Esimerkkikokoelma riskien arvioinneista ja YTM-asetusta tukevista mahdollisista välineistä
### ASIAKIRJAN TIEDOT

#### Muutosasiakirja

**Taulukko 1: Asiakirjan tila**

<table>
<thead>
<tr>
<th>Versio</th>
<th>Laatija(t)</th>
<th>Kohtta</th>
<th>Muutoksen kuvaus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ohjeversio 0.1 15.2.2007</td>
<td>Dragan JOVICIC</td>
<td>Kaikki</td>
<td>“Yhteisiä turvallisuusmenetelmiä koskevien suositusten ensimmäisen erän” version 1.0 &quot;käyttöoppaan&quot; ensimmäinen versio. Tämä on myös ensimmäinen versio YTM-työryhmälle muodollista tarkistusta varten toimitetusta asiakirjasta.</td>
</tr>
<tr>
<td>Ohjeversio 0.2 7.6.2007</td>
<td>Dragan JOVICIC</td>
<td>Kaikki</td>
<td>Asiakirjan jäsentäminen uudelleen siten, että se vastaa YTM-suosituksen version 4.0 rakennetta. Suosituksen version 1.0 päivittäminen/nuollallinen tarkistusmenetely YTM-työryhmässä.</td>
</tr>
<tr>
<td>Kaikki kohdat</td>
<td></td>
<td></td>
<td>Kaikki</td>
</tr>
<tr>
<td>Ohjeversio 0.3 20.7.2007</td>
<td>Dragan JOVICIC</td>
<td>Lisäykset</td>
<td>Lisäysten uudelleen järjestäminen ja uusien lisäysten laatiminen. Uusi lisäys, johon on kerätty kaikki kaaviot, joilla havainnollistetaan ja helpotetaan oppaan lukemista ja ymmärtämistä.</td>
</tr>
<tr>
<td>Kaikki kohdat</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Ohjeversio 0.4 16.11.2007 | Dragan JOVICIC | Kaikki kohdat | Asiakirjan päivittäminen siten, että  
- kehitetään mahdollisimman pitkälle voimassa olevia x kohtia,  
- kehitetään edelleen näkökohtia, joihin viitataan "järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisella",  
- luodaan linkki CENELEC:n V-sykliliin (eli standardin EN 50 126 kaavioon 8 ja 10),  
- kehitetään edelleen yhteistyötä ja yhteensopivuutta sellaisten rautatiealan eri toimijoiden välillä, joiden toimilla voi olla vaikutusta rautatiejärjestelmän turvallisuuteen,  
- selvennetään todisteita (esim. vaaraloki ja turvallisuusarvio), joilla on määrä osoittaa arviointiin lielle, että YTM:n riskinarkoointimenettelyä sovelletaan oikein.  
Asiakirjaa päivitetään myös viraston ensimmäisen sisäisen tarkistuksen perusteella. |
| Ohjeversio 0.5 27.2.2008 | Dragan JOVICIC | Kaikki kohdat | Asiakirjan päivittäminen YTM-suosituksen allekirjoitettun version mukaisesti.  
Asiakirjan päivittäminen Christophe Cassirin ja Marcus Anderssonin viraston sisäisen tarkistuksen tuleksa esittämän huomautusten

**Viite:** ERA/GUI/02-2008/SAF

**Versio:** 1.1

**Sivu:** 2/112
## Taulukko 1: Asiakirjan tila

<table>
<thead>
<tr>
<th>Versio Päiväys</th>
<th>Laatija(t)</th>
<th>Kohta</th>
<th>Muutoksen kuvaus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>perusteella.</td>
</tr>
<tr>
<td></td>
<td>Kaikki kohdat</td>
<td>Listäykset</td>
<td>Asiakirjan tai suosituksen kohtien uudelleennumeroinnin loppuunsaattaminen. YTM-suositksen soveltamisesimerkkien sisällyttäminen asiakirjaan.</td>
</tr>
</tbody>
</table>

### Uuden asiakirjan otsikko ja rakenne: ”Esimerkkikokoelma riskien arvioinnista ja YTM-asetusta tukevista mahdollisista välineistä”

<table>
<thead>
<tr>
<th>Ohjeversio 0.1 23.5.2008</th>
<th>Dragan JOVICIC</th>
<th>Kaikki</th>
<th>”Käyttöoppaan” version 0.5 kahten täydentävään asiakirjaan jakamisen tuloksena laaditun asiakirjan ensimmäinen versio.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ohjeversio 02 3.9.2008</td>
<td>Dragan JOVICIC</td>
<td>Kaikki</td>
<td>Asiakirjan päivittäminen:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Euroopan komission yhteisiä turvallisuusmenetelmiä koskevan asetuksen mukaisesti (Ref. 3),</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 1. heinäkuuta 2008 yhdessä rauteteiden yhteenliitettävyyttä ja turvallisuutta käsittelevän komitean (RISC) jäsenten kanssa järjestetyn työpajan tuloksena saatujen huomautusten mukaisesti,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• YTM-työryhmän jäseniltä (Norjan, Suomen, Yhdistyneen kuningaskunnan ja Ranskan kansalliset turvallisuusviranomaiset, CER, EIM, Jens BRABAND (UNIFE) ja Stéphane ROMEI (UNIFE)) saatujen huomautusten mukaisesti.</td>
</tr>
<tr>
<td>Ohjeversio 1.0 10.12.2008</td>
<td>Dragan JOVICIC</td>
<td>Kaikki</td>
<td>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.</td>
</tr>
</tbody>
</table>
Sisällysluettelo

ASIAKIRJAN TIEDOT ........................................................................................................ 2
  Muutosasiakirja ........................................................................................................... 2
  Sisällysluettelo ........................................................................................................... 4
  Luettelo kaavioista ...................................................................................................... 5
  Luettelo taulukoista .................................................................................................... 6

0. JOHDANTO .................................................................................................................. 7
  0.1. Soveltamisala ........................................................................................................ 7
  0.2. Soveltamisalan ulkopuolelle jäävät asiat ................................................................ 8
  0.3. Asiakirjan käyttöä ohjaava periaate ..................................................................... 8
  0.4. Asiakirjan kuvaus ............................................................................................... 8
  0.5. Viiteasiakirjat ...................................................................................................... 9
  0.6. Yleiset määritelmät, käsitteet ja lyhenteet ............................................................ 10
  0.7. Erityiset määritelmät .......................................................................................... 10
  0.8. Erityiset käsitteet ja lyhenteet ............................................................................ 10

YTM-ASETUKSEN ARTIKLOJA KOSKEVAT SELVENNYKSET ......................................... 12
  1 artikla Tarkoitus ...................................................................................................... 12
  2 artikla Soveltamisala .............................................................................................. 12
  3 artikla Määritelmät .................................................................................................. 14
  4 artikla Merkittävät muutokset ................................................................................ 16
  4 artiklan 1 kohta ..................................................................................................... 16
  4 artiklan 2 kohta ..................................................................................................... 16
  5 artikla Riskinhalintamenetely ............................................................................... 17
  6 artikla Riippumaton arviointi ................................................................................ 18
  7 artikla Turvallisuusarviointikertomukset ................................................................ 19
  8 artikla Riskinhalinta / sisäiset ja ulkoiset tarkastukset ............................................. 20
  9 artikla Palaute ja tekninen kehitys ......................................................................... 21
  10 artikla Voimaantulo .............................................................................................. 22

LIITE I - YTM-ASETUKSESSA SÄÄDETTYÄ MENETTELYÄ KOSKEVAT SELVENNYKSET ...................................................................................................................... 23
  1. RISKINHALINTAMENETTELLYYN SOVELLETTAVAT YLEISET PERIAATTEET .... 23
     1.1. Yleiset periaatteet ja velvoitteet ...................................................................... 23
     1.2. Rajapintojen hallinta ....................................................................................... 31
  2. RISKINARVIOINTIMENETTELLYN KUVAUS ................................................................ 34
     2.1. Yleinen kuvaus – YTM:n riskinarviointimenettelyn ja CENELECin V-syklin vastaavuus .............................................................. 34
     2.2. Vaarojen tunnistaminen .................................................................................. 41
     2.3. Menetelyohjeiden käyttö ja riskinarviointi ......................................................... 44
     2.4. Ohjeiston käyttö ja riskinarviointi ................................................................... 46
     2.5. Ekspliitiittinen riskin estimointi ja evaluointi .................................................... 47
  3. TURVALLISUUSVAATIMUSTEN MUKAISUUDEN OSOITTAMINEN ................................ 51
  4. VAAROJEN HALLINTA ................................................................................................ 54
     4.1. Vaarojen hallintamenettely ................................................................................ 54
     4.2. Tietojen vaihto .................................................................................................. 55
5. RISKINHALLINTAMENETTELYN SOVELTAMISTA KOSKEVA NÄYTTÖ ................. 58

YTM-ASETUksen LIITE II ................................................................................................................. 61

Edellytykset, jotka arviointiluentoon on täytettävä................................................................. 61

LISÄYS A: LISÄSELVENNYKSET .................................................................................................. 62

A.1. Johdanto........................................................................................................................ 62
A.2. Vaarojen luokittelut.............................................................................................................. 62
A.3. Teknisten järjestelmien hyväksyttävää riskitasoa koskeva peruste (RAC-TS) .................. 62
A.4. Turvallisuusarviointiin perustuvaa näyttö........................................................................... 73

LISÄYS B: EISMERKKEJÄ RISKINARVIOINTIPROSESSIA TUKEVISTA TEKNIKOISTA JA VÄLINEISTÄ .................................................................................................................. 76

LISÄYS C: EISMERKKEJÄ ................................................................................................................. 77

C.1. Johdanto........................................................................................................................ 77
C.2. Esimerkkejä 4 artiklan 2 kohdassa tarkoitetusta merkittävää muutosta koskevien perusteiden soveltamisesta .................. 77
C.3. Esimerkkejä rautatiealan toimijoiden välisistä rajapinnoista........................................... 78
C.4. Esimerkkejä yleisesti hyväksyttävien riskien määrittelyä koskevista menetelmissä .......... 79
C.5. Riskinarviointiesimerkkei: merkittävä organisatorinen muutos............................................. 81
C.6. Riskinarviointiesimerkkei: merkittävä operatiivinen muutos – ajotuntemuksen muutos .... 83
C.7. Esimerkki teknisesti merkittävän muutoksen riskinarvioinnista (CGS) ...................... 85
C.8. Esimerkki rautatietunneleiden riskinarviointia koskevasta ruotsalaisesta ohjeesta BVH 585.30 ................................................................. 87
C.9. Esimerkki järjestelmähallinnon riskinarvioinnista Kööpenhaminan metrossa .................... 90
C.10. Esimerkki: vaarallisten aineiden rautatiekuljetusten riskin laskeminen OTIF:n ohjeiden mukaan................................................................................. 93
C.11. Uuden liikkuvan kalustotyypin hyväksymistä koskeva riskinarviointiesimerkki ...................... 95
C.12. Riskinarviointiesimerkkei merkittävästä toiminnallisesta muutoksesta – Kuljettajan yksin suorittama toiminto................................................................................................................. 97
C.13. Esimerkki: oheiston käyttö uusia saksalaisia lukitusjärjestelmiä koskevien turvallisuusvaatimusten määrittämiseksi .................................................................................................................. 99
C.14. Esimerkki eksplisiittistä hyväksyttävää riskitasoa koskevasta perusteesta: saksalaisen FFB:n (junansuojajärjestelmä) radiopohjainen toiminto.............................................................. 101
C.15. Esimerkki: RAC-TS:n sovellettavuustestistä ......................................................................... 102
C.16. Esimerkkejä vaaroja koskevan asiakirjan mahdollisista rakenneperusteista ..................... 103
C.17. Esimerkki: rautatietoiminnan yleisestä vaaraluettelosta .................................................. 111

Luettelo kaavioista

Kaavio 1: YTM-asetuksen riskinhallintakehys ............................................................................... 25
Kaavio 2: Yhdennetuiksi tarkoitetut turvallisuusohjelmisjärjestelmä (SMS) ja YTM. ..................... 27
Kaavio 3: Esimerkkejä turvallisuusarvioiden välisistä nippuvuussuhteista (laadittu standardin EN 50 129 kaavion 9 pohjalta) ............................................................................................................. 29
Kaavio 4: Standardin EN 50 126 kaavion 10 mukainen yksinkertaistettu V-syklilatauhoja. ........ 34
Kaavio 5: Standardin EN 50 126 kaaviossa 10 kuvattu V-syklilatauhoja (CENELECin järjestelmän elinkaari) .. 35
Kaavio 6: Asianmukaisten turvallisuustoimenpiteiden valinta riskien hallitsemiseksi ............... 40
Kaavio 7: Yleisesti hyväksyttävät riskit ........................................................................................ 43
Kaavio 8: Yleisesti hyväksyttävien riskien toimintataajuuden vaarojen suodattaminen ............. 43
Kaavio 9: Hyväksyttävää riskitasoa koskevien perusteiden pyramidi ........................................... 48
Kaavio 10: Standardin EN 50 129 kaavio A.4: Vaarojen määrittely järjestelmän rajojen näkökulmasta ...........51
Kaavio 11: Alemman tason vaiheiden turvallisuusvaatimusten johtaminen....................................................52
Kaavio 12: Jäsennelty asiakirjahierarkia ........................................................................................................58
Kaavio 13: Teknisen järjestelmän kaksinkertainen rakenne .............................................................................65
Kaavio 14: RAC-TS:n sovellettavuustestin kulkukaavio ..............................................................................67
Kaavio 15: Esimerkki muutoksesta, joka ei ole merkittävä Puhelinviesti tasoristeyksen valvomiseksi. ........77
Kaavio 16: Radanvarren silmukan korvaaminen radioviestimeen perustuvalta osajärjestelmällä .............85

Luettelo taulukoista

Taulukko 1: Asiakirjan tila......................................................................................................................................2
Taulukko 2: Viiteasiakirjat ..................................................................................................................................9
Taulukko 3: Käsitteet ..........................................................................................................................................10
Taulukko 4: Lyhenteet ......................................................................................................................................10
Taulukko 5: Tyyppiesimerkki kalibroidusta riskimatriisista ............................................................................71
Taulukko 6: Esimerkki vaarojen koskevasta asiakirjasta liitteessä C olevassa C.5 kohdassa tarkoitetun
organisatorisen muutoksen tapauksessa .........................................................................................................105
Taulukko 7: Esimerkki valmistajan laatimasta kalustoyksikön ohjaus- ja hallintaosajärjestelmän vaaroja
koskevasta asiakirjasta. ..................................................................................................................................106
Taulukko 8: Esimerkki vaarojen koskevasta asiakirjasta: turvallisuuteen liittyvien tietojen siirtämisen muille
toimijoille .......................................................................................................................................................109
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 alakohdassa tarkoitettua riskien arviointia, toimia kehitetyn YTM -asetuksen soveltamisesta yhteisössä annetun direktiivin - 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, joiden toimilla on vaikutusta rautatiejärjestelmien turvallisuuteen ja joiden on sovellettava suoraan tai välillisesti YTM-asetuksen vaatimusten täyttämiseksi, jos ne ovat toimijoiden mielestä soveltuviampaa. Tässä asiakirjassa esitetty esimerkit ja lisätiedot eivät ole tyhjentäviä, eivätkä ne kata kaikkia mahdollisia tilanteita, joissa merkittäviät 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 soveltamisopan (Ref. 4) kanssa, mutta sillä ei korvata YTM-asetusta.


(1) Tällaisia toimijoita ovat rautatiejärjestelmän yhteentoimivuudesta yhteisössä annetun direktiivin 2008/57/EY 2 artiklan r kohdassa määrätetyt hankinta työskentelijät tai valmistajat, jotka ovat asetuksen mukaan "hakijoita", tai niiden toimittajat ja palveluntarjoajat.
0.2. Soveltamisalan ulkopuolelle jäädvat 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 riskinhallintamenettelyyn soveltamiseen liittyviä mahdollisia sopimusehtoja tai järjestelmiä. 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 välisiä rapointoihini liittyvien turvallisuusriskeihin 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. Tässä asiakirjassa eivät tarkoitetut luettavaksi itsenäisenä asiakirjana, eikä sillä korvata YTM-asetusta (Ref. 3). Vertailun helpottamiseksi YTM-asetuksen jokaisen artiklan on kopioitu tämän asiakirjaan. Kyseistä artiklata on selvennetty tarvittaessa YTM-asetuksen soveltamisopassa (Ref. 4). Artiklan jälkeen esitettyissä 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) Liiitteessä 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.
### 0.5. Viiteasiakirjat

#### Taulukko 2: Viiteasiakirjat

<table>
<thead>
<tr>
<th>[Ref N:o]</th>
<th>Otsikko</th>
<th>Viite</th>
<th>Versio</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Ref 4]</td>
<td>Rautatieturvallisuusdirektiivi 6 artiklan 3 kohdan a alakohdassa tarkoitetussa riskien arvioinnissa sovellettavan yhteisen turvallisuusmenetelmän hyväksymisestä koskevan komission asetuksen soveltamisopas</td>
<td>ERA/GUI/01-2008/SAF</td>
<td>1.0</td>
</tr>
<tr>
<td>[Ref 6]</td>
<td>Turvallisuusjohtamisjärjestelmän arviointiperusteet rautatieylistysten ja infrastruktuurin hallintoa varten</td>
<td>Turvallisuusjohtamisjärjestelmän (SMS) arviointiperusteet Osa A: Turvallisuustodistukset ja -luvat</td>
<td>31.5.2007</td>
</tr>
<tr>
<td>[Ref 8]</td>
<td>Rautatiesovelukset - Toimintavarmuuden, käytännösmuodon, kunnossapideltävyysen ja turvallisuuden (RAMS) määrittely ja esittäminen (RAMS) – Osa 1: Perusvaatimukset ja yleiset menetelmät</td>
<td>EN 50126-1</td>
<td>Syyskuu 2006</td>
</tr>
<tr>
<td>[Ref 9]</td>
<td>Rautatiesovelukset - Toimintavarmuuden, käytännösmuodon, kunnossapideltävyysen ja turvallisuuden (RAMS) määrittely ja esittäminen (RAMS) – Osa 2: Standardin EN 50126-1 soveltamisopas</td>
<td>EN 50126-2 (ohje)</td>
<td>Lopullinen ehdotus (Elokuu 2006)</td>
</tr>
<tr>
<td>[Ref 10]</td>
<td>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)</td>
<td>RID-asiantuntijakomitean hyväksymä OTIF:in ohje,</td>
<td>24.11.2005</td>
</tr>
<tr>
<td>[Ref 12]</td>
<td>Euroopan rautatieviraston turvallisuusysikutkin laatima, toteutettavuustutkimus &quot;Apportionment of safety targets (to TSI sub-systems) and consolidation of TSI from a safety point of view&quot; WP1.1 - Assessment of the feasibility to apportion Common Safety Targets</td>
<td>WP1.1</td>
<td>1.0</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Käsite</th>
<th>Määritelmä</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virasto</td>
<td>Euroopan rautatievirasto (ERA)</td>
</tr>
<tr>
<td>Opas</td>
<td>”Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan alakohdassa tarkoitetussa riskien arvioinnissa sovelletavan yhteisen turvallisuusmenetelmän hyväksymisestä [..] annetun komission asetuksen (EY) N:o …/. soveltamisopas”</td>
</tr>
<tr>
<td>YTM-asetus</td>
<td>”Komission asetus (EY) N:o …/.., annettu [..], Euroopan parlamentin ja neuvoston direktiivin 2004/49/EY 6 artiklan 3 kohdan alakohdassa tarkoitetussa riskien arvioinnissa sovelletavan yhteisen turvallisuusmenetelmän hyväksymisestä” (Ref. 3)</td>
</tr>
</tbody>
</table>

