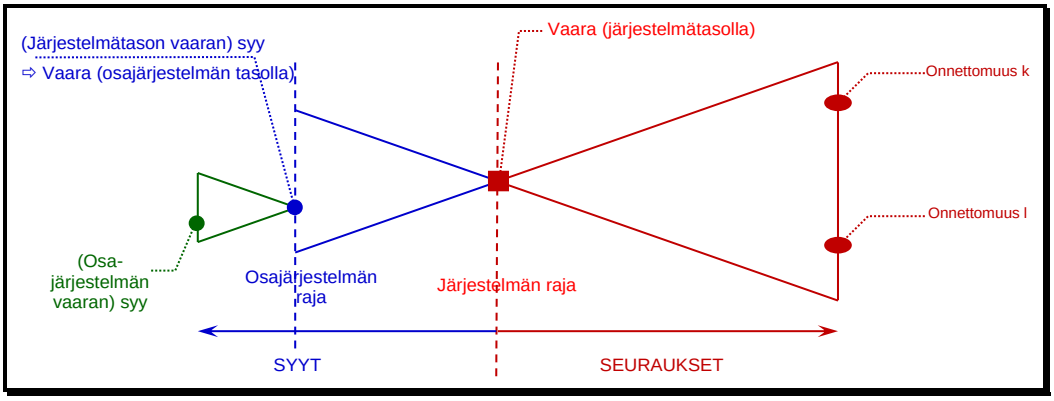
3.1. Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

[G 1] Kuten edellä 2.1.1 kohtaa koskevassa G 3–G 6 kohdassa selvennetään, ”järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen” kattaa CENELECin V-syklin vaiheet 6–10 (katso kaavion 5 laatikko 3). Ks. 2.1.1 kohtaa koskeva G 3 kohta.

[G 2] Ks. myös tämän asiakirjan 2.1.1 kohtaa koskeva G 4 kohta.

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] Yksi esimerkki turvallisuusarvioinneista ja -analyyseista, joita voidaan suorittaa osajärjestelmän tasolla, on kausaalianalyysit: katso kaavio 10. Sen osoittamiseksi, että osajärjestelmä on panoksia koskevien turvallisuusvaatimusten mukainen, voidaan kuitenkin käyttää mitä tahansa menetelmää.

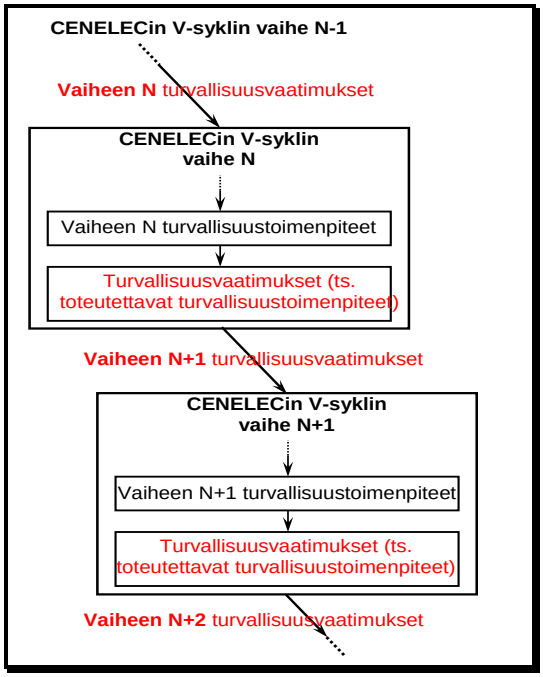


Kaavio 10: Standardin EN 50 129 kaavio A.4: Vaarojen määrittely järjestelmän rajojen näkökulmasta

[G 2] Järjestelmien ja osajärjestelmien vaarojen ja niiden syiden hierarkkinen jäsentely voidaan toistaa kaaviossa 5 esitetyn CENELECin V-syklin ”vaarojen tunnistaminen ja kausaalianalyysitoiminnot” (tai muun soveltuvan menetelmän) alemmilla tasoilla. Myös menettelyohjeiden ja vastaavien ohjeistojen käyttö sekä eksplisiittiset analyysit ja arvioinnit voidaan toistaa järjestelmän kehittämissyklin jokaisessa vaiheessa, jotta osajärjestelmän tasolla tunnistettujen turvallisuustoimenpiteiden perusteella saadaan määritettyä ne turvallisuusvaatimukset, jotka on täytettävä seuraavassa vaiheessa. Tämä on havainnollistettu kaaviossa 11.

[G 3] Ks. myös tämän asiakirjan 2.1.1 kohtaa koskeva G 4 kohta.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu



Kaavio 11: Alemman tason vaiheiden turvallisuusvaatimusten johtaminen

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] Myös kaikki kaaviossa 5 esitetyn CENELECin V-syklin laatikon 3[(14)] toiminnot arvioidaan siten riippumattomasti.

[G 2] Arviointielinten toteuttaman riippumattoman arvioinnin tyyppiä ja tarkkuutta (toisin sanoen yksityiskohtainen tai silmämääräinen arviointi) tarkastellaan 6 artiklaa koskevissa selvennyksissä.

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] Esimerkiksi tulipalon sammuttaminen voi johtaa uuteen vaaraan (tukehtumiseen), joka edellyttää uusia turvallisuustoimenpiteitä (kuten erityistä menettelyä matkustajien evakuoimiseksi). Toinen esimerkki on karkaistun lasin käyttö sen välttämiseksi, ettei ikkuna hajoa törmäyksessä ja matkustajat vahingoitu lasin sirpaleista tai sinkoudu ikkunasta. Tällöin

(14) *YTM:n ja kaavion 5 (ts. CENELEC-standardin 50 126 kaaviossa 10 esitetyn V-syklin) toimien vastaavuutta kuvataan 2.1.1 kohdassa. 2.1.1 kohtaa koskevassa G 3 kohdassa luetellaan, mitkä CENELECin toiminnot sisältyvät YTM:n vaiheeseen ”järjestelmän turvallisuusvaatimustenmukaisuuden osoittaminen”.*

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

uutena vaarana on se, että hätäevakuointi vaunujen ikkunoista on selvästi vaikeampaa, mikä voi johtaa turvallisuusvaatimuksiin, joiden takia tietyt ikkunat on suunniteltava siten, että ne mahdollistavat evakuoinnin.

[G 2] Esimerkki toiminnallisesta muutoksesta on kielto, jolla estetään kaikki vaarallisten aineiden kuljetukset tiheästi asutettujen alueiden läpi menevillä raiteilla. Tällaiset kuljetukset on siten hoidettava käyttämällä vaihtoehtoista reittiä ja tunneleita, mistä aiheutuu erityyppisiä vaaroja.

[G 3] Muita esimerkkejä vaaroista, joita voidaan tunnistaa järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisen yhteydessä, esitetään standardin EN 50 129 liitteessä A.4.3.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. VAAROJEN HALLINTA

4.1. Vaarojen hallintamenettely

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] Myös CENELEC-standardeissa 50 126-1 {Ref. 8} ja 50 129 {Ref. 7} suositellaan vaaroja koskevan asiakirjan käyttöä turvallisuuteen liittyvien tietojen rekisteröimiseksi, hallitsemiseksi ja valvomiseksi.

[G 2] Järjestelmän monimutkaisuuden mukaan toimijalla voi olla yksi tai useampia vaaroja koskeva asiakirja. Molemmissa tapauksissa arviointielin tekee vaaroja koskevalle asiakirjalle tai asiakirjoille riippumattoman arvioinnin. Yksi mahdollinen ratkaisu on pitää yllä:

(a) yhtä ”sisäistä vaaroja koskevaa asiakirjaa” toimijan vastuulla olevan osajärjestelmän kaikkien sisäisten turvallisuusvaatimusten hallitsemiseksi. Asiakirjan koko ja hallintatehtävien määrä on riippuvainen sen rakenteesta ja tietenkin osajärjestelmän monimutkaisuudesta. Koska vaaroja koskevaa asiakirjaa käytetään sisäisiä hallintatehtäviä varten, sitä ei tarvitse toimittaa muille toimijoille. Sisäinen vaaroja koskeva asiakirja sisältää kaikki tunnistetut vaarat, joita hallitaan, ja niihin liittyvät vahvistettavat turvallisuustoimenpiteet;
(b) yhtä ”ulkoista vaaroja koskevaa asiakirjaa” vaarojen ja niihin liittyvien turvallisuustoimenpiteiden (joita toimija ei voi itse toteuttaa kaikilta osin) siirtämiseksi muille toimijoille 1.2.2 kohdan mukaisesti. Tavallisesti tämä toinen vaaroja koskeva asiakirja on pienempi ja edellyttää vähemmän hallintatehtäviä (katso liitteessä LISÄYS C olevassa C.16.4. kohdassa esitetty esimerkki).

[G 3] Jos useiden vaaroja koskevien asiakirjojen hallinta vaikuttaa monimutkaiselta, toinen mahdollinen vaihtoehto on hallita kaikkia edellä a ja b kohdassa tarkoitettuja vaaroja ja niihin liittyviä toimenpiteitä yhdellä ainoalla vaaroja koskevalla asiakirjalla mutta laatia kaksi kertomusta vaaroja koskevasta asiakirjasta (katso esim. liitteessä LISÄYS C oleva C.16.3. kohta):

(a) yksi kertomus sisäisestä vaaroja koskevasta asiakirjasta, joka ei kuitenkaan välttämättä ole tarpeellinen, jos vaaroja koskeva asiakirja on jäsennelty hyvin riippumattoman arvioinnin mahdollistamiseksi;
(b) yksi kertomus ulkoisesta vaaroja koskevasta asiakirjasta vaarojen ja niihin liittyvien turvallisuustoimenpiteiden siirtämiseksi muille toimijoille.

[G 4] Kuten 4.2 kohdassa todetaan, hankkeen lopussa kun järjestelmä on hyväksytty:

(a) kaikkia vaaroja, jotka siirretään muille toimijoille, hallinnoidaan siirron toteuttavan toimijan ulkoisella vaaroja koskevalla asiakirjalla. Koska vaarat sisällytetään muiden toimijoiden vaaroja koskeviin asiakirjoihin ja niitä hallinnoidaan tällaisilla asiakirjoilla, kyseisen toimijan ei enää tarvitse hallinnoida niitä (osa)järjestelmän elinkaaren aikana;
(b) kaikkia asiaan liittyviä turvallisuustoimenpiteitä ei kuitenkaan pidä vahvistaa vaaroja koskevassa asiakirjassa; tätä koskevat perusteet esitetään 4.2 kohtaa koskevassa G 9

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

kohdassa. On järkevää, että organisaatio, joka siirtää käyttörajoitukset, ilmoittaa selvästi vaaroja koskevassa asiakirjassa, että asiaan liittyviä turvallisuustoimenpiteitä ei ole vahvistettu.

[G 5] Vastaavasti kaikkia sisäisiä vaaroja koskevia asiakirjoja pidetään yllä (osa)järjestelmän koko elinkaaren ajan. Tämä mahdollistaa sen, että tunnistettuihin vaaroihin liittyvien riskien valvonnan edistymistä voidaan seurata (osa)järjestelmän käytön ja kunnossapidon aikana, toisin sanoen myös sen käyttöönoton jälkeen: katso kaaviossa 5 esitetyn CENELECin V-syklin laatikko 4.

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] Vaaroja ja niihin liittyviä turvallisuustoimenpiteitä koskevat tiedot, jotka saadaan muilta toimijoilta (katso 1.2.2 kohta), sisältävät myös kaikki eri osajärjestelmiin sovellettavat oletukset(15) ja käyttörajoitukset(15) (joita kutsutaan myös turvallisuuteen liittyviksi sovellusehdoiksi), ja tapauksen mukaan valmistajien määrittämät yleisiä sovelluksia ja yleisiä tuotteita koskevat turvallisuusarviot.

[G 2] Liitteessä LISÄYS C olevassa C.16. kohdassa esitetään esimerkki vaaroja koskevan asiakirjan rakenteesta.

4.2. Tietojen vaihto

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] Kun kyse on esimerkiksi junan ETCS-laitteiston matkanmittausosajärjestelmästä, valmistaja voi validoida algoritmit laboratoriossa simuloimalla teoreettisia signaaleja, joita välimatkan lukulaitteet voivat tuottaa. Matkanmittausosajärjestelmän kattava validointi edellyttää kuitenkin rautatieyrityksen ja infrastruktuurin haltijan apua validoinnin toteuttamiseksi käyttämällä todellista junaa ja todellista junan pyörän ja kiskojen kosketusta.

[G 2] Toinen esimerkki on tapaukset, joissa valmistajat siirtävät rautatieyrityksille käyttöön tai kunnossapitoon liittyviä teknisen laitteiston turvallisuustoimenpiteitä. Rautatieyrityksen on pantava täytäntöön tällaiset turvallisuustoimenpiteet.

[G 3] Jotta asianomaiset organisaatiot voivat käsitellä yhdessä tällaisia vaaroja, niihin liittyviä turvallisuustoimenpiteitä ja riskejä, on hyödyllistä, jos ne tunnistanut organisaatio esittää

(15) *Ks. "yleisen tuotteen" ja "yleisen sovelluksen" turvallisuusarviota ja "oletuksia ja käyttörajoituksia" koskevat lisäselvennykset tämän asiakirjan 1.1.5 kohtaa koskevasta G 5 kohdasta ja alaviitteistä (9) ja (10).*

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

kaikki tarvittavat selvennykset, jotta ongelma ymmärretään selkeästi. On mahdollista, että vaarojen, turvallisuustoimenpiteiden ja riskien alkuperäistä sanamuotoa on muutettava, jotta ne voidaan ymmärtää ilman, että niistä on keskusteltava uudelleen. Vaarojen yhteinen uudelleenarviointi voi johtaa uusiin turvallisuustoimenpiteisiin.

[G 4] Vastaanottava toimija, joka vastaa vastaanotettujen tai uusien turvallisuustoimenpiteiden toteuttamisesta, hallitsemisesta ja vahvistamista, rekisteröi omaan vaaroja koskevaan asiakirjaansa kaikki asiaa koskevat vaarat niihin liittyvine turvallisuustoimenpiteineen (sekä siirretyt että yhteisesti tunnistetut).

[G 5] Jos turvallisuustoimenpidettä ei ole vahvistettu kaikilta osin, on määritettävä selvä käyttörajoitus (esim. lieventävät toiminnalliset toimenpiteet), ja se on rekisteröitävä vaaroja koskevaan asiakirjaan. On mahdollista, että teknisiä/suunnitteluun liittyviä turvallisuustoimenpiteitä

(a) ei ole toteutettu oikein;
(b) ei ole toteutettu täysimääräisesti;
(c) ei ole tarkoituksella toteutettu lainkaan, esimerkiksi koska vaaroja koskevaan asiakirjaan merkittyjen turvallisuustoimenpiteiden sijaan toteutetaan muita turvallisuustoimenpiteitä (esim. kustannussyistä). Koska tällaisia turvallisuustoimenpiteitä ei ole vahvistettu, ne on yksilöitävä selvästi vaaroja koskevassa asiakirjassa. Lisäksi on esitettävä näyttö siitä /perustelut sille, miksi toteutetut turvallisuustoimenpiteet ovat asianmukaisempia[16], ja osoitettava, että korvaavat turvallisuustoimenpiteet täyttävät järjestelmälle asetetut turvallisuusvaatimukset;
(d) jne.

Tällaisissa tapauksissa teknisiä/suunnitteluun liittyviä turvallisuustoimenpiteitä ei voida hallita ja vahvistaa vaarojen hallintamenettelyssä. Asiaan liittyvät vaarat ja turvallisuustoimenpiteet on jätettävä avoimiksi vaaroja koskevassa asiakirjassa, jottei käytetä väärin muiden järjestelmien turvallisuustoimenpiteitä soveltamalla ”vastaavan ohjeiston” hyväksyttävää riskitasoa koskevaa periaatetta.

[G 6] Yleensä turvallisuustoimenpiteet, joita ”ei toteuteta oikein” ja/tai joita ”ei toteuteta täysimääräisesti” havaitaan varhaisessa vaiheessa järjestelmän elinkaarta, ja ne korjataan ennen järjestelmän hyväksymistä. Jos ne kuitenkin havaitaan liian myöhään, jotta tekninen turvallisuustoimenpide voitaisiin toteuttaa oikein ja täysimääräisesti, toteutuksesta ja hallinnoinnista vastaavan organisaation on yksilöitävä ja rekisteröitävä vaaroja koskevaan asiakirjaan arvioitavaa järjestelmää koskevat selvät käyttörajoitukset. Nämä käyttörajoitukset ovat usein arvioitavan järjestelmän toiminnallisia sovellusrajoitteita.

[G 7] Lisäksi voi olla hyödyllistä merkitä vaaroja koskevaan asiakirjaan, toteutetaanko asiaa koskevat turvallisuustoimenpiteet oikein järjestelmän elinkaaren myöhemmässä vaiheessa vai jatketaanko järjestelmän käyttöä soveltamalla yksilöityjä käyttörajoituksia. Vaaroja koskevaan asiakirjaan voi olla hyödyllistä merkitä myös perustelut sille, miksei asiaan liittyviä teknisiä turvallisuustoimenpiteitä toteuteta oikein/täysimääräisesti.

[G 8] Toimija, joka vastaanottaa käyttörajoitukset:

(a) vie ne kaikki omaan vaaroja koskevaan asiakirjaansa;
(b) varmistaa, että arvioitavan järjestelmän käyttöehdot vastaavat kaikkia vastaanotettuja käyttörajoituksia;

---

(16) *Jos alunperin määritettyjen turvallisuustoimenpiteiden sijaan toteutetaan eri turvallisuustoimenpiteet, myös ne on merkittävä vaaroja koskevaan asiakirjaan.*

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(c) varmentaa ja validoi, että arvioitava järjestelmä on näiden käyttörajoitusten mukainen.

[G 9] Asianomaisten organisaatioiden yhteisen päätöksen mukaan:

(a) joko asiaan liittyvät tekniset turvallisuustoimenpiteet toteutetaan oikein suunnitelman myöhemmässä vaiheessa.
Käyttörajoitusten siirron hoitava organisaatio valvoo jatkossakin asiaan liittyvien turvallisuustoimenpiteiden oikeaa teknistä toteutusta. Niin kauan kuin vastaavia teknisiä turvallisuustoimenpiteitä ei toteuteta täysimääräisesti, asiaa koskevia turvallisuustoimenpiteitä ei voida vahvistaa eikä niihin liittyviä vaaroja hallinnoida kyseisen organisaation vaaroja koskevalla asiakirjalla. Tämä on varmistettava, vaikka siirretyt käyttörajoitukset otettaisiinkin sillä välin käyttöön.

(b) tai asiaan liittyviä teknisiä turvallisuustoimenpiteitä ei panna täytäntöön suunnitelmassa myöhemmässä vaiheessa. Järjestelmää käytetään siten edelleenkin soveltamalla asiaan liittyviä käyttörajoituksia koko elinkaaren ajan. Tällöin voidaan toteuttaa seuraavat toimet:

(1) organisaatio, joka siirtää käyttörajoitukset, ei merkitse asiaan liittyviä turvallisuustoimenpiteitä ”vahvistetuiksi” toimenpiteiksi vaaroja koskevaan asiakirjaansa. Tällä varmistetaan se, että käytettäessä kyseistä järjestelmää ohjeistona muissa hankkeissa vastaavia turvallisuusnäkökohtia ei jätetä huomiotta. Vaikka toinen toimija päättäisikin hallinnoida asiaan liittyviä riskejä toisin, käyttörajoitusten viennin hoitavan organisaation on hyödyllistä osoittaa selvästi vaaroja koskevassa asiakirjassaan, että asiaan liittyviä turvallisuustoimenpiteitä ei ole vahvistettu, tai

(2) järjestelmämäärittelyä voidaan muuttaa siten, että käyttörajoitukset sisällytetään järjestelmän soveltamisalaan (toisin sanoen järjestelmää koskeviin oletuksiin) ja turvallisuusvaatimuksiin. Tällä mahdollistetaan vaarojen hallinta. Näin ollen jos järjestelmää käytetään ohjeistona toisessa sovelluksessa:

(i) uutta järjestelmää on käytettävä samoin ehdoin (eli on noudatettava kyseisiin oletuksiin liittyviä käyttörajoituksia), tai
(ii) hakijan on tehtävä poikkeamien osalta täydentävä riskinarviointi käyttämällä kyseisiä oletuksia.

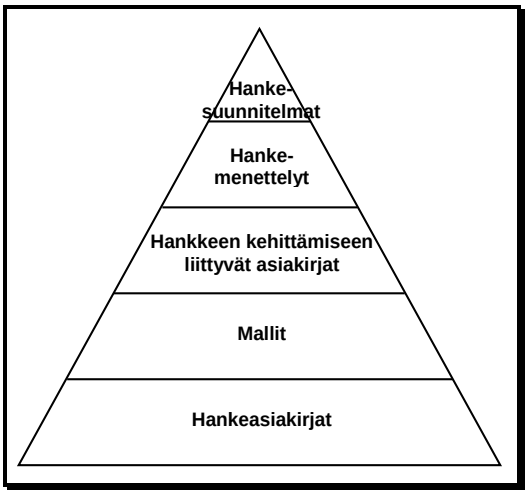
Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

5. RISKINHALLINTAMENETTELYN SOVELTAMISTA KOSKEVA NÄYTTÖ

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] Infrastruktuurin haltijan ja rautatieyrityksen turvallisuusjohtamisjärjestelmässä (SMS) tarkastellaan jo näitä vaatimuksia. Vaikka turvallisuusjohtamisjärjestelmä ei olekaan pakollinen, rautatiealan muut toimijat, joita merkittävä muutos koskee, soveltavat yleensä vähintäänkin hanketasolla laadunhallintamenettelyä (QMP) ja/tai turvallisuusjohtamismenettelyä (SMP). Nämä molemmat menettelyt perustuvat joko yrityksen tai vähintään hankkeen sisäiseen jäsenneltyyn asiakirjahierarkiaan. Niissä tarkastellaan myös toimintavarmuuden, käyttövarmuuden, kunnossapidettävyyden ja turvallisuuden (RAMS) hallinnoinnin dokumentointitarpeita. Tällainen jäsennelty dokumentointi voi koostua periaatteessa seuraavista osista (katso myös kaavio 12):

(a) **Hankesuunnitelmissa** kuvataan hankkeen jonkin toiminnon hallinnoimiseksi käyttöön otettavaa organisaatiota.
(b) **Hankemenettelyissä** kuvataan yksityiskohtaisesti, miten jokin tietty tehtävä toteutetaan. Tavallisesti yritys on laatinut menettelyt ja ohjeet, joita sovelletaan sellaisinaan. Uusia hankemenettelyjä laaditaan vain, jos on kuvattava kyseiseen hankkeeseen liittyvä tietty tehtävä.
(c) **Hankkeen kehittämiseen liittyvät asiakirjat** laaditaan kaaviossa 5 esitetyn järjestelmän elinkaaren mukaisesti.
(d) **Yritys- tai vähintääk hankekohtaiset mallit** tuotetaan erityyppisiä laadittavia asiakirjoja varten.



Kaavio 12: Jäsennelty asiakirjahierarkia

(e) **Hankeasiakirjat** laaditaan hankkeen aikana, ja ne ovat välttämättömiä yrityksen laadunhallinta- ja turvallisuusjohtamismenettelyjä koskevien vaatimusten noudattamisen osoittamiseksi.

Tämä on yksi tapa täyttää dokumentoitua näyttöä koskevat tarpeet. Myös muut tavat ovat mahdollisia edellyttäen, että niillä täytetään YTM:ää koskevat perusteet.

[G 2] CENELEC-standardien mukaan järjestelmän yhdenmukaisuus toiminnallisten ja turvallisuusvaatimusten kanssa on osoitettava turvallisuusarviota koskevassa asiakirjassa (tai turvallisuuskertomuksessa). Vaikka turvallisuusarvio ei olekaan pakollinen, sen avulla saadaan jäsennellyn turvallisuusperusteita koskevan asiakirjan muodossa:

(a) näyttö laadunhallinnasta,
(b) näyttö turvallisuusjohtamisesta,

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(c) näyttö toiminnallisesta ja teknisestä turvallisuudesta.

Sillä voidaan samalla tukea ja opastaa arviointielimiä YTM-asetuksen oikean soveltamisen riippumattomassa arvioinnissa.

[G 3] Turvallisuusarviossa kuvataan ja esitetään tiivistäen, miten yrityksen tai hankkeen laadunhallinta- ja/tai turvallisuusjohtamismenettelyjen tuloksena laaditut hankeasiakirjat ovat sidoksissa järjestelmän kehittämisprosessissa järjestelmän turvallisuuden osoittamiseen. Turvallisuusarvio ei yleensä sisällä suuria määriä yksityiskohtaisia todisteita ja perusteluja, mutta siinä esitetään tarkat viitteet tällaisiin asiakirjoihin.

[G 4] **Teknisten järjestelmien turvallisuusarvio:** CENELEC-standardeja voidaan käyttää ohjeina turvallisuusarvioiden laatimiseksi ja/tai jäsentelemiseksi:

(a) katso standardi EN 50 129 {Ref. 7} ”Rautatiesovellukset – Tietoliikenne-, merkinanto- ja tietojenkäsittelyjärjestelmät – Turvallisuuteen liittyvät elektroniset järjestelmät”, ohjeen EN 50 126-2 {Ref. 9} liite H.2 sisältää myös ehdotuksen merkinantojärjestelmien turvallisuusarvion rakenteeksi;
(b) katso ohjeen EN 50 126-2 {Ref. 9} liitteestä H.1 liikkuvan kaluston turvallisuusarvion rakenne;
(c) katso ohjeen EN 50 126-2 {Ref. 9} liitteestä H.3 infrastruktuurien turvallisuusarvion rakenne.