**Taulukko 4: Lyhenteet**

<table>
<thead>
<tr>
<th>Lyhenne</th>
<th>Merkitys</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS</td>
<td>Ohjaus-, hallinta- ja merkinantojärjestelmä (Control Command and Signalling)</td>
</tr>
<tr>
<td>CSM (YTM)</td>
<td>Yhteinen turvallisuusmenetelmä</td>
</tr>
<tr>
<td>CST (YTT)</td>
<td>Yhteiset turvallisuustavoitteet</td>
</tr>
<tr>
<td>EC</td>
<td>Euroopan komissio</td>
</tr>
<tr>
<td>ERA</td>
<td>Euroopan rautatievirasto</td>
</tr>
<tr>
<td>IM</td>
<td>Infrastruktuurin hallija(t)</td>
</tr>
<tr>
<td>ISA</td>
<td>Riippumaton turvallisuuden arvioija</td>
</tr>
<tr>
<td>OTIF</td>
<td>kansainvälisten rautatiekuljetusten hallitustenvälinen järjestö (Intergovernmental Organisation for International Carriage by Rail)</td>
</tr>
<tr>
<td>MS</td>
<td>Jäsenvaltio</td>
</tr>
<tr>
<td>NOBO</td>
<td>Ilmoitettu laitos</td>
</tr>
<tr>
<td>NSA</td>
<td>Kansallinen turvallisuusviranomainen</td>
</tr>
<tr>
<td>OMP</td>
<td>Laadunhallintamenettely</td>
</tr>
<tr>
<td>OMS</td>
<td>Laadunhallintajärjestelm</td>
</tr>
<tr>
<td>RISC</td>
<td>Rautateiden yhteentoimivuutta ja turvallisuutta käsittelevä komitea</td>
</tr>
<tr>
<td>RU</td>
<td>Rautatievirasto</td>
</tr>
<tr>
<td>SMP</td>
<td>Turvallisuusjohtamisemenettely</td>
</tr>
</tbody>
</table>
**Taulukko 4: Lyhenteet**

<table>
<thead>
<tr>
<th>Lyhenne</th>
<th>Merkitys</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>Turvallisuusjohtamisjärjestelmä</td>
</tr>
<tr>
<td>SRT</td>
<td>Rautatietunnelien turvallisuus</td>
</tr>
<tr>
<td>TBC</td>
<td>Täydennetään myöhemmin</td>
</tr>
<tr>
<td>TSI</td>
<td>Yhteenotomivuuden tekniset eritelmät</td>
</tr>
</tbody>
</table>
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 kunnossapitomenettely),

Viite: ERA/GUI/02-2008/SAF
Versio: 1.1
Sivu 12/112

(d) rautatieyöryyksien/infrastruktuurin haltiljan organisointiosassa 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 monimuutkaiset" järjestelmät (kuten asemia ja tunneleita käsitellään 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 rautateidien yhteentoimivuusdirektiivin (Ref. 2) mukaan esimerkiksi suurten nopeuksien rautatiejärjestelmän uudentyypisen liikkuvan kaluston on oltava yhdenmukainen suurten nopeuksien rautatiejärjestelmän liikkuvaa kalustoa koskevien yhteentoimivuuden teknisten eriteimiä kanssa. Vaikka yhteentoimivuuden tekniset eriteimet kattavat valtaosin arvioitavana olevan järjestelmän, ne eivät kata tärkeitä ohjaamooh liitetyvien tehokkaiden liitetyvien, ja yhteistä turvallisuusmenetelmää on sovelletava sen varmistamiseksi, että kaikki innimieliset teknikoihin liittyvät kohtuullisesti ennakoitavan vaarat (toisin sanoen kuuluttajan, liikkuvan kaluston ja rautatiejärjestelmän muiden osien välisiin rajapintoihin liittyvät vaarat) tunnistetaan ja niitä valvotaan asianmukaisesti.
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.

[9]

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 (f) of Directive 2008/57/EC.

[9]

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;
(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 safety 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;


---

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

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

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.

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.

5 artikla Riskinhallintamenetelly

5 artiklan 1 kohta

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

5 artiklan 2 kohta

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

Liisäselvennystä ei pidetä tarpeellisena.
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] Lisäselvonnystä 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 2] Eri arviointiin (NSA, NOBO ja ISA) tehtävien ja vastuiden sekä niiden välisen välttämättömän 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 määrätä, miten:
(a) tarkastetaan todisteiden pohjalta, että YTM:n riskinhallintaa- ja riskinarviointimenettelyjä sovelletaan oikein, ja
(b) tuetaan hakijaa arvioitavaa 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.

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.

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.

7 artikla Turvallisuusarviointikertomukset

7 artiklan 1 kohta

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

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.
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 hyväksyty CENELEC-standardeissa: katso standardin EN 50 129 kohta 5.5.2 ja standardin EN 50 126-2 kohta 5.9. CENELEC-standardeissa hakijat tai rippumattomat turvallisuuden arvioijat soveltavat ristiinhyväksynnän tai vastavuoroisen tunnistamisen periaatetta yleisiin tuotteisiin ja yleisiin sovelluksiin

[G 2] Vastavuoroista tunnistamista on sovelletava myös uusien tai mukautettujen järjestelmien hyväksynnässä, jos niiden riskiarviointi ja järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen toteutetaan CENELEC-standardien vaatimusten 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. lisätietoja "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.
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;
(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.

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.

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.
1. **RISKINHALLINTAMENETTELYYN SOVELLETTAVAT YLEISET PERIAATTEET**

1.1. **YLEiset periaatteen 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 liittyvät riskinarviointimenetely, Kaavion kutakin laatikkoa/toimea kuvataan tarvittaessa yksityiskohtaisemmin tämän asiakirjan erillisessä kohdassa.


(a) järjestelmän yleisperiaatteista, järjestelmän toiminnoista jne. Nämä voidaan kuvata periaatteessa alustavassa järjestelämääriittelyssä;

(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 järjestelämääriittelyn yhteydessä, mahdollistavat sen, että hakija, alihankkijat, kansallinen turvallisuusviranomainen, ilmoittettu laitos ja riippumaton turvallisuuden arvioija voivat
tarvittaessa sopia jo varhaisessa vaiheessa hankkeessa sovellettavista menettelyohjeista tai vastaavista ohjeistoista.
Kaavio 1: YTM-asetuksen riskinhallintakehys
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 infrastrukturiin haltijan turvallisusjohtamisjärjestelmässä (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 väkivaltua rautatiejärjestelmän turvallisuuteen, on yleensä käytössä vähintään hanketasoilla (katso 5.1 kohta 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 ohjet:

(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 näkökohtista.

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

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.

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.

Kaaviossa 2 esitetään YTM:n ja "turvallisuusjohtamisjärjestelmien ja riskinarviointimenettelyjen" välinen suhde.
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 välittämätöntä 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 turvallisudesta. Tässä yhteydessä on varmistettava, että:

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

Jos toimijat eivät pääse sopimukseen niille asettettavista 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 4]** Yleensä hakijasäärätään hankkeeseen osallistuvien toimijoiden ja näiden toimijoiden eri osajärjestelmiä ja laitteiden "turvallisuustasot" ja "turvallisuusvaatimukset":

(a) hakijan ja asianomaisten toimijoiden (alihankkijoiden) välissä sopimuksissa;
(b) turvallisuusasunnetelmassa tai muussa samaa tarkoituksa varten laadittaessa 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) lisäykseä A.4 esitettyä käytännöä.
Järjestelmän "turvallisuustasojen" ja "turvallisuusvaatimusten" jaottelu osajärjestelmien ja laitteiden ja siten asianomaisten toimijoiden mukaan. Itse hakija mukaan luettuna, voidaan tarkentaa/laajentaa kattamaan "järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisen": katso kaavio 1. CENELEC:n V-syklin (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.


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

[G 6] CENELEC:n mukaan valmistajan on annettava riskinarvioinninä dokumentoitu näyttö yleistä tuotetta (tai yleistä sovellusta) koskevissa turvallisuusarviointeissa ja varoja koskevissa

---

(9) Käsittely "yleistä sovellusta ja yleistä tuotetta koskevat turvallisuusarviot" on lainattu CENELEC-standardeista, joissa turvallisuusarvioidon on kolmenlaisia (ks. Kaavio 3):
(a) \textit{Yleistä tuotetta koskeva turvallisuusarvio} (sovelluksesta riippumaton). Yleistä tuotetta voidaan käyttää uudelleen erilaissyissä riippumattomissa sovelluksissa;
(b) \textit{Yleistä sovellusta koskeva turvallisuusarvio} (sovellusluokka). Yleistä sovellusta voidaan käyttää uudelleen tiettyyn luokkaan/laajin kuuluvissä sovelluksissa, joilla on yhteisiä toimintoja;
(c) \textit{Erittäistä sovellusta koskeva turvallisuusarvio} (erityinen sovellus). Erittäistä sovellusta käytetään ainoastaan yhtä tiettyä asennustavata varten.
asiakirjoissa. Tällaiset turvallisuusarviot ja vaaroja koskevat asiakirjat sisältävät kaikki oletukset ja yksilöidyit "käyttörajoitukset" (ts. turvallisuuteen liittyvät sovellusehdot), joita sovelletaan asiana liittyviin yleisiin tuoteesiin (tai yleisiin sovelluksiin). Nämä olenn kun yleistä tuotetta ja yleistä sovellusta käytettään erityisen sovelluksen yhteydessä, on osoitettava, että nämä oletukset ja "käyttörajoitukset" (tai turvallisuuteen liittyviä sovellusehodoja) koskevat vaatimukset täyttävät 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.


Continuation of the footnote


Yleisen tuotteen ja yleisen sovelluksen turvallisuusarviointiin liittyvien "turvallisuusarviointien" ja "turvallisuusanalyyseiden" rajat ja voimassaolo määritävät tällaisten oletusten ja käyttörajoituksen rakenne. Jos tarkasteltava erityinen sovellus ei täytä näitä vaatimuksia, vastaavat "turvallisuusarviointit" ja "turvallisuusanalyyset" (esim. kausialanalyyset) on päivityttävät tai korvattavaa uusilla. Tämä käytäntö on yhdenmukainen seuraavan yleisen turvallisuusperiaatteet kanssa: "Jos erityisen isoja järjestelmiä suunnitellaan perustuu yleisiin sovelluksiin tai yleisiin oletteisiin, on osoitettava, että erityinen (iso) järjestelmä on kaikkien niiden oletusten ja käyttörajoituksen mukainen (joita kutsutaan CENELECissä turvallisuuteen liittyväksensä asioihin, jotka viedään yleisen sovelluksen tai yleisen tuotteen vastaaviin turvallisuusasioihin (ks. kaaviot 3)".

Jos erityisen sovellus ei ole yhdenmukainen joidenkin oletusten tai käyttörajoituksen kanssa osajärjestelmän tasolla (esim. toiminnallisten turvallisuusvaatimusten osalta), vastaavat oletukset ja käyttörajoitukset voidaan siirtää korkeammalle tasolle (ts. yleensä järjestelmatasolle). Nämä oletukset ja käyttörajoitukset yksilöidään selkeästi kyseisen osajärjestelmän "erityisen sovelluksen turvallisuusarvioissa". Tämä on edottoman tärkeää, jotta tällaisissa riippuvuustapauksissa voidaan varmistaa, että kunkin turvallisuusarvon turvallisuuteen liittyvät sovellusehdot täyttävät korkeammien tason turvallisuusarvoissa tai että ne siirretään osaksi kaikkein korkeimman tason turvallisuusarvon (ts. järjestelmän turvallisuusarvon) turvallisuuteen liittyviä sovellusehodoja.
turvallisuussuunnitelmien tai turvallisuusorganisaatioihin. Vastuiden jakamisesta eri toimijoiden kesken neuvottelua ja siitä sovitaan tavallisesti alustavan järjestelmämääräisellä yhteydessä (ts. hankkeen alussa), jos sellainen laaditaan.


[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] Lisaselvennystä 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 rautatieviruksen toiminnallisia syistä infrastruktuurin hallitsemaan määritetty muutokset infrastruktuurin, rautatieturvallisuusdirektiiviin {Ref. 1} liitteen III l 2 kohdan g alakohdan vaatimusten nojalla rautatieviruksen valvoo myös yleisiä toimia sen varmistamiseksi, että kaikki toimijat ottavat huomioon vaikeudet tehdään oikein. Vaikka vastuu säilyykin rautatieviruksella, kyseisen infrastruktuurin hallitsemaan velvollisuutena on silti antaa tietoa muille rautatieviruksille, jos infrastruktuurin muutoksella on vaikutusta myös niihin. Infrastruktuurin hallitseman on mahdollisesti toteuttettava riskinarviointi YTM:n mukaisesti, jos asiaa koskeva muutos on sen kannalta merkittävä.


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

(a) toimien hoitaminen; yleensä toimien hoitaminesta 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);
(e) odotetut tuotokset.
Nämä perusteet määritetään niiden yritysten turvallisuusruutuine (taa muissa asioissa asiakirjoissa), joita kyseiset rajapinnat koskevat.

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

[G 5] Rajapintojen hallinnassa on tarkasteltava myös riskejä, jotka voivat syntyä rajapinnoissa ihmisperiaatteiden kanssa (käytön ja kunnossapitollisesta 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.

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] Rautatiejärjestysten 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 määrätty 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 turvallisuusruutuine massassa: katso 0.2. kohta.

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

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

[G1] 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. Kaavioissa 1 esitetyyn YTM:n riskinhallintamenettelyn ja CENELECin standardin kaavioissa 10 esitetyn V-syklin vastaavuuden osoittamiseksi CENELECin V-sykli toistetaan kaavioissa 5:

(a) Kaavioissa 1 esitetty YTM:n "alustava järjestelmämäärittely" vastaa CENELECin V-syklin vaihetta 1, ts. järjestelmäkäsitteen määrittelyä (katso kaavioissa 5 esitetyt laatikko 1);

(b) Kaavioissa 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
Alustava järjestelmämäärittely YTM:ssä

1. Käsitys
2. Järjestelmämäärittely ja käyttöehdot
3. Riskianalyysi
4. Järjestelmävaatimukset
5. Turvallisuusvaatimukset
6. Suunnittelu ja toteutus
7. Valmistus
8. Asennus
9. Järjestelmän validointi (turvallisuushyväksyntä ja käyttöönotto mukaan luettuna)
10. Järjestelmän hyväksyminen
11. Käyttö ja ylläpito
12. Suorituksen seuranta
13. Muutokset ja jälkiasennus
14. Käytöstä poisto ja hävittäminen

Laatikko 1
Laatikko 2
Laatikko 3
Laatikko 4

Turvallisuusvaatimusten osoittaminen

Kaavio 5: Standardin EN 50 126 kaaviossa 10 kuvattu V-sykl (CENELECin järjestelmän elinkaari)
YTM:n riskinarviointimenettelyyn tuotoksia ovat (toistojen jälkeen – katso kaavio 1):

(a) "järjestelmämäärittely" päivitetynä "riskianalyysin" ja "riskinarvioinnin" tuloksena määritteilyillä "turvallisuusvaatimuksilla" (katso 2.1.6 kohta);
(b) "järjestelmämääristamisten ja osajärjestelmien mukaisuus" eri osajärjestelmien ja osien mukaan (kaavion 5 vaihe 5);
(c) "vaarajoissa koskeva asiakirja", johon merkitään:

1. kaikki tunnistetut vaarat ja niihin liittyvät turvallisuustoimenpiteet
2. 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 eriteilledä järjestelmävaatimuksia.

Järjestelmämäärittely, jota on päivitetty riskinarvioinnin tuloksilla, ja vaarajoissa 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".

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 kaikiksen 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 toiminnallisuissa ja organisatorisissa muutoksissa valmistusvaihetta ei oteta huomioon).

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 (katso edellä esitetty luettelo ja kaavio 5). Nämä vaiheet kattavat suunnittelun, valmistuksen, asentamisen, varmennus- ja validointitoimet, jaasian liittyvät RAMS-toimet ja järjestelmän hyväksynnän.

"Järjestelmän turvallisuusvaatimusten mukaisuuden osoittamisessa" yleisperiaatteena on, että riskinarvioinnissa keskitetään 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.

Kaaviossa 5 esitetyn perinteisen CENELECin V-syklin vertailun tuloksena voidaan siten todeta, että:
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 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).
Yleensä hakija päättää hankkeen erityisvaatimusten ja kyseisten kolmen periaatteen soveltamisesta saamansa kokemuksen perusteella, mikä hyväksyttävää riskitasoa koskeva periaate on asianmukaisin tunnistettujen vaarojen hallitsemiseksi.

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


Riskin vähentäminen hyväksyttävälle tasolle voi edellyttää riskianalyysi- ja riskinarviointitapauksia toistamista useita kertoja, kunnes asianmukaiset turvallisuustoimenpiteet saadaan yksilöityä.

Käytössä olevien järjestelmien ja menettelyohjeiden soveltamiseen perustuvien järjestelmien nykyisten jäännösriskien katsotaan olevan hyväksyttävät käytännössä saatujen kokemusten perusteella. Ekspliittisten riskin estimoinnin tuloksena saatu jäännöski perustuu asiointijärjestelyyn ja sitä järjestelyjä analyysissä tekemiin oletuksiin tai onnettomuuksia tai käyttökokemuksia koskeviin tietokannoihin. Ekspliittisten riskin estimoinnin jäännöskiä ei voida siten vahvistaa välttämättä käytännössä. Jäännöski osoittaminen edellyttää järjestelmän pitkäaikaisesta käytöstä, seurantaa ja vastaavista järjestelmistä saatujen kokemusten hyvän, menettelyohjeiden soveltamisella ja muihin vastaaviin ohjeistoihin vertaamisella on se etu, että näin vältetään sellaisten tarpeettoman tukojen turvallisuusvaatimusten määrityt, jotka voivat perustua ekspliittisissä riskin estimoinnissa käytettyihin kohtuuttoman varovaisiin (turvallisuus)oletuksiin. Arvioitavan järjestelmän ei kuitenkaan välttämättä tarvita täyttää kaikkia menettelyohjeiden tai vastaavien ohjeistojen turvallisuusvaatimuksia. Tällöin ekspliittisen riskin estimoinnin soveltamisella on se etu, että sillä vältetään arvioitavan järjestelmän liian tarkka suunnittelu ja mahdollistetaan kustannustehokkampi suunnittelu, jota ei ole kokeilltu aiemmin.