Kuten edellä esitetyistä viitteistä käy ilmi, teknisten järjestelmien turvallisuusarvion rakenne ja sen sisältö on riippuvainen järjestelmästä, jota turvallisuusvaatimusten mukaisuuden osoittaminen koskee.

Ohjeen EN 50 126-2 {Ref. 9} liitteessä H tarkastellussa turvallisuusarviossa esitetään ainoastaan esimerkkejä, eikä se välttämättä sovellu käytettäväksi kaikissa samantyyppisissä järjestelmissä. Siksi esimerkkiä käytettäessä on arvioitava sen soveltuvuutta kunkin sovelluksen kannalta.

[G 5] **Rautatiejärjestelmien organisatorisia ja toiminnallisia näkökohtia koskeva turvallisuusarvio:**

Tällä hetkellä ei ole käytössä erityistä standardia, jossa määritetään rautatiejärjestelmän organisatoristen ja toiminnallisten näkökohtien turvallisuusarvion rakenne ja sisältö ja annetaan ohjeita turvallisuusarvion laatimiseksi. Koska turvallisuusarviolla pyritään kuitenkin osoittamaan jäsennellysti, että järjestelmä vastaa sille asetettuja turvallisuusvaatimuksia, samantyyppistä turvallisuusarvion rakennetta voidaan soveltaa teknisiin järjestelmiin. 5.1 kohtaa koskevassa G 4 kohdassa esitetyissä viitteissä esitetään ohjeita ja tarkastuslista näkökohdista, jotka on otettava huomioon arvioitavan järjestelmän tyypistä riippumatta. Organisatoristen ja toiminnallisten muutosten hallinta edellyttää samanlaisia laadunhallinta- ja turvallisuusjohtamismenettelyjä kuin teknisten muutosten hallintakin, ja järjestelmän yhdenmukaisuus määritettyjen turvallisuusvaatimusten kanssa on osoitettava. CENELEC-standardien vaatimukset, joita ei sovelleta organisatorisiin ja toiminnallisiin näkökohtiin, liittyvät yksinomaan teknisen järjestelmän suunnitteluun, kuten ”laitteiston luontainen varmistus vikaantuessa” -periaatteisiin, sähkömagneettiseen yhteensopivuuteen (EMC) jne.

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.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Järjestelmän monimutkaisuuden mukaan tämä näyttö voidaan esittää yhdessä tai useammassa turvallisuusarviossa. Katso 5.1 kohtaa koskevasta G 4 ja G 5 kohdasta teknisten järjestelmien ja toiminnallisten ja organisatoristen näkökohtien turvallisuusarvion rakenne.

[G 2] Katso myös mahdolliset esimerkit todisteista liitteessä A olevasta A.4. kohdasta.

[G 3] Rautatiealan teknisten järjestelmien ja osajärjestelmien käyttöiän odotetaan yleensä olevan noin 30 vuotta. On todennäköistä, että tällaisen pitkän ajanjakson aikana järjestelmiin tehdään merkittäviä muutoksia. Tällaisille järjestelmille ja niiden rajapinnoille voitaisiin siten tehdä täydentäviä riskinarviointeja ja laatia asiaan liittyvät asiakirjat, joita on tarkistettava, täydennettävä ja jotka on siirrettävä vaaroja koskevia asiakirjoja käyttävien eri toimijoiden ja organisaatioiden kesken. Tämä edellyttää, että asiakirjojen valvontaan ja kokoonpanon hallintaan sovelletaan suhteellisen tiukkoja vaatimuksia.

[G 4] Tällöin on järkevää, että yritys, joka arkistoi kaikki riskinarviointiin ja riskinhallintaan liittyvät tiedot, varmistaa, että tulokset/tiedot tallennetaan fyysiselle välineelle, joka on luettavissa/saatavissa järjestelmän koko elinkaaren ajan (eli 30 vuoden ajan).

[G 5] Tätä vaatimusta voidaan perustella muun muassa seuraavasti:

(a) tällä varmistetaan, että kaikki arvioitavaa järjestelmää koskevat turvallisuusanalyysit ja turvallisuuteen liittyvät asiakirjat ovat saatavissa järjestelmän koko käyttöiän. Näin ollen

(1) jos samaan järjestelmään tehdään uusia merkittäviä muutoksia, järjestelmän viimeisin dokumentaatio on saatavissa;

(2) jos järjestelmän käyttöiän aikana ilmenee ongelmia, on hyödyllistä voida palata asiaan liittyviin turvallisuusanalyyseihin ja turvallisuusasiakirjoihin;

(b) tällä varmistetaan, että arvioitavana olevaa järjestelmää koskevat turvallisuusanalyysit ja turvallisuusasiakirjat ovat saatavilla, jos järjestelmää käytetään toisessa sovelluksessa vastaavana ohjeistona.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

YTM-ASETUKSEN LIITE II

Edellytykset, jotka arviointielinten on täytettävä

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] Lisäselvennystä ei pidetä tarpeellisena.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

LISÄYS A: LISÄSELVENNYKSET

A.1. Johdanto

A.1.1. Lisäyksen tarkoituksena on helpottaa tämän asiakirjan lukemista. Asiakirjassa ei anneta suurta määrää erilaista tietoa, vaan tässä lisäyksessä käsitellään tarkemmin monimutkaisempia aiheita.

A.2. Vaarojen luokittelu

A.2.1. Vaarojen luokittelua/jaottelua koskevat ohjeet annetaan standardin EN 50 126-1 {Ref. 8} kohdassa 4.6.3. ja ohjeen EN 50 126-2 {Ref. 9} liitteessä B.2.

A.3. Teknisten järjestelmien hyväksyttävää riskitasoa koskeva peruste (RAC-TS)

A.3.1. Teknisten järjestelmien hyväksyttävän riskitason yläraja

A.3.1.1. RAC-TS:ää käsitellään asiakirjan {Ref. 4} 2.5.4 kohdassa.

A.3.1.2. RAC-TS:n tarkoituksena on täsmentää hyväksyttävän riskitason yläraja teknisille järjestelmille, joiden turvallisuusvaatimuksia ei voida johtaa menettelyohjeista eikä vertailusta muihin vastaaviin ohjeistoihin. RAC-TS määrittelee näin ollen viitearvon, jonka avulla teknisten järjestelmien riskinarviointimenetelmät voidaan kalibroida. Kuten tämän asiakirjan lisäyksessä A olevassa A.3.6. kohdassa kuvataan, tämän viitearvon tai hyväksyttävän riskitason ylärajan avulla voidaan määrittää hyväksyttävä riskitaso myös teknisten järjestelmien muille toimintavioille, jotka eivät voi uskottavasti ja suoraan johtaa tuhoisiin seurauksiin (kuten muihin vakaviin tilanteisiin). RAC-TS ei kuitenkaan ole riskinarviointimenetelmä.

A.3.1.3. RAC-TS on semikvantitatiivinen peruste. Sitä sovelletaan sekä teknisen järjestelmän satunnaisiin laitteistovikoihin että järjestelmällisiin vikoihin/virheisiin. Se käsittää näin ollen myös teknisen järjestelmän järjestelmälliset viat/virheet, jotka voivat johtua järjestelmän kehittämisprosessissa (kuten eritelmien laadinnassa, suunnittelussa, toteutuksessa ja vahvistamisessa) tehdyistä inhimillisistä erehdyksistä. RAC-TS ei kuitenkaan kata inhimillisiä erehdyksiä, jotka on tehty teknisten järjestelmien toiminnan ja kunnossapidon aikana.

A.3.1.4. CENELEC-standardin 50 129 liitteiden A.3 ja A.4 mukaan järjestelmällisiä vikoja/virheitä ei voida selvittää määrällisesti, minkä vuoksi kvantitatiivinen tavoite on esitettävä ainoastaan satunnaisten laitteistovikojen osalta, kun taas järjestelmällisiin vikoihin/virheisiin sovelletaan kvalitatiivisia menetelmiä[17]. *”Koska järjestelmällisten vikojen eheystasoa ei voida arvioida kvantitatiivisin menetelmin, tietyllä turvallisuuden eheystasolla toteutettavan*

(17) *CENELEC-standardien 50 126, 50 128 ja 50 129 mukaan satunnaisia laitteistovikoja kuvaava kvantitatiivinen luku on yhdistettävä aina turvallisuuden eheystasoon, jotta systemaattisia vikoja/virheitä voidaan hallita. Tämän vuoksi RAC-TS:n arvo $10^{-9}\,h^{-1}$ edellyttää lisäksi sellaisen asianmukaisen prosessin käynnistämistä, jossa myös systemaattisia vikoja/virheitä hallinnoidaan oikealla tavalla. Merkinnän luettavuuden helpottamiseksi siinä kuitenkin viitataan usein ainoastaan teknisen järjestelmän satunnaisiin laitteistovikoihin.*

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

järjestelmän yhteydessä menetelmät, välineet ja tekniikat, joiden katsotaan tehokkaasti käytettyinä varmistavan asianmukaisen luottamustason, ryhmitellään turvallisuuden eheystason mukaisesti."

A.3.1.5. Vastaavasti CENELEC-standardien mukaan teknisten järjestelmien ohjelmistojen eheyttä ei voida esittää määrällisesti. CENELEC-standardi 50 128 sisältää ohjeet turvallisuuteen liittyvien ohjelmistojen kehittämiseksi vaaditun turvallisuuden eheystason mukaisesti. Niitä sovelletaan ohjelmistojen suunnitteluun, varmentamiseen, vahvistamiseen ja laadunvarmistukseen.
CENELEC-standardin 50 128 mukaan turvatoimintoja toteuttavan ohjelmoitavan sähköisen valvontajärjestelmän korkein mahdollinen turvallisuuden eheystaso (SIL) ohjelmiston kehittämisprosessissa on SIL 4, mikä vastaa kvantitatiivista siedettävää vaaratasoa 10^{-9} h^{-1}.

A.3.1.6. Koska järjestelmällisiä vikoja/virheitä ei voida esittää määrällisesti, niitä on hallittava laadullisesti ottamalla käyttöön laatu- ja turvallisuusprosessi, joka vastaa arvioitavan järjestelmän edellyttämää turvallisuuden eheystasoa.

(a) laatuprosessin tarkoituksena on "minimoida inhimillisten erheiden esiintyvyys kaikissa elinkaaren vaiheissa ja siten pienentää järjestelmällisten vikojen riskiä järjestelmässä"
(b) turvallisuusprosessin tarkoituksena on *"vähentää edelleen turvallisuuteen liittyvien inhimillisten erheiden esiintyvyyttä koko elinkaaren aikana ja siten minimoida turvallisuuteen liittyvien järjestelmävikojen jäännösriski".*

A.3.1.7. Ohjeet järjestelmällisten vikojen/virheiden esiintyvyyden hallitsemiseksi sekä ohjeet mahdollisille suunnittelutoimenpiteille, joilla suojaudutaan yhteisvioilta ja yhteisvioittumistavoilta (Common Cause/Mode Failures, CCF/CMF) ja joilla varmistetaan, että tällaisten vikojen/virheiden ilmetessä tekninen järjestelmä ohjautuu vikaturvalliseen tilaan, esitetään seuraavissa standardeissa:

(a) CENELEC-standardissa 50 126-1 {Ref. 8} ja sen ohjeessa 50 126-2 {Ref. 9} luetellaan CENELEC-standardin 50 129 lausekkeet ja määritetään niiden sovellettavuus muita kuin merkinantojärjestelmiä koskevaan dokumentoituun näyttöön: katso ohjeen 50 126-2 {Ref. 9} taulukko 9.1. Luettelossa annetaan ohjeet, miten järjestelmästä johtuvia vikoja ja arvioitavaan järjestelmään ympäristöstä aiheutuvia vaikutuksia on käsiteltävä;

Esimerkiksi suunnittelun ominaispiirteitä koskevat tekniikat/toimenpiteet esitetään CENELEC-standardin 50 129 {Ref. 7} taulukossa E.5: *"Suunnittelun ominaispiirteet (mainittu kohdassa 5.4) seuraavista seikoista aiheutuvien vikojen välttämiseksi ja hallitsemiseksi:*

(1) *"mahdollisesti jäljelle jääneet suunnitteluviat";*
(2) *"ympäristöolot";*
(3) *"väärinkäyttö- ja toimintavirheet";*
(4) *"ohjelmiston mahdolliset jäännösviat";*
(5) *"inhimilliset tekijät";*

CENELEC-standardin 50 129 {Ref. 7} liitteissä D ja E esitetään tekniikat ja toimenpiteet, joiden avulla voidaan välttää turvallisuuteen liittyvien sähköisten merkinantojärjestelmien järjestelmällisiä viikoja ja hallita satunnaisia laitteistovikoja ja järjestelmällisiä vikoja/virheitä. Monia näistä tekniikoista ja toimenpiteistä voidaan soveltaa myös muihin kuin merkinantojärjestelmiin ohjeen 50 126-2 {Ref. 9} taulukon 9.1 mukaisesti.

(b) CENELEC-standardi 50 128 sisältää ohjeet turvallisuuteen liittyvien ohjelmistojen kehittämiseksi arvioitavan ohjelmiston edellyttämän turvallisuustason (SIL 0–SIL 4) mukaisesti.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

A.3.1.8. RAC-TS vastaa näin ollen korkeinta mahdollista eheystasoa, jota voidaan vaatia CENELEC- ja IEC-standardien mukaisesti. Tiedonhaun helpottamiseksi IEC-standardin 61508-1 ja CENELEC-standardin 50 129:n vaatimukset esitetään seuraavassa:

(a) IEC 61508-1: *”Tässä standardissa vahvistetaan alaraja kohdennetuille vikatoimenpiteille, joiden toteuttamista voidaan vaatia vaarallisisten vikatyyppien yhteydessä. Näiden toimenpiteiden katsotaan vastaavan turvallisuuden eheystason 4 alarajaa. Turvallisuuteen liittyvät järjestelmät, jotka eivät ole monimutkaisia, voidaan joissakin tapauksissa suunnitella pienempien kohdennettuja vikatoimenpiteitä koskevien arvojen mukaisesti, mutta taulukossa esitetyt luvut vastaavat rajaa, joka voidaan nykyoloissa saavuttaa melko monimutkaisissa järjestelmissä (esimerkiksi ohjelmoitavat turvallisuuteen liittyvät sähköiset järjestelmät).”*

(b) EN 50129: *”Toimintoa, jonka kvantitatiiviset vaatimukset ylittävät 10^{-9} h^{-1}, käsitellään jommallakummalla tavalla:*

(1) *jos toiminto voidaan jakaa toiminnallisesti riippumattomiin osafunktioihin, THR (varmuusvikataajuus) voidaan jakaa näiden osafunktioiden ja kullekin osafunktiolle osoitetun SIL:n kesken.*

(2) *jos toimintoa ei voida jakaa, on vähintään pantava täytäntöön SIL 4:n edellyttämät toimenpiteet ja menetelmät, ja toiminnon yhteydessä on käytettävä muita teknisiä ja operatiivisia toimenpiteitä, jotta vaadittava THR voidaan saavuttaa.”*

A.3.1.9. Kaikkien teknisten järjestelmien kvantitatiivinen turvallisuusvaatimus on tämän jälkeen rajoitettava tähän lukuun. Jos korkeampi suojataso on tarpeen, sitä ei voida saavuttaa ainoastaan yhdellä järjestelmällä. Järjestelmän rakennetta on muutettava esimerkiksi käyttämällä samanaikaisesti kahta toisistaan riippumatonta järjestelmää, jotka ristiintarkastavat toisensa turvallisten tulosten varmistamiseksi. Tämä kuitenkin väistämättä lisää teknisen järjestelmän kehityskustannuksia.

Huomautus: Jos mukana on jo käytössä olleita toimintoja, esimerkiksi täysin mekaanisia järjestelmiä, joille voidaan toiminnallisten kokemusten perusteella saavuttaa korkeampi eheystaso, turvallisuustaso voidaan kuvata erityisellä menettelyohjeella tai turvallisuusvaatimukset voidaan asettaa olemassa olevan järjestelmän kanssa tehtävän vastaavuusarvioinnin (ohjeiston) perusteella. YTM:n soveltamisalalla RAC-TS:ää on sovellettava ainoastaan silloin, kun menettelyohjeita tai ohjeistoja ei voida käyttää.

A.3.1.10. Tämän perusteella voidaan esittää seuraava yhteenveto:

(a) CENELEC-standardien 50 126, 50 128 ja 50 129 mukaan kehittämisprosessin järjestelmällisiä vikoja/virheitä ei voida kuvata määrällisesti;

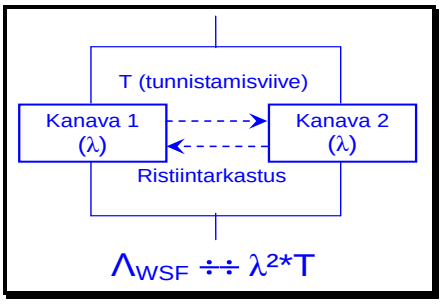
(b) järjestelmällisten vikojen/virheiden esiintyvyyttä ja niiden jäännösriskiä on valvottava ja hallittava soveltamalla asianmukaisia laatu- ja turvallisuusprosesseja, jotka vastaavat arvioitavalta järjestelmältä edellyttyä turvallisuuden eheystasoa;

(c) korkein saavutettavissa oleva turvallisuuden eheystaso on SIL 4 sekä satunnaisten laitteistovikojen että teknisten järjestelmien järjestemällisten vikojen/virheiden osalta;

(d) tämä turvallisuuden eheystason raja SIL 4 merkitsee sitä, että teknisten järjestelmien korkeimman siedetyn vikatason THR (eli varmuusvikataajuus) on oltava alle 10^{-9} h^{-1}.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

A.3.1.11. Tekninen järjestelmä voi saavuttaa siedettävän vikatason $10^{-9}\,h^{-1}$, kun sillä on joko ”vikaturvallinen rakenne” (joka määritelmänsä mukaisesti on tällaisen turvallisuustason mukainen) tai ”kaksinkertainen rakenne” (esim. kaksi riippumatonta käsittelykanavaa, jotka ristiintarkastavat toisensa).



Kaavio 13: Teknisen järjestelmän kaksinkertainen rakenne

Kaksinkertaisen rakenteen osalta voidaan osoittaa, että teknisen järjestelmän väärää opastetta koskeva kokonaisvirhe (Λ_{WSF}) on verrannollinen λ^2*T:hen, jossa

(a) λ^2 on yhden kanavan väärää opastetta koskevan vikatason neliö;

(b) T on aika, joka kuluu siihen, että toinen kanava tunnistaa toisen kanavan väärää opastetta koskevan (koskevat) virheen (virheet). Tämä aika on tavanomaisesti moninkertaisesti suurempi kuin kanavan prosessointiaika/kierros. T on yleensä huomattavasti alle 1 sekunnin.

A.3.1.12. Tämän kaavan (λ^2*T) avulla voidaan teoreettisesti osoittaa (ottaen huomioon ainoastaan teknisen järjestelmän satunnaiset laitteistohäiriöt – ks. myös liitteessä A oleva kohta A.3.1.13.), että RAC-TS:n kvantitatiivinen vaatimus 10^{-9} h^{-1} on saavutettavissa. Järjestelmällisiä vikoja/virheitä on hallittava prosessin avulla: katso liitteessä A oleva kohta A.3.1.6. Esimerkiksi

(a) kun kanavan luotettavuusluvun keksimääräinen vikaantumisväli (MTBF) on 10 000 tuntia, ja varovaisen oletuksen mukaan kaikki kanavan viat ovat vaarallisia, kanavan väärää opastetta koskeva vika on 10^{-4} h^{-1};

(b) näin on jopa silloin kun toisen kanavan väärää opastetta koskevan (koskevien) vian (vikojen) tunnistamiseen kuluu 10 minuuttia (eli $\approx 2*10^{-3}$ tuntia), mikä on niin ikään varovainen oletus.

Väärää opastetta koskeva kokonaisvirhe on $\Lambda_{WSF} \approx 2 * 10^{-10}\ h^{-1}$

A.3.1.13. Käytännössä, kun arvioidaan tällaisen kaksinkertaisen rakenteen väärää opastetta koskevaa kokonaisvikaa, on otettava huomioon toimenpiteet, joita on suunnitteluvaiheessa toteutettu yhteisvioilta ja yhteisvioittumistavoilta (CCF/CMF) suojautumiseksi ja sen varmistamiseksi, että tekninen järjestelmä ohjautuu CCF/CMF-vikojen/virheiden ilmetessä vikaturvalliseen tilaan. Tässä väärää opastetta koskevan kokonaisvirheen (Λ_{WSF}) arvioinnissa on näin ollen otettava huomioon:

(a) kaikille kanaville yhteiset osat, esim. ainoat tai yhteiset syötteet kaikille kanaville, yhteinen virtalähde, komparaattorit, valitsimet ym.;

(b) aika, joka kuluu passiivisten tai piilevien vikojen tunnistamiseen. Monimutkaisilla teknisillä järjestelmillä tämä aika voi olla erilaisten suuruusluokkien vuoksi yli 1 sekuntia;

(c) yhteisvikojen ja yhteisvioittumistapojen (CCF/CMF) vaikutukset.

Tätä aihetta koskevat ohjeet annetaan standardeissa, joihin viitataan tämän asiakirjan lisäyksessä A olevassa kohdassa A.3.1.7.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

A.3.2. RAC-TS:n sovellettavuustestin kulkukaavio

A.3.2.1. RAC-TS:ää voidaan soveltaa teknisen järjestelmän vioista aiheutuviin vaaroihin jäljempänä kaaviossa 14 esitetyllä tavalla.

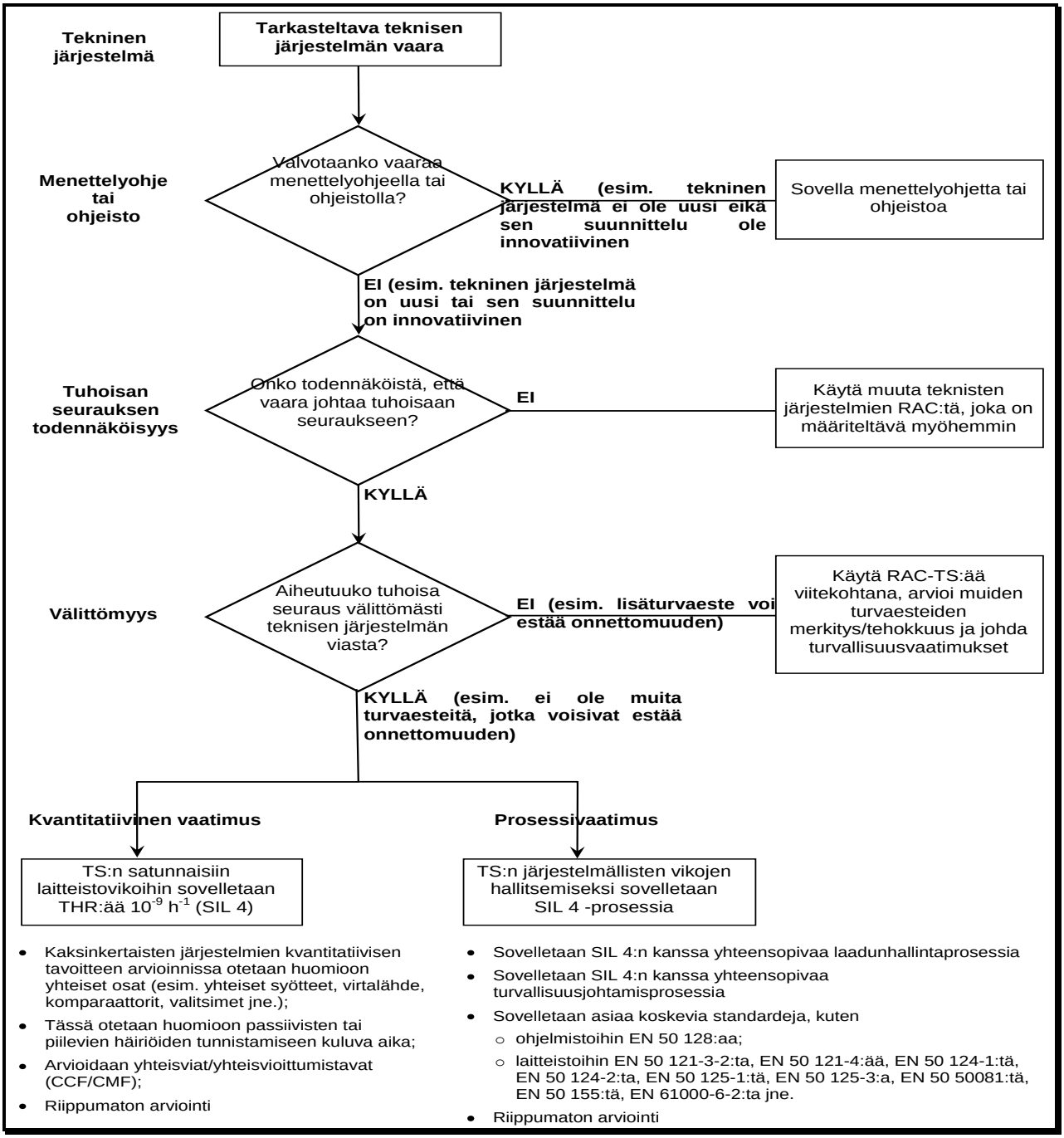
A.3.2.2. Kulkukaavion soveltamisesta esitetään esimerkkitapaus liitteessä C olevassa C.15.