Jos arvioitavan järjestelmän tunnistettuja vaaroja ja niihin liittyvää riskiä ei voida hallita menettelyohjelma, soitetaan esimerkiksi arvioidaan suorittaa riskitaso sovelletaan, on toteutettava ekspliittinen riskin estimointi vaarallisten tilanteiden määrällistä tai laadullisten analyysien pohjalta. Tällainen tilanne syntyy, kun arvioitava järjestelmä on täysin uusi (tai suunniteltu on innovatiivinen) tai kun järjestelmä poikkeaa menettelyohjeesta tai ohjeistosta. Ekspliittisessä riskin

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.
estimations in the risk evaluation that the selected risk acceptance principles are used consistently.

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.

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.

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.

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.

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.
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:

(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 "turvallisuvaatimuksesi". Täytettävien turvallisuusvaatimusten määrä on tällöin pienempi kuin toteutettaessa molemmat toimenpiteet B ja C.

(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 "turvallisuusvaatimuksesi". Tarkasteltavan vaaran hallitsemiseksi on käytettävä muita turvallisuustoimenpiteitä (kaavion 6 toimenpiteet E ja F):

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

(i) kun eurooppalaisessa liikenteenvalvontajärjestelmässä (ETCS) on käytettävä turvallisuuden vuoksi hätäjarruja, järjestelmä käyttää niin sanotun MAXIMUM SAFE FRONT END -toimintoa varmistaakseen, että juna todella pysähtyy ennen vararapisteen 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 liittyvä turvallisuustoimenpiteeseen, jota voidaan käyttää junan pysäytymiseksi lähis 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.

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


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

(a) empirisessä 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).


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.

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.

Johnkin 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 riskilukutusten väliseen suhteeseen FN-käyrissä tai riskimatriisessa. Kaaviossa 7 esitettään tätä koskeva esimerkki;
(b) tai jos riskiin liittyvä vahinko on niin pieni, ettei sen torjumiseksi ole järkevää toteuttaa turvallisuustoimenpiteitä.
Lisaaksi jos tunnistetaan tarkkuudeltaan erilaisia vaaroja (toisin sanoen yhtäältä korkean tason vaaroja ja toisaalta tarkasti määritellyjä osavaaroja), on ryhdyttävä varotoimiin, jotta niitä ei luokitella väärin yleisesti hyväksyttyviin riskeihin liittyviksi vaaroiksi. Yleisesti hyväksyttyviin riskeihin liittyvien vaarojen osuus ei saa ylittää tiettyä prosenttiosuutta (esimerkiksi y prosenttia) järjestelmän kokonaisriskistä. Osuuden tarkastaminen on välttämätöntä, jottei uusutta pienennetä jakamaan vaaroja useisiin alhaisen tason osavaaroihin. Jos vaara ilmaistaan usein erilaisina "piennempänä" osavaaroina, niistä jokainen voidaan luokitella helposti yleisesti hyväksyttyviin riskeihin liittyviksi vaaroiksi arvioitaessaen sitenäisesti, kun taas yhdessä arvioituna ne luokitellaan vaaraksi, jolla on merkittävä riski (toisin sanoen yhdeksi korkean tason vaaraksi). Osuuden arvo (esimerkiksi y prosenttia) määrityy järjestelmätasolla sovellettavien hyväksyttävän riskitaustan koskevien perustuiden mukaan. Osuuden arvon perustaksi ja arvioinnin pohjaksi voidaan ottaa samankaltaisia ohjeistoista saatua toiminnallinen kokemus.

Edellä käsitellyt kaksi tarkastusta (x ja y prosentteina ilmaistu osuus) mahdollistavat sen, että riskinarvioinnissa voidaan keskityä kaikkein tärkeimmäihin vaaroihin ja että kaikkia merkittäviä riskejä valvotaan (katso kaavio 8).

Hakija on vastuussa arvojen x prosenttia ja y prosenttia määrittämänsä asiantuntija-arvion pohjalta ja siitä, että arviointielin suorittaa niiden riippumattoman arvioinnin, sanotun kuitenkaan rajoittamaan jäsenvaltion lainsäädännöllisiä vaatimuksia. Suurussuorukka voi olla esimerkiksi x = 1 prosenttia ja y = 10 prosenttia, jos arvoa voidaan pitää hyväksyttyvänä asiantuntija-arvion pohjalta.

2.2.2 kohdan mukaan luokitettu "yleisesti hyväksyttyihin riskeihin" edellyttää arviointielimen toteuttamaa riippumattomaa arviointia.
2.2.4. During the hazard identification, safety measures may be identified. They shall be registered in the hazard record according to section 4.


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.

[2.2.5.][G 1] Vaikka riski saattaisiin hyväksyttävälle tasolle, hakija voi silti päätä, että vaarojen tarkempia tunnistamisen on välttämätöntä. Hakija voi esimerkiksi löytää kustannustehokkampia 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.

[2.2.6.][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.

[2.3.1.][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.

[2.3.2.][G 1] Lisäselvennystä ei pidetä tarpeellisena.
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.
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.

[2.3.8.]

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.

[2.4.1.]

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.

[2.4.2.]

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

[2.4.2.]

Esimerkiksi tunnelien turvallisuuteen tai vaarallisten aineiden kuljetusten turvallisuuteen liittyvät tietty näkökohdat voivat vaatia erityistarkastelua ja olla riippuvaisia käyttö- ja ympäristölänsuhteista, on välttämätöntä tarkastaa jokaisen hankkeen yhteydessä, että järjestelmää käytetään samoissa olosuhteissa.
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 vastaavuusanalyysseista 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 esitetty
"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 hyväksyttävänä, edellyttäen että (katso kaavion 1 piste tyynyrät):

1) 2.3.2 kohdassa esitetty menettelyohjeen soveltamisen ehdot täyttävät;
2) 2.4.2 kohdassa esitetty ohjeiston käyttöä koskevat ehdot täyttävät;

(b) hyväksyttävää riskitasoa koskevia eksplisiittisiä perusteita sovelletaan, kun halutaan arvioida eksplisiittisen riskin estimoinnin avulla hallittavien riskien hyväksyttävyyttä (katso kaaviossa 1 esitetty kolmatta periaatetta koskeva sitten ympyrä). Ne voidaan määrittää rautatiejärjestelmän eri tasojen mukaan ja niitä voidaan kuvata "perusteiden pyramiin" (katso kaavio 9), joka alkaa korkein tason hyväksyttävää riskitasoa koskevisista perusteista (ilmastunut esimerkiksi yhteiskunnallisen tai yksilöllisenä riskinä) ja ulottuu osajärjestelmiin ja osiin asti (tekiset järjestelmät), käyttöväheineen ihmisoperaattorit ja järjestelmän osajärjestelmiens kunnossapitotoimet mukaan luettuna. Vaikka hyväksyttävää riskitasoa koskevien perusteiden tarkoituksena on taata järjestelmän turvallinen toiminta ja vaikka ne liittyvät siten yhteisiin turvallisuusvaihteisiin ja kansallisii viitearvoihin, niiden välille on hyvin vaikeaa muodostaa matemaattistia mallia: katso yksityiskohtaiset tiedot (Ref. 12).

Hyväksyttävää riskitasoa koskevaa eksplisiittisten perusteiden tarkkuuden on vastattava merkittävän muutoksen tärkeyttä ja monimuutkaisuutta. Esimerkiksi liikkuvan kaluston jonkin akselityyppin muuttamisen yhteydessä ei ole välttämättöä arvioida koko rautatiejärjestelmää. Hyväksyttävää riskitasoa koskevien perusteiden määrittämisessä voidaan keskittyä liikkuvan kalustoon. Vastaavasti käytössä olevaan rautatiejärjestelmään tehtäviä suuria muutoksia tai lisäyksiä ei pidä arvioida yksinomaan yksittäisten lisättävien toimintojen tai muutosten turvallisuusointuksen 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 vastavurooista tunnustamista jäsenvaltioiden välillä, yhdenmukaistaistetaan viraston käynnissä olevien
hyväksyttävää riskitasoa koskeviin perusteisiin liittyvien toimien pohjalta. Kun lisätietoja on saatavana, ne sisällytetään tähän asiakirjaan.


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.


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.
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.
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.

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.

Ks. myös tämän asiakirjan 2.1.1 kohtaa koskeva G 4 kohta.

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.

Yksi esimerkki turvallisuusarvioineista ja -analyseista, joita voidaan suorittaa osajärjestelmän tasolla, on kausaalialaylsit: katso kaavio 10. Sen osoittamiseksi, että osajärjestelmän on panoksia koskevien turvallisuusvaatimusten mukainen, voidaan kuitenkin käyttää mitä tahansa menetelmää.

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

Ks. myös tämän asiakirjan 2.1.1 kohtaa koskeva G 4 kohta.
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.


[G2] Arviointielinten toteuttaman riippumattoman arvioinnin tyyppiä ja tarkkuutta (toisin sanoen yksityiskohtainen tai silmämääriä arviointi) tarkastellaan 6 artiklaa koskevissa selvennyskissä.

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.

[G1] Esimerkiksi tulipalon sammuttamisen voi johtaa uuteen vaaraan (tukehtumiseen), joka edellyttää uusia turvallisuustoimenpiteitä (kuten erityistä menettelyä matkustajien evakuoinniseksi). Toinen esimerkki on karkaistun lasin käyttö sen välttämiseksi, ettei ikkuna hajoa törämäksessä 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 toiminnat sisältyvät YTM:n vaiheeseen "järjestelmän turvallisuusvaatimustenmukaisuuden osoittaminen".
uutena vaarana on se, että hätäevakuointi vaunujen ikkunoista on selvästi vaikeampaa, mikä
voi johtaa turvallisuusvaatimuksiin, joiden takia tietty 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.
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 arviointiin tekee vaaroja koskevalle asiakirjalle tai asiakirjoiolle riippumattoman arvioinnin. Yksi mahdollinen ratkaisu on pitää yllä:

(a) yhtä "sisäistä vaaroa 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 hallintatehtävää varten, sitä ei tarvitse toimittaa muille toimijoille. Sisäinen vaaroja koskeva asiakirja sisältää kaikki tunnistetut vaarat, joita hallitaan, ja niihin liittyvät vahvistettavat turvallisuustoimenpiteet;

(b) yhtä "ulkosta vaaroa 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 liitteesä 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 tarkoitetuja vaaroja ja niihin liittyviä toimenpiteitä yhdellä ainoalla vaaroja koskevalla asiakirjalla mutta laatia kaksi kertomusta vaaroja koskevasta asiakirjasta (katso esim. liitteesä LISÄYS C oleva C.16.3. kohta):

(a) yksi kertomus sisäisestä vaaroa koskevasta asiakirjasta, joka ei kuitenkaan välttämättä ole tarpeellinen, jos vaaroja koskeva asiakirja on jäsennely hyvin riippumattoman arvioinnin mahdollistamiseksi;

(b) kysymys ulkoisesta vaaroa koskevasta asiakirjasta vaarojen ja niihin liittyvien turvallisuustoimenpiteiden siirtämiseksi muille toimijoille.

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

(a) kaikkia vaaroja, jotka siirretään muille toimijoille, hallinnoidaan siirron toteuttavan toimijan ulkoisella vaaroa koskevalla asiakirjalla. Koska vaarat sisältyttävät muiden toimijoiden vaaroja koskeviin asiakirjoihin ja niitä hallinnoidaan tällaisilla asiakirjoilla, kyseisen toimijan ei enää tarvitse hallinnoida niitä (osa)järjestelmän elinkaaren aikana;

(b) kaikkia asiain liittyviä turvallisuustoimenpiteitä ei kuitenkaan pidä vahvistaa vaaroja koskevassa asiakirjassa; tätä koskevat perusteet esitetään 4.2 kohtaa koskevassa G 9
kohdassa. On järkevää, että organisaatio, joka siirtää käyttörajoitukset, ilmoittaa selvästi vaaroja koskevassa asiakirjassa, että asiaan liittyviä turvallisuustoimenpiteitä ei ole vahvistettu.


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\(^{15}\) (joiden kutsutaan myös turvallisuuteen liittyviksi sovellusehdoiksi), ja tapauksen mukaan valmistajien määrittämät yleisiä sovelluksia ja yleisiä tuotteita koskevat turvallisuusarviot.


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 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” turvallisuusarvoista ja ”oletuksia ja käyttörajoituksia” koskevat lisäselvennykset tämän asiakirjan 1.1.5 kohtaa koskevasta G 5 kohdasta ja alaviitteistä (9) ja (10).
kaikki tarvittavat selvennykkset, jotta ongelma ymmärretään selkeästi. On mahdollista, että vaarojen, turvallisuustoimenpiteiden ja riskien alkuperäästä sanamuotoa on muuttettava, jotta ne voidaan ymmärtää ilman, että niistä on keskusteltava uudelleen. Vaarojen yhteinen uudelleenarviointi voi johtaa uusiin turvallisuustoimenpiteisiin.

[V4] Vastaanottava toimija, joka vastaa vastaanotettujen tai uusien turvallisuustoimenpiteiden toteuttamisesta, hallitsemisesta ja vahvistamisesta, rekisteröi omaan vaaroja koskevaan asiakirjaan kaikki asiaa koskevat vaarat niihin liittyvine turvallisuustoimenpiteineen (sekä siirretyt että yhteisesti tunnistetut).

[V5] Jos turvallisuustoimenpidettä ei ole vahvistettu kaikilta osin, on määritettävä selvä käyttörajoitus (esim. lientävät toiminnalliset toimenpiteet), ja se on rekisteröiltävä vaaroja koskevaa asiakirjaa. On mahdollista, että teknisiä/suunnittelun 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 yksilöiltävä selvästi vaaroissa asiakirjassa. Lisäksi on esitetävä näyttö siitä /perustelut sille, miksi toteutetut turvallisuustoimenpiteet ovat asianmukaisempia(16), ja osoitettava, että korvaavat turvallisuustoimenpiteet täyttävät järjestelmälle asetetut turvallisuusvaatimukset;
(d) jne.

Tällaisissa tapauksissa teknisiä/suunnittelun liittyviä turvallisuustoimenpiteitä ei voida hallita ja vahvistaa vaarojen hallintamenettelystä. Asiaan liittyvät vaarat ja turvallisuustoimenpiteet on täytettävä avoimiksi vaaroja koskevassa asiakirjassa, jottei käytetä väärin muiden järjestelmien turvallisuustoimenpiteitä soveltamalla "vastaavan ohjeiston" hyväksyttävää risikitasiotpäätöstä koskevaa periaatetta.


[V7] Lisäksi voi olla hyödyllistä merkitä vaaroja koskevan asiakirjan, toteutetaanko asiaa koskevat turvallisuustoimenpiteet oikein järjestelmän elinkaaren myöhemmässä vaiheessa vai jatketaanko järjestelmän käyttöä soveltamalla yksilöityjä käyttörajoituksia. Vaaroja koskevan asiakirjan voi olla hyödyllistä merkitä myös perustelut sille, miksei asiaan liittyviä teknisiä turvallisuustoimenpiteitä toteuteta oikein/täysimääräisesti.

[V8] Toimija, joka vastaanottaa käyttörajoitukset:
(a) vie ne kaikki omaan vaaroja koskevan 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.
(c) varmentaa ja validoi, että arvioitava järjestelmä on näiden käyttörajoituksen mukainen.

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 otettaisiin sillä välin käyttöön.

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

(1) organisaatio, joka siirtää käyttörajoituksen, 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 päättää jatkossakin hallinnoida asiana liittyviä riskejä toisin, käyttörajoitusten viennin hoitavan organisaation on hyödyllistä osoittaa selvästi vaaroja koskevalla asiakirjalla, että asiana 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. Näm on kellon jos järjestelmää käytetään ohjeistona toisessa sovelluksessa:

(i) uutta järjestelmää on käytettävä samoin ehdoine eli on noudatettava kyseisiin oletuksiin liittyviä käyttörajoituksia), tai

(ii) hakijan on tehtävä poikkeamien osalta täydentävä riskinarviointi käyttämällä kyseisiä oletuksia.
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.


(a) **Hankesuunnitelmissa** kuvataan hankkeen jonkin toiminnon hallinnoimeksi käyttöön otettavaa organisaatiota.

(b) **Hankemenettelyissä** kuvataan yksityiskohtaisesti, miten jokin tietty tehtävä toteutetaan. Tavallisesti yritys on laatimut menettelyt ja ohjeet, joita sovelletaan sellaisinaan. Uusia hankemenetelyjä laaditaan vain, jos on kuvattava kyseiseen hankkeeseen liittyvä tietty tehtävä.

(c) **Hanckeekehittämiseen liittyvä** asiakirjat laaditaan kaavioissa 5 esitetyn järjestelmän elinkaaren mukaisesti.

(d) **Yritys- tai vähintään hankekohtaiset mallit** tuotetaan erityyppisiä laadittavia asiakirjoja varten.

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

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

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

(a) näyttö laadunhallinnasta,

(b) näyttö turvallisuusjohtamisesta,
(c) näyttö toiminnallisesta ja teknisestä turvallisuudesta.

Sillä voidaan samalla tukea ja opastaa arviointieliimiä YTM-asetuksen oikean soveltamisen rippumattomassa arvioinnissa.


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

(a) katso standardi EN 50 129 {Ref. 7} "Rautatiesovelukset – Tietoliikenne-, merkinanto- ja tietojenkäsittelyjärjestelmät – Turvallisuuteen liittyvät elektroniset järjestelmät", ohjeen EN 50 126-2 {Ref. 9} liite H.2 sisältää myös ehtoituksen merkinantojärjestelmien turvallisuusarvon rakentekseksi;

(b) katso ohjeen EN 50 126-2 {Ref. 9} liitteestä H.1 liite H.1 kaluston turvallisuusarvon rakenne;

(c) katso ohjeen EN 50 126-2 {Ref. 9} liitteestä H.3 infrastruktuurien turvallisuusarvon rakenne.

Kuten edellä esitetystä viitteistä käy ilmi, teknisten järjestelmien turvallisuusarvon rakene 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 välittämättä sovellu käytettäväksi kaikissa samantyyppisissä järjestelmissä. Siksi esimerkkejä käytettäessä on arvioitava sen soveltuvuutta kunkin sovelluksen kannalta.

[5.5] Rautatiejärjestelmien organisatorisia ja toiminnallisia näkökohtia koskeva turvallisuusarvio:

Tällä hetkellä ei ole käytössä erityistä standardia, jossa määritetään rautatiejärjestelmän organisatoristen ja toiminnallisten näkökohtien turvallisuusarvon rakenne ja sisältö ja annetaan ohjeita turvallisuusarvon laatimiseksi. Koska turvallisuusarviolla pyritään kuitenkin osoittamaan jäsennellysti, että järjestelmä vastaa sille asetettuja turvallisuusvaatimuksia, samantyyppistä turvallisuusarvon rakennetta voidaan soveltaa teknisiin järjestelmiin. 5.1 kohtaa koskemassa G 4 kohdassa esitettyissä viitteissä esitetään ohjeita ja tarkastuslistua näkökohtia, jotka on otettava huomioon arvioitan järjestelmän tyyppistä riippumattu. Organisatoristen ja toiminnallisten muutosten hallinta edellyttää samanlaisia laadunhallintaa- ja turvallisuusjohtamismenettlejä 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 "laiteiston luontainen varmistus vikaantuessa" -periaatteisiin, sähkömagneettiseen yhteenopisuuteen (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.
Järjestelmän monimutkaisuuden mukaan tämä näyttö voidaan esittää yhdessä tai useammassa turvallisuusarviossa. Katso 5.1 kohta koskevasta G 4 ja G 5 kohdasta teknisten järjestelmien ja toiminnallisten ja organisatoristen näkökohtien turvallisuusarvion rakenne.

Katso myös mahdolliset esimerkit todisteista liitteessä A olevasta A.4. kohdasta.

Rautatiealan teknisten järjestelmien ja osajärjestelmien käyttöön odotetaan yleensä olevan noin 30 vuotta. On todennäköistä, että tällaisen pitkän ajanjakson aikana järjestelmiin tehdään merkittäviä muutoksia. Tällaisille järjestelmissä ja niiden rajapinnoille voitaisiin siten tehdä täydentäviä riskinarviointeja ja laatia asiakaan liittyvät asiakirjat, joita on tarkistettava, täydennettävä ja jotka on siirrettävä varoja koskevia asiakirjoja käytävien eri toimijoiden ja organisaatioiden kesken. Tämä edellyttää, että asiakirjojen valvontaan ja kokoonpanoon hallintaan sovelletaan suhteellisen tiukkoja vaatimuksia.

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).

Tätä vaatimusta voidaan perustella muun muassa seuraavasti:

(a) tällä varmistetaan, että kaikki arviotavana 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 asian liittyviin turvallisuusanalyseihin ja turvallisuusasiakirjoihin;

(b) tällä varmistetaan, että arviotavana olevaa järjestelmää koskevat turvallisuusanalyysit ja turvallisuusasiakirjat ovat saatavilla, jos järjestelmää käytetään toisessa sovelluksessa vastaavana ohjeistona.
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.
LISÄYS A: LISÄSELVENNYKSET

A.1. Johdanto

A.1.1. Lisäyksen tarkoituksena on helpottaa tämän asiakirjan lukemista. Asiakirjassa ei anneta suurta määrää erilaista tietoa, vaan tällä 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 hyväksyttävän riskitasoa koskeva peruste (RAC-TS)

A.3.1. Teknisten järjestelmien hyväksyttävän riskitason yläraja

A.3.1.1. RAC-TS:ää käsittelään asiakirjan (Ref. 4) 2.5.4 kohdassa.


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 satunnaisen laitteistovikojen osalta, kun taas järjestelmällisiä vikoihin/virheiin sovelletaan kvantitatiivisia menetelmiä(17). "Koska järjestelmällisten vikojen eheyttäosa ei voida arvioida kvantitatiivisin menetelmin, tietyllä turvallisuuden eheyttäosa toteutettavan

(17) CENELEC-standardien 50 126, 50 128 ja 50 129 mukaan satunnaisiin laitteistovikoja kuvaava kvantitatiivinen luku on yhdistettävä aina turvallisuuden eheyttäsoonto, 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.
järjestelmän yhteydessä menetelmät, välineet ja tekniikat, joiden katsotaan tehokkaasti käsittävän asianmukaisen luottamustason, ryhmitellään turvallisuuden eheyystason mukaisesti."


CENELEC-standardin 50 128 mukaan turvatoimintoja toteuttavan ohjelmointavan sähköisen valvontajärjestelmän korkein mahdollinen turvallisuuden eheyystaso (SIL) ohjelmiston kehitettämisprosessissa on SIL 4, mikä vastaa kvantitaatiivista siedettävää vaaratasona 10⁻⁸ 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 eheyystason.

(a) laatuprosessin tarkoituksena on "minimoida inhimillisten erheiden esiintyvyys kaikissa elinkaaren vaiheissa ja siten pienentää järjestelmällisten vikojen/riskiä järjestelmämää"

(b) turvallisuusprosessin tarkoituksena on "vähentää edelleen turvallisuuteen liittyvien inhimillisten erheiden esiintyvyyttä koko elinkaaren aikana ja siten minimoida turvallisuuteen liittyvien järjestelmävikojen jäänmääräriski".

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

(a) CENELEC-standardissa 50 126-1 (Ref. 8) ja sen ohjeessa 50 126-2 (Ref. 9) luettelaan CENELEC-standardin 50 129 lausekkeet ja määrätään niiden sovelletavuus muiden kuin merkinantojärjestelmän koskevan dokumentoituun näyttöön: katso ohjeen 50 126-2 (Ref. 9) taulukko 9.1. Luettelossa annetaan ohjeet, miten järjestelmästä johtuvia vikoja ja arvioitavaa järjestelmän 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 suunnitteluvaiat";
2) "ympäristöönot";
3) "väärinkäyttö- ja toimintavirheet";
4) "ohjelmiston mahdolliset jäännösvaiat";
5) "inhimilliset tekijät";

CENELEC-standardin 50 129 (Ref. 7) liitteissä D ja E esitetään teknikat ja toimenpiteet, joiden avulla voidaan välttää turvallisuuteen liittyvien sähköisten merkinantojärjestelmien järjestelmällisiä viikoja ja hallita satunnaisia laitteistovikoja ja järjestelmällisiä vikoja/virheitä. Monia näistä teknikoista ja toimenpiteistä voidaan soveltaa myös muinakin kuin merkinantojärjestelmään ohjeen 50 126-2 (Ref. 9) taulukon 9.1 mukaisesti.

(b) CENELEC-standardin 50 128 sisältää ohjeet turvallisuuteen liittyvien ohjelmistojen kehittämiseksi arvioitavan ohjelmiston edellyttämän turvallisuustason (SIL 0–SIL 4) mukaisesti.
A.3.1.8. RAC-TS vastaa näin ollen korkeinta mahdollista eheystasoaa, 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 viskatoimenpiteille, joiden toteuttamista voidaan vaatia vaarallisisten vikatyyppeihin yhteydessä. Näiden toimenpiteiden katsotaan vastaavan turvallisuuden eheystason 4 alarajaa. Turvallisuuteen liittyvät järjestelmät, jotka eivät ole monimutkaisia, voidaan joissakin tapauksissa suunnitella pienemmän kohdennettujen viskatoimenpiteitensä koskevien arvojen mukaisesti, mutta taulukossa esitetty 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 jommallakkumalla tavalla:

1. jos toiminto voidaan jakaa toiminnallisesti riippumattomiin osafunktioihin, THR (varmuusvikataajuus) voidaan jakaa näiden osafunktioiden ja kullekin osafunktioille 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 teknistä ja operatiivisia toimenpiteitä, jotta vaadittava THR voidaan saavuttaa."


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 vastaavuusarviointin (ohjeiston) perusteella. YTM:n soveltomisalalla RAC-TS:ää on sovellettaa 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 kehitämisprosessin järjestelmällisiä vikoja/virheitä ei voida kuvata määrällisesti;
(b) järjestelmällisten vikojen/virheiden esiintyvyyttä ja niiden jännöskertymiä voidaan arvioittaa yhdistäen asiainmukaiset hallintatarkastukset ja järjestelmän toiminnan päivitystöjen yhteydessä;
(c) korkeilla hallintatarkastuksilla on voida arvioida vikojen/virheiden esiintyvyys
(d) järjestelmällisiä vikoja ja virheitä, jotka voidaan arvioitaa käytännössä.
A.3.1.11. Tekninen järjestelmä voi saavuttaa siedettävän vikatason 10^{-3} h^{-1}, kun sillä on joko "vikaturvallinen rakenne" (joka määritelmänä mukaisesti on tällaisen turvallisuustason mukainen) tai "kaksinkertainen rakenne" (esim. kaksi riippumatonä käsittelykanavaa, jotka ristiintarkastavat toisensa).

Kaksinkertaisen rakenteen osalta voidaan osoittaa, että teknisen järjestelmän väärrä opastetta koskeva kokonaisvirhe (\(\Lambda_{\text{WSF}}\)) on verratnollinen :\(^{2}\)T:hen, jossa

(a) \(\lambda^2\) on yhden kanavan väärrää opastetta koskevan vikatason neliö;

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


(a) kun kanavan luotettavuuslувun kaksimaaariainen vikaantumisvåli (MTBF) on 10 000 tunttia, ja varovaisen oletuksen mukaan kaikki kanavan viat ovat vaarallisia, kanavan väärrää opastetta koskeva vika on \(10^{-4}\) h^{-1};

(b) näin on jopa silloin kun toisen kanavan väärrää opastetta koskevan (koskevien) vian (vikojen) tunnistamiseen kuluu 10 minuuttia (eli \(2 \times 10^3\) tunttia), mikä on niin ikään varovainen oletus. Väärrää opastetta koskeva kokonaisvirhe on \(\Lambda_{\text{WSF}} \approx 2 \times 10^{-10} \text{ h}^{-1}\)

A.3.1.13. Käytännössään, kun arvioidaan tällaisen kaksinkertaisen rakenteen väärrää opastetta koskevaa kokonaisvirkaa, on otettava huomioon toimenpiteet, joita on suunniteltuvaiheessa toteutettu yhteisviiotila ja yhteisviiotumistavoilta (CCF/CMF) suojautumiseksi ja sen varmistamiseksi, että tekninen järjestelmän ohjautuu CCF/CMF-vikojen/virheiden ilmetessä vikaturvalliseen tilaan. Tällä väärrää opastetta koskevan kokonaisvirheen (\(\Lambda_{\text{WSF}}\)) 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 järjestelmissä tämä aika voi olla erilaisten suuruusluokkien vuoksi yli 1 sekuntia;

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

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

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

A.3.3. **YTM-asetuksen 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 liittyyvien merkitystellisten rajapintojen suunnittelu otetaan huomioon, ihmisoperaattorit ja niiden toimet eivät sisälly tekniseen järjestelmään. Kunnossapitoprosessi kuvalaan kunnossapito-ohjeissa, mutta se ei varsinaisesti ole osa teknistä järjestelmää.
A.3.4. "Teknisen järjestelmän" määritelmä koskeva selvenys

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 kokooppano ja sisällys ovat seuraavat:

![Diagram](http://www.era.europa.eu)

**Kaavio 14: RAC-TS:n sovellettavuustestin kulkuavio**
Tämä käsittää CENELEC eurauksiin. Tässä tapauksessa RAC-litteiset vaatimukset sisältävät toimintavikojen todellisen vaikutus kokonaistavoitteen perusteella kunkin tapahtuman ja siten tarkasteltavassa skenaariossa asetettavia viat RAC-seurauksiin".

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 päätyy sen hyväksyntään". Tämä käsittää CENELEC-standardin 50 126-1 (Ref. 8) kaaviossa 10 esitetyn V-sykin vaiheet 1–10.

(b) "Siinä otetaan huomioon inhimilliseen toimintaan liittyvien merkityksellisten rajapintojen suunnittelu. Ihmisoperaattorit ja niiden toimet eivät kuitenkaan sisällä tekniseen järjestelmään." Vaikka inhimillisen tekijän teknisen järjestelmän toiminnan ja kunnossapidon aliksan aiheuttamat virheet eivät kuulu varsinaiseen tekniseen järjestelmään, ne on otettava huomioon suunnittelussa ihmisooperaattorien rajapintoja.

(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 tukeviset teknisen järjestelmän määritelmän on kuitenkin sisälizzievällä riittävän yksityiskohtaisesti kaikki merkitykselliset vaatimukset (esimerkiksi säännölliset virheet eivät kuulu kunnossapiden tai korjauvat huoltoimenpiteet virkatapaustuksissa). 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 kokonaisvalotteeksi tuhoisiin seurauksiin johtaville tapahtumarajalle. Tämän kokonaisvalotteen 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.


**Euroopan rautatievirasto**
Esimerkkikokoelmia riskien arvioinnista ja YTM-asetuksista tukevista mahdollisista välineistä
(a) toiminto määritellään tässä yhteydessä "tavoittelavaksi erityiseksi päämääräksi tai tavoitteenä, joka voidaan täsmentää tai kuvata viittaamatta sen saavuttamisessa tarvittaviin fyysisiin keinoihin"
(b) toiminto (niin sanottu musta laatikko) muuttaa panosparametrin (esimerkiksi materiaali, energia ja tieto) päämäärään liittyviki tuotosparametreiksi (esimerkiksi materiaali, energia ja tieto).
(c) toiminnon arviointi on riippumaton sen teknisestä toteutuksesta.

A.3.5.4. RAC-TS:ää sovelletaan seuraaviin toimintotyypeihin:
(a) kalustoysikössä olevan ETCS-osajärjestelmän esimerkki:
   (1) "tarjoaa kuljettajalle tietoa, jonka avulla hän voi ohjata junaa turvallisesti ja käyttää jarrujärjestelmää ylinopeuslaitteessa". Radanvarresta saatujen tietojen (sallittu nopeus) ja kalustoysikössä olevan ETCS-osajärjestelmän tekemän junan nopeuslaskelman perusteella kuljettaja ja kalustoysikössä oleva ETCS-osajärjestelmä voivat valvoa, ettei juna ylittä sallittua nopeutta. RAC-TS:ää sovelletaan junan nopeuden arviointiin kalustoysikössä olevilla järjestelmillä, koska:
      (i) muita (välittämiä) lisäesteitä ei ole, sillä myös kuljettajalle toimitettu tieto arvioidaan;
      (ii) junan ylinopeus saattaa suistaa junan raiteilla, ja tällainen onnettomuus voi johtaa tuhoisiin seurauksiin.
   (2) "tarjoaa kuljettajalle tietoa, jonka avulla hän voi ohjata junaa turvallisesti ja käyttää jarrujärjestelmää salliun kulkuvalin rikkomistapauksessa";
(b) raidevirtapiirin esimerkki: "havaitsee raidesuuden käytön". RAC-TS:ää voidaan soveltaa sellaisenaan tähän toimintoon ainoastaan, jos lukituksessa ei ole toteutettu "sekvenssi-valvonta"-toimintaa;
(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 toimintotaso (informatiivisissa liitteissä tasojen mainitana viisi). Kaiken kaikkiaan standardissa prEN 0015380-4 määritellään useita satoja järjestelmien liittyviä toimintoja;
(b) yleisesti on suositeltavaa valita toiminnot standardin prEN 0015380-4 kolmelta ensimmäiseltä tasolta (ei alemmilta tasolilta) ja ottaa tässä yhteydessä huomioon myös tuotteet jaettelu koskien rakenteen;
(c) standardin prEN 0015380-4 soveltamisalan ulkopuolisten toimintojen asiantuntija-avioon perustuvassa vertailussa.
Viraston on vielä käsittelä näitä standardin prEN 0015380-4:n toimintoesimerkkejä työstääksään yleisesti hyväksytyjä 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.
A.3.5.7. A.3.5.4. kohdan esimerkkejä ja lisäksi A.3.5.6. kohdassa esitetty esimerkit osoittavat selvästi, ettei RAC:n näitä toimintoja käytetä jaetettuja vikataajuutta koskevien perusteiden perusteen mukaan tuhoisina. Tämä ainoastaan annetaan tiedoksi, koska kallistumatoiminnan vika ei johda tuhoisiin seurauksiin.


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 $10^{-9} \text{h}^{-1}$ väljempiä turvallisuusvaatimuksia. Tässä asiakirjassa ei suosita eikä kehoteta käyttämään mitään tiettyä menetelmää. Tässä ainoastaan annetaan tiedoksi, miten RAC-TS:ää voidaan soveltaa jaetettujen menetelmien jaetettujen kalibroinnissa. Tätä näkökohtaa on kehitettävä edelleen yleisesti hyväksyttävien riskien ja hyväksyttävää riskitasoita koskevien perusteen alalla tehtävällä viraston toimilla.

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

A.3.6.2. Esimerkki 1: Riskin välitön vaihtoehdo

(a) RAC-TS:ää voidaan soveltaa helposti skenaarioihin, jotka eroavat ainoastaan muuttamalla riippumattomalla parametrilla YTM-asetuksen (Ref. 3) 2.5.4. kohdassa määritelystä RAC-TS:n viite-ehdoista.

(b) Oletetaan, että tietyn parametrille p risksuhde on moninkertaistava. Oletetaan, että p∗ sisältyy viite-ehdoon, kun taas vaihtoehtoisessa skenaarioissa voidaan soveltaa p²:ää. Tässä tapauksessa merkityksellinen on ainoastaan parametrisuhde p∗/p², ja esintymistihyyttä voidaan pienentää. Tämä menetetty voidaan toistaa, jos parametrit ovat riippumattomia.

(c) Esimerkki:

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

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

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

A.3.6.3. Esimerkki 2: Riskimatriisin kalibrointi

(a) Jotta RAC-TS:ää voidaan käyttää asianmukaisesti riskimatriisiissa, matriisin on koskettava oikea järjestelmätaso (joka on verrattavissa lisäksessä A olevassa A.3.5. kohdassa mainituun tason).
(b) RAC-TS määrittelee yhden riskimatriisin kentän siedettäväksi, eli se vastaa koordinaattia (tuhoissa seuraus, esiintymistiheys $10^{-3}$ h$^{-1}$): katso taulukon 5 punainen kenttä. Kaikki suurempaan esiintymistiheyyteen liittyvät kentät on merkittävä "sietämättömiksi". On pantava myös merkille, että ainoastaan tapauksessa, joka voi uskottavasti ja suoraan johtaa tuhoisaan seuraukseen, onnettomuksien esiintymistiheys on sama kuin toimintavikojen esiintymistiheys.

(c) Tämän jälkeen voidaan täyttää matriisin muut kentät, mutta riskien välttämisen tai luokien 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", ekstrapolooidaan lineaarisesti matriisin muuhun kenttiin. Tämä tarkoittaa, että kaikki saman riven (tai rivin alapuolen) kentät saavat niin ikään merkinnän "hyväksyttävä". Myös alapuoliset kentät voidaan merkitä "hyväksyttäviksi".