A.3.3. YTM-asetukseen sisältyvä teknisen järjestelmän määritelmä

A.3.3.1. RAC-TS:ää sovelletaan ainoastaan teknisiin järjestelmiin. YTM-asetuksen 3 artiklan 22 kohdassa ”tekninen järjestelmä” määritellään seuraavasti:

’teknisellä järjestelmällä’ tarkoitetaan tuotetta tai tuotekokonaisuutta, mukaan lukien suunnittelu, toteutus ja tukiasiakirjat. Teknisen järjestelmän kehittäminen alkaa sen vaatimusten erittelystä ja päättyy sen hyväksyntään. Vaikka inhimilliseen toimintaan liittyvien merkitystellisten rajapintojen suunnittelu otetaan huomioon, ihmisoperaattorit ja niiden toimet eivät sisälly tekniseen järjestelmään. Kunnossapitoprosessi kuvataan kunnossapito-ohjeissa, mutta se ei varsinaisesti ole osa teknistä järjestelmää.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu



Kaavio 14: RAC-TS:n sovellettavuustestin kulkukaavio

A.3.4. ”Teknisen järjestelmän” määritelmää koskeva selvennys

A.3.4.1. Teknisen järjestelmän määritelmässä kuvataan teknisen järjestelmän ulottuvuus: *”teknisellä järjestelmällä tarkoitetaan tuotetta tai tuotekokonaisuutta, mukaan lukien suunnittelu, toteutus ja tukiasiakirjat.”* Määritelmän mukaisesti teknisen järjestelmän kokoonpano ja sisällys ovat seuraavat:

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(a) fyysiset osat, jotka muodostavat teknisen järjestelmän
(b) (mahdolliset) liitännäiset ohjelmistot
(c) teknisen järjestelmän suunnittelu ja toteutus, mukaan lukien tarvittaessa yleisen tuotteen konfigurointi tai parametrisointi erityistä sovellusta koskevien erityisvaatimusten mukaisesti
(d) tukiasiakirjat, joita tarvitaan

(1) teknisen järjestelmän kehittämiseen
(2) teknisen järjestelmän käyttämiseen ja kunnossapitoon;

A.3.4.2. Tähän määritelmään liittyvillä huomautuksilla täsmennetään tarkemmin teknisen järjestelmän ulottuvuutta:

(a) *”Teknisen järjestelmän kehittäminen alkaa sen vaatimusten erittelystä ja päättyy sen hyväksyntään”*. Tämä käsittää CENELEC-standardin 50 126-1 {Ref. 8} kaaviossa 10 esitetyn V-syklin vaiheet 1–10.

(b) *”Siinä otetaan huomioon inhimilliseen toimintaan liittyvien merkityksellisten rajapintojen suunnittelu. Ihmisoperaattorit ja niiden toimet eivät kuitenkaan sisälly tekniseen järjestelmään.”* Vaikka inhimillisen tekijän teknisen järjestelmän toiminnan ja kunnossapidon aikana aiheuttamat virheet eivät kuulu varsinaiseen tekniseen järjestelmään, ne on otettava huomioon suunniteltaessa ihmisoperaattorien rajapintoja. Tavoitteena on minimoida ihmisoperaattorien rajapintojen huonosta suunnittelusta johtuvat inhimilliset erehdykset.

(c) *”Kunnossapito ei sisälly määritelmään, mutta kunnossapito-ohjeet kattavat sen.”* Tämä tarkoittaa, ettei RAC-TS:ää tarvitse soveltaa teknisen järjestelmän toimintaan ja kunnossapitoon; nämä molemmat perustuvat suurelta osin henkilöstön suorittamiin prosesseihin ja toimenpiteisiin.
Teknisten järjestelmien kunnossapidon tukemiseksi teknisen järjestelmän määritelmän on kuitenkin sisällettävä riittävän yksityiskohtaisesti kaikki merkitykselliset vaatimukset (esimerkiksi säännölliset ehkäisevät huoltotoimenpiteet tai korjaavat huoltotoimenpiteet vikatapauksissa). Teknisen järjestelmän määritelmään ei kuitenkaan kuulu se, miten kyseisen teknisen järjestelmän kunnossapito on järjestettävä ja toteutettava, sillä se sisältyy vastaaviin kunnossapito-ohjeisiin.

A.3.4.3. Katso myös lisäyksessä A oleva A.3.1.

A.3.5. Teknisten järjestelmien toiminnot, joihin RAC-TS:ää sovelletaan

A.3.5.1. RAC-TS:n määritelmän mukaan sitä sovelletaan teknisen järjestelmän suorittamien toimintojen vääriin opasteisiin, jos ne *”voivat uskottavasti ja **suoraan** johtaa tuhoisiin seurauksiin”*: katso asiakirjan {Ref. 4} 2.5.4. kohta.

A.3.5.2. RAC-TS:ää voidaan soveltaa myös toimintoihin, joihin liittyy teknisiä järjestelmiä mutta joiden viat **eivät voi *”suoraan** johtaa tuhoisiin seurauksiin”*. Tässä tapauksessa RAC-TS on asetettava kokonaistavoitteeksi tuhoisiin seurauksiin johtavalle tapahtumasarjalle. Tämän kokonaistavoitteen perusteella kunkin tapahtuman ja siten tarkasteltavassa skenaariossa mukana olevan teknisen järjestelmän toimintavikojen todellinen vaikutus on johdettava liitteessä A olevan A.3.6. kohdan mukaisesti.
RAC-TS:n tällaisesta käytöstä on vielä keskusteltava, ja siitä on sovittava YTM-työryhmässä.

A.3.5.3. Mihin teknisen järjestelmän toimintoihin RAC-TS:ää sovelletaan? IEC-standardin 61226:2005-mukaan

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) toiminto määritellään tässä yhteydessä ”tavoiteltavaksi erityiseksi päämääräksi tai tavoitteeksi, joka voidaan täsmentää tai kuvata viittaamatta sen saavuttamisessa tarvittaviin fyysisiin keinoihin”
(b) toiminto (niin sanottu musta laatikko) muuttaa panosparametrit (esimerkiksi materiaali, energia ja tieto) päämäärään liittyviksi tuotosparametreiksi (esimerkiksi materiaali, energia ja tieto).
(c) toiminnon arviointi on riippumaton sen teknisestä toteutuksesta.

A.3.5.4. RAC-TS:ää sovelletaan seuraaviin toimintotyyppeihin:

(a) kalustoyksikössä olevan ETCS-osajärjestelmän esimerkit:

(1) ”tarjoaa kuljettajalle tietoa, jonka avulla hän voi ohjata junaa turvallisesti ja käyttää jarrujärjestelmää ylinopeustilanteessa”. Radanvarresta saatujen tietojen (sallittu nopeus) ja kalustoyksikössä olevan ETCS-osajärjestelmän tekemän junan nopeuslaskelman perusteella kuljettaja ja kalustoyksikössä oleva ETCS-osajärjestelmä voivat valvoa, ettei juna ylitä sallittua nopeutta. RAC-TS:ää sovelletaan junan nopeuden arviointiin kalustoyksikössä olevilla järjestelmillä, koska:

(i) muita (välittömiä) lisäesteitä ei ole, sillä myös kuljettajalle toimitettu tieto arvioidaan;
(ii) junan ylinopeus saattaa suistaa junan raiteilta, ja tällainen onnettomuus voi johtaa tuhoisiin seurauksiin.

(2) ”tarjoaa kuljettajalle tietoa, jonka avulla hän voi ohjata junaa turvallisesti ja käyttää jarrujärjestelmää sallitun kulkuluvan rikkomistapauksessa”;

(b) raidevirtapiirin esimerkki: ”havaitsee raideosuuden käytön”. RAC-TS:ää voidaan soveltaa sellaisenaan tähän toimintoon ainoastaan, jos lukituksessa ei ole toteutettu ”sekvenssivalvonta”-toimintoa;
(c) esimerkki pisteestä: ”valvo pisteen sijaintia)”.

A.3.5.5. Joissakin standardeissa määritellään myös toimintoja, joihin RAC-TS:ää saatetaan soveltaa. Esimerkiksi

(a) standardin prEN 0015380-4 {Ref. 13} (ModTrain Work) normatiivisessa osassa määritetään kolme hierarkkista toimintotasoa (informatiivisissa liitteissä tasoja mainitaan viisi). Kaiken kaikkiaan standardissa prEN 0015380-4 määritellään useita satoja juniin liittyviä toimintoja;
(b) yleisesti on suositeltavaa valita toiminnot standardin prEN 0015380-4 kolmelta ensimmäiseltä tasolta (ei alemmilta tasoilta) ja ottaa tässä yhteydessä huomioon myös tuotteen jaottelua koskevan rakenteen;
(c) standardin prEN 0015380-4 soveltamisalan ulkopuolisten toimintojen asianmukainen toimintotaso on määritettävä asiantuntija-arvioon perustuvassa vertailussa.

Viraston on vielä käsiteltävä näitä standardin prEN 0015380-4:n toimintoesimerkkejä työstäessään yleisesti hyväksyttyjä riskejä ja riskitasoa koskevia perusteita.

A.3.5.6. RAC-TS:ää sovelletaan myös esimerkiksi standardin prEN 0015380-4:n seuraavaan toimintoon: *”kallistuman valvonta”* (koodi = CLB). Toimintoa voidaan käyttää järjestelmän tasolla kahdella tavalla:

(a) Ensimmäinen tapaus: junan on kallistuttava mutkissa matkustusmukavuuden vuoksi, ja on valvottava, että junan ulottuma on radan infrastruktuurin mukainen.
(b) Toinen tapaus: junan on kallistuttava mutkissa ainoastaan matkustajamukavuuden vuoksi, eikä tarpeen ole valvoa, että junan ulottuma vastaa radan infrastruktuuria.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

Ensimmäisessä tapauksessa RAC-TS:ää sovelletaan, mutta toisessa sitä ei sovelleta, koska kallistumatoiminnon vika ei johda tuhoisiin seurauksiin.

A.3.5.7. A.3.5.4. kohdan esimerkki b ja lisäyksessä A olevassa A.3.5.6. kohdassa esitetyt esimerkit osoittavat selvästi, ettei toiminnoista, joihin RAC-TS:ää kaikissa tapauksissa sovelletaan, voida laatia ennalta määriteltyä luetteloa. Soveltaminen riippuu aina siitä, miten näitä osajärjestelmän toimintoja käytetään järjestelmässä.

A.3.5.8. Esimerkki RAC-TS:n soveltamisesta esitetään liitteessä C olevassa C.15. kohdassa.

A.3.6. Esimerkit RAC-TS:n soveltamisesta

A.3.6.1. Johdanto

(a) tässä kohdassa esitetään esimerkkejä, miten muiden vaaratilanteiden vikataajuus voidaan määrittää ja miten voidaan johtaa arvoa $10^{-9}\,h^{-1}$ väljempiä turvallisuusvaatimuksia. Tässä asiakirjassa ei suosita eikä kehoteta käyttämään mitään tiettyä menetelmää. Tässä ainoastaan annetaan tiedoksi, miten RAC-TS:ää voidaan soveltaa joidenkin laajasti käytettyjen menetelmien kalibroinnissa. Tätä näkökohtaa on kehitettävä edelleen yleisesti hyväksyttävien riskien ja hyväksyttävää riskitasoa koskevien perusteiden alalla tehtävillä viraston toimilla.

(b) RAC-TS:ää voidaan itse asiassa soveltaa vain hyvin harvoissa tapauksissa, koska käytännössä vain muutamat teknisen järjestelmän toimintaviat johtavat suoraan onnettomuuksiin, joiden seuraukset voivat olla tuhoisia. Jotta perustetta voidaan soveltaa vaaroihin, joiden seuraukset eivät ole tuhoisia, ja jotta voidaan määrittää vikataajuutta koskeva tavoite, eri parametrien, kuten vakavuuden vs. esiintymistiheyden välillä voidaan siten määrittää vaihtosuhteita (trade-offs) (esimerkiksi kalibroimalla tähän perusteeseen perustuva riskimatriisi).

A.3.6.2. Esimerkki 1: Riskin välitön vaihtosuhde

(a) RAC-TS:ää voidaan sovetaa helposti skenaarioihin, jotka eroavat ainoastaan muutamalla riippumattomalla parametrilla YTM-asetuksen {Ref. 3} 2.5.4. kohdassa määritellyistä RAC-TS:n viite-ehdoista.

(b) Oletetaan, että tietylle parametrille p riskisuhde on moninkertaistava. Oletetaan, että p* sisältyy viite-ehtoon, kun taas vaihtoehtoisessa skenaariossa voidaan soveltaa p‘:tä. Tässä tapauksessa merkityksellinen on ainoastaan parametrisuhde p*/p’, ja esiintymistiheyttä voidaan pienentää. Tämä menettely voidaan toistaa, jos parametrit ovat riippumattomia.

(c) Esimerkki:

(1) Oletetaan, että asiantuntija-arvion mukaan tuhoisan seurauksen todellinen esiintymistodennäköisyys on kymmenen kertaa pienempi kuin YTM-asetuksen {Ref. 3} 2.5.4 kohdan viite-ehtojen mukainen todennäköisyys. Turvallisuusvaatimus on tällöin $10^{-8}\,h^{-1}$ eikä $10^{-9}\,h^{-1}$.

(2) Oletetaan, että toisella teknisellä järjestelmällä on (seurauksista riippumaton) lisäturvallisuuseste, joka on tehokas 50 prosentissa tapauksista.

(3) Turvallisuusvaatimus on tällöin $5*10^{-7}\,h^{-1}$ (toisin sanoen $0{,}5*10^{-8}\,h^{-1}$) eikä $10^{-9}\,h^{-1}$.

A.3.6.3. Esimerkki 2: Riskimatriisin kalibrointi

(a) Jotta RAC-TS:ää voidaan käyttää asianmukaisesti riskimatriisissa, matriisin on koskettava oikeaa järjestelmätasoa (joka on verrattavissa lisäyksessä A olevassa A.3.5. kohdassa mainittuun tasoon).

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(b) RAC-TS määrittelee yhden riskimatriisin kentän siedettäväksi, eli se vastaa koordinaattia (tuhoisa seuraus, esiintymistiheys $10^{-9}\,h^{-1}$): katso taulukon 5 punainen kenttä. Kaikki suurempaan esiintymistiheyteen liittyvät kentät on merkittävä ”sietämättömiksi”. On pantava myös merkille, että ainoastaan tapauksessa, joka voi uskottavasti ja suoraan johtaa tuhoisaan seuraukseen, onnettomuuksien esiintymistiheys on sama kuin toimintavikojen esiintymistiheys.

(c) Tämän jälkeen voidaan täyttää matriisin muut kentät, mutta riskien välttämisen tai luokkien porrastamisen kaltaiset vaikutukset on otettava huomioon. Yksinkertaisimmassa tapauksessa, jossa porrastaminen tehdään lineaarisesti ja dekadisesti (kuvattu taulukossa 5 nuolella), kenttä, joka voidaan merkitä RAC-TS:n perusteella ”hyväksyttäväksi”, ekstrapoloidaan lineaarisesti matriisin muihin kenttiin. Tämä tarkoittaa, että kaikki saman rivin (tai rivin alapuolen) kentät saavat niin ikään merkinnän ”hyväksyttävä”. Myös alapuoliset kentät voidaan merkitä ”hyväksyttäviksi”.

Taulukko 5: Tyyppiesimerkki kalibroidusta riskimatriisista

(Vaaran aiheuttaman) onnettomuuden esiintymistiheys	**Riskitaso**			
Yleinen (10^{-4} tunnissa)	**Sietämätön**	**Sietämätön**	**Sietämätön**	**Sietämätön**
Todennäköinen (10^{-5} tunnissa)	**Sietämätön**	**Sietämätön**	**Sietämätön**	**Sietämätön**
Satunnainen (10^{-6} tunnissa)	**Hyväksyttävä**	**Sietämätön**	**Sietämätön**	**Sietämätön**
Vähäinen (10^{-7} tunnissa)	**Hyväksyttävä**	**Hyväksyttävä**	**Sietämätön**	**Sietämätön**
Epätodennäköinen (10^{-8} tunnissa)	**Hyväksyttävä**	**Hyväksyttävä**	**Hyväksyttävä**	**Sietämätön**
Ei uskottava (10^{-9} tunnissa)	**Hyväksyttävä**	**Hyväksyttävä**	**Hyväksyttävä**	**Hyväksyttävä**
	Merkityksetön	Marginaalinen	Kriittinen	Tuhoisa
	Vaaran seurauksien (eli onnettomuuksien) turvallisuustasot			

(d) Kun matriisi on täytetty, sitä voidaan soveltaa myös vaaroihin, joiden seuraukset eivät ole tuhoisia. Jos esimerkiksi jonkin tällaisen toimintavian vakavuus luokitellaan ”kriittiseksi”, kalibroidun riskimatriisin perusteella onnettomuuksien sallittu taajuus voi olla enintään ”epätodennäköinen” (tai jopa vähemmän).

(e) On pantava merkille, että riskimatriisin käyttö saattaa johtaa ylivarovaisiin tuloksiin, kun sitä sovelletaan toimintavikojen esiintymistiheyksiin (kuten toimintavikoihin, jotka eivät voi johtaa suoraan onnettomuuksiin).

A.3.6.4. Muiden riskinarviointimenetelmien kalibrointiperiaate

Myös muita riskinarviointimenetelmiä, esimerkiksi ehdotettu riskiprioritettiin perustuva järjestelmä taikka VDV-standardin 331 tai IEC-standardin 61508 mukainen riskikaavio, voidaan kalibroida vastaavalla menetelmällä kuin riskimatriisi:

(a) Ensimmäinen vaihe: luokittele RAC-TS:n viitearvo siedettäväväksi ja suuremman esiintymistiheyden tai suuremman vakavuuden omaavat arvot sietämättömiksi RAC-TS:iksi.

(b) Toinen vaihe: käytä kyseessä olevan menetelmän vaihtosuhdemenetelmiä (trade off) riskin siedettävyyden ekstrapoloimiseksi vaaroihin, joiden seuraukset eivät ole tuhoisia (käytä lähtökohtana lineaarista riskin vaihtosuhdetta).

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(c) Kolmas vaihe: niiden vaarojen osalta, joiden seuraukset eivät ole tuhoisia, RAC-TS voidaan tämän jälkeen johtaa kalibroidun riskinarviointimenetelmän avulla vertaamalla koordinaattia (esiintymistiheys, vakavuus) näin saatuun FN-käyrään.

A.3.7. RAC-TS:ää koskevat päätelmät

A.3.7.1. YTM:n asetuksen mukaisessa yleisessä riskinarvioinnissa hyväksyttävää riskitasoa koskevia perusteita tarvitaan, jotta voidaan määrittää, milloin riski(e)n jäännöstasosta tulee hyväksyttävä ja milloin näin ollen eksplisiittinen riskin estimointi voidaan lopettaa.

A.3.7.2. RAC-TS (10^{-9} h^{-1}) on teknisten järjestelmien suunnittelutavoite.

A.3.7.3. RAC-TS:n tärkeimmät tavoitteet ovat:

(a) vahvistaa hyväksyttävän riskitason yläraja ja tämän perusteella viitearvo, jonka avulla teknisten järjestelmien riskinarviointimenetelmät voidaan kalibroida;
(b) mahdollistaa teknisten järjestelmien vastavuoroinen tunnustaminen, sillä riskinarvioinnit ja turvallisuusarvioinnit tehdään saman hyväksyttävää riskitasoa koskevan perusteen mukaisesti kaikissa jäsenvaltioissa;
(c) säästää kustannuksissa, sillä RAC-TS ei edellytä tarpeettoman korkeita kvantitatiivisia turvallisuusvaatimuksia;
(d) edistää valmistajien välistä kilpailua. Erilaisten hyväksyttävää riskitasoa koskevien perusteiden käyttö joko hakijan tai jäsenvaltion osalta johtaisi siihen, että teollisuuden olisi osoitettava teknisten järjestelmiensä vaatimustenmukaisuus useilla erilaisilla tavoilla. Tämä vaarantaisi valmistajien kilpailukyvyn ja tekisi tuotteista tarpeettoman kalliita.

A.3.7.4. Teknisten järjestelmien osalta on aina osoitettava, että RAC-TS:ään sisältyvä semikvantitatiivinen vaatimus täyttyy. YTM-asetuksen nojalla RAC-TS:ää on sovellettava ainoastaan teknisiin järjestelmiin, joiden tunnistettuja vaaroja ei voida hallita asianmukaisesti soveltamalla menettelyohjeita tai vertaamalla niitä muihin vastaaviin ohjeistoihin. Näin voidaan asettaa alhaisempia turvallisuusvaatimuksia, kunhan yleinen turvallisuustaso voidaan säilyttää.

A.3.7.5. Teknisten järjestelmien hyväksyttävää riskitasoa koskevaa yhtenäistettyä semikvantitatiivista perustetta tarvitaan vain, jollei menettelyohjeita tai ohjeistojavoida käyttää.

A.3.7.6. Koska järjestelmällisten vikojen/virheiden turvallisuuden eheystason on oltava vähintään SIL 4, teknisten järjestelmien satunnaisten laitteistovikojen turvallisuuden eheystason on niin ikään oltava vähintään SIL 4. Tämä vastaa suurinta siedettävää vaaratasoa (THR eli varmuusvikataajuus) 10^{-9} h^{-1}. CENELEC-standardin 50 129 mukaan tiukempia turvallisuusvaatimuksia ei voida saavuttaa pelkästään yhdellä järjestelmällä; järjestelmän rakennetta on muutettava, ja on esimerkiksi käytettävä kahta järjestelmää, mikä väistämättä lisää radikaalisti teknisen järjestelmän kustannuksia. Katso lisätietoja lisäyksessä A olevasta A.3.1. kohdasta.

A.3.7.7. Lisäyksessä A olevassa A.3.6. kohdassa kuvataan, miten RAC-TS:ää voidaan käyttää viitearvona kalibroitaessa tiettyjä riskinarviointimenetelmiä, kun teknisistä järjestelmistä mahdollisesti aiheutuvat seuraukset eivät ole tuhoisia.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

A.4. Turvallisuusarviointiin perustuva näyttö

A.4.1. Tässä kohdassa opastetaan, mitä näyttöä arviointielimelle yleensä toimitetaan riippumatonta arviointia ja turvallisuushyväksynnän saamista varten; tämä ei kuitenkaan rajoita jäsenvaltion kansallisten vaatimusten soveltamista. Tätä kohtaa voidaan käyttää tarkastuslistana, jonka avulla varmistetaan, että kaikki asiaan liittyvät merkitykselliset näkökohdat on otettu huomioon ja dokumentoitu YTM-asetuksen soveltamisen yhteydessä.

A.4.2. Turvallisuussuunnitelma: CENELEC kehottaa laatimaan turvallisuussuunnitelman hankkeen alussa tai, jos tämä ei ole hankkeessa luontevaa, sisällyttämään asiaa koskevan kuvauksen johonkin muuhun merkitykselliseen asiakirjaan. Jos arviointielimet nimitetään hankkeen alussa, turvallisuussuunnitelmalle on hankittava myös niiden lausunto. Lähtökohtaisesti turvallisuussuunnitelmassa kuvataan

(a) käyttöön otettu organisaatio ja kehityksessä ja riskinarvioinnissa mukana olevan henkilöstön pätevyys
(b) kaikki turvallisuuteen liittyvät toimenpiteet, joita suunnitellaan toteutettaviksi hankkeen eri vaiheissa sekä odotettavissa olevat tulokset.

A.4.3. Järjestelmän määrittelyvaiheessa vaadittava näyttö:

(a) järjestelmäkuvaus:
    (1) järjestelmän käyttöalan/rajojen kuvaus
    (2) toimintojen kuvaus
    (3) järjestelmärakenteen kuvaus
    (4) toiminta- ja ympäristöolosuhteiden kuvaus;
(b) ulkoisten rajapintojen kuvaus;
(c) sisäisten rajapintojen kuvaus;
(d) elinkaaren vaiheiden kuvaus;
(e) turvallisuusperiaatteiden kuvaus;
(f) riskinarvioinnin rajat määrittävien oletusten kuvaus.

A.4.4. Jotta riskinarviointi voidaan tehdä, järjestelmämäärittelyssä otetaan huomioon suunnitellun muutoksen asiayhteys:

(a) jos suunnitellulla muutoksella muutetaan olemassa olevaa järjestelmää, järjestelmämäärittelyssä on kuvattava sekä järjestelmä ennen muutosta että suunniteltu muutos;
(b) jos suunnitellun muutoksen avulla on tarkoitus rakentaa uusi järjestelmä, kuvauksessa ainoastaan määritellään järjestelmä, sillä kuvausta olemassa olevasta järjestelmästä ei ole saatavilla.

A.4.5. Vaarojen tunnistamisvaiheessa vaadittava näyttö:

(a) vaarojen tunnistamismenetelmien ja -välineiden kuvaus ja perustelut (mukaan lukien rajoitukset) (ylhäältä alas -menetelmä, alhaalta ylös -menetelmä, HAZOP-menetelmä jne.);
(b) tulokset:
    (1) vaarojen luettelo
    (2) järjestelmän (rajat) vaarat
    (3) osajärjestelmän vaarat
    (4) rajapinnan vaarat
    (5) turvallisuustoimenpiteet, jotka voidaan yksilöidä tässä vaiheessa.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

A.4.6. Seuraava näyttö vaaditaan myös riskinarviointivaiheesta:

(a) Kun menettelyohjeita käytetään vaarojen valvonnassa, on osoitettava, että arvioitava järjestelmä täyttää kaikki menettelyohjeiden asiaa koskevat vaatimukset. Tässä yhteydessä on osoitettava, että asiaa koskevia menettelyohjeita sovelletaan oikein.