### Taulukko 5: Tyypiesimerkki kalibroidusta riskimatriisista

<table>
<thead>
<tr>
<th>(Vaaran aiheuttaman) onnettomuuden esiintymistiheys</th>
<th>Riskitaso</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yleinen (10$^{-3}$ tunnissa)</td>
<td>Sietämätön</td>
</tr>
<tr>
<td>Todennäköinen (10$^{-3}$ tunnissa)</td>
<td>Sietämätön</td>
</tr>
<tr>
<td>Satunnainen (10$^{-3}$ tunnissa)</td>
<td>Hyväksyttävä</td>
</tr>
<tr>
<td>Vähäinen (10$^{-3}$ tunnissa)</td>
<td>Hyväksyttävä</td>
</tr>
<tr>
<td>Epätodennäköinen (10$^{-3}$ tunnissa)</td>
<td>Hyväksyttävä</td>
</tr>
<tr>
<td>Ei uskottava (10$^{-3}$ tunnissa)</td>
<td>Hyväksyttävä</td>
</tr>
<tr>
<td>Merkityksenä</td>
<td>Marginaalinen</td>
</tr>
<tr>
<td>Vaaran seurauksien (eli onnettomuksien) turvallisuustasot</td>
<td></td>
</tr>
</tbody>
</table>

(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 onnettomuksien sallittu taajuus voi olla enintään "epätodennäköinen" (tai jopa vähemmän).

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

### A.3.6.4. Muiden riskinarviointimenetelmiin kalibroidinta

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


(b) Toinen vaihe: käytä kyseessä olevan menetelmän vaihtosuhdemenetelmiä (trade off) riskin siedettävyyden ekstrapoloimiseksi vaaroihin, joiden seuraukset eivät ole tuhoisia (käytä lähtökohtana lineaarista riskin vaihtosuhdetta).
(c) Kolmas vaihe: niiden vaarojen osalta, joiden seuraukset eivät ole tuhoisia, RAC-TS voidaan tämän jälkeen johtaa kalibroidun riskinarviointimenetelmän avulla vertaamalla koordinaattia (esiintymistihys, vakavuus) näin saatuun FN-käyrään.

A.3.7. RAC-TS:ää koskevat päätelmat

A.3.7.1. YTM:n asetuksen mukaisessa yleisessä riskinarviinnissa hyväksyttävää riskitason perusteita tarvitaan, jotta voidaan määrittää, milloin riski(ene) jäännöstä on tulee hyväksyttävä ja milloin näin ollen ekspisitiivinen 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 riskinarviointimenetelmän voidaan kalibroida;
(b) mahdollistaa teknisten järjestelmien vastavuoroinen tunnustaminen, sillä riskinarviointi ja turvallisuusarvioinnit tehdään saman hyväksyttävän riskitasoan koekuvan perusteentuksen mukaisesti kaikissa jäsentenvaltiossa;
(c) säästää kustannuksissa, sillä RAC-TS ei edellytä tarpeettoman korkeita kvantitatiivisia turvallisuusvaatimuksia;
(d) edistää valmistajien välistä kilpailua. Erilaisten hyväksyttävän riskitasoan koskevien perusteiden käyttö joko hakijan tai jäsentenvaltion osalta johtaisi siihen, että teollisuuden olisi osoitettava teknisten järjestelmienä vaatimustenmukaisuus useilla erilaisilla tavoin. Tämä vaarantaisi valmistajien kilpailukyvyn ja tekisi tuotteistapaneelien kalliita.


A.3.7.5. Teknisten järjestelmien hyväksyttävää riskitasoaa koskevaa yhtenäistettyä semikvantitatiivista perustetta tarvitaan vain, jollei menettelyohjeita tai ohjeistojavaiota käytetä.

A.3.7.6. Koska järjestelmällisten viikoenvirheiden turvallisuuden eheydestä on oltava vähintään SIL 4, teknisten järjestelmien satunnaisnestien laitteistovikojen turvallisuuden eheydestä on niin ikään oltava vähintään SIL 4. Tämä vastaa suurinta siedettävää vaaratason (THI eli varmuusväkataajuus) 10⁻⁹ h⁻¹. CENELEC-standardin 50 129 mukaan tiukempia turvallisuusvaatimuksia ei voida saavuttaa pelkästään yhdelä järjestelmällä; järjestelmän rakennetta on muutettava, ja on esimerkiksi käytettävä kahta järjestelmää, mikä vääristämättä lisää radikaalisti teknisen järjestelmän kustannuksia. Katso lisätietoja lisäyksessä A olevasta A.3.1. kohdasta.

A.4. Turvallisuusarviointiin perustuva näyttö

A.4.1. Tässä kohdassa opastetaan, mitä näyttöä arviointiopimulle 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 asian liittyvät merkitykselliset näkökohdat on otettu huomioon ja dokumentoitu YTM-asetuksen soveltamisen yhteydessä.

A.4.2. Turvallisuusarviointi: CENELEC kehottaa laatimaan turvallisuusarviointimatalajen hankkeen alussa tai, jos tämä ei ole hakkeessa luonteessa, sisällyttämään asiana koskevan kuvaksen johonkin muuhun merkitykselliseen asiakirjaan. Jos arviointiopimet nimetään hankkeen alussa, turvallisuusarvioinnit ovat hankittava myös niiden lausunto. Lähtökohtaisesti turvallisuusarviointimatalajissa 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 käyttöolajen/rajojen kuvaus
   (2) toimintojen kuvaus
   (3) järjestelmäraakenetteen kuvaus
   (4) toiminta- ja ympäristöolosuhteiden kuvaus;
(b) ulkoisten rajapintojen kuvaus;
(c) sisäisten rajapintojen kuvaus;
(d) elinkaaren vaiheiden kuvaus;
(e) turvallisuusperiaatteiden kuvaus;
(f) riskinarvioinnin rajat määrättävien oletusten kuvaus.

A.4.4. Jotta riskinarviointi voidaan tehdä, järjestelmämäärittelyssä otetaan huomioon suunnitellun mutoksen asiayhteyes:

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

A.4.5. Vaarojen tunnistamisvaiheessa vaadittava näyttö:

(a) vaarojen tunnistamismenetelmiä ja -välineiden kuvaus ja perustelut (mukaan lukien rajoitukset) (yläätä alas-menetelmä, alhaalta ylös -menetelmä, HAZOP-menetelmä jne.);
(b) tulokset:
   (1) vaarojen luettelo
   (2) järjestelmän (rajoj) vaarat
   (3) osajärjestelmän vaarat
   (4) rajoinnan vaarat
   (5) turvallisuustoimenpiteet, jotka voidaan yksilöidä tässä vaiheessa.
A.4.6. Seuraava näyttö vaaditaan myös riskinarviointiavaiheesta:

(a) Kun menetelyohjeita käytetään vaarojen valvonnassa, on osoitettava, että arvioitava järjestelmä täyttää kaikki menetelyohjeiden asiala koskevat vaatimukset. Tässä yhteydessä on osoitettava, että asiaa koskevia menetelyohjeita 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 ohjeiston 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 rajoituksista);
   (2) on yksilöitänä käytetään kaikkia vaarantumisriskiä ja perustelu niiden kriittisissä olosuhteissa perustelujen ja perustelut (mukaan luettuina inhimilliset tekijät);
   (3) on esitettävä ja luokiteltava riski kunhan kaikista riskiä:
      (i) vaaran seurauksien estimointi ja perustelut (sisältää oletukset ja olosuhteet)
      (ii) vaaran esiintymistahdon estimointi ja perustelut (sisältää oletukset ja olosuhteet)
      (iii) vaarojen luokittelu niiden kriittisyyden ja esiintymistahdon perusteella;
   (4) on yksilöitänä asianmukaiset lisätehtävät riskiarvioinnissa ja perusteltu riski tulee hyväksyttävä (riskin evaluointivaiheen jälkeinen toistuva prosessi).

A.4.7. Riskin evaluointiin vaadittu näyttö:

(a) Kun toteutetaan eksplisiittinen riskin estimointi:
   (1) kunhan kaikista riskinarviointiperusteiden määrittely ja perustelut
   (2) on osoitettava ja esitettävä perustelut siitä, että turvallisuusvaatimukset ja turvallisuusvaatimukset kattavat kaikki vaarat hyväksyttävän tason mukaisesti (edellä mainitun riskinarviointiperusteen mukaisesti);

(b) YTM-asetuksen 2.3.5 ja 2.4.3 kohdan nojalla menetelyohjeita soveltamalla ja vastaaviin ohjeistoihin vertaamalla katettuja yhteyksiä pidetään implisiittisesti hyväksyttävänä edellyttäen, että (katso kaavion 1 pisteempyrä):
   (1) 2.3.2 kohdan mukaiset käyttöohjeiden soveltamisedellytykset täytetään
   (2) 2.4.2 kohdan mukaiset ohjeiston käyttöä koskevat edellytykset täytetään.

Riskinarviointiperusteet ovat implisiittisiä näille kahdeelle hyväksyttävälle riskitasoa koskevalle periaatteelle.

A.4.8. Vaarojen hallintaa koskeva näyttö:

(a) kaikkien vaarojen ja seuraavien tietojen kirjaaminen vaaroja koskevaan asiakirjaan:
   (1) tunnistettu vaara
   (2) turvallisuusvaatimukset, jotka estävät vaaran esiintymisen tai lieventävät sen seurauksia
   (3) toimenpiteiden turvallisuusvaatimukset
   (4) järjestelmän merkityksellinen osa
(5) turvallisuustoimipiteistä 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) prosessin 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
itetyn turvallisuustuotannon hankkiminen).

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
kohta 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 suosittelee, että edellä mainittu näyttö ryhmitellään uudelleen ja
että siitä laaditaan yhteenveto yhteen asiakirjaa, joka toimitetaan arviointielimelle: katso 5.1
kohta koskevat G 4 ja G 5 kohta.
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 ohjetaan hakemaan lisätietoa muista standardeista.
LISÄYS C: ESIMERKKJEÄ

C.1. Johdanto

C.1.1. Tämän lisäyksen tarkoituksena on helpottaa tämän asiakirjan lukemista. Lisäysessä esitetään yhteenvento 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 sääliy luottamuksellisena
(c) esimerkit, joiden alkuperää ei mainita, laati viraston henkilöstö aiemman ammatillisen kokemuksensa perusteella.

Kunin esimerkin osalta selvitetään, mikä on sovellutun prosessin ja YTM-asetuksen edellyttämän prosessin välein 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 työssä 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.


---

Kaavio 15: Esimerkki muutoksesta, joka ei ole merkittävä Puhelinviesti tasoristeysen valvomiseksi.
C.2.3. Olemassa oleva järjestelmä: ennen kuin suunniteltu muutos tehtiin, saapuvan junan suuntaa koskeva tieto välitettiin automaattisesti puhelimen sointiään avulla tasoristeyksen operaattorille. Sointiääni oli erilainen riippuen siitä, mistä puhelu tuli.

C.2.4. Suunniteltu muutos: käytössä olleesta puhelinjärjestelmästä oli tuloska vanhanaikainen, ja se oli korvattava uudella digitaalisella järjestelmällä, minkä vuoksi teknisesti merkityksellistä tietoa ei enää voitu välittää puhelimen sointiäänen avulla. Uudessa järjestelmässä on täsmälleen sama riippumatta siitä, ettei kyseistä muutosta arviointielimen täysimääräistä soveltamista, johon kuuluu muun muassa vaarojen kirjaiminen.

C.2.5. Vaikka muutoksella näyttää olevan mahdollisia turvallisuusvaikutuksia (riski siitä, ettei tasoristeyksen puomia suljeta ajoissa), muut artiklan 2 kohtaan sisältyvät perusteet, kuten:
- alhainen monimutkaisuusaste
- alhainen innovatiivisuusaste, ja
- 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 riittävä tehtävällä, jossa vanha tekninen järjestelmä korvataan toimintamenettelystä (henkilöstö ristiintarkastaa toisensa), ylläpidetään sama turvallisuustaso. On selvitettävä, edellyttäikö tämä yhteisen turvallisuusmenetelmän täysimääräistä soveltamista, johon kuuluu muun muassa varojen kirjaaminen ja arvointielimen toteuttama riippumaton arviointi. Tässä tapauksessa on kuitenkin kyseenalaista, olisiko tästä mitään lisää, 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 turvallisuustoimenpiteitä, joilla varmistetaan junien turvallinen siirtyminen yhdestä infrastruktuurista toiseen
- (b) Infrastruktuurin haltija – Rautatieyritys: käytössä saattaa olla infrastruktuuriperusteisia erityisiä toimintasääntöjä, joita junan kuljetus on noudatettava
- (c) Infrastruktuurin haltija – Valmistaja: valmistajien osajärjestelmillä saattaa olla käyttötarjoituksia, joita infrastruktuurin haltija on noudatettava
- (d) Infrastruktuurin haltija – Palveluntarjoaja: käytössä saattaa olla erityisiä infrastruktuurin kunnossapitotarjoituksia, joita kunnossapitotoimia tekevien alihankkijoiden on noudatettava
- (e) Rautatieyritys – Valmistaja: valmistajien osajärjestelmillä saattaa olla käyttötarjoituksia, joita rautatieyrityksen on noudatettava
(f) Rautatieyritys – Palveluntarjoaja: käytössä saattaa olla erityisiä infrastruktuurin kunnossapito-ajoituksia, joita kunnossapidon alihankijan on noudatettava

(g) Rautatieyritys – Kalustoysikköjen hallitajat: käytössä saattaa olla kalustoysikkökohtaisia käyttöajoituksia, joita kyseisiä kalustoysikköjä 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 työteetään 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 hallitajan tai rautatieyrityksen tai valmistajan alihankintana tilaamat toiminnot, kuten kunnossapidon, lipunmyynnin ja suunnittelupalvelut.

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

(a) Johtajaminen: hakijan (rautatieyritys);

(b) Panokset:

1. vastaaviin hankkeisiin perustuvat vaalaluettelo(t)
2. kaikkien rajanpinnan, tuotosten 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
2. junan valmistajan turvallisuusjohtaja
3. junan hakijan suunnittelijohtaja
4. junan valmistajan suunnittelijohtaja
5. junan hakijan kunnossapitojen kilostö (osin P/T-analyysista riippuen)

(e) Tuotokset:

1. yhteisesti hyväksytty kertomus tunnistetuista vaaroista
2. vaaroja koskeva asiakirjaan liittyvät turvallisuustoimenpiteet ja vastuiden selvä
   kuvaus.

C.4. Esimerkkkejä 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 pienentämäiseksi edelleen) ole järkeväät toteuttaa lisäturvallisuustoimenpiteitä". Mikäli vaarojen aiheuttama riskitaso määrätään yleisesti hyväksyttäväksi vaaran tunnistamisvaiheessa, näitä vaaroja ei voida arvioidua syvällisemmin riskinarviointiprosessissa. Edellä lainattu yleisesti hyväksyttäviä riskejä koskeva määritelmä
on jossain määrin tulkinnanvarainen. Tämän vuoksi asetuksessa todetaan, että asiantuntijoiden tehtävässä on luokitella vaarat, joiden riskit ovat yleisesti hyväksyttyviä.


C.4.2. **Kvantitatiivisten perusteiden johtaminen**

C.4.2.1. Yleisesti hyväksyttävät riskit voidaan määrittellä siten, että ne kattavat riskit, jotka ovat paljon pienempiä kuin tietyn vaaraluokan hyväksyttävät riskit. Tilastotietojen avulla voi olla mahdollista laskea, mikä on rautatiejärjestelmiin 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 kunink 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 yltä 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 päätättä, onko riski yleisesti hyväksyttävällä riskitasolla. Nämä tapahtuut 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 riskiejä, ei yltä järjestelmätason kokonaisriskille määritettyä suhdetta (esim. y %): katso 2.2.3 kohta ja 2.2.3 kohtaa koskeva G 2 kohta.
C.5. Riskinarviointiesimerkki: merkittävä organisatorinen muutos

C.5.1. **Huomautus:** Tämä riskinarvioinnin esimerkki ei perustu yhteiseen turvallisuusmenetelmän soveltamiseen, sillä se laadittiin ennen YTM-asetusta. Tässä esimerkissä on tarkoitus:
(a) yksilöidä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä
(b) varmistaa jäljittetvyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä:
(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.


C.5.3. Infrastruktuurin haltijan organisaatioyksikön, joka suoritti muutokseen saakka kunnossapidotoimia (muita kuin merkinantoa ja telemaatattisia 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 kunnossapidotoimia, kuten raitieiden täyttö, raidesepellyksen puhdistus ja kasvillisuuden valvonta.
(b) Näitä tehtäviä pidettiin riittävänä turvallisuuden ja toiminnan täsmällisyden kannalta. Ne olivat noudatettavina, jotta löydettäisiin oikeat toimenpiteet sen varmistamiseksi, ettei tilanne heikkene, kun monet turvallisuusasioista vastaavat henkilöt lähevät infrastruktuurin haltijan organisaatiosta.
(c) Organisaation muutoksen aikana ja sen jälkeen turvallisuuden ja täsmällisyden 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 organisatsiossa suunniteltujen muutosten kuvaus
(3) "irtautuvan osaston" ja muiden lähiorganisaatioiden tai fyysisen ympäristön rajapinnat voitiin kuvata ainoastaan lyhyesti. Rajojen ei voitu esittää 100-prosenttisen selvästi;
(b) vaarojen tunnistaminen [2.2 kohta]:
(1) asiantuntijaryhmän aivorihi:
   (i) tunnistetaan kaikki vaarat, jotka voivat vaikuttaa olennaisesti suunnitellusta organisaatiomuutoksesta aiheutuvaan riskiin
(ii) yksilöidään mahdolliset toimenpiteet riskin hallitsemiseksi;

(2) vaaralan 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]:
Muutos edeltäneen järjestelmän katsottiin olevan hyväksyttävällä turvallisuustasolla. Sitä käytettiin näin ollen "ohjeistona", jonka perusteella organisaatiomuutokselle johdettiin hyväksyttävää riskitasoa koskeva peruste (RAC);

(d) ekspilisiittinen riskin estimointi [2.5 kohta]:
Kaikille vaaroille, joiden riskit lisääntyvät organisaatiomuutoksen vuoksi, yksilöidään riskin vähentämistoimenpiteet. Jäänmöriskiä verrataan ohjeiston RAC:hen, ja todetaan, onko määrätevä 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 muuttaivat koko ajan. Päätetyt toimen tehokkuutta valvottiin säännöllisesti sen selvittämiseksi, olivatko olosuhteet muuttuneet ja oliko riskinarviointia tarpeen ajantasaisista
(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 päätelemistä oli se, että riskinarviointia ja vaaroja koskevaa asiakirjaa on päivitetävä jatkuvasti, koska uusia päättöksiä tehtiin ja toimenpiteitä toteutettiin organisaatiomuutoksen aikana. Riskinarviointi katsoi esimerkiksi myös alihankkijoiden ja yrittäjien rajapintaan liittyvän riskin.

Vaaroja koskevassa asiakirjassa käytetty rakenne ja kentät sekä otteita joistakin kirjaustuksista esitetään lisäksi C 16.2. kohdassa;

(g) riippumaton arviointi [6 artikla]:
Lisäksi kolmas osapuoli toteutti riippumattoman arvioinnin, jossa
(1) tarkistettiin, että riskien hallinta ja riskinarviointi on tehdyt 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 rautatiealan käytössä olevia menetelmiä, joita sovelletaan jo organisaatiomuutosten riskien arvioinnissa. Esimerkin riskinarviointi täytäntöön kaikki YTM-asetuksessa säädetty edellytystä. Siinä sovelletaan kahta kolmesta hyväksyttävää riskitasoa koskevasta periaatteesta, jotka perustuvat YTM-asetuksen yhtenäistetyyn lähestymistapaan:

(a) "ohjeiston" avulla määritettään hyväksyttävää riskitasoa koskeva peruste, jota tarvitaan organisaatiomuutoksesta aiheutuvan riskin hyväksyttävyyden arvioimiseksi;
(b) "ekspilisiittinen riskin estimointi ja evaluointi":
(1) arvioidaan muutoksen poikkeamat ohjeistosta
(2) yksilöidään toimenpiteet, joilla vähennetään muutoksen lisäämiä riskejä
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 lisäävaa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttamaan lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista riskinarviointiesimerkki ei perustu yhteisen turvallisuusmenetelmän

C.6.2. Esimerkki koskee operatiivista muutosta, jonka yhteydessä rautatieyritys halusi ottaa käyttöön uusia reittejä ja mahdollisesti lisätä kuljettajien työskentelyaikaa (mukaan lukien työkykerto 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 reitteillä ja mahdollisesti tavanomaisen työaikansa ulkopuolella, opasteiden sivuuttamisen mahdollisuus vaaratilanteissa taikka ylinopeuden tai tilapäisten nopeusrajoitteiden huomiota jättäminen mahdollisuus olla olemassa.
   - Kun tätä alustavaa riskinarviointia verrataan YTM-asetuksen 4 artiklan 2 kohtaan sisältyyvien 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 seurauks: edellä mainitut kuljettajan virheet voivat johtaa tuhoisiin seurauksiin
      (3) uutus: rautatieyritys saattaa ottaa käyttöön kuljettajille uusia työskentelytapoja
      (4) muutoksen monitutkaisuus: työntentiin muuttaminen saattaa olla monitutkaista, koska se voi edellyttää nykyisten työoloisuhteiden täysimäärittävää arviointia ja muuttamista.
   (b) järjestelmämäärittely [2.1.2 kappale]:
   - Järjestelmämäärittelyssä kuvattiin alun perin:
      (1) aiemmat työolot: työajat, työvuorot jne.
      (2) työaikojen muutokset
      (3) rajapinta koskevat seikat (esim. rajapinta infrastruktuurin haltijan kanssa)
   - Toistojen aikana järjestelmämääritellyä muutettii lisäämällä siihen riskinarviointiprosessista saadut turvallisuusvaatimukset. Keskeiset henkilöstön...
edustajat osallistuivat tähän vaarojen tunnistamista ja järjestelmämäärittelyn ajantasaitaistamista koskevaan toistuvaa prosessiin.

(c) vaarojen tunnistaminen [2.2 kohta]:

Uusien reittien ja työvuorojen vaarat ja mahdolliset turvallisuustoimenpiteet yksilöitiin asiantuntijoiden aivorihessä, johon osallistui myös kuljettajien edustajia. Kuljettajien tehtäviä muuttuessa olosuhteissa tarkasteltiin sen arvioimiseksi, vaikuttavatko ne kuljettajiin, heidän työmääräänsä, maantielteluunen ulottuvuuteen ja työvuorojärjestelmän mukaiseen työaikaan. Rautatieyritys kuului myös työntekijäliittoja selvittääkseen, saataisiinko niiltä lisätietoja, ja tarkasteli uudelleen väsymykseen ja sairauksiin liittyviä riskejä, joita tuntemattomilla reitteillä tehdystä aiempaa pidemmistä matkoista johtuvan ylityön lisääntymisen saattaa aiheuttaa.

Kulleen vaaralle osoitettiin riskin ja seurauksien vakavuus on saaduksi korvaamaan, ja ehdotetun muutoksen vaikutusta arvioitiin suhteessa näihin riskeihin (lisääntynyt, muuttumaton tai alentunut).

(d) menettelyohjeiden käyttö [2.3 kohta]:


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

Tarkistetut menettelyohjeet otettiin käyttöön rautatieyhtyksen turvallisuusjohtamisjärjestelmässä. Niitä valvottiin, ja tarkistusmenetely 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 rautatieyhtyksen vaarojen hallintaprosessi voi olla osa riskien kirjaamiseksi ja hallitsemiseksi toteuttavalla turvallisuusjohtamisjärjestelmällä. Tunnistetut vaarat ja turvallisuusvaatimukset (eli viittaukset tarkistettuihin toimintamenettelyihin) merkittiin vaaroja koskevaan asiakirjaan, jonka avulla riskejä hallitettiin.Tarkan tarkistettuja menettelyjä valvottiin ja muutettiin tarvittaessa sen varmistamiseksi, että tunnistettuja vaaroja valvotaan asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(g) riippumaton arviointi [6 artikla]:

Rautatieyhtyksen pätevää, arviointiprosessin ulkopuolinen työntekijä arvioi riskinarvioinnin ja riskinhallinnon prosessin. Hän arvioi sekä menettelyn että sen tulokset eli yksilöidytt turvallisuusvaatimukset. Rautatieyhtyys perusti uuden järjestelmän täytäntöönpanoa koskevan päätöksensä tämän asiayhteenpitäjän laatimaan riippumattomaan arvioon.

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 jälitettävyyys käytössä olevan menetelman ja YTM-asetukseen perustuvan menetelman välillä;

(c) perustella, mitä lisäävää YTM-asetuksen (mahdollisesti) edellyttämät lisävaatimukset tuovat.


![Kaavio 16: Radanvarren silmukan korvaaminen radioviestimeen perustuvalla osajärjestelmällä](image-url)
C.7.5. YTM-prosessiin verrattuna tässä yhteydessä käytin läpi seuraavat vaiheet (katso myös kaavio 1):

(a) muutoksen merkittävyyden arviointi [4 artikla]:

Muutoksen merkittävyyttä arvioitiin 4 artiklan 2 kohdana sisältävien 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 suunnittelemuun 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 riskinarviointiin ja vaarojen tunnistamisen (katso 2.1.1 kappale) prosessia ja hyödynnetään asiantuntijaryhmän aivoriää, jotta voidaan:

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

Kun silmukka ja siten radioviestin antavat merkin, vaarana on, että lähestyvälle junalle annetaan liikkumislupaa, joka ei ole turvallinen siksi, että edellä kulkenut junaa 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) viivästynyttä välitys tai talletetuista tietopakettia välitys ilmavälissä

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

(f) menettelyohjeiden soveltaminen [2.3 kohta]:

(1) Standardin EN 50159-2 (Rautatiesovellukset - Osa 2: Avoimien viestintä ja järjestelmiä turvallisuuteen liittyvää viestintä) sisältävät turvallisuusvaatimukset, joiden avulla voidaan valvoa, että seuraavankaltaiset uudet vaarat ovat hyväksyttävällä turvallisuustasolla:

(i) tiedonsalauka ja suojelu
(ii) viestien jakotoskus ja aikaleimaus
(g) järjestelmän turvallisuusvaatimusten mukaisuuden osoittaminen [3 kohta]:

(1) turvallisuusvaatimusten täyttöönpanon seuranta "radioviestin+GSM"-osajärjestelmän kehittämisprosessissa

(2) sen varmentaminen, että suunniteltu ja asennettu järjestelmä täyttää turvallisuusvaatimukset

(h) vaarojen hallinta [4.1 kohta]:

Riskinarvioinnissa ja hyväksytvää riskitasoa koskevan kolmen periaatteessa tunnistetut vaarat, turvallisuusvaatimusten täytäntöönpano on annettu ohjeessa BVH turvallisuustaso. Tämä esimerkki riskinarviointiä varmentaa käytännössä tässä esimerkissä:

(i) riippumaton arviointi [6 artikla]:

Lisäksi kolmas osapuoli toteuttaa riippumattoman arvioinnin, jolla

(1) varmistetaan, että riskinhallinta ja riskinarviointi tehdään asianmukaisesti

(2) varmistetaan, että tekninen arviointi on asianmukainen ja että muutosta edeltävän turvallisuustaso säilyy ennallaan.

C.7.6. Tämä esimerkki osoittaa, miten yhteisen turvallisuusmenetelmän edellyttämää kolmea hyväksytvää riskitasoa koskevaa periaatetta voidaan soveltaa täydentävästi määrittelyssä arvioidaan olevan järjestelmän turvallisuusvaatimukset. Tämän esimerkin riskinarviointi täyttää kiinni YTM-asetuksen mukaiset vaatimukset. Joista on esitetty yhteenveto kaaviossa 1, mukaan lukien vaarojen koheeseen asiakirjan hallintaan 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) yksilöitä vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä

(b) varmistaa jäljitettävyys käytössä olevan menetelman ja YTM-asetukseen perustuvan menetelman välillä;

(c) perustella, mitä lisäarvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.


C.8.2. Tässä esimerkissä on tarkoitus verrata YTM-processiä ja ohjetta BVH 585.30, jota Ruotsin ratainfrastruktuurin hallittu 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:
(a) ohje BVH 585.30 sisältää seuraavat samat kohdat:

1. järjestelmäkuvaus [2.1.2 kohta]:
   Ohjeessa edellytetään yksityiskohtaisa järjestelmäkuvausta, joka sisältää
   (i) tunnelin kuvauksen
   (ii) raitteen 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 laitaan "onnottomusluettelo", joka sisältää tunnistetut
   mahdolliset onnettomuustyyppit, joilla arvioidaan olevan merkittävä vaikutus tunnelin
   riskitasoon ja joita on tarkasteltava myöhemmässä arvioinnissa. Esimerkkejä
   onnettomuksista:
   (i) "matkustajajunan suistuminen raiteella"
   (ii) "tavarajunan suistuminen raiteella"
   (iii) "onnottomuus, 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. Ohjeessa
   edellytetään, että riskianalyysi tehdään kaikissa tapauksissa

4. ekspansioninen riskien estimointi ja evaluointi [2.5 kohta]:
   (i) ohjeessa suositetaan yleisesti käymään kunkin onnettomuuden osalta läpi
       koko tapahtumapaupu (Event Tree), joka perustuu kvantitatiiviseen
       riskiarviointiin. Koska riskianalyysin tarkoituksena on kuitenkin arvioida
       tunnelin kokonaisturvallisuustasoa eikä niinkään turvallisuuden yksittäisiä
       näkökohtia yksityiskohtaisemmalla tasolla, kaikkien skenaarioiden seuraukset
       kootaan yhteen, jotta voidaan selittää tunnelin kokonaisriskitaso;
   (ii) sen selvitännäkässä, onko tunnelin kokonaisriskitaso hyväksyttävällä
       riskitasolla, käytetään seuraavia erityistä hyväksyttävää riskitasoa koskevaa
       perustetta: "rataosielikeen tunnelkilometrillä on yhtä turvallista kuin
       rataosielikseen ulkoilmaiskiskokilometreillä tasoristeystä poisluikien". Tämä
       peruste muunnetaan F-N-käyräksi, jonka pohjana käytetään aiemmin
       Ruotsissa tapahtuneiden rautatieonnettomuuksien tietoja, ja se
       ekstrapoloidaan kattamaan myös ne seuraukset, jotka ei ole tilastointi;
   (iii) tunnelin kokonaisriskitasoa koskevan perusteen lisäksi esitetään myös muita
       vaatimuksia, jotka on täytettävä ja jotka koskevat erityisesti tunnelien
       evakuointia ja pelastuspalvelujen saatavuutta:
       (a) varmistetaan, että palavasta junasta on mahdollista pelastautua
           omatoimisesti "uskokavassa pahimmassa tapauksessa" (tätä koskevat
           arviointiperusteet on niin ikään esitettävä); 
       (b) tunnelli on suunniteltava siten, että pelastustoimet voidaan toteuttaa
           tietystä skenaarioissa;

5. riskinarvoinnin tulos [2.1.6 kohta]:
   Riskinarvoinnin tuloksena saadaan:
   (i) luettelo turvallisuustoimenpiteistä sellaisen vähimmäisstandardin mukaisesti,
       joka perustuu yhteentoimivuuden tekniseen eritelmään (YTE)
"Rautatietunneleiden turvallisuus" ja tunnelin suunnittelussa sovellettaviin kansallisiin sääntöihin, ja
(ii) kaikki riskinarvioinnissa tarpeellisiksi todetut lisäturvallisuustoimenpiteet, ja
niiden tarkoitus. Riskinarvioinnissa todetaan, että toimenpiteistä on päätettävä
seuravassa tärkeysjärjestyksessä:
- onnettomuksien 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 hyväksyttävyyys arvioidaan
ilman, että hyväksyttävää kokonaisriskitasoa koskeva perustetta jaetaan
erityyppisten onnettomuuksien tai niiden taustalla olevien vaarojen mukaan.

Kaikki turvallisuustoimenpiteet kuitenkin luetellaan. Tämä koskee sekä
"vähimmäisstandardiin" perustuvia että riskinarvioinnissa välittömätkösi todettuja
toimenpiteitä: katso edellä a kohdan 5 kohdan ii luettelokohdan
Turvallisuustoimenpiteiden luetelossa on mainittava, koskevatko toimenpiteet
tunnelin infrastruktuuria, raitteita, toimintoja tai liikkuvaa kalustoa, ja mitä
tavoitteita toimenpiteillä on a kohdan 5 kohdan ii luetelomaksokohdan

(7) riippumaton arviointi [6 artikla]:
Riippumaton kolmannen osapuolen tekemä arviointi on pakollinen, jotta voidaan:
(i) varmistaa, että ohjeessa BVH 585.30 suositeltu riskiarviointiprosessi on
suoritettu asianmukaisesti
(ii) hyväksä riskianalyysi
(iii) varmistaa hankkeen tulevan turvallisuusjohtamisjärjestelmän toteuttamistavan
selkeä kuvaus;
Riippumaton arvioija ja hankkeen turvallisusoikeistajat allekirjoittavat
hallitta ja kuka vastaa mistäkin toimenpiteestä.

(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

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
C.8.5. YTM:n säännökset ovat yleisluonteisempia kuin ohje BVH 585.30 sikäli kuin niiden perusteella voidaan soveltaa kolmea erilaista hyväksyttävää riskitasoa koskevia osia, yksilöidä vastaavat riskien arviointi- ja suunnitelmatoimien vaatimustenmukaisuutta ja yhteisen metodikompleksin käyttöä. 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 jäljitettävyyttä 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 turvallisuusmenetelmän käytännön. Varsinaista esimerkkiä ei kuitenkaan voida siirtää käytäntöön tai käyttää ohjeistona muun merkittävän riskin estimointia koskevan kolmannen periaatteen mukaisesti.

C.9.2. Tämä esimerkki koskee monimutkaista kuljetta jostakin metrojärjestelmässä Kokonaisuudessaan, sen teknisiä osajärjestelmiä (kuten automaattista raitioliikennontäyttämistä ja liikkuvaa kalustoa), järjestelmän käyttöä ja kunnossapitoa. Järjestelmä ja sen osajärjestelmät arvioidaan riskinarviointiin perustuvan lähestymistavan avulla. Hanke kattoi myös järjestelmän käyttämistä vastaavan yleisyyden turvallisuusyhteyden ja järjestelmän sertifiointiin. Tämä liittyy rautatieyhteysten ja infrastruktuurin hallinnan valmiuksiin ylläpitää koko järjestelmää turvallisesti sen elinkaaren ajan.

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

(a) järjestelmäkuvaus [2.1.2 kohta]:

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

(b) vaarojen tunnistaminen [2.2 kohta]:

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

(d) ohjeissa ei varsinaisesti vaadita osoittamaan vaatimustenmukaisuutta ja varmentamaan turvallisuustoimenpiteiden asianmukaisuus. Ohjeissa todetaan kuitenkin, että hankeen turvallisuustoimenpiteiden vaatimustenmukaisuus on tarkoitus asettaa periaatteista ja ne pannaan asianmukaisesti täytäntöön.
(esim. automaattinen junansuoajärjestelmä ja liikkuvaa kalusto), joilla on merkitystä turvallisuuteen liittyville toiminnolle ja jotka vaikuttavat keskeisesti matkustajien ja henkilöstön turvallisuuden varmistamiseen

(3) toimijoiden (sopimuspuolet, teknisten osajärjestelmien toimittajat ja rakennusurakoiden tekijät) välisen 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 kuljettajatontta ajoa koskeva BOSTrab-asetus (Saksan asetus, jota sovelletaan kaupunkien rautateieverkoihin)

(2) VDV-asiakirjat (saksalaiset menettelyohjeet), jotka sisältävät sellaiselle laitteistolle asetettavat vaatimukset, jolla varmistetaan asemien matkustajaturvallisuus kuljettajatomassa 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 käytettiin koko rautatiejärjestelmän turvallisuushallinnassa ja riskinarvioinnissa

(ii) standardia EN 50 129 käytettiin koko merkinnantojärjestelmässä

(iii) standardia EN 50 128 käytettiin teknisten osajärjestelmien ohjelmistojen kehittämisessä (muutakin 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 uudenkaisten laitteiden turvallisuustason. Näitä käytössä olevia järjestelmiä käyttettiin vastaavin ohjeistoja, joista johdettiin hyväksyttävää riskitasoa koskeva peruste sen osalta, mikä on onnettomuuksien hyväksyttävä esiintymistohys 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 toiminta liittyvät ihmishallinniset tekijät)

(3) riskejä vähentävien toimenpiteiden yksilöinti

(4) sen arvioiminen, onko koko järjestelmän riskitaso hyväksyttävä

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

(1) järjestelmän monimitkaisuuteen 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
osajärjestelmän tasolla. Turvallisuusvaatimusten täyttyminen on varmistettu järjestelmätasolla integroimalla eri osajärjestelmät, välleen 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 toimitti johtajalle niiden merkinnän.

(h) riskinhallintaa ja riskinarviointia koskeva näyttö [5 kohta]:
Riskinarvioinnin tulos dokumentointiin virallisesti, ja niiden tukena oli CENELEC-standardien vaatimusten mukainen turvallisuusarvio:

1. turvallisuusarvio koko järjestelmästä
2. turvallisuusarvio kustakin osajärjestelmästä (mukaan lukien merkinannon
   osajärjestelmät ja rakennusurakat)
3. turvallisuusarvio rakennusurakoista (asemat, tunneilit, maasilat, penkereet)
4. turvallisuusarvio rakentamisesta
5. turvallisuusarvio kalustoystiköistä
6. turvallisuusarvio toimijasta (rautatieyksikön ja infrastrukturan valtajain
   turvallisuusjohtamisjärjestelmän sertifioinnin tukemana, eli osoitus hakijan
   valmiuksista käyttää ja ylläpitää järjestelmää turvallisesti
   (6) riippumaton arviointi [6 artikla]:
   Riippumaton turvallisuusarvio, joka toimi yhteistyössä teknisen
   valontaviranomaisen (eli Tanskiaan liikenneministeriön) edustajien kanssa, valvoi koko
   prosessia ja teki siitä arviointiin. Riippumattoman turvallisuusarvioin tehtävät on
   vahvistettu asiaa koskevassa menettelyohjeessa. Tehtäviin kuului
   (1) varmistaa, että riskinhallinta ja riskinarviointi toteutetaan asianmukaisesti;
   (2) varmistaa, että järjestelmä soveltuu tarkoitukseen ja että sen käyttö ja
   kunnossapito on turvallista koko järjestelmä elinkaaren aikana;
   (3) suosittaa hyväksyntää tekniselle valontaviranomaiselle.