(b) Kun vastaavia ohjeistoja käytetään vaarojen valvonnassa:

(1) on määritettävä merkityksellisten ohjeistojen turvallisuusvaatimukset arvioitavan järjestelmän osalta;
(2) on osoitettava, että arvioitavaa järjestelmää käytetään samoissa toiminta- ja ympäristöristöolosuhteissa kuin merkityksellistä ohjeistoa. Jos tätä ei voida osoittaa, on osoitettava, että poikkeamat ohjeistosta arvioidaan asianmukaisesti;
(3) on esitettävä näyttö siitä, että ohjeistojen turvallisuusvaatimukset pannaan asianmukaisesti täytäntöön arvioitavassa järjestelmässä.

(c) Kun eksplisiittistä riskin estimointia käytetään vaarojen hallinnassa:

(1) on esitettävä riskinarviointimenetelmien ja -välineiden (kvalitatiivinen, kvantitatiivinen tai semikvantitatiivinen analyysi, muu kuin regressioanalyysi jne.) kuvaus ja perustelut (mukaan luettuina rajoitukset);
(2) on yksilöitävä kunkin vaaran olemassa olevat turvallisuustoimenpiteet ja riskiä vähentävät tekijät (mukaan luettuina inhimilliset tekijät);
(3) on evaluoitava ja luokiteltava riski kunkin vaaran osalta:

(i) vaaran seurauksien estimointi ja perustelut (sisältää oletukset ja olosuhteet)
(ii) vaaran esiintymistiheyden estimointi ja perustelut (sisältää oletukset ja olosuhteet)
(iii) vaarojen luokittelu niiden kriittisyyden ja esiintymistiheyden perusteella;

(4) on yksilöitävä asianmukaiset lisäturvallisuustoimenpiteet, joiden avulla kunkin vaaran riskeistä tulee hyväksyttäviä (riskin evaluointivaiheen jälkeinen toistuva prosessi).

A.4.7. Riskin evaluoinnista vaadittu näyttö:

(a) Kun toteutetaan eksplisiittinen riskin estimointi:

(1) kunkin vaaran riskinarviointiperusteiden määrittely ja perustelut
(2) on osoitettava ja esitettävä perustelut sille, että turvallisuustoimenpiteet ja turvallisuusvaatimukset kattavat kaikki vaarat hyväksyttävän tason mukaisesti (edellä mainitun riskinarviointiperusteen mukaisesti);

(b) YTM-asetuksen 2.3.5 ja 2.4.3 kohdan nojalla menettelyohjeita soveltamalla ja vastaaviin ohjeistoihin vertaamalla katettuja riskejä pidetään implisiittisesti hyväksyttävinä edellyttäen, että (katso kaavion 1 pisteympyrä):

(1) 2.3.2 kohdan mukaiset käyttöohjeiden soveltamisedellytykset täytetään
(2) 2.4.2 kohdan mukaiset ohjeiston käyttöä koskevat edellytykset täytetään.

Riskinarviointiperusteet ovat implisiittisiä näille kahdelle hyväksyttävää riskitasoa koskevalle periaatteelle.

A.4.8. Vaarojen hallintaa koskeva näyttö:

(a) kaikkien vaarojen ja seuraavien tietojen kirjaaminen vaaroja koskevaan asiakirjaan:

(1) tunnistettu vaara
(2) turvallisuustoimenpiteet, jotka estävät vaaran esiintymisen tai lieventävät sen seurauksia
(3) toimenpiteiden turvallisuusvaatimukset
(4) järjestelmän merkityksellinen osa

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(5) turvallisuustoimenpiteistä vastaava toimija
(6) vaaran tila (esim. avoinna, ratkaistu, poistettu, siirretty, hallittu jne.)
(7) kirjaamisen, tarkistamisen ja valvonnan päivämäärä kunkin vaaran osalta;

(b) kuvaus siitä, miten vaaroja hallitaan tehokkaasti koko elinkaaren aikana;
(c) kuvaus tiedonvaihdosta vaarojen rajapinnoilla olevien osapuolten välillä ja vastuunjaosta.

A.4.9. Riskinarvioinnin ja arviointiprosessin laatua koskeva näyttö:

(a) prosessiin osallistuvien henkilöiden ja heidän pätevyytensä kuvaus
(b) eksplisiittisten riskin estimointien osalta prosessissa käytettyjen tietojen, aineiston ja tilastojen kuvaus ja niiden asianmukaisuutta koskevat perustelut (esimerkiksi käytettyä tietoa koskeva herkkyystutkimus).

A.4.10. Turvallisuusvaatimusten mukaisuuden osoittaminen:

(a) käytettyjen standardien luettelo
(b) suunnittelun ja toimintaperiaatteiden kuvaus
(c) näyttö korkeatasoisen turvallisuusjärjestelmän soveltamisesta hankkeessa: katso 1.1.2 kohtaa koskeva G 3 kohta;
(d) turvallisuusarviointikertomusten yhteenveto (kuten vaarojen syiden arviointi), joka osoittaa turvallisuusvaatimusten täyttymisen
(e) vaarojen syiden arvioinnissa käytettyjen menetelmien ja välineiden (FMECA- ja FTA-analyysi jne.) kuvaus ja perustelut
(f) turvallisuuden tarkistamista ja vahvistamista koskevien testien yhteenveto.

A.4.11. Turvallisuusarvio: CENELEC suosittaa, että edellä mainittu näyttö ryhmitellään uudelleen ja että siitä laaditaan yhteenveto yhteen asiakirjaan, joka toimitetaan arviointielimelle: katso 5.1 kohtaa koskevat G 4 ja G 5 kohta.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

LISÄYS B: ESIMERKKEJÄ RISKINARVIOINTIPROSESSIA TUKEVISTA TEKNIIKOISTA JA VÄLINEISTÄ

B.1. Esimerkkejä YTM-asetuksen soveltamisalaan kuuluvassa riskinarvioinnissa käytettävistä menetelmistä ja välineistä on ohjeen EN 50126-2 {Ref. 9} liitteessä E. Yhteenveto tekniikoista ja välineistä esitetään taulukossa E.1. Taulukossa kuvataan kaikki tekniikat, ja tarvittaessa ohjataan hakemaan lisätietoa muista standardeista.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

LISÄYS C: ESIMERKKEJÄ

C.1. Johdanto

C.1.1. Tämän lisäyksen tarkoituksena on helpottaa tämän asiakirjan lukemista. Lisäyksessä esitetään yhteenveto kootuista esimerkeistä, millä pyritään helpottamaan YTM-asetuksen soveltamista.

C.1.2. Riskinarviointien ja turvallisuusarviointien esimerkit, jotka esitetään tässä lisäyksessä, eivät perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä ne toteutettiin ennen YTM-asetusta. Esimerkit voidaan luokitella seuraavasti:

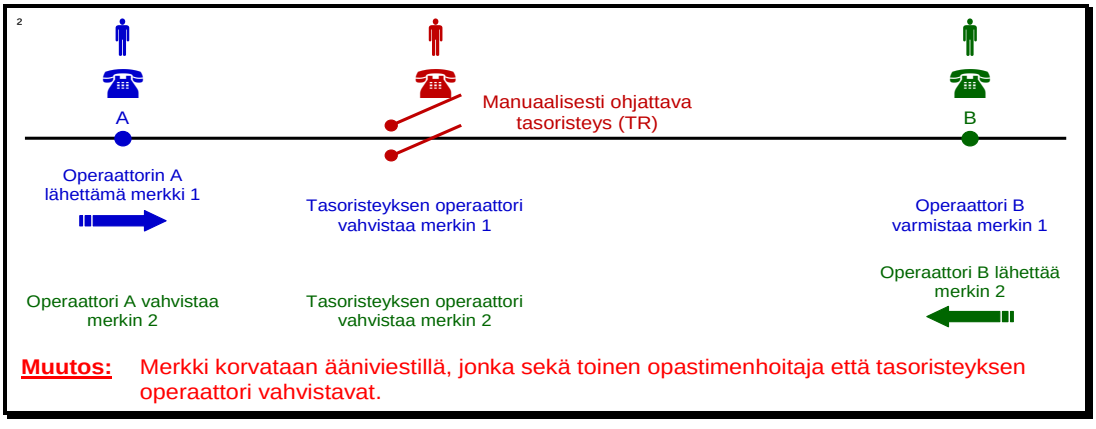
(a) esimerkit, joissa viitataan niiden alkuperään, on saatu YTM-työryhmän asiantuntijoilta
(b) esimerkit, joiden alkuperäviittaukset on tarkoituksella jätetty pois, on niin ikään saatu YTM-työryhmän asiantuntijoilta. Asiantuntijat pyysivät, että alkuperä säilyy luottamuksellisena
(c) esimerkit, joiden alkuperää ei mainita, laati viraston henkilöstö aiemman ammatillisen kokemuksensa perusteella.

Kunkin esimerkin osalta selvitetään, mikä on sovelletun prosessin ja YTM-asetuksen edellyttämän prosessin välinen suhde, sekä esitetään YTM:n (mahdollisesti) edellyttämiä lisätoimia koskevat perustelut ja lisäarvo.

C.2. Esimerkkejä 4 artiklan 2 kohdassa tarkoitettua merkittävää muutosta koskevien perusteiden soveltamisesta

C.2.1. Virasto työstää parhaillaan määritelmää siitä, mitä voidaan pitää ”merkittävänä muutoksena”. Tässä kappaleessa esitetään yksi esimerkki meneillään olevan työn tuloksista eli siitä, miten 4 artiklan 2 kohdan perusteita sovelletaan.

C.2.2. Manuaalisesti ohjatun tasoristeyksen muutoksen yhteydessä muutetaan opastimenhoitajien tapaa välittää tieto saapuvan junan suunnasta tasoristeyksen ihmisoperaattorille. Muutos esitetään kaaviossa 15.



Kaavio 15: Esimerkki muutoksesta, joka ei ole merkittävä Puhelinviesti tasoristeyksen valvomiseksi.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.2.3. Olemassa oleva järjestelmä: ennen kuin suunniteltu muutos tehtiin, saapuvan junan suuntaa koskeva tieto välitettiin automaattisesti puhelimen sointiäänen avulla tasoristeyksen operaattorille. Sointiääni oli erilainen riippuen siitä, mistä puhelu tuli.

C.2.4. Suunniteltu muutos: käytössä olleesta puhelinjärjestelmästä oli tulossa vanhanaikainen, ja se oli korvattava uudella digitaalisella järjestelmällä, minkä vuoksi teknisesti merkityksellistä tietoa ei enää voitu välittää puhelimen sointiäänen avulla. Uudessa järjestelmässä sointiääni on täsmälleen sama riippumatta siitä, keneltä opastimenhoitajalta puhelu tulee. Tämän vuoksi kyseinen toiminto päätettiin hoitaa seuraavan toimintamenettelyn avulla:

(a) Junan lähtiessä opastimenhoitaja ilmoittaa suullisesti tasoristeyksen operaattorille saapuvan junan suunnan.
(b) Tieto varmistetaan aikataulusta, ja sekä tasoristeyksen operaattori että muut opastimenhoitajat varmistavat tiedon, jotta operaattorin väärinymmärrys voidaan välttää.

Suunniteltu muutos ja siihen liittyvä toimintamenettely kuvataan kaaviossa 15.

C.2.5. Vaikka muutoksella näyttää olevan mahdollisia turvallisuusvaikutuksia (riski siitä, ettei tasoristeyksen puomia suljeta ajoissa), muut 4 artiklan 2 kohtaan sisältyvät perusteet, kuten:

(a) alhainen monimutkaisuusaste
(b) alhainen innovatiivisuusaste, ja
(c) helppo valvonta

voivat viitata siihen, ettei suunniteltu muutos ole merkittävä.

C.2.6. Tässä esimerkissä jonkinlainen turvallisuusarviointi tai perustelut ovat kuitenkin tarpeen, jotta voidaan osoittaa, että turvallisuuden kannalta kriittisessä tehtävässä, jossa vanha tekninen järjestelmä korvataan toimintamenettelyllä (henkilöstö ristiintarkastaa toisensa), ylläpidetään sama turvallisuustaso. On selvitettävä, edellyttäisikö tämä yhteisen turvallisuusmenetelmän täysimääräistä soveltamista, johon kuuluu muun muassa vaarojen kirjaaminen ja arviointielimen toteuttama riippumaton arviointi. Tässä tapauksessa on kuitenkin kyseenalaista, olisiko tästä mitään lisäarvoa, mikä viittaa siihen, ettei kyseistä muutosta voida pitää merkittävänä.

C.3. Esimerkkejä rautatiealan toimijoiden välisistä rajapinnoista

C.3.1. Alla on muutamia esimerkkejä rautatiealan toimijoiden välisistä rajapinnoista ja yhteistyöperusteista:

(a) Infrastruktuurin haltija – Infrastruktuurin haltija: molemmissa infrastruktuureissa määrätään turvallisuustoimenpiteistä, joilla varmistetaan junien turvallinen siirtyminen yhdestä infrastruktuurista toiseen
(b) Infrastruktuurin haltija – Rautatieyritys: käytössä saattaa olla infrastruktuuriperusteisia erityisiä toimintasääntöjä, joita junan kuljettaja on noudatettava;
(c) Infrastruktuurin haltija – Valmistaja: valmistajien osajärjestelmillä saattaa olla käyttörajoituksia, joita infrastruktuurin haltijan on noudatettava
(d) Infrastruktuurin haltija – Palveluntarjoaja: käytössä saattaa olla erityisiä infrastruktuurin kunnossapitorajoituksia, joita kunnossapitotoimia tekevien alihankkijoiden on noudatettava
(e) Rautatieyritys – Valmistaja: valmistajan osajärjestelmillä saattaa olla käyttörajoituksia, joita rautatieyrityksen on noudatettava

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(f) Rautatieyritys – Palveluntarjoaja: käytössä saattaa olla erityisiä infrastruktuurin kunnossapitorajoituksia, joita kunnossapidon alihankkijan on noudatettava

(g) Rautatieyritys – Kalustoyksikköjen haltijat: käytössä saattaa olla kalustoyksikkökohtaisia käyttörajoituksia, joita kyseisiä kalustoyksikköjä käyttävän rautatieyrityksen on noudatettava

(h) Valmistaja – Valmistaja: turvallisuuteen liittyviä teknisiä rajapintoja hallitaan kahdella eri valmistajan osajärjestelmällä

(i) Valmistaja – Palveluntarjoaja: valmistaja hallinnoi vaaroja koskevaa asiakirjaa silloin, kun työ teetetään alihankintana yrityksellä, joka on niin pieni, ettei sillä ole kyseisen hankkeen edellyttämää turvallisuusorganisaatiota

(j) Palveluntarjoaja – Palveluntarjoaja: vastaava esimerkki kuin edellä j kohdassa.

C.3.2. Palveluntarjoajat toteuttavat kaikki infrastruktuurin haltijan tai rautatieyrityksen tai valmistajan alihankintana tilaamat toiminnot, kuten kunnossapidon, lipunmyynnin ja suunnittelupalvelut.

C.3.3. Seuraava esimerkki esitetään rajapintojen hallinnan ja siihen liittyvän vaarojen yksilöinnin havainnollistamiseksi. Esimerkki koskee junan valmistajan ja hakijan (rautatieyritys) välistä rajapintaa. Siinä kuvataan, miten 1.2.1 kohtaa koskevassa G 3 kohdassa vaaditut keskeiset perusteet voidaan täyttää:

(a) Johtajaminen: hakija (rautatieyritys);

(b) Panokset:

(1) vastaaviin hankkeisiin perustuva(t) vaaraluettelo(t)
(2) kaikkien rajanpinnan panosten ja tuotosten (P/T) kuvaus, mukaan lukien suorituksen erityispiirteet;

(c) Menetelmät: katso ohjeen EN 50 126-2 {Ref. 9} liite A.2

(d) Vaaditut osanottajat:

(1) hakijan (rautatieyritys) turvallisuusjohtaja
(1) junan valmistajan turvallisuusjohtaja
(2) junan hakijan suunnittelujohtaja
(3) junan valmistajan suunnittelujohtaja
(4) junan hakijan kunnossapitohenkilöstö (osin P/T-analyysista riippuen)
(5) junan kuljettajat (osin P/T-analyysista riippuen);

(e) Tuotokset:

(1) yhteisesti hyväksytty kertomus tunnistetuista vaaroista
(2) vaaroja koskevaan asiakirjaan liittyvät turvallisuustoimenpiteet ja vastuiden selkeä kuvaus.

C.4. Esimerkkejä yleisesti hyväksyttävien riskien määrittelyä koskevista menetelmistä

C.4.1. Johdanto

C.4.1.1. Yleisesti hyväksyttävät riskit määritellään YTM-asetuksessa riskeiksi, jotka ovat *”niin pieniä, ettei (riskin pienentämiseksi edelleen) ole järkevää toteuttaa lisäturvallisuustoimenpiteitä”*. Mikäli vaarojen aiheuttama riskitaso määritetään yleisesti hyväksyttäväksi vaaran tunnistamisvaiheessa, näitä vaaroja ei voida arvioida syvällisemmin riskinarviointiprosessissa. Edellä lainattu yleisesti hyväksyttäviä riskejä koskeva määritelmä

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

on jossain määrin tulkinnanvarainen. Tämän vuoksi asetuksessa todetaan, että asiantuntijoiden tehtävänä on luokitella vaarat, joiden riskit ovat yleisesti hyväksyttäviä.

C.4.1.2. On vaikeaa määritellä yhteisesti tätä tarkempaa yleisesti hyväksyttävän riskitason perustetta, jota voitaisiin soveltaa kaikilla mahdollisilla järjestelmätasoilla, joilla kyseessä olevia vaaroja saatetaan tunnistaa, ja jossa otettaisiin huomioon myös erilaiset riskin välttämistekijät, joita sovelluksissa voi olla. Koska on kuitenkin tärkeää varmistaa, että asiantuntijoiden arviot ovat helppotajuisia ja jäljitettäviä, on hyödyllistä antaa joitakin ohjeita siitä, miten yleisesti hyväksyttävä riskitaso määritellään. Perusteet yleisesti hyväksyttävän riskitason määrittelemiseksi voivat olla kvantitatiivisia, kvalitatiivisia tai semikvalitatiivisia. Alla on muutamia esimerkkejä siitä, miten voidaan määrittää yleisesti hyväksyttävän riskitason kvantitatiivista tai semikvantitatiivista arviointia koskevat perusteet.

C.4.1.3. Alla olevat esimerkit havainnoillistavat kyseistä periaatetta. Esimerkit ovat peräisin julkaisusta *"Die Gefährdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal + Draht (100) 9/2008.*

C.4.2. Kvantitatiivisten perusteiden johtaminen

C.4.2.1. Yleisesti hyväksyttävät riskit voidaan määritellä siten, että ne kattavat riskit, jotka ovat paljon pienempiä kuin tietyn vaaraluokan hyväksyttävät riskit. Tilastotietojen avulla voi olla mahdollista laskea, mikä on rautatiejärjestelmien tämänhetkinen riskitaso, ja siten todeta, että laskettu taso on hyväksyttävä. Kun tätä tasoa kuvaava luku jaetaan vaarojen lukumäärällä (N) (mielivaltaisesti voidaan esimerkiksi olettaa, että rautatiejärjestelmässä on noin N = 100 vaarojen pääluokkaa), saadaan kunkin vaaraluokan hyväksyttävä riskitaso. Tämän jälkeen voidaan todeta, että vaaran, johon liittyy riski, joka on kaksi suuruusluokkaa pienempi kuin hyväksyttävä vaarakohtainen riskitaso (tämä on 2.2.3 kohtaa koskevan G 1 kohdan parametri x %), katsotaan olevan yleisesti hyväksyttävällä riskitasolla.

C.4.2.2. On kuitenkin tarkistettava, etteivät kaikki hyväksyttävälle riskitasolle luokitellut vaarat yhdessä ylitä järjestelmätason kokonaisriskille määritettyä suhdetta (esim. y %): katso 2.2.3 kohta ja 2.2.3 kohtaa koskeva G 2 kohta.

C.4.3. Yleisesti hyväksyttävien riskien arviointi

C.4.3.1. Edellä olevissa esimerkeissä määritettyjä yleisesti hyväksyttävän riskitason raja-arvoja voidaan käyttää kalibroitaessa kvalitatiivisia välineitä, kuten riskimatriiseja, riskikaaviota tai riskiprioriteetteja, mikä auttaa asiantuntijoita päättämään, luokitellaanko riskit yleisesti hyväksyttäviksi. On tärkeää korostaa, että kvantitatiivisten arvojen käyttö yleisesti hyväksyttävän riskitason perusteina ei tarkoita, että tarpeen on tehdä täsmällinen riskin estimointi tai riskinarviointi, ennen kuin voidaan päättää, onko riski yleisesti hyväksyttävällä riskitasolla. Näin tapahtuu tehtäessä vaaran tunnistamisvaiheessa karkea arvio asiantuntijoiden arvion perusteella.

C.4.3.2. Lisäksi on tärkeää tarkistaa, että kaikkien sellaisten vaarojen yhteisvaikutus, joihin liittyy yleisesti hyväksyttävällä riskitasolla olevia riskejä, ei ylitä järjestelmätason kokonaisriskille määritettyä suhdetta (esim. y %): katso 2.2.3 kohta ja 2.2.3 kohtaa koskeva G 2 kohta.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.5. Riskinarviointiesimerkki: merkittävä organisatorinen muutos

C.5.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.5.2. Esimerkki koskee organisatorista muutosta. Hakija piti muutosta merkittävänä. Muutoksen arvioinnissa sovellettiin riskinarviointiin pohjautuvaa lähestymistapaa.

C.5.3. Infrastruktuurin haltijan organisaatioyksikön, joka suoritti muutokseen saakka kunnossapitotoimia (muita kuin merkinantoa ja telemaattisia toimintoja), oli osallistuttava kilpailuun muiden samalla alalla työskentelevien yritysten kanssa. Tämän välittömänä seurauksena kilpailuasemaan joutuneen infrastruktuurin haltijan erillistä yksikköä oli supistettava ja henkilöstöä ja tehtäviä oli kohdennettava uudelleen.

C.5.4. Vaikutusten kohteena olleen infrastruktuurin haltijan huolenaiheet:

(a) Muutoksen kohteena ollut infrastruktuurin haltijan henkilöstö vastasi hätätilanteita koskevasta kunnossapidosta ja korjauksista, joita vaadittiin infrastruktuurien äkillisissä virhetapauksissa. Henkilöstö teki lisäksi joitakin suunniteltuja tai hankeperusteisia kunnossapitotoimia, kuten raiteiden täyttö, raidesepellyksen puhdistus ja kasvillisuuden valvonta.
(b) Näitä tehtäviä pidettiin kriittisinä turvallisuuden ja toiminnan täsmällisyyden kannalta. Ne oli näin ollen arvioitava, jotta löydettäisiin oikeat toimenpiteet sen varmistamiseksi, ettei tilanne heikkene, kun monet turvallisuusasioista vastaavat henkilöt lähtevät infrastruktuurin haltijan organisaatiosta.
(c) Organisaation muutoksen aikana ja sen jälkeen turvallisuuden ja täsmällisyyden tason oli säilyttävä ennallaan.

C.5.5. Yhteiseen turvallisuusmenetelmään verrattuna tässä yhteydessä käytiin läpi seuraavat vaiheet (katso myös kaavio 1):

(a) järjestelmäkuvaus [2.1.2 kohta]:
    (1) nykyisen organisaation (eli muutosta edeltäneen infrastruktuurin haltijan organisaation) hoitamien tehtävien kuvaus
    (2) infrastruktuurin haltijan organisaatiossa suunniteltujen muutosten kuvaus
    (3) ”irtautuvan osaston” ja muiden lähiorganisaatioiden tai fyysisen ympäristön rajapinnat voitiin kuvata ainoastaan lyhyesti. Rajoja ei voitu esittää 100-prosenttisen selvästi;
(b) vaarojen tunnistaminen [2.2 kohta]:
    (1) asiantuntijaryhmän aivoriihi:
        (i) tunnistetaan kaikki vaarat, jotka voivat vaikuttaa olennaisesti suunnitellusta organisaatiomuutoksesta aiheutuvaan riskiin

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(ii) yksilöidään mahdolliset toimenpiteet riskien hallitsemiseksi;

(2) vaaran luokitteleminen:

(i) vaaraan liittyvän riskin vakavuuden perusteella: korkea, kohtalainen, alhainen riski
(ii) muutoksen vaikutusten perusteella: lisääntynyt, muuttumaton, pienentynyt riski;

(c) ohjeiston käyttö [2.4 kohta]:

Muutosta edeltäneen järjestelmän katsottiin olevan hyväksyttävällä turvallisuustasolla. Sitä käytettiin näin ollen ”ohjeistona”, jonka perusteella organisaatiomuutokselle johdettiin hyväksyttävää riskitasoa koskeva peruste (RAC);

(d) eksplisiittinen riskin estimointi [2.5 kohta]:

Kaikille vaaroille, joiden riskit lisääntyvät organisaatiomuutoksen vuoksi, yksilöidään riskin vähentämistoimenpiteet. Jäännösriskiä verrataan ohjeiston RAC:hen, ja todetaan, onko määriteltävä lisätoimenpiteitä;

(e) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

(1) riskinarviointi ja vaaroja koskeva asiakirja osoittivat, ettei vaaroja voida hallita, ennen kuin ne on tarkistettu ja ennen kuin on osoitettu, että turvallisuusvaatimukset (eli valitut turvallisuustoimenpiteet) on pantu täytäntöön
(2) riskinarviointi ja vaaroja koskeva asiakirja muuttuivat koko ajan. Päätettyjen toimien tehokkuutta valvottiin säännöllisesti sen selvittämiseksi, olivatko olosuhteet muuttuneet ja oliko riskinarviointia tarpeen ajantasaistaa
(3) mikäli toteutetut toimenpiteet eivät olleet riittävän tehokkaita, riskinarviointia ja vaaroja koskeva asiakirja päivitettiin ja niitä valvottiin uudelleen;

(f) vaarojen hallinta [4.1 kohta]:

Tunnistetut vaarat ja turvallisuustoimenpiteet kirjattiin vaaroja koskevaa asiakirjaan, jonka avulla niitä hallittiin. Yksi esimerkin päätelmistä oli se, että riskinarviointia ja vaaroja koskevaa asiakirjaa on päivitettävä jatkuvasti, koska uusia päätöksiä tehtiin ja toimenpiteitä toteutettiin organisaatiomuutoksen aikana. Riskinarviointi kattoi esimerkiksi myös alihankkijoiden ja yrittäjien rajapintaan liittyvän riskin.

Vaaroja koskevassa asiakirjassa käytetty rakenne ja kentät sekä otteita joistakin kirjauksista esitetään lisäyksessä C olevassa C.16.2. kohdassa;

(g) riippumaton arviointi [6 artikla]:

Lisäksi kolmas osapuoli toteutti riippumattoman arvioinnin, jossa

(1) tarkistettiin, että riskien hallinta ja riskinarviointi on tehty asianmukaisesti
(2) tarkistettiin, että organisaatiomuutos on asianmukainen ja että sen avulla voidaan säilyttää sama turvallisuustaso, joka oli ennen muutosta.

C.5.6. Esimerkki osoittaa, että yhteisen turvallisuusmenetelmän edellyttämät periaatteet ovat rautatiealalla käytössä olevia menetelmiä, joita sovelletaan jo organisaatiomuutosten riskien arvioinnissa. Esimerkin riskinarviointi täyttää kaikki YTM-asetuksessa säädetyt edellytykset. Siinä sovelletaan kahta kolmesta hyväksyttävää riskitasoa koskevasta periaatteesta, jotka perustuvat YTM-asetuksen yhtenäistettyyn lähestymistapaan:

(a) ”ohjeiston” avulla määritetään hyväksyttävää riskitasoa koskeva peruste, jota tarvitaan organisaatiomuutoksesta aiheutuvan riskin hyväksyttävyyden arvioimiseksi;
(b) ”eksplisiittinen riskin estimointi ja evaluointi”:

(1) arvioidaan muutoksen poikkeamat ohjeistosta
(2) yksilöidään toimenpiteet, joilla vähennetään muutoksen lisäämiä riskejä

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(3) arvioidaan, onko hyväksyttävä riskitaso saavutettu.

C.6. Riskinarviointiesimerkki: merkittävä operatiivinen muutos – ajotuntien muutos

C.6.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.6.2. Esimerkki koskee operatiivista muutosta, jonka yhteydessä rautatieyritys halusi ottaa käyttöön uusia reittejä ja mahdollisesti lisätä kuljettajien työskentelyaikaa (mukaan lukien työkierto ja työvuorot).

C.6.3. Yhteiseen turvallisuusmenetelmään verrattuna tässä yhteydessä käytiin läpi seuraavat vaiheet (katso myös kaavio 1):

(a) muutoksen merkittävyys [4 artikla]:

Rautatieyritys teki alustavan riskinarvioinnin, jossa todettiin, että operatiivinen muutos oli merkittävä. Koska kuljettajien oli toimittava uusilla reiteillä ja mahdollisesti tavanomaisen työaikansa ulkopuolella, opasteiden sivuuttamisen mahdollisuus vaaratilanteissa taikka ylinopeuden tai tilapäisten nopeusrajoitteiden huomiotta jättämisen mahdollisuus oli olemassa.

Kun tätä alustavaa riskinarviointia verrataan YTM-asetuksen 4 artiklan 2 kohtaan sisältyviin perusteisiin, muutos voidaan luokitella merkittäväksi myös seuraavien perusteiden mukaisesti:

(1) merkitys turvallisuuden kannalta: muutos vaikuttaa turvallisuuteen, koska kuljettajien työskentelytapojen muuttamisesta voi aiheutua tuhoisia seurauksia
(2) vian seuraus: edellä mainitut kuljettajan virheet voivat johtaa tuhoisiin seurauksiin
(3) uutuus: rautatieyritys saattaa ottaa käyttöön kuljettajille uusia työskentelytapoja
(4) muutoksen monimutkaisuus: työtuntien muuttaminen saattaa olla monimutkaista, koska se voi edellyttää nykyisten työolosuhteiden täysimääräistä arviointia ja muuttamista.

(b) järjestelmämäärittely [2.1.2 kappale]:

Järjestelmämäärittelyssä kuvattiin alun perin:

(1) aiemmat työolot: työajat, työvuorot jne.
(2) työaikojen muutokset
(3) rajapintaa koskevat seikat (esim. rajapinta instrastruktuurin haltijan kanssa)

Toistojen aikana järjestelmämäärittelyä muutettiin lisäämällä siihen riskinarviointiprosessista saadut turvallisuusvaatimukset. Keskeiset henkilöstön

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

edustajat osallistuivat tähän vaarojen tunnistamista ja järjestelmämäärittelyn ajantasaistamista koskevaan toistuvaan prosessiin.

(c) vaarojen tunnistaminen [2.2 kohta]:

Uusien reittien ja työvuorojen vaarat ja mahdolliset turvallisuustoimenpiteet yksilöitiin asiantuntijoiden aivoriihessä, johon osallistui myös kuljettajien edustajia. Kuljettajien tehtäviä muuttuneissa olosuhteissa tarkasteltiin sen arvioimiseksi, vaikuttavatko ne kuljettajiin, heidän työmääräänsä, maantieteelliseen ulottuvuuteen ja työvuorojärjestelmän mukaiseen työaikaan.
Rautatieyritys kuuli myös työntekijäliittoja selvittääkseen, saataisiinko niiltä lisätietoja, ja tarkasteli uudelleen väsymykseen ja sairauksiin liittyviä riskejä, joita tuntemattomilla reitteillä tehdyistä aiempaa pidemmistä matkoista johtuvan ylityön lisääntyminen saattaa aiheuttaa.
Kullekin vaaralle osoitettiin riskin ja seurauksien vakavuuden taso (korkea, kohtalainen, matala), ja ehdotetun muutoksen vaikutusta arvioitiin suhteessa näihin riskeihin (lisääntynyt, muuttumaton tai alentunut).

(d) menettelyohjeiden käyttö [2.3 kohta]:

Työajan ja väsymyksen riskeihin liittyviä menettelyohjeita käytettiin aiempien työskentelyolojen muuttamiseen ja uusien turvallisuusvaatimusten määrittelemiseen. Tämän jälkeen laadittiin tarvittavat toimintasäännöt uuden työvuorojärjestelmän menettelyohjeiden mukaisesti. Kaikki tarvittavat osapuolet otettiin mukaan tarkistettuihin toimintamenettelyihin ja muutoksen toteuttamista koskevaan sopimukseen.

(e) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

Tarkistetut toimintamenettelyt otettiin käyttöön rautatieyrityksen turvallisuusjohtamisjärjestelmässä. Niitä valvottiin, ja tarkistusmenettely otettiin käyttöön sen varmistamiseksi, että tunnistettuja vaaroja valvotaan asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(f) vaarojen hallinta [4.1 kohta]:

Katso tältä osin edellä oleva kohta, sillä rautatieyrityksillä vaarojen hallintaprosessi voi olla osa riskien kirjaamiseksi ja hallitsemiseksi toteutettavaa turvallisuusjohtamisjärjestelmää. Tunnistetut vaarat ja turvallisuusvaatimukset (eli viittaukset tarkistettuihin toimintamenettelyihin) merkittiin vaaroja koskevaan asiakirjaan, jonka avulla riskejä hallittiin.
Tarkistettuja menettelyjä valvottiin ja muutettiin tarvittaessa sen varmistamiseksi, että tunnistettuja vaaroja valvotaan asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(g) riippumaton arviointi [6 artikla]:

Rautatieyrityksen pätevä, arviointiprosessin ulkopuolinen työntekijä arvioi riskinarvioinnin ja riskinhallinnan prosessin. Hän arvioi sekä menettelyn että sen tulokset eli yksilöidyt turvallisuusvaatimukset.

Rautatieyritys perusti uuden järjestelmän täytäntöönpanoa koskevan päätöksensä tämän asiantuntijan laatimaan riippumattomaan arvioon.

C.6.4. Tämä esimerkki osoittaa, että rautatieyrityksen soveltamat periaatteet ja menetelmä ovat yhteisen turvallisuusmenetelmän mukaisia. Riskinhallinta- ja riskinarviointiprosessissa noudatettiin kaikkia YTM-asetuksen vaatimuksia.

.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.7. Esimerkki teknisesti merkittävän muutoksen riskinarvioinnista (CCS)

C.7.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

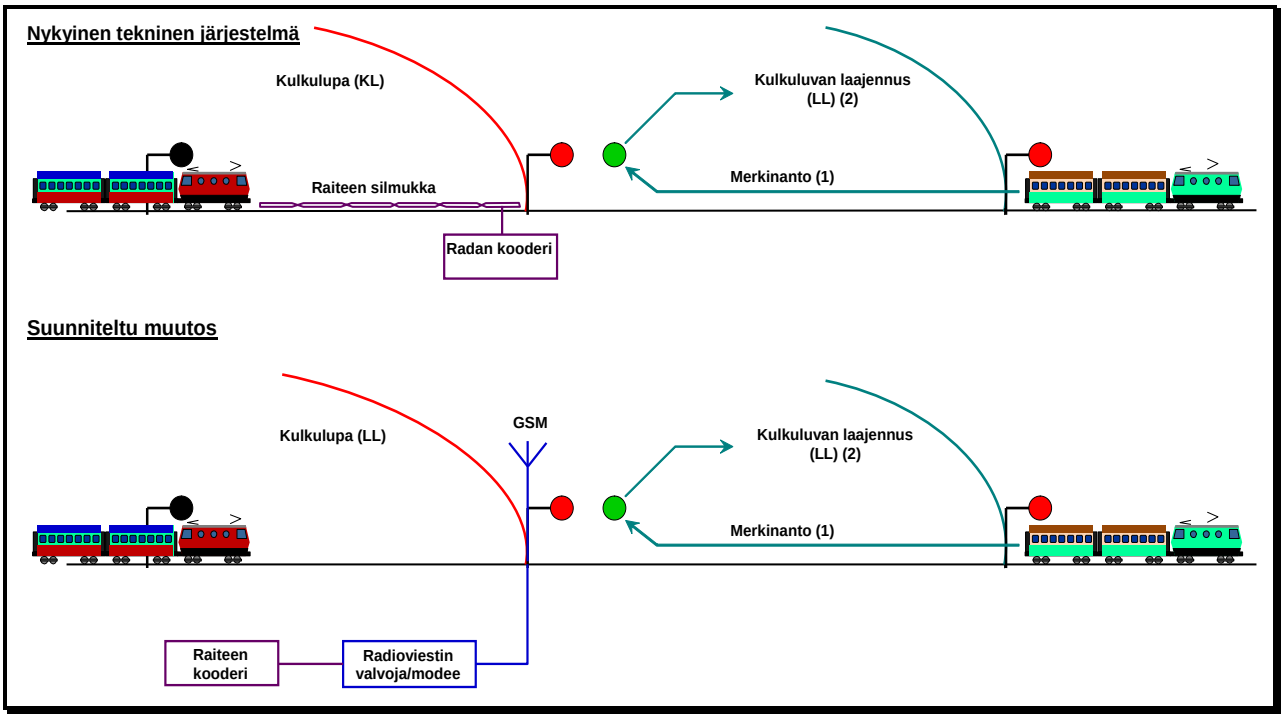
(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.7.2. Esimerkki koskee ohjaus- ja hallintajärjestelmän teknistä muutosta. Valmistaja piti muutosta merkittävänä. Muutoksen arvioinnissa sovellettiin riskinarviointiin perustuvaa lähestymistapaa.

C.7.3. Muutoksen kuvaus: muutos koskee opastinta edeltävän radanvarren silmukan korvaamista radioviestimeen ja GSM:ään perustuvalla osajärjestelmällä (katso kaavio 16).

C.7.4. Huolenaihe: järjestelmän turvallisuustason säilyttäminen samana muutoksen jälkeen.



Kaavio 16: Radanvarren silmukan korvaaminen radioviestimeen perustuvalla osajärjestelmällä

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.7.5. YTM-prosessiin verrattuna tässä yhteydessä käytiin läpi seuraavat vaiheet (katso myös kaavio 1):

(a) muutoksen merkittävyyden arviointi [4 artikla]:

Muutoksen merkittävyyttä arvioitiin 4 artiklan 2 kohdaan sisältyvien perusteiden mukaisesti. Muutosta pidettiin merkittävänä lähinnä monimutkaisuutta ja uutuutta koskevien perusteiden nojalla.

(b) järjestelmäkuvaus [2.1.2 kohta]:

(1) nykyisen järjestelmän kuvaus: silmukka ja sen tehtävät ohjaus- ja hallintajärjestelmässä
(2) hakijan ja valmistajan suunnitteleman muutoksen kuvaus
(3) silmukan ja muun järjestelmän toiminnallisten ja fyysisten rajapintojen kuvaus

Nykyisessä järjestelmässä silmukan ja kooderin tehtävänä on antaa merkki lähestyvästä junasta, kun merkin takana (eli lähestyvän junan edessä) oleva raideosa vapautuu: katso kaavio 16.

(c) vaarojen tunnistaminen [2.2 kohta]:

Tässä tapauksessa sovelletaan toistuvaa riskinarvioinnin ja vaarojen tunnistamisen (katso 2.1.1 kappale) prosessia ja hyödynnetään asiantuntijaryhmän aivoriihtä, jotta voidaan:

(1) tunnistaa vaarat, jotka vaikuttavat olennaisesti suunnitellun muutoksen aiheuttamaan riskiin
(2) yksilöidä mahdolliset toimenpiteet riskin hallitsemiseksi

Kun silmukka ja siten radioviestin antavat merkin, vaarana on, että lähestyvälle junalle annetaan liikkumislupa, joka ei ole turvallinen siksi, että edellä kulkenut juna on edelleen merkinantopisteen edessä olevalla alueella. Riskiä on pienennettävä hallintatoimien avulla, jotta se saadaan hyväksyttävälle tasolle.

(d) ohjeiston käyttö [2.4 kohta]:

Muutosta edeltäneen järjestelmän (silmukka) arvioidaan olevan hyväksyttävällä turvallisuustasolla. Sitä käytetään näin ollen ohjeistona, jonka avulla radioviestinnän osajärjestelmän turvallisuusvaatimukset määritetään.

(e) eksplisiittinen riskin estimointi ja evaluointi [2.5 kohta]:

(1) ”silmukka”- ja ”radioviestin+GSM” -järjestelmien erot arvioidaan eksplisiittisessä riskin estimoinnissa ja evaluoinnissa. ”Radioviestin+GSM” -osajärjestelmän osalta voidaan yksilöidä seuraavat uudet vaarat:

(i) hakkerien ilmavälissä välittämä epäluotettava tieto, sillä ”radioviestin+GSM” -järjestelmä on avoin lähetysjärjestelmä
(ii) viivästynyt välitys tai talletettujen tietopakettien välitys ilmavälissä

(2) eksplisiittinen riskin estimointi ja RAC-TS:n käyttö radioviestimen valvojan osalta;

(f) menettelyohjeiden soveltaminen [2.3 kohta]:

(1) Standardiin EN 50159-2 (*Rautatiesovellukset - Osa 2: Avoimien viestinsiirtojärjestelmien turvallisuuteen liittyvä viestintä*) sisältyvät turvallisuusvaatimukset, joiden avulla voidaan valvoa, että seuraavankaltaiset uudet vaarat ovat hyväksyttävällä turvallisuustasolla:

(i) tiedonsalaus ja suojelu
(ii) viestien jaksotus ja aikaleimaus

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(2) esimerkiksi standardin EN 50 128 käyttö radioviestimen valvojan ohjelmiston kehittämiseen

(g) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

(1) turvallisuusvaatimusten täytäntöönpanon seuranta ”radioviestin+GSM”-osajärjestelmän kehittämisprosessissa
(2) sen varmentaminen, että suunniteltu ja asennettu järjestelmä täyttää turvallisuusvaatimukset

(h) vaarojen hallinta [4.1 kohta]:

Riskinarvioinnissa ja hyväksyttävää riskitasoa koskevan kolmen periaatteen soveltamisessa tunnistetut vaarat, turvallisuustoimenpiteet ja niihin perustuvat turvallisuusvaatimukset merkitään vaaroja koskevaan asiakirjaan, jonka avulla niitä hallitaan.

(i) riippumaton arviointi [6 artikla]:

Lisäksi kolmas osapuoli toteuttaa riippumattoman arvioinnin, jolla

(1) varmistetaan, että riskinhallinta ja riskinarviointi tehdään asianmukaisesti
(2) varmistetaan, että tekninen muutos on asianmukainen ja että muutosta edeltänyt turvallisuustaso säilyy ennallaan.

C.7.6. Tämä esimerkki osoittaa, miten yhteisen turvallisuusmenetelmän edellyttämää kolmea hyväksyttävää riskitasoa koskevaa periaatetta voidaan sovelta täydentävästi määriteltäessä arvioitavana olevan järjestelmän turvallisuusvaatimukset. Tämän esimerkin riskinarviointi täyttää kaikki YTM-asetuksen mukaiset vaatimukset, joista on esitetty yhteenveto kaaviossa 1, mukaan lukien vaaroja koskevan asiakirjan hallintaa ja kolmannen osapuolen tekemää riippumatonta turvallisuusarviota koskevat vaatimukset.

C.8. Esimerkki rautatietunneleiden riskinarviointia koskevasta ruotsalaisesta ohjeesta BVH 585.30

C.8.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.8.2. Tässä esimerkissä on tarkoitus verrata YTM-prosessia ja ohjetta BVH 585.30 , jota Ruotsin ratainfrastruktuurin haltija Banverket käyttää uusien rautatietunneleiden suunnittelussa ja varmentaakseen, että tunnelien suunnittelussa ja rakentamisessa saavutetaan riittävä turvallisuustaso. Ohjeiden ja YTM:n yhteiset piirteet ja erot luetellaan jäljempänä; yksityiskohtaiset riskinarvioinnin vaatimukset on annettu ohjeessa BVH 585.30.

C.8.3. Kaavion 1 mukaiseen YTM-prosessiin verrattuna:

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) ohje BVH 585.30 sisältää seuraavat samat kohdat:

(1) järjestelmäkuvaus [2.1.2 kohta]:

Ohjeessa edellytetään yksityiskohtaista järjestelmäkuvausta, joka sisältää

(i) tunnelin kuvauksen
(ii) raiteen kuvauksen
(iii) liikkuvan kaluston kuvauksen (mukaan lukien kaluston henkilöstö)
(iv) liikenteen ja suunniteltujen toimintojen kuvauksen
(v) ulkopuolisen avun kuvauksen (mukaan lukien pelastuspalvelut)

(2) vaarojen tunnistaminen [2.2 kohta]:

Ohjeessa ei vaadita nimenomaisesti vaaran tunnistamista. Siinä vaaditaan tunnistamaan riskit ja laatimaan ”onnettomuusluettelo”, joka sisältää tunnistetut mahdolliset onnettomuustyypit, joilla arvioidaan olevan merkittävä vaikutus tunnelin riskitasoon ja joita on tarkasteltava myöhemmässä arvioinnissa. Esimerkkejä onnettomuuksista:

(i) ”matkustajajunan suistuminen raiteilta”
(ii) ”tavarajunan suistuminen raiteilta”
(iii) ”onnettomuus, jossa on mukana vaarallisia aineita”
(iv) ”tulipalo kalustoyksikössä”
(v) ”matkustajajunan ja kevyen/raskaan esineen törmäys”
(vi) jne.

(3) ohjeessa ei edellytetä menettelyohjeiden tai vastaavien ohjeistojen soveltamista. Ohjeissa edellytetään, että riskianalyysi tehdään kaikissa tapauksissa

(4) eksplisiittinen riskien estimointi ja evalutointi [2.5 kohta]:

(i) ohjeessa suositetaan yleisesti käymään kunkin onnettomuuden osalta läpi koko tapahtumapuu (Event Tree), joka perustuu kvantitatiiviseen riskinarviointiin. Koska riskianalyysin tarkoituksena on kuitenkin arvioida tunnelin kokonaisturvallisuustasoa eikä niinkään turvallisuuden yksittäisiä näkökohtia yksityiskohtaisemmalla tasolla, kaikkien skenaarioiden seuraukset kootaan yhteen, jotta voidaan selvittää tunnelin kokonaisriskitaso;
(ii) sen selvittämisessä, onko tunnelin kokonaisriskitaso hyväksyttävällä riskitasolla, käytetään seuraavia erityistä hyväksyttävää riskitasoa koskevaa perustetta: *”rautatieliikenne tunnelikilometrillä on yhtä turvallista kuin rautatieliikenne ulkoilmakiskokilometreillä tasoristeykset poislukien”*. Tämä peruste muunnetaan F-N-käyräksi, jonka pohjana käytetään aiemmin Ruotsissa tapahtuneiden rautatieonnettomuuksien tietoja, ja se ekstrapoloidaan kattamaan myös ne seuraukset, joita ei ole tilastoitu;
(iii) tunnelin kokonaisriskitasoa koskevan perusteen lisäksi esitetään myös muita vaatimuksia, jotka on täytettävä ja jotka koskevat erityisesti tunnelien evakuointia ja pelastuspalvelujen saatavuutta:

- varmistetaan, että palavasta junasta on mahdollista pelastautua omatoimisesti ”uskottavassa pahimmassa tapauksessa” (tätä koskevat arviointiperusteet on niin ikään esitettävä);
- tunneli on suunniteltava siten, että pelastustoimet voidaan toteuttaa tietyissä skenaarioissa;

(5) riskinarvioinnin tulos [2.1.6 kohta]:

Riskinarvioinnin tuloksena saadaan:

(i) luettelo turvallisuustoimenpiteistä sellaisen vähimmäisstandardin mukaisesti, joka perustuu yhteentoimivuuden tekniseen eritelmään (YTE)

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

”Rautatietunneleiden turvallisuus” ja tunnelin suunnittelussa sovellettaviin kansallisiin sääntöihin, ja

(ii) kaikki riskinarvioinnissa tarpeellisiksi todetut lisäturvallisuustoimenpiteet, ja niiden tarkoitus. Riskinarvioinnissa todetaan, että toimenpiteistä on päätettävä seuraavassa tärkeysjärjestyksessä:

- onnettomuuksien ehkäisy
- onnettomuuksien seurauksien lieventäminen
- evakuoinnin helpottaminen
- pelastustoimien helpottaminen

(6) vaarojen hallinta [4.1 kohta]:

Ohjeessa ei varsinaisesti vaadita laatimaan vaaroja koskevaa asiakirjaa. Tämä liittyy siihen seikkaan, että arviointi on kokonaisvaltainen, minkä vuoksi yksittäisiä vaaroja ei arvioida eikä valvota. Tunnelin kokonaisriskin hyväksyttävyys arvioidaan ilman, että hyväksyttävää kokonaisriskitasoa koskevaa perustetta jaetaan erityyppisten onnettomuuksien tai niiden taustalla olevien vaarojen mukaan.

Kaikki turvallisuustoimenpiteet kuitenkin luetellaan. Tämä koskee sekä ”vähimmäisstandardiin” perustuvia että riskinarvioinnissa välttämättömiksi todettuja toimenpiteitä: katso edellä a kohdan 5 kohdan ii luetelmakohta. Turvallisuustoimenpiteiden luettelossa on mainittava, koskevatko toimenpiteet tunnelin infrastruktuuria, raiteita, toimintoja tai liikkuvaa kalustoa, ja mitä tavoitteita toimenpiteillä on a kohdan 5 kohdan ii luetelmakohdan mukaisesti. Ohjeessa ei kuitenkaan vaadita varsinaisesti toteamaan, mitä vaaroja turvallisuustoimenpiteillä hallitaan ja kuka vastaa mistäkin toimenpiteestä.

(7) riippumaton arviointi [6 artikla]:

Rippumaton kolmannen osapuolen tekemä arviointi on pakollinen, jotta voidaan:

(i) varmistaa, että ohjeessa BVH 585.30 suositeltu riskiarviointiprosessi on suoritettu asianmukaisesti
(ii) hyväksyä riskianalyysi
(iii) varmistaahankkeen tulevan turvallisuusjohtamisjärjestelmän toteuttamistavan selkeä kuvaus;

Riippumaton arvioija ja hankkeen turvallisuuskoordinaattori allekirjoittavat lopullisen riskianalyysiasiakirjan.

(b) ohje BVH 585.30 eroaa YTM-prosessista seuraavissa kohdissa:

(1) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

ohjeessa BVH 585.30 ei vaadita esittämään selvitystä siitä, miten yksilöidyt turvallisuusvaatimukset pannaan täytäntöön, eikä varmentamaan, että lopullinen tunneli täyttää mainitut turvallisuusvaatimukset. Siinä ainoastaan kuvataan, miten nämä vaatimukset on siirrettävä eteenpäin, jotta voidaan varmistaa, että niitä noudatetaan rakennusvaiheessa.

Ohjeen mukaan turvallisuusvaatimusten avulla on varmistettava, että riskianalyysi on tehty asianmukaisesti ja avoimesti ja että se voidaan hyväksyä hankkeessa.