C.9.5. Hankkeessa toimittajalta saatu näyttö (eli turvallisuusarvioinnit ja teknisten osajärjestelmien ja
   rakennustöiden yksityiskohtainen tukiaineisto) toimitettiin hakijan turvallisuusjohtajalle.
   Turvallisuuden hallintaorganisaatio ja riippumaton turvallisuuden arvioita tarkastivat todisteet,
   ja riippumattoman turvallisuuden arviointiin päätelmat kirjattiin arviointikertomukseen.
   Hakijan turvallisuusjohto tarkisti riippumattoman turvallisuusarviointikertomuksen ja välitti sen
   hakijalle, joka puolestaan toimiti kaikki asiakirjat tekniselle valontaviranomaiselle (eli
   Tanskiaan liikenneministeriöllä) lopullista hyväksyntää varten.

C.9.6. Tästä esimerkistä käy ilmi, että rautatiehallintajlossa sovelletaan jo käytännössä yhteisen
   turvallisuusmenetelmän edellyttämää periaatteita. Esimerkin riskinarviointi täyttää kaikki YTM-
   asetuksesta johtuvat velvollisuudet. Siinä sovelletaan erityisesti kaikkia YTM:n yhdenäisen
   lähemystenmista uutakin kolmea hyväksyntää riskitasoa koskevaa periaatetta.
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 jäljitettävyyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;
(c) perustella, mitä lisäävää YTM-asetuksen (mahdollisesti) edellyttämät lisäävaiheet tuovat.


C.10.2. Yhteisen välisen kansainvälisten rautatiekuljetusten järjestön (OTIF) ohjeiden keskeinen sisältö on sopuosinnassa YTM:n tavoitteessa, mutta ohje on YTM:ää suppeampi. Tavoitteena OTIF:n "ohjeessa on saavutettava entistä yhdenmukaisempia lähemytystapaa vaarallisten aineiden kuljetusten riskinarviointiin kansainvälistä rautatiekuljetuksia koskevan yleissopimuksen (COTIF) jäsenvaltoissa, ja tehdä siten yksittäisistä riskinarvioineista keskenään vertailukelpoisia". Sillä tuetaan näin ollen sitä, että COTIF:n jäsenvaltiot hyväksyvät vastavuoroisesti vaarallisten aineiden rautatiekuljetuksia koskevat riskinarvioinnit.

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

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

(1) kyse on yleisestä riskinarvioinnin lähestymistavasta, joka kuitenkin perustuu ainoastaan ekspliittiseen riskin estimointiin (eli kolmanneen hyväksyttävään riskitasoa koskevaan YTM:n periaatteeseen);

(2) OTIF:n riskinarviointi 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 perusteluissa;

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

(1) Soveltamisala on eri. YTM:ää on sovellettaa ainoastaan rautatiejärjestelmän merkittäviin muutoksiin, kun taas OTIF:n ohjetta on sovellettaa vaarallisten aineiden rautatiekuljetukuksiin siitä riippumatta, onko kyse rautatiejärjestelmän merkittävää muutoksesta vai ei.

(2) OTIF:n ohje ei tarjoa riskinhallinnan yhteydessä mahdollisuutta valita kolmesta hyväksyttävää riskitasoa koskevasta periaatteesta. Se sallii ainoastaan kolmannen periaatteen ekspliittisen riskin estimoinnin soveltamisen. Riskinarvioinnin on lisäksi perustuttava yksinomaan kvantitatiiviseen eikä kvalitatiiviseen arvioon. Kvalitatiivista riskinarvioanalyyseä voidaan soveltaa ainoastaan tietyissä tapauksissa, joissa vertaillaan riskiä pienentäviä (turvallisuus)toimenpidenvaihtoehdoja.
(3) OTIF:n ohje edellyttää siedettävän tason (ALARP) periaatteen soveltamista, jonka avulla voidaan määrätä, voidaanko ylimääräisillä turvallisuustoimenpiteillä kohtuullisin kuluin vähentää arvioitua riskiä entisestään.

(4) OTIF:n ohje ei sisällä "yleisesti hyväksyttävään riskitasoon liittyvien vaarojen" käsitettä, jonka perusteella riskinarvioinnissa voitaisi keskityä vaikutuseltaan keskeisimmän vaaroihin. Ohjeessa suositetaan kuitenkin vähentämään mahdollisten onnettomuukskaanairoiden 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) riskii vaikuttavien (turvallisuus)toimenpiteiden valinta- eikä täytäntöönpanoprosessia
(ii) riskinhyväksytäpprosessia
(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 suorittama riippumatonta arviointia, jolla varmistettaisiin yhteisen lähestymistavan asianmukaisen soveltaminen.

C.10.4. OTIF:n ohjeen ja YTM:n vertailusta käy ilmi niiden yhtenevyyssä 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 vallitsevan käsittäntöihin: 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, jolla voidaan käsitellä mahdollisista välineistä turvallisuusbemerkilöön vähentää arvioitua riskiä entisestään.

C.10.5. OTIF:n ohjeen soveltaminen YTM:n asetuksen yhteydessä (siinä tapauksessa, että vaarallisten aineiden kuljetus merkitsee intrastukurin haltijan tai rautatieverkosta kansan merkittävää muutosta) ei kuitenkaan aiheuta ongelmia, koska ohje on sopusoinnussa erityisen riskinarvioinnin kolmannen periaatteen soveltamisen kanssa.
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-asetuksen perustuvan menetelmän välillä;

(c) perustella, mitä lisäävää YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan osoituksena. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin YTM:n prosessiin verrattuna riskinarvioinnin mukaista riskan analysiä.

Riskinarviointi tehtiin uuden liikkuvan kaluston käyttöönottoon liittyvien riskien evaluoinnissa. Riskinarviointiesimerkki

(a) järjestelmäkuvaus [2.1.2 kohta]:

Kaikille suunnittelun vaiheille oli asetettu vaatimuksia, 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 vaatimuksia, jotka koskivat vaunun käyttöä ja kunnossapitoa;

3) valmistusvaihe: valmistajan tekninen dokumentaatio, mukaan lukien piirustukset, standardit, laskelmat, analyysit jne. Uusien tai innovatiivisten rakenteiden tai uusien käyttöalojen syvällisen riskinarviointi;

4) varmennusvaihe:

(i) valmistaja varmensi vaunun teknisen suorituskyvyn (testikertomukset, laskelmat, toiminnallisten vaatimusten ja standardien noudattamista koskevat varmennukset);
(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 ylös pään suuntautuvaa lähestymistapaa, jossa eri valmistajat arvioivat risksarjoja, jotka johtuivat osajärjestelmien komponenttien vioista. Jako osajärjestelmiin käytettiin alhaalta ylöspäin suuntautuvaa lähestymistapaa, jossa eri valmistajat arvioivat
Tätä kohtaa sovellettiin järjestelmä rakentamisessa, käytössä ja jatkuvasti. Jäljellä olevat vaarat kirjattiin vaaroja koskevaan asiakirjaan yhdessä
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

(c) hyväksyttävää riskitasoa koskevien periaatteiden soveltaminen [2.1.4 kohta]:
Koko järjestelmälle tehtiin eksplisiittinen riskin estimointi. Yksittäisiä vaaroja olisi kuitenkin voitu arvioida myös menetellyöiden 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 turvallisempia kuin aiempi. Standardin EN 50126 riskimatriisien käytettiin tunnistettujen vaarojen karttoitamiseen. Lisäksi sovellettiin erilaisia

(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
loppullinen turvallisuuskertomus, jossa varmennettiin, että turvallisuusvaatimukset olit 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 hyväksytävällä
riskitasolla oleviin riskiin, ei kuitenkaan sisällytetyt 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. Hyväksytävää 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

(b) varmistaa jäljitettävyyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan

(c) perustella, mitä lisäarvoa YTM-asetukseen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on
aattaa 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 päättyi, että kuljettajan oli
vastattava tunten yksin ohjauksesta (ainoastaan kuljettajan ohjaama, AKO) reitillä, jolla oli
aiakaisemmin kalustoyksikössä avustaja, joka autoi kuljettajaa tunten lähettämisessä.

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

(a) muutoksen merkityksellisyys [4 artikla]:

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

Jos tätä alustavaa riskinarviointia verrataan YTM-asetuksen 4 artiklan mukaisiin
perusteisiin, muutos on mahdollista luokitella merkittäväksi myös seuraavien
perusteiden nojalla:
(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) uutus: kuljettajan yksin suorittama toimenpide saattaa edellyttää uudenlaisia junan ohjaustapoja, joiden riskit on arvioitava;

(b) järjestelmämäärityt [2.1.2 kappale]:
Järjestelmämäärityksessä kuvattiin:
(1) käytössä ollut järjestelmä, minkä yhteydessä selitettiin tarkasti, mitä tehtäviä kuljettaja suoritti ja missä tehtävissä kalustoyksikössä ollut avustaja avusti kuljettajaa;
(2) kuljettajan vastuualueiden muutos junassa avustaneen henkilöstön poiston vuoksi;
(3) toiminnon muutosten hallitsemista koskevat tekniset vaatimukset;
(4) kalustoyksikössä olevan avustavan henkilöstön, kuljettajan ja radan varrella olevan infrastruktuurin haltijan henkilöstön väliset rajapinnat;

Toistojen aikana järjestelmämäärityltä päivitettiin riskinarvioinnin perusteella laadituilla turvallisuusvaatimuksilla. Keskeiset henkilöt (mukaan lukien kuljettajat, henkilöstön edustajat ja infrastruktuurin haltija) osallistuivat tähän toistuvaan Procssiin, jossa vaarat tunnistettiin ja järjestelmämäärityttä 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 infrastruktuurin ja edellyttää muutoksia esimerkiksi asemille (kuten peilien/videovalvontajärjestelmän [CCTV] asentaminen laiturielle);

Kuljettajien suorittavatikki tulevat uudet tehtävät tutkittiin tarkoin, jotta voitiin tunnistaa kaikki mahdolliset vaarat, joita saatattaisi ilmetä sen jälkeen, kun kalustoyksikössä olevasta avustavasta henkilöstöstä luovutus. Vaarojen tunnistamisen yhteydessä selvitettiin erityisesti, mitä keskeisiä toiminnallisia vaaroja voisi ilmetä asemilla, nykyisillä reiteillä, joissa saatati apua kalustoyksikössä olevalta avustavalta henkilöstöltä tai junan varressa olevalta henkilöstöltä, mukaan lukien junien turvallinen lähtö, kuljettajaa liittyvä erityiskykyys, liikkuva kalusto (esimerkiksi oven avaus/sulkeutumisen varmistaminen), huoltovaatimukset jne. Kaikkien tunnistettujen vaarojen osalta määriteltiin riskin ja seurauksien vakavuutasto (korkea, kohtalainen, matala), ja ehdotetun muutoksen väikentäksä arvioitiin suhteessa näihin riskioihin (lisääntynyt, muuttumaton, pienentynyt).

(d) menettelyohjeiden [2.3 kohdassa]:
Sekä menettelyohjeista (eli ainoastaan kuljettajan ohjaamaa toimintoa koskevia standardeja) että vastaavia ohjeistoja käytettiin turvallisuusvaatimusten määrittämiseksi tunnistetulle 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 lähtössä liikkeelle;
(3) tarkistuslista, jonka avulla varmistetaan, että kuljettajan ohjaamo on asianmukainen, kun otetaan huomioon rautatiejärjestelmän (sekä kalustoysikön 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.

Rautatieteeryksen 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 rautatieteeryksillä vaarojen hallintaprosessi voi riskien kirjaamisen ja hallinnon osalta sisältyä niiden turvallisuusjohtamisjärjestelmään. Tunnistetut vaarat ja niihin liittyvät riskejä koskevat turvallisuustoinenpiteet eli viitataan kalustoysikkossä ja radan varrella olevaan lisälaitteistoon ja toimintamenettelyjen tarkistamiseen, kirjattiin vaaroja koskevaan asiakirjaan.

Tarkistettuja menettelyjä valvottiin ja tarkistettiin tarvittaessa, jotta voitiin varmistaa, että tunnistettuja vaaroja valvotiin asianmukaisesti rautatiejärjestelmän toiminnan aikana.

(g) riippumaton arviointi [6 artikla]:

Arvionprosessista riippumaton rautatieteeryksen pätevän henkilön arvioi riskinarviointeihin ja riskinhallintan prosessit. Hän arvioi sekä menettelyn että sen tulokset eli yksilöidyt turvallisuusvaatimukset.

Rautatieteerytys perusti uuden järjestelmän toteuttamispäätöksensä pätevän henkilön laatimaan riippumattoman arviointikertomukseen.

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

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

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

(a) yksilöidän vastaavuudet käytössä olevien riskinarviointimenetelmien ja yhteisen turvallisuusmenetelmän välillä

(b) varmistaa jäljittävyyys käytössä olevan menetelmän ja YTM-asetukseen perustuvan menetelmän välillä;

(c) perustella, mitä lisärvoa YTM-asetuksen (mahdollisesti) edellyttämät lisävaiheet tuovat.

On korostettava, että tämä esimerkki annetaan ainoastaan tiedoksi. Sen tarkoituksena on auttaa lukijaa ymmärtämään paremmin yhteistä turvallisuusmenetelmää. Varsinaista esimerkkejä ei kuitenkaan voida siirtää käyttöön tai käyttää ohjeistona muun merkittävän
Järjestelmä on määriteltynä siten, että se on riippumaton TM:a uolisten järjestelmien rajapinnat määriteltiin erittäin tarkasti. Tällä tavoin komponenttien arvioidun

C.13.1. Riskianalyysi tehtiin CENELEC-standardien (EN 50126 ja EN 50129) mukaisesti, ja se käsittelee seuraavia vaiheita:

(a) jäähdyttely
(b) laitteiden tunnistaminen
(c) laitevalintain ja kvantifiointi.

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

C.13.3. Riskianalyysi tehtiin CENELEC-standardien (EN 50126 ja EN 50129) mukaisesti, ja se käsittelee seuraavia vaiheita:

(a) jäähdyttely
(b) laitteiden tunnistaminen
(c) laitevalintain ja kvantifiointi.

C.13.4. Järjestelmämäärittelyssä oli määritelty 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 määritettiin erittäin selkeästi ilman, että lukituksen sisäisä toimintoja selvitettiin yksityiskohtaisesti.

C.13.5. Tämän jälkeen vaarat tunnistettiin ainoastaan rajapintojen osalta, jotta pystyttäisiin yleisellä tasolla (eli vältettäisiin riippuvuus joistakin tietyistä rakenteista). Huomioon otettiin ainoastaan teknisistä viioista johtuvat vaarat. Kunink 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 viipamaton. Tällä tavoin komponenttien arvioidun voitettavuuden perusteella voitiin laskea kunink vaaran esiintymis todennäköisyys, jota voitiin pitää uusien sähköisten lukituslaitteiden hyväksyttävänä vaaratasona (varmuusvikatajuus, THR).


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

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

C.13.12. Lisätietoa näistä riskinarvioinnista:
(a) Ziegler, P., Kupfer, L., Wunder, H.: "Erfahrungen mit der Risikoanalyse ESTW (DB AG)", Signal+Draht, 10, 2003, s. 10–15, ja

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

C.14.2. CENELEC-standarden mukainen riskianalyysi tehtii täysin uudelle toimintamenettelylelle, jonka käyttöönotto Saksan tavanomaisilla rautatiejärjestelyillä suunniteltiin (mutta jota ei koskaan otettu käyttöön). Suunnitelma mukaan junien turvallisuustoiminto perustuu ainaa ainoastaan radiopohjaan (reitti ja juna) valvontaan. Koska aiempia menettelyohjeita (hyväksyttyjä

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-perusten

C.14.4. Tämä riskinarviointiesimerkki osoittaa, miten yleinen eksplisiittinen peruste voidaan johtaa (YTM:n asetuksen kolmannen hyväksyttävää riskitasoa koskevan perusteen osalta) uusille järjestelmissä, joille ei ole soveltuu menettelyohjeita eikä ohjeistoja. Tämän jälkeen uudelle järjestelmälle tehty riskianalyysi perustui CENELEC-standardeihin ja vastasi siten hyvin
YTM-prosessia. Esimerkin riskinarvointi täyttää YTM-asetuksen vaatimukset, mutta siinä ei
viitata vaaroja koskevan asiakirjan hallintaan eikä vaadita osoittamaan, että arvioitava
järjestelmä on yksilöityjen turvallisuusvaatimusten mukainen.


C.15. **Esimerkki RAC-TS:n sovellettavuustestistä**

C.15.1. Tässä liitteessä on tarkoitus havainnollistaa kulustoysikössä olevan ETCS-osajärjestelmän

C.15.2. toiminnon osalta, miten ETCS-osajärjestelmän

C.15.3. toiminnon kuvaus

C.15.4. kalustoyksikössä oleva ETCS

C.15.5. jarrutuksen hallintatoiminnolle. Tässä yhteydessä

C.15.6. kalustoyksikössä oleva ETCS

C.15.7. käyttävät junan nopeutta

C.15.8. kuljettajalle ohjaan ja varmistaa, ettei nopeus ylitä sallittua;

C.15.9. samanaikaisesti kalustoyksikössä oleva ETCS-osajärjestelmä valvoo, ettei juna

C.15.10. milloinkaan ylitä sallittua nopeusrajoitusta. Ylinopeustapauksissa järjestelmä jarruttaa

C.15.11. automaattisesti.

C.15.12. Sekä kuljettajalla että kulustoysikössä oleva ETCS-osajärjestelmä käyttävät junan nopeutta

C.15.13. koskevaa arviota, joka julistaa arviota, jonka kalustoysikössä oleva ETCS-osajärjestelmä laskee.


C.15.15. nopeuden arviointiin?"

C.15.16. Kulkuavion 14 soveltaminen, ja vastaukset eri kysymyksiin:

C.15.17. (a) Teknisen järjestelmän tarkasteltava vaara:

C.15.18. "ETCS:lle ohjeistetun turvallisen nopeuden yllä提minen" (katso UNISIG SUBSET 091).

C.15.19. (b) Voidaanko vaaraa hallita menettelyohjeiden tai ohjeiston avulla?