C.8.4. Ohjeen vertailu YTM:ään osoittaa näin ollen, että:

(a) ohje BVH 585.30 kattaa YTM:n keskeiset osat, vaikka ohjeiden laajuus ja tarkoitus eivät ole täysin samat
(b) ohjeessa BVH 585.30 arvioidaan rautatietunnelin kokonaisriskitasoa
(c) vaaroja ei hallita erikseen, ja vaarojen hallintaan ei keskitytä yhtä voimakkaasti

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(d) ohjeissa ei varsinaisesti vaadita osoittamaan vaatimustenmukaisuutta ja varmentamaan turvallisuustoimenpiteiden asianmukaista noudattamista. Ohjeessa todetaan kuitenkin, että hankkeen turvallisuuskoordinaattorin tehtävänä (ohjeen BVH 585.30 mukainen rooli ja pätevyys) on varmistaa, että riskianalyysin päätelmät pannaan täytäntöön suunnitteluun liittyvissä asiakirjoissa ja piirustuksissa, sekä valvoa, että ne pannaan asianmukaisesti täytäntöön myös rakennusvaiheessa.

C.8.5. YTM:n säännökset ovat yleisluonteisempia kuin ohje BVH 585.30 sikäli kuin niiden perusteella voidaan soveltaa kolmea erilaista hyväksyttävää riskitasoa koskevaa periaatetta. Ohjeen BVH 585.30 soveltaminen YTM-asetuksen yhteydessä ei kuitenkaan aiheuta ongelmia, koska ohje on eksplisiittistä riskin estimointia koskevan kolmannen periaatteen mukainen.

C.9. Esimerkki järjestelmätason riskinarvioinnista Kööpenhaminan metrossa

C.9.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.9.2. Tämä esimerkki koskee monimutkaista kuljettajatonta metrojärjestelmää kokonaisuudessaan, sen teknisiä osajärjestelmiä (kuten automaattista kulunvalvontaa ja liikkuvaa kalustoa), järjestelmän käyttöä ja kunnossapitoa. Järjetelmä ja sen osajärjestelmät arvioitiin riskinarviointiin perustuvan lähestymistavan avulla. Hanke kattoi myös järjestelmän käyttämisestä vastaavan yrityksen turvallisuusjohtamisjärjestelmän sertifioinnin. Tämä liittyy rautatieyrityksen ja infrastruktuurin haltijan valmiuksiin ylläpitää koko järjestelmää turvallisesti sen elinkaaren ajan.

C.9.3. YTM-prosessiin verrattuna tässä yhteydessä käytiin läpi seuraavat vaiheet (katso myös kaavio 1):

(a) järjestelmäkuvaus [2.1.2 kohta]:

(1) järjestelmän suorituskykyvaatimusten kuvaus
(2) toimintasääntöjen kuvaus
(3) eri toimijoiden, erityisesti eri teknisten osajärjestelmien, välisten rajapintojen ja vastuiden selkeä kuvaus
(4) korkean tason järjestelmävaatimusten kuvaus (hyväksyttävän onnettomuuksien esiintymistason ja siedettävän tason määrittelyn perusteella)

(b) vaarojen tunnistaminen [2.2 kohta]:

(1) vaarojen analysoinnin alustava järjestelmätaso
(2) järjestelmätason toiminnallinen analysointi, jossa korostetaan kaikkia osajärjestelmiä eikä vain niitä, jotka ovat selvästi kriittisiä turvallisuuden kannalta

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(esim. automaattinen junansuojajärjestelmä ja liikkuva kalusto), joilla on merkitystä turvallisuuteen liittyville toiminnoille ja jotka vaikuttavat keskeisesti matkustajien ja henkilöstön turvallisuuden varmistamiseen

(3) toimijoiden (sopimuspuolet, teknisten osajärjestelmien toimittajat ja rakennusurakoiden tekijät) välinen tiivis koordinointi, jotta voidaan

(i) tunnistaa järjestelmällisesti kaikki kohtuullisesti ennakoitavissa olevat vaarat
(ii) yksilöidä mahdolliset toimet kaikkien tunnistettujen vaarojen hallitsemiseksi ja saattamiseksi hyväksyttävälle riskitasolle

(c) menettelyohjeiden käyttö [2.3 kohta]:

Käytettiin erilaisia menettelyohjeita, standardeja ja asetuksia, kuten:

(1) raitiovaunujen rakentamista ja toimintaa sekä kuljettajatonta ajoa koskeva BOStrab-asetus (Saksan asetus, jota sovelletaan kaupunkien rautatieverkkoihin)
(2) VDV-asiakirjat (saksalaiset menettelyohjeet), jotka sisältävät sellaiselle laitteistolle asetettavat vaatimukset, jolla varmistetaan asemien matkustajaturvallisuus kuljettajattomassa ajossa
(3) rautatiejärjestelmiä koskevat CENELEC-standardit (EN 50 126, 50 128 ja 50 129). Nämä standardit koskevat erityisesti teknisiä rautatiejärjestelmiä. Ne sisältävät kuitenkin yleisesti pätevän metodologisen lähestymistavan, ja ne on otettu laajaan käyttöön Kööpenhaminan metrossa:

(i) standardia EN 50 126 käytetiin koko rautatiejärjestelmän turvallisuushallinnassa ja riskinarvioinnissa
(ii) standardia EN 50 129 käytettiin koko merkinantojärjestelmässä
(iii) standardia EN 50 128 käytettiin teknisten osajärjestelmien ohjelmistojen kehittämisessä (mukaan lukien niiden varmentaminen ja vahvistaminen)

(4) tunnelien palosuojelustandardit (NEPA 130)
(5) yhdyskuntarakentamisen ja rakennusurakoiden standardit (Euro Codes)

(d) ohjeiston käyttö [2.4 kohta]:

Metron turvallisuustason oli vastattava Saksan, Ranskan tai Yhdistyneen kuningaskunnan uudenaikaisten laitteiden turvallisuustasoa. Näitä käytössä olevia järjestelmiä käytettiin vastaavina ohjeistoina, joista johdettiin hyväksyttävää riskitasoa koskeva peruste sen osalta, mikä on onnettomuuksien hyväksyttävä esiintymistiheys Kööpenhaminan metrossa

(e) eksplisiittinen riskin estimointi ja evaluointi [2.5 kohta]:

(1) erityisiin vaaroihin liittyvien riskien estimointi;
(2) tunnelien ilmanvaihdon valvonta hätätapauksissa (mukaan lukien palokunnan toimintaan liittyvät inhimilliset tekijät)
(3) riskejä vähentävien toimenpiteiden yksilöinti
(4) sen arvioiminen, onko koko järjestelmän riskitaso hyväksyttävä

(f) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kappale]:

(1) järjestelmän monimutkaisuuteen sopeutetut hallinnolliset ja tekniset toimet järjestelmän turvallisuuden osoittamiseksi;
(2) järjestelmän turvallisuusvaatimusten jaottelu teknisiin osajärjestelmiin ja rakennusurakoihin sekä kaikkiin turvallisuuteen liittyviin metron toimintoihin;
(3) sen osoittaminen, että kukin rakennettu osajärjestelmä täyttää sille asetetut turvallisuusvaatimukset;
(4) jos turvallisuustoimenpiteet on toteutettu useamman kuin yhden osajärjestelmän avulla, sen osoittaminen, ettei turvallisuusvaatimusten täyttymistä voitu todeta

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

osajärjestelmän tasolla. Turvallisuusvaatimusten täyttyminen on varmistettu järjestelmätasolla integroimalla eri osajärjestelmät, välineet ja menettelyt;

(5) sen osoittaminen, että koko järjestelmä on korkeatasoisten turvallisuusvaatimusten mukainen;

(g) vaarojen hallinta [4.1 kohta]:

Tunnistetut vaarat, niihin liittyvät turvallisuustoimenpiteet ja niihin perustuvat turvallisuusvaatimukset kirjattiin ylös vaaroja koskevaan asiakirjaan, jonka avulla niitä hallittiin. Hankkeen kokonaisturvallisuudesta vastaava johtaja vastasi vaaroja koskevasta asiakirjasta. Suunnittelun ja rakentamisen aikana esiin tulleet toiminnalliset vaarat sekä käyttöön ja kunnossapitoon liittyvät vaarat sisällytettiin vaaroja koskevaan asiakirjaan.

(h) riskinhallintaa ja riskinarviointia koskeva näyttö [5 kohta]:

Riskinarvioinnin tulokset dokumentointiin virallisesti, ja niiden tukena oli CENELEC-standardien vaatimusten mukainen turvallisuusarvio:

(1) turvallisuusarvio koko järjestelmästä
(2) turvallisuusarvio kustakin teknisestä osajärjestelmästä (mukaan lukien merkinannon osajärjestelmät ja rakennusurakat)
(3) turvallisuusarvio rakennusurakoista (asemat, tunnelit, maasillat, penkereet)
(4) turvallisuusarvio rakentamisesta
(5) turvallisuusarvio kalustoyksiköstä
(6) turvallisuusarvio toimijasta (rautatieyrityksen ja infrastruktuurin haltijan turvallisuusjohtamisjärjestelmän sertifioinnin tukemana, eli osoitus hakijan valmiuksista käyttää ja ylläpitää järjestelmää turvallisesti)

(i) riippumaton arviointi [6 artikla]:

Riippumaton turvallisuuden arvioija, joka toimi yhteistyössä teknisen valvontaviranomaisen (eli Tanskan liikenneministeriön) edustajien kanssa, valvoi koko prosessia ja teki siitä arvioinnin. Riippumattoman turvallisuusarvioijan tehtävät on vahvistettu asiaa koskevassa menettelyohjeessa. Tehtäviin kuului

(1) varmistaa, että riskinhallinta ja riskinarviointi toteutetaan asianmukaisesti;
(2) varmistaa, että järjestelmä soveltuu tarkoitukseensa ja että sen käyttö ja kunnossapito on turvallista koko järjestelmän elinkaaren aikana;
(3) suosittaa hyväksyntää tekniselle valvontaviranomaiselle.

C.9.4. Koko hankkeen tukena oli asianmukainen laadunhallintaprosessi.

C.9.5. Hankkeessa toimittajilta saatu näyttö (eli turvallisuusarvioinnit ja teknisten osajärjestelmien ja rakennustöiden yksityiskohtainen tukiaineisto) toimitettiin hakijan turvallisuusjohtajalle. Turvallisuuden hallintaorganisaatio ja riippumaton turvallisuuden arvioija tarkastivat todisteet, ja riippumattoman turvallisuuden arvioijan päätelmät kirjattiin arviointikertomukseen.
Hakijan turvallisuusjohto tarkisti riippumattoman turvallisuusarviointikertomuksen ja välitti sen hakijalle, joka puolestaan toimitti kaikki asiakirjat tekniselle valvontaviranomaiselle (eli Tanskan liikenneministeriölle) lopullista hyväksyntää varten.

C.9.6. Tästä esimerkistä käy ilmi, että rautatiealalla sovelletaan jo käytännössä yhteisen turvallisuusmenetelmän edellyttämiä periaatteita. Esimerkin riskinarviointi täyttää kaikki YTM-asetuksesta johtuvat velvollisuudet. Siinä sovelletaan erityisesti kaikkia YTM:n yhtenäisen lähestymistavan mukaista kolmea hyväksyttävää riskitasoa koskevaa periaatetta.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.10. Esimerkki: vaarallisten aineiden rautatiekuljetusten riskin laskeminen OTIF:n ohjeiden mukaan

C.10.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.10.2. Valtioiden välisen kansainvälisten rautatiekuljetusten järjestön (OTIF) ohjeiden keskeinen sisältö on sopusoinnussa YTM:n tavoitteen kanssa, mutta ohje on YTM:ää suppeampi. Tavoitteena OTIF:n *”ohjeessa on saavuttaa entistä yhdenmukaisempi lähestymistapa vaarallisten aineiden kuljetusten riskinarviointiin kansainvälisiä rautatiekuljetuksia koskevan yleissopimuksen (COTIF) jäsenvaltioissa, ja tehdä siten yksittäisistä riskinarvioinneista keskenään vertailukelpoisia”*. Sillä tuetaan näin ollen sitä, että COTIF:n jäsenvaltiot hyväksyvät vastavuoroisesti vaarallisten aineiden rautatiekuljetuksia koskevat riskinarvioinnit.

C.10.3. YTM:ään ja kulkukaavioon 1 verrattuna:

(a) OTIF:n ohjeella on seuraavat yhteneväiset kohdat:

(1) kyse on yleisestä riskinarvioinnin lähestymistavasta, joka kuitenkin perustuu ainoastaan eksplisiittiseen riskin estimointiin (eli kolmanteen hyväksyttävää riskitasoa koskevaan YTM:n periaatteeseen);
(2) OTIF:n riskinaviointi koostuu seuraavista vaiheista:

(i) riskinarviointivaihe, joka käsittää

- vaarojen tunnistamisvaiheen
- riskin estimointivaiheen;

(ii) riskinarviointivaihe, joka perustuu (hyväksyttävää) riskitasoa koskevaan perusteeseen, jota ei ole vielä yhdenmukaistettu. Useat kansalliset erityispiirteet voivat siten vaikuttaa näihin perusteisiin;

(b) OTIF:n ohje eroaa YTM:stä seuraavien seikkojen osalta:

(1) Soveltamisala on eri. YTM:ää on sovellettava ainoastaan rautatiejärjestelmän merkittäviin muutoksiin, kun taas OTIF:n ohjetta on sovellettava vaarallisten aineiden rautatiekuljetuksiin siitä riippumatta, onko kyse rautatiejärjestelmän merkittävästä muutoksesta vai ei.
(2) OTIF:n ohje ei tarjoa riskinhallinnan yhteydessä mahdollisuutta valita kolmesta hyväksyttävää riskitasoa koskevasta periaatteesta. Se sallii ainoastaan kolmannen periaatteen eli eksplisiittisen riskin estimoinnin soveltamisen. Riskinarvioinnin on lisäksi perustuttava yksinomaan kvantitatiiviseen eikä kvalitatiiviseen arvioon. Kvalitatiivista riskinanalyysia voidaan soveltaa ainoastaan tietyissä tapauksissa, joissa vertaillaan riskiä pienentäviä (turvallisuus)toimenpidevaihtoehtoja.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) OTIF:n ohje edellyttää siedettävän tason (ALARP) periaatteen soveltamista, jonka avulla voidaan määrittää, voidaanko ylimääräisillä turvallisuustoimenpiteillä kohtuullisin kuluin vähentää arvioitua riskiä entisestään.
(4) OTIF:n ohje ei sisällä ”yleisesti hyväksyttävään riskitasoon liittyvien vaarojen” käsitettä, jonka perusteella riskinarvioinnissa voitaisiin keskittyä vaikutukseltaan keskeisimpiin vaaroihin. Ohjeessa suositetaan kuitenkin vähentämään mahdollisten onnettomuusskenaarioiden määrää siten, että tarkasteltavaksi jää kohtuullinen määrä perusskenaarioita (katso {Ref. 10}:n 3.2 §).
(5) OTIF:n ohjeen mukaisessa prosessissa keskitytään riskinarviointiin, mutta siihen ei sisälly

(i) riskiin vaikuttavien (turvallisuus)toimenpiteiden valinta- eikä täytäntöönpanoprosessia
(ii) riskinhyväksyntäprosessia
(iii) prosessia, jossa osoitetaan järjestelmän olevan turvallisuusvaatimusten mukainen
(iv) prosessia, jossa riskeistä tiedotetaan muille asianomaisille toimijoille (katso tätä seuraava kohta).

(6) Ohjeessa ei täsmennetä, mitä näyttöä riskinarviointiprosessista on toimitettava.
(7) vaarojen hallintaa ei edellytetä;
(8) Ohjeessa ei edellytetä kolmannen osapuolen suorittamaa riippumatonta arviointia, jolla varmistettaisiin yhteisen lähestymistavan asianmukainen soveltaminen.

C.10.4. OTIF:n ohjeen ja YTM:n vertailusta käy ilmi niiden yhtenevyys siitä huolimatta, etteivät niiden soveltamisalat ja tavoitteet ole täsmälleen samat. YTM on yleisempi kuin OTIF:n ohje, ja siten myös joustavampi. Toisaalta YTM käsittää myös useampia riskinhallintatoimia:

(a) sen perusteella voidaan soveltaa kolmea riskinarviointiperiaatetta, jotka perustuvat rautatiealan vallitseviin käytäntöihin: katso 2.1.4 kappale;
(b) sitä on sovellettava ainoastaan merkittäviin muutoksiin, ja lisäriskianalyysi on tehtävä ainoastaan vaaroista, jotka eivät ole yleisesti hyväksyttävällä riskitasolla;
(c) se sisältää sellaisten turvallisuustoimenpiteiden valinnan ja täytäntöönpanon, joilla on tarkoitus valvoa tunnistettuja vaaroja ja niihin liittyviä riskejä;
(d) sillä yhdenmukaistetaan riskinarviointiprosessia, mukaan lukien:

(1) riskinarviointiperusteiden yhdenmukaistaminen, jota virasto käsittelee työssään, joka liittyy yleisesti hyväksyttäviin riskeihin ja yleisesti hyväksyttävää riskitasoa koskeviin perusteisiin
(2) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen
(3) riskinarviointiprosessin tulokset ja näyttö
(4) turvallisuuteen liittyvien tietojen vaihto rajapinnoilla toimivien toimijoiden välillä
(5) kaikkien tunnistettujen vaarojen ja niihin liittyvien turvallisuustoimenpiteiden hallinnointi vaaroja koskevan asiakirjan avulla
(6) YTM:n asianmukaisesta soveltamisesta tehtävä kolmannen osapuolen riippumaton arviointi.

C.10.5. OTIF:n ohjeen soveltaminen YTM:n asetuksen yhteydessä (siinä tapauksessa, että vaarallisten aineiden kuljetus merkitsee intrastuktuurin haltijan tai rautatieyrityksen kannalta merkittävää muutosta) ei kuitenkaan aiheuta ongelmia, koska ohje on sopusoinnussa erityisen riskinarvioinnin kolmannen periaatteen soveltamisen kanssa.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.11. Uuden liikkuvan kalustotyypin hyväksymistä koskeva riskinarviointiesimerkki

C.11.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.11.2. Tämä riskinarvioinnin esimerkki koskee uudentyyppisen liikkuvan kaluston hyväksyntää. Riskinarviointi tehtiin uuden tavaravaunun käyttöönottoon liittyvien riskien evaluoimiseksi.

C.11.3. Muutoksen tarkoituksen oli lisätä tietyllä rahtilinjalla tehtävien tavarankuljetusten tehokkuutta, määrää, suorituskykyä ja luotettavuutta. Koska vaunuja oli tarkoitus käyttää rajat ylittävässä liikenteessä, tarvittiin lisäksi kahden eri kansallisen turvallisuusviranomaisen hyväksyntä. Hakijana oli rahtiliikenteen harjoittaja, joka puolestaan omisti kuljetettavia tuotteita valmistavan tehtaan.

C.11.4. Hanke koostui uuden liikkuvan kaluston rakentamisesta, valmistuksesta, muokkaamisesta, käyttöönotosta ja tarkistamisesta. Riskinanalyysissa varmistettiin, että uusi suunnittelu täytti kunkin osajärjestelmän ja koko järjestelmän turvallisuusvaatimukset.

C.11.5. Riskianalyysissa viitataan CENELEC-standardin EN 50126 menettelyihin ja määritelmiin, ja riskianalyysi tehtiin tämän standardin mukaisesti.

C.11.6. YTM:n prosessiin verrattuna riskinarvioinnissa oli seuraavat vaiheet:

(a) järjestelmäkuvaus [2.1.2 kohta]:

Kaikille suunnittelun vaiheille oli asetettu vaatimukset, jotka koskivat turvallisuuden varmentamista koskevaa dokumentointia ja järjestelmäsuunnittelun kuvausta:

(1) suunnitteluvaihe: käyttäjien vaatimusten alustava kuvaus;
(2) määritelmävaihe: toiminnallinen eritelmä, sovellettavat tekniset standardit, testaus- ja varmennussuunnitelma. Vaihe käsitti myös käyttäjien vaatimukset, jotka koskivat vaunun käyttöä ja kunnossapitoa;
(3) valmistusvaihe: valmistajan tekninen dokumentaatio, mukaan lukien piirrustukset, standardit, laskelmat, analyysit jne. Uusien tai innovatiivisten rakenteiden tai uusien käyttöalojen syvällinen riskinarviointi;
(4) varmennusvaihe:

(i) valmistaja varmensi vaunun teknisen suorituskyvyn (testikertomukset, laskelmat, toiminnallisten vaatimusten ja standardien noudattamista koskevat varmennukset);

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(ii) sellaisten riskiä vähentävien toimenpiteiden ja testikertomusten dokumentointi, joilla voidaan osoittaa vaunujen soveltuvuus rautatieinfrastruktuuriin;
(iii) huolto- ja koulutusmateriaali, käyttöohjeet jne.

(5) hyväksyntävaihe:

(i) valmistajan turvallisuustodistus ja turvallisuutta koskeva näyttö (turvallisuusarvio);
(ii) tavaravaunua ja siitä laadittua dokumentaatiota koskeva käyttäjän hyväksyntä;

(b) vaarojen tunnistaminen [2.2 kohta]:

Tätä kohtaa sovellettiin järjestelmällisesti kaikissa suunnittelun vaiheissa. Aluksi käytettiin alhaalta ylöspäin suuntautuvaa lähestymistapaa, jossa eri valmistajat arvioivat riskisarjoja, jotka johtuivat osajärjestelmien komponenttien vioista. Jako osajärjestelmiin oli seuraavanlainen:

(1) kuljetusalusta
(2) jarrutusjärjestelmä
(3) keskuspuskimet
(4) jne.

Tämän jälkeen sovellettiin täydentävää ylhäältä alaspäin suuntautuvaa lähestymistapaa aukkojen tai puuttuvien tietojen löytämiseksi. Riskit, joita ei voitu välittömästi hyväksyä, siirrettiin vaaroja koskevaan asiakirjaan lisäkäsittelyä ja luokittelua varten.

(c) hyväksyttävää riskitasoa koskevien periaatteiden soveltaminen [2.1.4 kohta]:

Koko järjestelmälle tehtiin eksplisiittinen riskin estimointi. Yksittäisiä vaaroja olisi kuitenkin voitu arvioida myös menettelyohjeiden tai vastaavien ohjeistojen avulla. Periaatteena on, että kaikkien uusien osajärjestelmien on oltava vähintään yhtä turvallisia kuin niillä korvattavien osajärjestelmien, minkä ansiosta uusi järjestelmä on kokonaisuudessaan turvallisempi kuin aikaisempi. Standardin EN 50126 riskimatriisia käytettiin tunnistettujen vaarojen kartoittamiseen. Lisäksi sovellettiin erilaisia hyväksyttävää riskitasoa koskevia lisäperusteita, kuten

(1) yksittäisen virheen ei pidä johtaa tilanteeseen, josta voi olla vakavia seurauksia ihmisille, kalustolle tai ympäristölle;
(2) ellei tätä voida välttää teknisen rakentamisen keinoin, se on estettävä toimintasääntöjen tai kunnossapitovaatimusten avulla. Tätä sovellettiin ainoastaan vaaroihin, joiden osalta vika oli mahdollista havaita, ennen kuin se johti vaaralliseen tilanteeseen;
(3) osille, joiden vioittuvuus on hyvin todennäköistä tai joiden vikoja ei voida havaita etukäteen eikä niitä voida ehkäistä toimintasääntöjä soveltamalla, on harkittava ylimääräisiä turvallisuustoimintoja ja esteitä;
(4) kaksinkertaisia järjestelmiä, joiden osat saattavat vikaantua käytön aikana ilman, että sitä havaitaan, on suojattava kunnossapitotoimenpiteillä, joilla ehkäistään kaksinkertaisuuden menetys;
(5) lopullinen turvallisuustaso oli hallinnollinen päätös, joka perustui kvantitatiiviseen ja kvalitatiiviseen riskianalyysiin.

(d) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

Kaikki tunnistetut riskit ja vaarat kirjattiin ylös, ja niiden luetteloa tutkittiin ja päivitettiin jatkuvasti. Jäljellä olevat vaarat kirjattiin vaaroja koskevaan asiakirjaan yhdessä rakentamisessa, käytössä ja kunnossapidossa toteutettavista riskiä vähentävistä toimenpiteistä laaditun vastaavan luettelon kanssa. Tämän perusteella laadittiin

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

lopullinen turvallisuuskertomus, jossa varmennettiin, että turvallisuusvaatimukset oli täytetty;

(e) vaarojen hallinta [4.1 kohta]:

Kuten edellä on todettu, vaarat ja niihin liittyvät turvallisuustoimenpiteet kirjattiin vaaroja koskevaan asiakirjaan, jossa oli ajantasaiset tiedot kaikista yksilöidyistä vaaroista ja turvallisuustoimenpiteistä. Vaaroja, jotka liittyivät ilman toimenpiteitä hyväksyttävällä riskitasolla oleviin riskeihin, ei kuitenkaan sisällytetty vaaroja koskevaan asiakirjaan;

(f) riippumaton arviointi [6 artikla]:

Tähän merkittävään muutokseen liittyvissä asiakirjoissa ei mainittu riippumatonta arviointia.

C.11.7. Tämä riskinarviointiesimerkki perustuu CENELEC-standardiin EN 50126 , ja se vastaa näin ollen hyvin YTM-prosessia. Esimerkin riskinarviointi täyttää YTM-asetuksen vaatimukset, lukuun ottamatta riippumattomaa arviointia koskevaa vaatimusta, jota ei täsmennetty erikseen vastaanotetuissa asiakirjoissa. Hyväksyttävää riskitasoa koskevia eksplisiittisiä perusteita sovellettiin, ja ne ilmaistiin selkeästi.

C.12. Riskinarviointiesimerkki merkittävästä toiminnallisesta muutoksesta – Kuljettajan yksin suorittama toiminto

C.12.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.12.2. Tämä esimerkki koskee toiminnalista muutosta, jossa rautatieyritys päätti, että kuljettajan oli vastattava junan yksin ohjauksesta (ainoastaan kuljettajan ohjaama, AKO) reitillä, jolla oli aikaisemmin kalustoyksikössä avustaja, joka auttoi kuljettajaa junan lähettämisessä.

C.12.3. YTM-prosessiin verrattuna käytössä olivat seuraavat vaiheet (katso myös kaavio 1):

(a) muutoksen merkityksellisyys [4 artikla]:

Rautatieyritys teki alustavan riskinarvioinnin, jossa todettiin, että toiminnallinen muutos oli merkittävä. Koska kuljettajan oli toimittava yksin ilman apua, oli otettava huomioon sen mahdollisuus, että matkustajat jäisivät ovien väliin tai putoaisivat raiteille (esim. jos ovet avautuvat väärällä puolella).

Jos tätä alustavaa riskinarviointia verrataan YTM-asetuksen 4 artiklan mukaisiin perusteisiin, muutos on mahdollista luokitella merkittäväksi myös seuraavien perusteiden nojalla:

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(1) merkitys turvallisuuden kannalta: muutos vaikuttaa turvallisuuteen, koska sillä, että kuljettajan on hallittava junan toimintoja aiemmasta kokonaan poikkeavalla tavalla, saattaa olla tuhoisia seurauksia;
(2) vian seuraukset: kuljettajan suorituskyvyn vaikutukset saattavat johtaa tuhoisiin seurauksiin, mikäli toimintoa ei valvota tehokkaasti;
(3) uutuus: kuljettajan yksin suorittama toimenpide saattaa edellyttää uudenlaisia junan ohjaustapoja, joiden riskit on arvioitava;

(b) järjestelmämäärittely [2.1.2 kappale]:

Järjestelmämäärittelyssä kuvattiin:

(1) käytössä ollut järjestelmä, minkä yhteydessä selitettiin tarkasti, mitä tehtäviä kuljettaja suoritti ja missä tehtävissä kalustoyksikössä ollut avustaja avusti kuljettajaa;
(2) kuljettajien vastuualueiden muutos junassa avustaneen henkilöstön poiston vuoksi;
(3) toiminnon muuutosten hallitsemista koskevat tekniset vaatimukset;
(4) kalustoyksikössä olevan avustavan henkilöstön, kuljettajan ja radan varrella olevan infrastruktuurin haltijan henkilöstön väliset rajapinnat;

Toistojen aikana järjestelmämäärittelyä päivitettiin riskinarvioinnin perusteella laadituilla turvallisuusvaatimuksilla. Keskeiset henkilöt (mukaan lukien kuljettajat, henkilöstön edustajat ja infrastruktuurin haltija) osallistuivat tähän toistuvaan prosessiin, jossa vaarat tunnistettiin ja järjestelmämäärittelyä päivitettiin.

(c) vaarojen tunnistaminen [2.2 kohta]:

Vaarat ja mahdolliset turvallisuustoimenpiteet yksilöitiin asiantuntijaryhmän aivoriihessä, johon osallistuivat muun muassa

(1) toiminnallista kokemusta hankkineet kuljettajien ja henkilöstön edustajat ;
(2) infrastruktuurin haltijan edustajat, sillä muutos saattoi vaikuttaa myös infrastruktuuriin ja edellyttää muutoksia esimerkiksi asemille (kuten peilien/videovalvontajärjestelmän [CCTV] asentaminen laitureille);

Kuljettajien suoritettaviksi tulevat uudet tehtävät tutkittiin tarkoin, jotta voitiin tunnistaa kaikki mahdolliset vaarat, joita saattaisi ilmetä sen jälkeen, kun kalustoyksikössä olevasta avustavasta henkilöstöstä luovuttaisiin. Vaarojen tunnistamisen yhteydessä selvitettiin erityisesti, mitä keskeisiä toiminnallisia vaaroja voisi ilmetä asemilla, nykyisillä reiteillä, joissa saatiin apua kalustoyksikössä olevalta avustavalta henkilöstöltä tai junan varressa olevalta henkilöstöltä, mukaan lukien junien turvallinen lähtö, kuljettajaan liittyvät erityiskysymykset, liikkuva kalusto (esimerkiksi oven avaus/sulkeutumisen varmistaminen), huoltovaatimukset jne.

Kaikkien tunnistettujen vaarojen osalta määriteltiin riskin ja seurauksien vakavuustaso (korkea, kohtalainen, matala), ja ehdotetun muutoksen vaikutuksia arvioitiin suhteessa näihin riskeihin (lisääntynyt, muuttumaton, pienentynyt).

(d) menettelyohjeiden [2.3 kohta] ja vastaavien ohjeistojen [2.4 kohta] käyttö:

Sekä menettelyohjeita (eli ainoastaan kuljettajan ohjaamaa toimintoa koskevia standardeja) ja vastaavia ohjeistoja käytettiin turvallisuusvaatimusten määrittämiseksi tunnistetuille vaaroille. Näihin turvallisuusvaatimuksiin kuuluivat:

(1) tarkistetut toimintamenettelyt kuljettajalle, jonka on pystyttävä toimimaan junassa turvallisesti ilman junasta saatavaa apua;
(2) kaikki muut junassa tai raiteilla tarvittavat laitteet, joiden avulla voidaan varmistaa turvallinen ja luotettava toiminta junan lähtiessä liikkeelle;

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

(3) tarkistuslista, jonka avulla varmistetaan, että kuljettajan ohjaamo on asianmukainen, kun otetaan huomioon rautatiejärjestelmän (sekä kalustoyksikön että radanvarren) ja kuljettajan välinen rajapinta;

Tarvittavia toimintasääntöjä tarkistettiin sovellettavien menettelyohjeiden ja vastaavien ohjeistojen mukaisesti. Kaikki tarvittavat osapuolet osallistuivat tarkistettuihin toimintamenettelyihin, ja suostuivat toteuttamaan muutoksen.

(e) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [kohta 3]:

Järjestelmä toteutettiin yksilöityjen turvallisuusvaatimusten (lisälaitteet ja tarkistetut menettelyt) mukaisesti. Vaatimusten mukaisten keinojen katsottiin takaavan asianmukaisesti arvioitavan järjestelmän riittävän turvallisuuden.

Rautatieyrityksen turvallisuusjohtamisjärjestelmässä otettiin käyttöön tarkistetut toimintamenettelyt. Niitä valvottiin ja tarkistettiin tarvittaessa, jotta voitiin varmistaa, että tunnistettuja vaaroja valvotaan asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(f) vaarojen hallinta [4.1 kohta]:

Katso edeltävä kohta, koska rautatieyrityksillä vaarojen hallintaprosessi voi riskien kirjaamisen ja hallinnan osalta sisältyä niiden turvallisuusjohtamisjärjestelmään. Tunnistetut vaarat ja niihin liittyviä riskejä koskevat turvallisuustoimenpiteet eli viittaus kalustoyksikössä ja radan varrella olevaan lisälaitteistoon ja toimintamenettelyjen tarkistamiseen, kirjattiin vaaroja koskevaan asiakirjaan.
Tarkistettuja menettelyjä valvottiin ja tarkistettiin tarvittaessa, jotta voitiin varmistaa, että tunnistettuja vaaroja valvottiin asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(g) riippumaton arviointi [6 artikla]:

Arviointiprosessista riippumaton rautatieyrityksen pätevä henkilö arvioi riskinarvioinnin ja riskinhallinnan prosessit. Hän arvioi sekä menettelyn että sen tulokset eli yksilöidyt turvallisuusvaatimukset.

Rautatieyritys perusti uuden järjestelmän toteuttamispäätöksensä pätevän henkilön laatimaan riippumattomaan arviointikertomukseen.

C.12.4. Tämä esimerkki osoittaa, että rautatieyrityksen soveltamat periaatteet ja prosessi ovat yhteisen turvallisuusmenetelmän mukaiset. Riskinhallinnan ja riskinarvioinnin prosesseissa täytettiin kaikki YTM-asetuksen mukaiset velvollisuudet.

C.13. Esimerkki: ohjeiston käyttö uusia saksalaisia lukitusjärjestelmiä koskevien turvallisuusvaatimusten määrittämiseksi

C.13.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.13.2. Deutsche Bahn oli tehnyt jo hyväksyttyä sähköistä järjestelmää koskevan riskianalyysin voidakseen johtaa siitä yleiset turvallisuusvaatimukset uusille sähköisille lukitusjärjestelmille. Kyseiset järjestelmät oli aiemmin hyväksytty saksalaisten menettelyohjeiden (Mü 8004) mukaisesti.

C.13.3. Riskianalyysi tehtiin CENELEC-standardien (EN 50126 ja EN 50129) mukaisesti, ja se käsitti seuraavat vaiheet:

(a) järjestelmämäärittely
(b) vaarojen tunnistaminen
(c) vaaran arviointi ja kvantifiointi.

C.13.4. Järjestelmämäärittelyssä oli määriteltävä huolella järjestelmän rajat, tehtävät ja rajapinnat. Suurimpana haasteena oli määritellä järjestelmä siten, että se on riippumaton lukitusjärjestelmän sisäisestä rakenteesta mutta edelleen yhteensopiva nykyisten lukitusjärjestelmien kanssa. Erityistä huomiota kiinnitettiin näin ollen siihen, että lukituksen kanssa yhteydessä olevien ulkopuolisten järjestelmien rajapinnat määriteltiin erittäin selkeästi ilman, että lukituksen sisäisiä toimintoja selvitettiin yksityiskohtaisesti.

C.13.5. Tämän jälkeen vaarat tunnistettiin ainoastaan rajapintojen osalta, jotta pysyttäisiin yleisellä tasolla (eli vältettäisiin riippuvuus joistakin tietyistä rakenteista). Huomioon otettiin ainoastaan teknisistä vioista johtuvat vaarat. Kunkin rajapinnan osalta tunnistettiin näin ollen kaksi yleistä vaaraa:

(a) lukitus välittää väärän tiedon rajapinnalle
(b) (oikea) tieto korruptoituu rajapinnalla.

C.13.6. Tämän jälkeen selvitettiin näiden rajapintojen yleisten vaarojen tarkemmat piirteet.

C.13.7. Seuraavassa vaiheessa arvioitiin nykyisen järjestelmän komponenttien osuus kustakin tunnistetusta vaarasta ja niistä laadittiin vikapuu. Tällä tavoin komponenttien arvioidun vioittuvuuden perusteella voitiin laskea kunkin vaaran esiintymistiheys, jota voitiin pitää uusien sähköisten lukituslaitteiden hyväksyttävänä vaaratasona (varmuusvikatajuus, THR).

C.13.8. Kansallinen turvallisuusviranomainen (EBA) valvoi riskianalyysia ja arvioi sen.

C.13.9. Riskianalyysin yhteydessä arvioitiin myös sähköisen järjestelmän ohjaus- ja näyttötoiminnot. Jälleen vertailukohteeksi otettiin jo käytössä ollut hyväksytty sähköinen lukitusjärjestelmä, jonka perusteella voitiin johtaa turvallisuusvaatimukset käyttöliittymän (MMI) toiminnoille, joilla hallitaan satunnaisvikoja ja järjestelmällisiä vikoja. Tämän perusteella määriteltiin turvallisuuden eheystasot (SIL) eri toiminnoille: vakiokäytön käyttöliittymätoiminnoille, hallinta-vapautus-toiminnolle (vajaatoiminta) ja näytön toimivuudelle.

C.13.10. Myös kansallinen turvallisuusviranomainen (EBA) valvoi riskianalyysia ja arvioi sen.

C.13.11. Nämä riskinarvioinnin esimerkit havainnoillistavat, kuinka YTM-asetuksen toista hyväksyttävää riskitasoa koskevaa perustetta (vertailujärjestelmä) voidaan käyttää uusien järjestelmien turvallisuusvaatimusten johtamisessa. Lisäksi esimerkit perustuivat CENELEC-standardeihin, minkä vuoksi ne vastaavat hyvin YTM-prosessia. Esimerkkien riskinarviointi täyttää YTM-asetuksen vaatimukset, jotka liittyvät soveltamisalan kattamiin vaiheisiin. Koska soveltamisala ei kuitenkaan kata suunnittelutoimintaa, arvioinnissa ei viitata vaaroja

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

koskevan asiakirjan hallintaan eikä sen osoittamiseen, että arvioitava järjestelmä on yksilöityjen turvallisuusvaatimusten mukainen.

C.13.12. Lisätietoa näistä riskinarvioinneista:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, s. 10–15, ja

(b) Bock, H., Braband, J., and Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, s. 234–253.

C.14. Esimerkki eksplisiittistä hyväksyttävää riskitasoa koskevasta perusteesta: saksalaisen FFB:n (junansuojajärjestelmä) radiopohjainen toiminto

C.14.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteisen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:

(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljitettävyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän muutoksen tapauksessa. Kaikkien merkittävien muutosten riskinarviointi on tehtävä YTM-asetuksen mukaisesti.

C.14.2. CENELEC-standardien mukainen riskianalyysi tehtiin täysin uudelle toimintamenettelylle, jonka käyttöönottoa Saksan tavanomaisilla rautatielinjoilla suunniteltiin (mutta jota ei koskaan otettu käyttöön). Suunnitelman mukaan junien turvallisuustoiminto perustuisi ainoastaan radiopohjaiseen (reitti ja juna) valvontaan. Koska aiempia menettelyohjeita (hyväksyttyjä rakentamissääntöjä) tai ohjeistoja tällaiselle uudelle järjestelmälle ei ollut, tehtiin eksplisiittinen riskin estimointi sen osoittamiseksi, että uusi menettely on turvallinen. Oli tarpeen osoittaa, että uudessa järjestelmässä matkustajaan kohdistuvan riskin taso ei ylittäisi hyväksyttävää riskitasoa (hyväksyttävää riskitasoa koskeva peruste).

C.14.3. Tämä hyväksyttävää riskitasoa koskeva peruste määritettiin niiden Saksassa tapahtuneiden onnettomuuksien tilastojen perusteella, joiden syynä katsottiin olevan merkinanto- ja ohjausjärjestelmä, ja perusteen luotettavuus tarkistettiin MEM-perusteen (maksimientropiamenetelmä) avulla. Turvallisuusvaatimusten täyttymisen osoittaminen tällä tavoin on sopusoinnussa Saksan EBO-asetuksen vaatimuksen kanssa; asetuksen nojalla rakennussäännöistä poikettaessa on säilytettävä "sama turvallisuustaso". Myös kansallinen turvallisuusviranomainen (EBA) valvoi riskianalyysia ja arvioi sen.

C.14.4. Tämä riskinarviointiesimerkki osoittaa, miten yleinen eksplisiittinen peruste voidaan johtaa (YTM:n asetuksen kolmannen hyväksyttävää riskitasoa koskevan perusteen osalta) uusille järjestelmille, joille ei ole soveltuvia menettelyohjeita eikä ohjeistoja. Tämän jälkeen uudelle järjestelmälle tehty riskianalyysi perustui CENELEC-standardeihin ja vastasi siten hyvin

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

YTM-prosessia. Esimerkin riskinarviointi täyttää YTM-asetuksen vaatimukset, mutta siinä ei viitata vaaroja koskevan asiakirjan hallintaan eikä vaadita osoittamaan, että arvioitava järjestelmä on yksilöityjen turvallisuusvaatimusten mukainen.

C.14.5. Lisätietoa tästä riskianalyysista: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, s. 10–15

C.15. Esimerkki RAC-TS:n sovellettavuustestistä

C.15.1. Tässä liitteessä on tarkoitus havainnollistaa kalustoyksikössä olevan ETCS-osajärjestelmän toiminnon osalta, miten 2.5.4 kohdan mukaista perustetta olisi sovellettava ja miten voidaan todeta, sovelletaanko tässä yhteydessä RAC-TS:ää.

C.15.2. Kalustoyksikössä oleva ETCS-osajärjestelmä on tekninen järjestelmä. Tässä yhteydessä tarkastellaan sen seuraavaa tehtävää: *"tarjoaa tarjoaa kuljettajalle tietoa, jonka avulla hän voi ohjata junaa turvallisesti ja käyttää jarrujärjestelmää ylinopeustilanteessa"*.

Toiminnon kuvaus: kalustoyksikössä oleva ETCS-osajärjestelmä laskee radanvarresta saadun tiedon (sallittu nopeus) avulla junan nopeuden, jonka perusteella

(a) kuljettaja ohjaa junaa ja varmistaa, ettei nopeus ylitä sallittua;
(b) samanaikaisesti kalustoyksikössä oleva ETCS-osajärjestelmä valvoo, ettei juna milloinkaan ylitä sallittua nopeusrajoitusta. Ylinopeustapauksissa järjestelmä jarruttaa automaattisesti.

Sekä kuljettaja että kalustoyksikössä oleva ETCS-osajärjestelmä käyttävät junan nopeutta koskevaa arviota, jonka kalustoyksikössä oleva ETCS-osajärjestelmä laskee.

C.15.3. Kysymys: "Sovelletaanko RAC-TS:ää junassa olevan osajärjestelmän suorittamaan junan nopeuden arviointiin?"

C.15.4. Kulkukaavion 14 soveltaminen, ja vastaukset eri kysymyksiin:

(a) Teknisen järjestelmän tarkasteltava vaara:

"ETCS:lle ohjeistetun turvallisen nopeuden ylittäminen" (katso UNISIG SUBSET 091).

(b) Voidaanko vaaraa hallita menettelyohjeiden tai ohjeiston avulla?

EI. Oletetaan, että ETCS-järjestelmän rakenne on uusi ja innovatiivinen. Tämän vuoksi menettelyohjeita tai ohjeistoja, joiden avulla vaarat voitaisiin hallita hyväksyttävälle riskitasolle, ei ole.

(c) Onko todennäköistä, että vaara voi johtaa tuhoisaan seuraukseen?

KYLLÄ, koska *"ETCS:lle ohjeistetun turvallisen nopeuden ylittäminen"* voi johtaa junan suistumiseen raiteilta, joka puolestaan saattaa aiheuttaa *"kuolemantapauksia ja/tai useita vakavia loukkaantumisia ja/tai merkittäviä ympäristövahinkoja"*.

(d) Onko tuhoisa seuraus suora tulos teknisen järjestelmän viasta?

KYLLÄ, jos muita turvaesteitä ei ole. Kalustoyksikössä olevan ECTS-osajärjestelmän laskema sama arvio junan nopeudesta annetaan sekä kuljettajalle että kalustoyksikössä olevan ETCS-osajärjestelmän jarrutuksen hallintatoiminnolle. Tämän vuoksi kun oletetaan, että kuljettaja ohjaa junaa (suorituskykyyn liittyvistä syistä) radanvarsitietojen mukaisella sallitulla enimmäisnopeudella, kuljettaja ja junan ETCS-osajärjestelmä eivät

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

havaitse, että juna ajaa ylinopeutta, mikäli junan nopeus on aliarvioitu. Tämä saattaa johtaa junan suistumiseen raiteilta ja siten tuhoisiin seurauksiin.

(e) Päätelmät:

(1) kvantitatiivisten vaatimusten osalta: sovelletaan varmuusvikataajuutta 10^{-9} h^{-1} kalustoyksikön ETCS-osajärjestelmän satunnaisiin laitteistovikoihin ja varmistetaan, että

(i) tämän kvantitatiivisen tavoitteen arvioinnissa otetaan kaksinkertaisten järjestelmien osalta huomioon yhteiset komponentit (esimerkiksi erilliset tai yhteiset syötteet kaikille kanaville, yhteinen virtalähde, komparaattorit, valitsimet jne.);
(ii) passiivisen tai piilevän vian tunnistamiseen kuluva aika on otettu huomioon;
(iii) yhteisvikojen ja yhteisvioittumistapojen (CCF/CMF) arviointi on tehty;
(iv) riippumaton arviointi on tehty;

(2) prosessivaatimusten osalta: sovelletaan SIL 4 -menetelmää kalustoyksikössä olevan ETCS-osajärjestelmän järjestelmällisten vikojen/virheiden hallintaan. Tämä edellyttää, että sovelletaan

(i) SIL 4:n mukaista laadunhallintaprosessia;
(ii) SIL 4:n mukaista turvallisuusjohtamisprosessia;
(iii) asianmukaisia standardeja, kuten

- ohjelmistojen kehittämiseen standardia EN 50 128;
- laitteistojen kehittämiseen muun muassa seuraavia standardeja: EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2;

(3) prosessi(e)n riippumaton arviointi.

C.16. Esimerkkejä vaaroja koskevan asiakirjan mahdollisista rakenteista

C.16.1. Johdanto

C.16.1.1. Vaaroja koskevaan asiakirjaan sisällytettävien tietojen vähimmäisvaatimukset esitetään YTM-asetuksen 4.1.2 kohdassa. Nämä tiedot on merkitty varjostetulla taustalla jäljempänä oleviin vaaroja koskevien asiakirjojen esimerkkeihin.

C.16.1.2. Vaaroja koskeva asiakirja ja mahdolliset lisätiedot, joilla kuvataan vaaroja ja niihin liittyviä turvallisuustoimenpiteitä, voidaan muotoilla monella tavalla. Esimerkiksi vaarat ja niihin liittyvät turvallisuustoimenpiteet voidaan esittää siten, että yhdessä kentässä annetaan aina yksi tieto. Riippumatta käytetystä rakenteesta on kuitenkin tärkeää, että vaaroja koskevasta asiakirjasta käy selvästi ilmi vaarojen ja niihin liittyvien turvallisuustoimenpiteiden yhteys. Yksi mahdollinen ratkaisu on, että vaaroja koskeva luettelo sisältää kunkin vaaran ja turvallisuustoimenpiteen osalta vähintään kentän, jossa on:

(a) selkeä kuvaus, joka sisältää viittaukset vaaran alkuperään ja hyväksyttävää riskitasoa koskevaan periaatteeseen, joka on valittu vaaran hallitsemiseksi. Tämän kentän avulla voidaan ymmärtää vaara ja siihen liittyvät turvallisuustoimenpiteet sekä selvittää, missä turvallisuusarvioinnissa ne on yksilöity.

Koska vaaroja koskevaa asiakirjaa käytetään ja ylläpidetään koko järjestelmän elinkaaren aikana (eli järjestelmän käytön ja kunnossapidon aikana), on hyvä varmistaa jäljitettävyys kunkin vaaran ja seuraavien seikkojen välillä:

(1) riski;

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) vaarojen syyt, jos ne ovat jo selvillä;
(3) vastaavat turvallisuustoimenpiteet sekä arvioitavana olevan järjestelmän rajat määrittelevät oletukset;
(4) vastaavat turvallisuusarvioinnit, joissa vaarat on tunnistettu;

Lisäksi turvallisuustoimenpiteiden (erityisesti niiden, jotka on siirrettävä muille toimijoille kuten hakijoille) sanamuodon sekä niihin liittyvien vaarojen ja riskien sanamuodon on oltava selkeä ja riittävä. ”Selkeä ja riittävä” tarkoittaa, että turvallisuustoimenpiden ja niihin liittyvien vaarojen kuvauksista käy ilmi, mitä riskejä niillä on tarkoitus hallita ilman, että tämä asia on selvitettävä vastaavista turvallisuusarvioinneista.

(b) hyväksyttävää riskitasoa koskeva periaate, jota on käytetty vaaran hallitsemiseksi, jotta voidaan tukea vastavuoroista tunnustamista ja auttaa arviointielintä arvioimaan YTM:n asianmukaista soveltamista;

(c) selkeät tiedot tilanteesta: tässä kentässä ilmoitetaan, onko vaara/turvallisuustoimenpide yhä avoinna vai onko se hallittu/vahvistettu.

(1) avointa vaaraa/turvallisuustoimenpidettä seurataan, kunnes se on hallittu/vahvistettu;
(2) vastaavasti hallittuja/vahvistettuja vaaroja/turvallisuustoimenpiteitä ei enää seurata, ellei järjestelmän toiminnassa tai kunnossapidossa tapahdu merkittäviä muutoksia: katso 2.1.1 kohtaa koskevan G 6 kohdan b alakohta. Jos näin on:

(i) YTM:ää sovelletaan uudelleen vaadittuun muutokseen sen 2 artiklan nojalla. Katso myös 2.1.1 kohtaa koskevan G 6 kohdan b alakohdan 1 alakohta;
(ii) kaikki varmennetut vaarat ja turvallisuustoimenpiteet tutkitaan uudelleen sen varmistamiseksi, ettei muutos vaikuta niihin. Jos muutos vaikuttaa niihin, vaaroja ja niihin liittyviä turvallisuustoimenpiteitä tarkastellaan uudelleen , ja niitä hallinnoidaan uudelleen vaaroja koskevan asiakirjan avulla;

Joissain tapauksissa saatetaan toteuttaa muita turvallisuustoimenpiteitä kuin niitä, jotka on kirjattu vaaroja koskevaan luetteloon (esimerkiksi kustannussyistä). Toteutetut turvallisuustoimenpiteet kirjataan vaaroja koskevaan luetteloon yhdessä näytön/perustelujen kanssa; näytöstä ja perusteluista on käytävä ilmi, miksi turvallisuustoimenpiteet ovat asianmukaisia, ja niillä on osoitettava, että näiden toimenpiteiden ansiosta järjestelmä täyttää turvallisuusvaatimukset.

(d) viittaus asiaa koskevaan näyttöön, joka koskee vaaran hallintaa tai turvallisuustoimenpiteen vahvistamista. Tästä kentästä löytyy myöhemmin näyttö, joka koskee vaaran hallitsemista ja turvallisuustoimenpite(id)en vahvistamista;

Vaaraa voidaan hallita vaaroja koskevassa asiakirjassa ainoastaan, jos kaikki vaaraan liittyvät turvallisuustoimenpiteet vahvistetaan etukäteen;

(e) organisaatio(t) tai yksikö(t), jotka vastaavat vaaran hallinnoinnista.