C.15.20. EI. Oletetaan, että ETCS-järjestelmän rakenne on uusi ja innovatiivinen. Tämän vuoksi

C.15.21. menettelyohjeita tai ohjeistoja, joiden avulla vaarat voitaisiin hallita hyväksyttävälle

C.15.22. riskitasolle, ei ole.

C.15.23. (c) Onko todennäköistä, että vaara voi johtaa tuloisaa seuraukseen?

C.15.24. KYLLÄ, koska "ETCS:lle ohjeistetun turvallisen nopeuden yllä提minen" voi johtaa junan

C.15.25. suistumiseen raitailta, joka puolestaan saattaa aiheuttaa "kuolentamataukaisa ja/tai

C.15.26. useita vakavia loukkaantumisia ja/tai merkittäviä ympäristövahinkoja".

C.15.27. (d) Onko tuloisaa seuraus suora tulos teknisen järjestelmän viasta?

C.15.28. KYLLÄ, jos muita turvaesteitä ei ole. Kalustoysikössä olevan ECTS-osajärjestelmän

C.15.29. laskema sama arvio junan nopeudesta annetaan sekä kuljettajalle että kalustoysikössä

C.15.30. olevan ECTS-osajärjestelmän jarrutuksen hallintatoiminnolle. Tämän vuoksi kun

C.15.31. oletetaan, että kuljettaja ohjaa juna (suorituskykyyn liittyvästä syistä) radanvarsitetojen

C.15.32. mukaisella sallitulla enimmäisnopeudella, kuljettaja ja junan ECTS-osajärjestelmä eivät
havaitse, että junaa ajaa ylinopeutta, mikäli junan nopeus on aliarvioitu. Tämä saattaa johtaa junan suistumiseen raitiolla ja siten tuhoisiin seurauihin.

(e) Päätelmät:

(1) kvantitatiivisten vaatimusten osalta: sovelletaan varmuusvikataajuutta $10^{-9}$ h$^{-1}$ kalustooyksikön 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 kuluvaa aika aina otettuna huomioon;

(iii) yhteisvikojen ja yhteisvikoittumistapojen (CCF/CMF) arviointi on tehty;

(iv) riippumaton arviointi on tehty;

(2) prosessivaatimusten osalta: sovelletaan SIL 4 -menetelmää kalustooyksikössä 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

1. ohjelmistojen kehittämiseen standardia EN 50 128;

2. 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.16.1.2. 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 käytetään siihen annettaa aina yksi tieto. Riippumattomuudesta käytetyistä 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) selkeää kuvaus, joka sisältää viittaukset vaaran alkuperään ja hyväksyttävä riskitaso koskevaan periaatteeseen, joka on valittu vaaran hallitsemiseksi. Tämän kentän avulla voidaan ymmärtää vaaraa ja siihen liittyvät turvallisuustoimenpiteet sekä selviittyä, missä turvallisuusarvioinnissa ne on yksilöity.

Koska vaaroja koskevaa asiakirjaa käytetään ja ylläpidetään koko järjestelmän elinkaaren aikana (elä järjestelmän käytön ja kunnossapidon aikana), on hyvä varmistaa jäljittelevyyys kunkin vaaran ja seuraavien seikkojen välillä:

(1) riski;
(2) vaarojen syyt, jos ne ovat jo selville;
(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. ”Selkeää ja riittävää” tarkoittaa, että turvallisuustoimenpiden ja niihin liittyvien vaarojen kuvauksista käy ilmi, mitä riskejä niillä on tarkoitus hallita ilman, että tämä asia on selvitettyä vastaavista turvallisuusarvioinnista.

(b) hyväksyttävää riskitason 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 alakohoa. 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 alakohoa;
   (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 vaarojen koskevan asiakirjan avulla;

Joissain tapauksissa saatetaan toteuttaa muita turvallisuustoimenpiteitä kuin niitä, jotka on kirjattu vaaraa koskevaan luetteloon (esimerkiksi kustannusyystä). Toteutetut turvallisuustoimenpiteet kirjataan vaarajoa koskevaan luetteloon yhdessä näyttöön/perustelujen kanssa; näytöstä ja perusteluista on käytettävän ilmi, miksi turvallisuustoimenpiteet ovat asianmukaisia, ja niillä on osoitettava, että näiden toimenpiteiden ansiosta järjestelmä täyttää turvallisuusvaatimukset.

(d) viittaus asianta koskevaan näyttöön, joka koskee vaaran hallintaa tai turvallisuustoimenpiteen vahvistamista. Tästä kuntästyö löytyy myöhemmin näyttö, joka koskee vaaran hallitsemista ja turvallisuustoimenpiteitä vahvistetettä etukäteen;

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 vaarao koskevan asiakirjan mahdollisesta sisällöstä annetaan ohjeen EN 50126-2 (Ref. 9) liitteessä A.3.
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.

<table>
<thead>
<tr>
<th>Vaaran kuvaus</th>
<th>Turvallisuustoimenpiteet</th>
<th>Tärkeys/ Turvallisuus Täsmällisyys</th>
<th>Täytäntöönpano (18)</th>
<th>Huomautuksia</th>
<th>Vastuu (18)</th>
<th>Alku- perä</th>
<th>Sovellettu hyväksyttävä riskitasoa koskeva periaate</th>
<th>Varmentami- sen vastuu- henkilö</th>
<th>Varmentamis- tapa</th>
<th>Tilanne xx.xx.xx</th>
</tr>
</thead>
</table>

(18) Nämä kaksi saraketta sisältävät tietoa/kenntiä tunnistettujen vaarojen hallinnasta vastaavista toimijoista.
C.16.3. Esimerkki kalustoyksikössä olevasta ohjau- 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 turvallisuusvaahtimia, 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 ohjau- ja hallintaosajärjestelmän vaaroja koskevasta asiakirjasta.**

<table>
<thead>
<tr>
<th>N°</th>
<th>HZD</th>
<th>Origin</th>
<th>Hazard description</th>
<th>Additional information</th>
<th>Actor in charge</th>
<th>Safety Measure</th>
<th>Used Risk Acceptance Principle</th>
<th>Exported</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HAZOP – kertomu</td>
<td>Junan enimmäisnopeus on asetettu liian suureksi (Vmax)</td>
<td>Kalustoyksikön osajärjestelmän väärrä konfigurointi (kunnossapitoenhenkilöstö). Kalustoyksikössä syötetty väärrä tieto (kuljettaja)</td>
<td>Rautatieyritys</td>
<td>• Määritellään hyväksyntämenetelly kalustoyksikössä olevalle Ekspлицiittinen riskin estimointi</td>
<td>Kylä</td>
<td>Hallittu (siirretty rautatieyritystelle)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reference: ERA/GUI/02-2008/SAF  
File Name: ERA-2008-0064-00-01-ENFI.doc  
Version: 1.1  
Page 106 of 112
<table>
<thead>
<tr>
<th>N°</th>
<th>HAZD</th>
<th>Origin</th>
<th>Hazard description</th>
<th>Additional information</th>
<th>Actor in charge</th>
<th>Safety Measure</th>
<th>Used Risk Acceptance Principle</th>
<th>Exported</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>s Rₓ</td>
<td>HAZOP-kertomus Rₓ</td>
<td>Kalustoysikössä olevan osajärjestelmän erityinen konfigurointiprosessi riippuu</td>
<td>Kalustoysikössä olevan osajärjestelmän erityinen konfigurointiprosessi riippuu, junan jarrutusjärjestelmän asetetusta turvamarginaaleista.</td>
<td>Rautatieyritys</td>
<td>Täsmennetään järjestelmänmäärittelyssä asianmukaisesti järjestelmän vaatimukset; Asetetaan junakohtaisesti jarrujärjestelmän riittävät turvamarginaalit.</td>
<td>Kylä</td>
<td>Hallittu (sirretty rautatieyritykselle)</td>
<td>Katso myös liitteessä C olevaa C.16.4.2. kohta</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HAZOP-kertomus Rₓ</td>
<td>Kalustoysikössä olevan osajärjestelmän erityistä konfigurointia ei ole päivitetty junan pyörän läpimittain osalta (kunnossapitohenkilöstö).</td>
<td>Konfigurointitietojen valmistelua ja kalustoysikössä olevaan osajärjestelmään siirtoa koskeva vika valmistajan menetyksessä.</td>
<td>Rautatieyritys</td>
<td>Määritellään menetellyt, jonka mukaisesti kunnossapitohenkilöstö määrittää junan pyörän läpimittain; Määritellään menetellyt junan pyörän läpimittain säännöllisesti päivittämisessä junassa olevaan osajärjestelmään.</td>
<td>Kylä</td>
<td>Hallittu (sirretty rautatieyritykselle)</td>
<td>Katso myös liitteessä C olevaa C.16.4.2. kohta</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>HAZOP-kertomus Rₓ</td>
<td>• Junan eminämiss Nopeus on asetettu liian suureksi (V_max) • Kalustoysikössä olevan osajärjestelmän konfigurointi (eli liikumislupa) on liian suurilla jarrutuskaarissa</td>
<td>•</td>
<td>Määritellään menetellyt, jonka mukaisesti kunnossapitohenkilöstö määrittää junan pyörän läpimittain; Määritellään menetellyt junan pyörän läpimittain säännöllisesti päivittämisessä junassa olevaan osajärjestelmään.</td>
<td>Kylä</td>
<td>Hallittu (sirretty rautatieyritykselle)</td>
<td>Katso myös liitteessä C olevaa C.16.4.2. kohta</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Vaaran nro</th>
<th>Vaaran alkuperä</th>
<th>Vaaran kuvaus</th>
<th>Lisätiedot</th>
<th>Vastaava toimija</th>
<th>Turvallisuustoimenpide</th>
<th>Vastaanottajan huomautukset</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 nro 2</td>
<td>HAZOP-kertomus Rx</td>
<td>Kalustoysikössä olevan osajärjestelmän erityinen konfigurointi (Liikuntasaliopaikka on liian sulava ja jarrutuskaariissa)</td>
<td>Kalustoysikössä olevan osajärjestelmän erityisen konfigurointi on nollattu (Vmax)</td>
<td>Rautatieyhteys</td>
<td>Täsmennettään järjestelmän määräyksellä asiannukuasta järjestelmän vaatimukset; Varmistetaan, että junakohtaisten jarrujärjestelmen turvamarginaalit ovat riittävät;</td>
<td>Katso edellä ensimmäisellä rivillä esitetty huomautus.</td>
</tr>
<tr>
<td>3 nro 3</td>
<td>HAZOP-kertomus Rx</td>
<td>Junan enimmäisnopeus on asetettu liian suureksi (Vmax)</td>
<td>Kalustoysikössä olevan osajärjestelmän erityistä konfigurointia ei ole päivitetty junan pyörän läpimittaan osalta (kunnossapitoenkielöstö).</td>
<td>Rautatieyhteys</td>
<td>Määritellään menettely, jonka mukaisesti kunnossapitoenkielöstö määritätään junan pyörän läpimittaan; Määritellään junassa olevan osajärjestelmänä sovellettava menettely junan pyörän läpimittaan säännölliseksi päivittämisiksi;</td>
<td>Kalustoysikössä olevan ohjaus- ja hallintaosajärjestelmän kunnossapito tapahtuu kunnossapitomenettelyyn MP, mukaisesti. Junan pyörän läpimittä päivitytään määrätyillä aikaväliillä P, -menettelyn mukaisesti. Tietojen syötämisprosessin osalta kuljettajia arvioidaan PCE -menettelyn perusteella.</td>
</tr>
<tr>
<td>4 nro 4</td>
<td>HAZOP-kertomus Rx</td>
<td>Suurella nopeudella (160 km/h) kulkevan Junan saapuminen</td>
<td>Tätä voidaan hallita ainoastaan kuljetajan valppauden avulla. Saapuminen ratsausvuoden Infrastruktuurin hallitja</td>
<td>Infrastruktuurin hallitja</td>
<td>Varmistaa, etteivät, junat, joissa ei ole aktiivista TM:n infrastruktuurin liikennejärjestelyjä säännöllään R15 –sääntöjen mukaisesti.</td>
<td></td>
</tr>
</tbody>
</table>
### Taulukko 8: Esimerkki vaaroja koskevasta asiakirjasta: turvallisuuteen liittyvien tietojen siirtäminen muille toimijoille

<table>
<thead>
<tr>
<th>Vaaran nro</th>
<th>Vaaran alkuperä</th>
<th>Vaaran kuvaus</th>
<th>Lisätiedot</th>
<th>Vastaava toimija</th>
<th>Turvallisuustoimenpide</th>
<th>Vastaanottajan huomautukset</th>
</tr>
</thead>
<tbody>
<tr>
<td>jne.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vaaran kuvaus:**

Muu rataosuudelle ilman, että kalustoajoksiin oleva osajärjestelmä on aktiivinen, ja ilman radanvarren merkinantojärjestelmää

**Vastaa toimija:**

Kalustoajoksiin olevaa ohjaus- ja hallintajärjestelmää

**Turvallisuustoimenpide:**

Kalustoajoksiin olevaa ohjaus- ja hallintajärjestelmää, liikennöyi kyseisillä rataosuksilla. Määritellään menettely liikennötäjärjestelyjä varten.

**Vastaanottajan huomautukset:**

Rautatieyhtiös

Kuljettajia koulutetaan säännöllisesti IM:n ja PIM DP-menettelyjen osalta. IM arvioi lisäksi kuljettajia IM:n infrastruktuuriin sovellettavien säätöjen (S) valossa.
C.17. **Esimerkki rautatietoiminnan yleisestä vaaraluettelosta**

C.17.1. Ranskan ja Saksan välisen DEUFRAKO-yhteistyön puitteissa toteutetun ROSA-hankkeen (rautateiden optimidun turvallisuuden arviointi) tarkoituksena oli muodostaa yleinen ja kattava vaarojen luettelo, joka käsittää rautateiden vakiotoiminnollisia vaaroja ja haasteita. Joillakin rautatehdasen ideoissa, ja se otetaan huomioon Ranskan ja Saksan rautateiden erityispiirteitä. Luettelossa käytetään tarkoituksena laatia kattava vaarojen luettelo, joka käsittää rautateiden vakiotoiminnan ja turvallisuustyön. Tavoitehallinnointia koskevien turvallisuustoimenpiteiden esteiden ja (SPH), Alla olevassa luetteloluonnoksessa mainittuja vaaroja kutsutaan ”lähtökohtaisiksi vaaroiksi” (SPH), joilla tarkoitetaan vaaroja, joista voitaisiin voimakkaasti ja syiden arviointi

C.17.2. Alla olevassa luetteloluonnoksessa mainittuja vaaroja kutsutaan ”lähtökohtaisiksi vaaroiksi” (SPH), joilla tarkoitetaan vaaroja, joista voitaisiin voimakkaasti ja syiden arviointi

C.17.3. ROSA-hankkeen mukainen vaarojen luettelo:

| SPH 01 | Alun perin vääрин määritely nopeusrajoitus | (liittyy infrastruktuuriin) |
| SPH 02 | Nopeusrajoituksen vääрин määritely | (junaan liittyvä) |
| SPH 03 | Vääarin määritetty jarrutusetäisyys / vääри nopeusprofiili | / vääär jarrutuskaaret |
| SPH 04 | Riittämätön hidastuminen (fyysiset syyt) | |
| SPH 05 | Väääřä/epäasianmukainen nopeus/jarrutuskäskey | |
| SPH 06 | Vääärin rekisteröity nopeus (junalla vääärä nopeus) |
| SPH 07 | Nopeusrajoitustieto ei välity oikein |
| SPH 08 | Junan räjhä pois |
| SPH 09 | Vääärä matkustussuunta | / tarkoituksellinen peruuttaminen – (SPH 08:n ja SPH 14:n yhdistelmä) |
| SPH 10 | Vääärin rekisteröity absoluuttinen/suhteellinen sijainti |
| SPH 11 | Junan paikannuksen epäonnistuminen |
| SPH 12 | Junan eheyden menetyks |
| SPH 13 | Junan mahdollisesti vääärä reitti |
| SPH 14 | Aikataloulin/liikkumisluvan välittämis/tiedottamisen virhe |
| SPH 15 | Opastimen rakenteellinen vika |
| SPH 16 | Vaihteen osan rikkoutuminen |
| SPH 17 | Vääärä vaihdekäskey |
| SPH 18 | Vaihteen vääärä asento |
| SPH 19 | Järjestelmän kohde opastimessa/liikenneullottomassa | (pois lukien painolasti) |
| SPH 20 | Vieras esine ohjausradalla/liikenneullottomassa |
| SPH 21 | Tieliikenteen käyttäjiä terostukseisella |
| SPH 22 | Liukumisen vaikutukset painolastiin |
| SPH 23 | Aerodynamisten voimien vaikutus junaan |
| SPH 24 | Junan varustus/osa/rahti loukkaa liikkumavuottomaa |
| SPH 25 | Junan epäasianmukainen liikenneullottoma | (radanvarsi) |
| SPH 26 | Kuorman vääärä jakauma |
| SPH 27 | Rikkoutunut pyörä, rikkoutunut akseli |
| SPH 28 | Kuuma akseli/pyörä/laakeri |
| SPH 29 | Telin, jousituksen viemennuksen vika |
| SPH 30 | Kalustoysiköön alustan/vaununkorin vika |
| SPH 31 | Luvaton kulku | (turvallisuusnäkökohta) |
| SPH 32 | Henkilö ylittää luvallisesti radan |
| 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 reunoa |
| 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 päättyovesta |
| SPH 41 | Junaa lähtee / vierii ovet avoinna (loukkaamaton liikenneulotuma) |
| SPH 42 | Henkilö putoaa kahden vaunun väliselle käytävälläalueelle |
| SPH 43 | Matkustaja nojautuu ulos ovesta |
| SPH 44 | Matkustaja kurkottautuu ikkunasta |
| SPH 45 | Henkilöstö/junan hoitaja kurkottautuu oviaukosta |
| SPH 46 | Henkilöstö/junan hoitaja kurkottautuu ikkunasta |
| SPH 47 | Ohittavan kalustoyksikön henkilöstö kurkottautuu portaalta |
| SPH 48 | Henkilö putoaa/kiipeää laiturilla 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 liikku matkustajavaihdon aikana |
| SPH 53 | Junassa on mahdollisesti loukkaantunut henkilö |
| SPH 54 | Tulipalo/räjähdyssäärä (junassa) – onnettomuusluokka, SPH 55:n ja SPH 56:n seurauks |
| SPH 55 | Epäasianmukainen lämpötila (junassa) |
| SPH 56 | Myrkytys/tekutummus (junassa) |
| SPH 57 | Tappava sähköisku (junassa) |
| SPH 58 | Henkilö putoaa laiturille (pois lukien matkustajien vaihto) |
| SPH 59 | Epäasianmukainen lämpötila (laiturilla) |
| SPH 60 | Myrkytys/tekutummus (laiturilla) |
| SPH 61 | Tappava sähköisku (laiturilla) |