C.16.1.3. Toinen esimerkki vaaroja koskevan asiakirjan mahdollisesta sisällöstä annetaan ohjeen EN 50126-2 {Ref. 9} liitteessä A.3.

Euroopan rautatievirasto ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● Ranska ● Puh. +33 (0)3 27 09 65 00 ● Faksi +33 (0)3 27 33 40 65 ●
http://www.era.europa.eu

C.16.2. Esimerkki vaaroja koskevasta asiakirjasta lisäyksessä C olevassa C.5. kohdassa tarkoitetun organisatorisen muutoksen tapauksessa

Taulukko 6: Esimerkki vaaroja koskevasta asiakirjasta liitteessä C olevassa C.5 kohdassa tarkoitetun organisatorisen muutoksen tapauksessa.

Vaaran kuvaus	**Turvallisuustoimenpiteet**	**Tärkeys/ Turvallisuus Täsmällisyys**	**Täytäntöön-pano**[18]	**Huomautuksia**	**Vastuu**[18]	**Alku-perä**	**Sovellettu hyväksyttä-vää riskitasoa koskeva periaate**	**Varmentami sen vastuu-henkilö**	**Varmen tamis-tapa**	**Tilanne xx.xx.xx**
Yritykseen jääneiden työntekijöiden motivaation heikkeneminen. Henkilöstöä lähtee tämän vuoksi jatkuvasti pois yrityksestä. Huonosti motivoituneet esimiehet	Uusi henkilöstön motivointihanke, joka toteutetaan pienryhmissä. Varojen uudelleenkohdentaminen siten, että yrityksen hoidettavaksi annetaan tärkeitä tehtäviä. Infrastruktuurin haltijan tiheämmin toteuttamat tarkastukset. Varojen kohdentamisella varmistetaan, että keskeinen henkilöstö pysyy samana koko prosessin ajan. Kiinnitetään erityistä huomiota siihen, että lähtevien työntekijöiden tiedot ja taidot siirretään heidän tehtäviään jatkaville henkilöille. jne.	Korkea/ Korkea	XYZ koordinoi. Alueiden on suunniteltava toimenpiteet raiteiden valvonnan, limittäisen henkilöstön ja esimiesten tekemän valvonnan lisäämiseksi	Tarkastusten lisääminen on kirjattava sopimuksiin. Jne.	Yritys-johtaja	Aivoriihi HAZID-kertomus R_X	Ei sovellu			Muuttuneet olosuhteet ovat pienentäneet merkittävästi tätä riskiä. Työympäristön arviointi on tehty, ja henkilöstöä on koulutettu.
Yrittäjien alihankkijoiden ammatti-taidottomuus, epä-pätevyys ja laadunvalvonnan puute	Vaaditaan enemmän dokumentoitua näyttöä pätevyydestä. Valvotaan järjestelmällisesti suoritettuja tehtäviä.	Korkea/ Kohtalainen	IM koordinoi. Alueiden on toteutettava toimenpiteet, jotka edellyttävät ammattitaitoa ja työn valvontaa	Toteutetaan sopimusten seurannassa. Aihe sopimusten tarkistamisen suunnitteluun.	Infra-struktuurin haltija	Aivoriihi HAZID - kertomus R_X	Ei sovellu	Turvallisuus-johtaja		Keskitytään enemmän jatkuvaan valvontaan (2 toiminnallista tarkistusta kuukaudessa ja toiminta-aluetta kohti)

(18) *Nämä kaksi saraketta sisältävät tietoja/kenttiä tunnistettujen vaarojen hallinnasta vastaavista toimijoista.*

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

Taulukko 6: Esimerkki vaaroja koskevasta asiakirjasta liitteessä C olevassa C.5 kohdassa tarkoitetun organisatorisen muutoksen tapauksessa.

Vaaran kuvaus	**Turvallisuustoimenpiteet**	**Tärkeys/ Turvallisuus Täsmällisyys**	**Täytäntöön-pano(18)**	**Huomautuksia**	**Vastuu(18)**	**Alku-perä**	**Sovellettu hyväksyttä-vää riskitasoa koskeva periaate**	**Varmentami sen vastuu-henkilö**	**Varmen tamis-tapa**	**Tilanne xx.xx.xx**
Tehtäviä ja vastuita koskeva epäselvyys yrityksen ja IM:n (intrastruktuurin haltijan) rajapinnalla.	Määritellään tehtävät ja vastuut. Kartoitetaan kaikki rajapinnat ja määritellään niille vastuuhenkilöt.	Kohtalainen/ Kohtalainen	Kukin alue erikseen	Toteutetaan kunnossapito-sopimuksen ja uudelleen-järjestelyä koskevan strategia-suunnitelman avulla	Alue-johtajat	Aivoriihi HAZID – kertomus R_X	Ei sovellu	Turvallisuus-johtaja		Alueet ovat esitelleet strategiansa.

C.16.3. Esimerkki kalustoyksikössä olevasta ohjaus- ja hallintaosajärjestelmästä laaditusta täydellisestä vaaroja koskevasta asiakirjasta

C.16.3.1. Tässä kohdassa esitetään esimerkki yksittäisestä vaaroja koskevasta asiakirjasta (katso 4.1.1 kohtaa koskeva G 3 kohta), jolla hallitaan sekä

(a) kaikkia sisäisiä turvallisuusvaatimuksia, joita sovelletaan toimijan vastuulla olevaan osajärjestelmään; että
(b) kaikkia tunnistettuja vaaroja ja niihin liittyviä turvallisuustoimenpiteitä, joita toimija ei voi panna täytäntöön ja joiden toteuttaminen on siirrettävä muille toimijoille.

Taulukko 7: Esimerkki valmistajan laatimasta kalustoyksikön ohjaus- ja hallintaosajärjestelmän vaaroja koskevasta asiakirjasta.

N° HZD	**Origin**	**Hazard description**	**Additional information**	**Actor in charge**	**Safety Measure**	**Used Risk Acceptance Principle**	**Exported**	**Status**
1	HAZOP – kertomu	Junan enimmäisnopeus on asetettu liian suureksi (Vmax)	Kalustoyksikön osajärjestelmän väärä konfigurointi (kunnossapitohenkilöstö). Kalustoyksikössä syötetty väärä tieto (kuljettaja)	Rautatieyritys	• Määritellään hyväksyntämenettely kalustoyksikössä olevalle	Eksplisiittinen riskin estimointi	Kyllä	Hallittu (siirretty rautatieyritykselle)

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

Taulukko 7: Esimerkki valmistajan laatimasta kalustoyksikön ohjaus- ja hallintaosajärjestelmän vaaroja koskevasta asiakirjasta.

N° HZD	Origin	Hazard description	Additional information	Actor in charge	Safety Measure	Used Risk Acceptance Principle	Exported	Status
	s R_X				järjestelmän konfigurointitiedon osajärjestelmälle; • Määritellään toimintamenetelmä, jonka mukaisesti kuljettaja syöttää tiedot;			Katso myös liitteessä C oleva C.16.4.2. kohta
2	HAZOP - kertomus R_X	Kalustoyksikössä olevan osajärjestelmän konfigurointi (eli liikkumislupa) on liian salliva jarrutuskaarissa	Kalustoyksikössä olevan osajärjestelmän erityinen konfigurointiprosessi riippuu • junan jarrutusjärjestelmään asetetuista turvamarginaaleista • junan jarrutusjärjestelmän reagointiviiveestä (etenkin tavarajunissa tämä riippuu välittömästi junan pituudesta)	Rautatieyritys	• Täsmennetään järjestelmämäärittelyssä asianmukaisesti järjestelmän vaatimukset; • Asetetaan junakohtaisesti jarrujärjestelmin riittävät turvamarginaalit	Eksplisiittinen riskin estimointi	Kyllä	Hallittu (siirretty rautatieyritykselle) Katso myös liitteessä C oleva C.16.4.2. kohta
3	HAZOP - kertomus R_X	• Junan enimmäisnopeus on asetettu liian suureksi (Vmax) • Kalustoyksikössä olevan osajärjestelmän konfigurointi (eli liikkumislupa) on liian salliva jarrutuskaarissa	Kalustoyksikössä olevan osajärjestelmän erityistä konfigurointia ei ole päivitetty junan pyörän läpimitan osalta (kunnossapitohenkilöstö).	Rautatieyritys	• Määritellään menettely, jonka mukaisesti kunnossapitohenkilöstö määrittää junan pyörän läpimitan; • Määritellään menettely junan pyörän läpimitan säännölliseksi päivittämiseksi junassa olevaan osajärjestelmään;	Eksplisiittinen riskin estimointi	Kyllä	Hallittu (siirretty rautatieyritykselle) Katso myös liitteessä C oleva C.16.4.2. kohta
			Konfigurointitietojen valmistelua ja kalustoyksikössä olevaan osajärjestelmään siirtoa koskeva vika valmistajan menettelyssä	Valmistaja	Määritellään menettely junan pyörän läpimitan päivittämiseksi junan konfigurointitietoihin	Eksplisiittinen riskin estimointi	Kyllä	Hallittu menettelyllä P_X
4	HAZOP - kertomus R_X	Suurella nopeudella (160 km/h) kulkevan junan saapuminen rataosuudelle ilman, että kalustoyksikössä oleva osajärjestelmä on aktiivinen, ja ilman radanvarren merkinantojärjestelmää.	Tätä voidaan hallita ainoastaan kuljettajan valppauden avulla. Saapuminen rataosuuden automaattisen junansuojajärjestelmän (ATP) alueelle riippuu kuljettajan ennen siirtymäaluetta antamasta hyväksynnästä. Mikäli hyväksyntää ei anneta, kalustoyksikössä oleva ohjaus- ja hallintajärjestelmä jarruttaa automaattisesti.	Infrastruk-tuurin haltija	Infrastruktuurin haltija varmistaa, etteivät junat, joissa ei ole aktiivista kalustoyksikössä olevaa ohjaus- ja hallintajärjestelmää, liikennöi kyseisillä rataosuuksilla. Määritellään menettely liikennejärjestelyjä varten.	Eksplisiittinen riskin estimointi	Kyllä	Hallittu (siirretty IM:lle) Katso myös liitteessä C oleva C.16.4.2. kohta
				Rautatieyritys	Varmistetaan, että kuljettajat ovat saaneet koulutuksta siirtymisessä rataosuudelle, joka kuuluu ATP-	Eksplisiittinen riskin estimointi	Kyllä	Hallittu (siirretty rautatieyritykselle)

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

Taulukko 7: Esimerkki valmistajan laatimasta kalustoyksikön ohjaus- ja hallintaosajärjestelmän vaaroja koskevasta asiakirjasta.

N° HZD	Origin	Hazard description	Additional information	Actor in charge	Safety Measure	Used Risk Acceptance Principle	Exported	Status
					alueeseen.			Katso myös liitteessä C oleva C.16.4.2. kohta
5	HAZOP -kertomus R_X	Kuljettavan näytöltä lukeman junan enimmäisnopeus on liian suuri (Vmax)	Kuljettajan rajapinnassa esitettävää tietoa valvotaan kalustoyksikössä olevalla SIL 4:n ohjaus- ja hallintaosajärjestelmällä, joka hätäjarruttaa, mikäli näytöllä oleva ja ennakoitu arvo/luku eroavat. Mikäli liikkumislupaa ei noudateta, kalustoyksikössä oleva ohjaus- ja hallintaosajärjestelmä hätäjarruttaa.	Valmistaja	Kehitetään junassa olevaa SIL 4:n ohjaus- ja hallintaosajärjestelmää	Eksplisiittinen riskin estimointi	Kyllä	Turvallisuusarvio, joka osoittaa, että riippumaton turvallisuusarvioija on arvioinut SIL 4 -osajärjestelmän
6	HAZOP -kertomus R_X	Juna lähtee ilman kuljettajan ja koneen välistä rajapintaa	Kalustoyksikössä olevan osajärjestelmän kaksinkertaisen rakenteen menetys	Valmistaja	Kehitetään junassa olevaa SIL 4:n ohjaus- ja hallintaosajärjestelmää	Eksplisiittinen riskin estimointi	Kyllä	Turvallisuusarvio, joka osoittaa, että riippumaton turvallisuusarvioija on arvioinut SIL 4 -osajärjestelmän
jne.								

C.16.4. Esimerkki vaaroja koskevasta asiakirjasta: tiedon siirto muille toimijoille

C.16.4.1 Tässä kappaleessa esitetään esimerkki vaaroja koskevasta asiakirjasta, jolla siirretään tunnistettuja vaaroja ja niihin liittyviä turvallisuustoimenpiteitä, joita kyseinen toimija ei voi toteuttaa, koskevat tiedot muille toimijoille. Katso 4.1.1. kohtaa koskeva G 1 kohta.
Tämä esimerkki on sama kuin liitteessä C olevassa C.16.3.

C.16.4.2. Taulukon 8 viimeisen sarakkeen avulla täytetään YTM-asetuksen 4.2 kohdan mukaiset vaatimukset. Ne voidaan täyttää monella tavalla. Yksi tapa on viitata välitetyt turvallisuustiedot vastaanottaneen toimijan esittämään näyttöön. Toinen tapa on järjestää näiden kahden toimijan välinen kokous, jossa pohditaan yhteisesti, mikä on asianmukainen ratkaisu riski(e)n hallitsemiseksi. Kokouksen tulokset voidaan kirjata yhteisesti hyväksyttyyn asiakirjaan (esimerkiksi kokouspöytäkirjaan), johon turvallisuuteen liittyvää tietoa siirtävä toimija voi viitata kirjatessaan vaarat omaan vaaroja koskevaan asiakirjaansa.

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

Taulukko 8: Esimerkki vaaroja koskevasta asiakirjasta: turvallisuuteen liittyvien tietojen siirtäminen muille toimijoille

Vaaran nro	Vaaran alkuperä		Vaaran kuvaus	Lisätiedot	Vastaava toimija	Turvallisuustoimenpide	Vastaanottajan huomautukset
	Nro taulukossa 7	Muu					
1	nro 1	HAZOP–kertomus R_X	Junan enimmäisnopeus on asetettu liian suureksi (Vmax)	Väärä kalustoyksikön osajärjestelmän erityinen konfigurointi (kunnossapitohenkilöstö). Junassa syötetty väärä tieto (kuljettaja)	Rautatieyritys	• Määritellään hyväksyntämenettely kalustoyksikössä olevalle järjestelmän konfigurointitiedon osajärjestelmälle; • Määritellään toimintamenetelmä, jonka mukaisesti kuljettaja syöttää tiedot;	• Junassa olevan ohjaus- ja hallintajärjestelmän konfigurointitiedot riippuvat liikkuvan kaluston fyysisistä ominaisuuksista. • Turvallisuusmarginaaleja sovelletaan tämän tiedon osalta yhteistyössä infrastruktuurin haltijan ja rautatieyrityksen kanssa. • Tämän jälkeen nämä tiedot syötetään valmistajan asianmukaisten menettelyjen mukaisesti kalustoyksikössä olevaan osajärjestelmään asennuksen, liikkuvan kaluston yhdistämisen ja ohjaus- ja hallintajärjestelmän hyväksynnän aikana. • Kuljettajat koulutetaan ja heitä arvioidaan suhteessa menettelyyn D_P. • Infrastruktuurin haltija arvioi kuljettajia myös suhteessa niihin sääntöihin, joita sovelletaan IM:n infrastruktuuriin.
2	nro 2	HAZOP-kertomus R_X	Kalustoyksikössä olevan osajärjestelmän konfigurointi (eli liikkumislupa on liian salliva jarrutuskaarissa	Kalustoyksikössä olevan osajärjestelmän erityinen konfigurointiprosessi riippuu: • junan jarrutusjärjestelmään asetetuista turvamarginaaleista • junan jarrutusjärjestelmän reagointiviiveestä (etenkin tavarajunissa tämä riippuu välittömästi junan pituudesta)	Rautatieyritys	• Täsmennetään järjestelmän määritelmässä asianmukaisesti järjestelmän vaatimukset; • Varmistetaan, että junakohtaisten jarrujärjestelmien turvamarginaalit ovat riittävät;	Katso edellä ensimmäisellä rivillä esitetty huomautus.
3	nro 3	HAZOP–kertomus R_X	• Junan enimmäisnopeus on asetettu liian suureksi (Vmax) • Kalustoyksikössä olevan osajärjestelmän konfigurointi (eli liikkumislupa) on liian salliva jarrutuskaarissa	Kalustoyksikössä olevan osajärjestelmän erityistä konfigurointia ei ole päivitetty junan pyörän läpimitan osalta (kunnossapitohenkilöstö).	Rautatieyritys	• Määritellään menettely, jonka mukaisesti kunnossapitohenkilöstö määrittää junan pyörän läpimitan; • Määritellään junassa olevaan osajärjestelmässä sovellettava menettely junan pyörän läpimitan säännölliseksi päivittämiseksi ;	• Kalustoyksikössä olevan ohjaus- ja hallintaosajärjestelmän kunnossapito tapahtuu kunnossapitomenettelyn MP_Z mukaisesti. • Junan pyörän läpimitta päivitetään määrätyllä aikavälillä P_W -menettelyn mukaisesti. • Tietojen syöttämisprosessin osalta kuljettajia arvioidaan P_{DE} -menettelyn perusteella.
4	nro 4	HAZOP-kertomus R_X	Suurella nopeudella (160 km/h) kulkevan junan saapuminen	Tätä voidaan hallita ainoastaan kuljettajan valppauden avulla. Saapuminen rataosuuden	Infrastruktuurin haltija	Infrastruktuurin haltija varmistaa, etteivät, junat, joissa ei ole aktiivista	TM:n infrastuktuurin liikennejärjestelyjä säännellään R_{TM} –sääntöjen mukaisesti.

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

Taulukko 8: Esimerkki vaaroja koskevasta asiakirjasta: turvallisuuteen liittyvien tietojen siirtäminen muille toimijoille

Vaaran nro	Vaaran alkuperä		Vaaran kuvaus	Lisätiedot	Vastaava toimija	Turvallisuustoimenpide	Vastaanottajan huomautukset
	Nro taulukossa 7	Muu					
			rataosuudelle ilman, että kalustoyksikössä oleva osajärjestelmä on aktiivinen, ja ilman radanvarren merkinantojärjestelmää	automaattisen junansuojajärjestlemän (ATP) alueelle riippuu kuljettajan ennen siirtymäaluetta antamasta hyväksynnästä. Mikäli hyväksyntää ei anneta, junassa oleva ohjaus- ja hallintajärjestelmä jarruttaa automaattisesti.		kalustoyksikössä olevaa ohjaus- ja hallintajärjestelmää, liikennöi kyseisillä rataosuuksilla. Määritellään menettely liikennejärjestelyjä varten.	
					Rautatieyritys	Varmistetaan, että kuljettajat ovat saaneet koulutuksta siirtymisessä rataosuudelle, joka kuuluu ATP-alueeseen.	• Kuljettajia koulutetaan säännöllisesti IM:n e P_{IM_DP} -menettelyjen osalta. • IM arvioi lisäksi kuljettajia IM:n infrastruktuuriin sovellettavien sääntöjen (S_R) valossa.
jne.							

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

C.17. Esimerkki rautatietoiminnan yleisestä vaaraluettelosta

C.17.1. Ranskan ja Saksan välisen DEUFRAKO-yhteistyön puitteissa toteutetun ROSA-hankkeen (rautateiden optimoidun turvallisuuden arviointi) tarkoituksena oli muodostaa yleinen ja kattava vaarojen luettelo, joka käsittää rautateiden vakiotoiminnot. Tavoitteena ja haasteena oli määritellä nämä vaarat mahdollisimman yksityiskohtaisesti, ottamatta kuitenkaan huomioon Ranskan ja Saksan rautateiden erityispiirteitä. Luettelon laadinnassa käytettiin kummankin valtion rautatieyhtiöiden (SNCF ja DB) olemassa olleita vaaraluetteloita, ja se ristiintarkastettiin muiden valtioiden vaaraluetteloiden kanssa. Vaikka tarkoituksena oli laatia kattava ja yleinen luettelo, tässä annettava luettelo on ainoastaan ohjeellinen esimerkki, joka voi olla apuna toimijoille, joiden on tunnistettava tietyn hankkeen vaarat. On todennäköistä, että tässä luettelossa annettuja vaaroja on vielä työstettävä ja täydennettävä, jotta ne vastaavat kulloinkin kyseessä olevan hankkeen erityispiirteitä.

C.17.2. Alla olevassa luetteloluonnoksessa mainittuja vaaroja kutsutaan ”lähtökohtaisiksi vaaroiksi” (SPH), joilla tarkoitetaan vaaroja, joista voitaisiin laatia sekä seurauksien että syiden arviointi vaarojen hallinnointia koskevien turvallisuustoimenpiteiden/esteiden ja turvallisuusvaatimusten määrittelemiseksi.

C.17.3. ROSA-hankkeen mukainen vaarojen luettelo:

SPH 01	Alun perin väärin määritelty nopeusrajoitus (liittyy infrastruktuuriin)
SPH 02	Nopeusrajoituksen väärä määrittely (junaan liittyvä)
SPH 03	Väärin määritetty jarrutusetäisyys / väärä nopeusprofiili / väärät jarrutuskaaret
SPH 04	Riittämätön hidastuminen (fyysiset syyt)
SPH 05	Väärä/epäasianmukainen nopeus/jarrutuskäskyt
SPH 06	Väärin rekisteröity nopeus (junalla väärä nopeus)
SPH 07	Nopeusrajoitustieto ei välity oikein
SPH 08	Juna vierii pois
SPH 09	Väärä matkustussuunta / tarkoituksellinen peruuttaminen – (SPH 08:n ja SPH 14:n yhdistelmä)
SPH 10	Väärin rekisteröity absoluuttinen/suhteellinen sijainti
SPH 11	Junan paikannuksen epäonnistuminen
SPH 12	Junan eheyden menetys
SPH 13	Junan mahdollisesti väärä reitti
SPH 14	Aikataulun/liikkumisluvan välittämisen/tiedottamisen virhe
SPH 15	Opastimen rakenteellinen vika
SPH 16	Vaihteen osan rikkoutuminen
SPH 17	Väärä vaihdekäsky
SPH 18	Vaihteen väärä asento
SPH 19	Järjestelmän kohde opastimessa/liikenneulottumassa (pois lukien painolasti)
SPH 20	Vieras esine ohjausradalla/liikenneulottumassa
SPH 21	Tieliikenteen käyttäjä tasoristeyksessä
SPH 22	Liukumisen vaikutukset painolastiin
SPH 23	Aerodynaamisten voimien vaikutus junaan
SPH 24	Junan varustus/osa/rahti loukkaa liikkumaulottumaa
SPH 25	Junan epäasianmukainen liikenneulottuma (radanvarsi)
SPH 26	Kuorman väärä jakauma
SPH 27	Rikkoutunut pyörä, rikkoutunut akseli
SPH 28	Kuuma akseli/pyörä/laakeri
SPH 29	Telin, jousituksen vaimennuksen vika
SPH 30	Kalustoyksikön alustan/vaununkorin vika
SPH 31	Luvaton kulku (turvallisuusnäkökohta)
SPH 32	Henkilö ylittää luvallisesti radan

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

SPH 33	Työntekijöitä radalla
SPH 34	Henkilö tunkeutuu luvattomasti radalle (huolimattomuus)
SPH 35	Henkilö putoaa laiturin reunalta raiteelle
SPH 36	Liukastuminen / henkilö liian lähellä laiturin reunaa
SPH 37	Henkilökuntaa työssä raiteiden lähellä, esimerkiksi viereisellä raiteella
SPH 38	Henkilö poistuu odottamatta junasta (pois lukien matkustajien vaihto)
SPH 39	Henkilö putoaa (sivu)ovesta
SPH 40	Henkilö putoaa päätyovesta
SPH 41	Juna lähtee / vierii ovet avoinna (loukkaamaton liikenneulottuma)
SPH 42	Henkilö putoaa kahden vaunun väliselle käytäväalueelle
SPH 43	Matkustaja nojautuu ulos ovesta
SPH 44	Matkustaja kurkottautuu ikkunasta
SPH 45	Henkilöstö/junan hoitaja kurottautuu oviaukosta
SPH 46	Henkilöstö/junan hoitaja kurottautuu ikkunasta
SPH 47	Ohittavan kalustoyksikön henkilöstö kurottautuu portaalta
SPH 48	Henkilö putoaa/kiipeää laiturilta kalustoyksikön ja laiturin väliseen tilaan
SPH 49	Henkilö putoaa/poistuu junasta, kun juna ei ole laiturilla
SPH 50	Henkilö putoaa ovialueella matkustajavaihdon aikana
SPH 51	Junan ovet sulkeutuvat, kun henkilöitä on ovien alueella
SPH 52	Juna liikkuu matkustajavaihdon aikana
SPH 53	Junassa on mahdollisesti loukkaantunut henkilö
SPH 54	Tulipalo/räjähdysvaara (junassa) – onnettomuusluokka, SPH 55:n ja SPH 56:n seuraus)
SPH 55	Epäasianmukainen lämpötila (junassa)
SPH 56	Myrkytys/tukehtuminen (junassa)
SPH 57	Tappava sähköisku (junassa)
SPH 58	Henkilö putoaa laiturille (pois lukien matkustajien vaihto)
SPH 59	Epäasianmukainen lämpötila (laiturilla)
SPH 60	Myrkytys/tukehtuminen (laiturilla)
SPH 61	Tappava sähköisku (laiturilla)

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