Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Tommi Hanttunen

Safety case -dokumentaatio turvalaite-projektissa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

19.4.2021

Tekijä Otsikko Sivumäärä Aika	Tommi Hanttunen Safety case -dokumentaatio turvalaiteprojektissa 34 sivua + 2 liitettä 19.4.2021
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine	Automaatiotekniikka
Ohjaajat	Turvalaiteasiantuntija Heli Tuominen Lehtori Kristian Junno

Safety case eli turvallisuusperustelu on EN 50xxx -standardien ja asetusten vaatima asiakirja, joka kokoaa projektin laadunhallinnan, turvallisuuden hallinnan sekä toiminnallisen ja teknisen turvallisuuden hallinnan yhteen. Velvoittavien EN-standardien mukaan turvallisuusperustelu kootaan kuuden eri otsikon alle, jotka ovat johdanto, laatujohtamisen raportti, turvallisuusjohtamisen raportti, teknisen turvallisuuden raportti, liittyvät safety caset ja lopputulos. Jokaiseen otsikon alle sisällytetään oleelliset todisteet siitä, että projektissa on noudatettu standardin vaatimuksia. Vaatimusten noudattamisen arvioi riippumaton arviointilaitos eli ISA, joka antaa päätöksen siitä, onko järjestelmä riittävän turvallinen ko. käyttötarkoitukseen ja -ympäristöön.

Safety case -työskentely toteutetaan osana projektia ja toiminnallinen turvallisuus huomioidaan projektin jokaisessa vaiheessa. Tarvittavaa aineistoa tuotetaan ja kootaan jokaisessa projektin elinkaaren vaiheessa. Tällä pyritään siihen, että kaikki tarvittava dokumentaatio on saatavilla riippumattoman arvioijan tarkasteltavaksi.

Safety caseen liittyy oleellisena myös YTM-asetuksen mukainen riskienhallinta, joka suoritetaan aina, kun rautatiejärjestelmään tehdään muutoksia, jotka ovat turvallisuuden kannalta merkittäviä. Riskienhallinnan tuloksena saadaan yksi turvallisuusperustelujen tärkeimmistä dokumenteista eli vaararekisteri, johon kirjataan kaikki riskienhallintaprosessiin liittyvät vaarat ja se, miten niitä hallitaan.

Avainsanat	Safety case, EN-standardi, ISA, YTM-asetus

Author	Tommi Hanttunen
Title	Safety Case Documentation in a Safety Device Project
Number of Pages	34 pages + 2 appendices
Date	19 April 2021
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Engineering
Instructors	Heli Tuominen, Safety Device Specialist Kristian Junno, Senior Lecturer

The purpose of the thesis work was to document the safety case process required by EN 50xxx standards and regulations and give guidance for doing so. Safety case brings together project quality management, safety management and operational and technical safety management. According to the mandatory EN standards, safety case is grouped under six different headings which are introduction, quality management report, safety management report, technical safety report, related safety cases and conclusion. All of this is inspected by an independent inspector, ISA.

Thesis work was done by firstly familiarizing with the current process of constructing safety cases and then getting to know better the required EN 50xxx standards. Risk assessment according to CSM regulation was also one of the topics to be familiared with. After getting acquainted with the mandatory topics needed to produce safety cases, process improvement began. The goal was to create a standard compliant process so that safety cases could be created systematically in the future. This was done by creating a process diagram that is compliant with the life cycle stages of EN standards and creating templates that complement the operations, so that they could be systematically created according to standards.

As a result of the thesis work, an operating model in accordance with the standards was created, as well as templates with which safety case work can be done systematically in the future.

Keywords	Safety case, EN standard, ISA, CSM Regulation

Sisällys

Lyhenteet

ISA	Riippumaton arviointilaitos.
JKV	Junien kulunvalvonta.
RATO	Ratatekniset ohjeet.
THR	Tolerable hazard rate, varmuusvikataajuus.
TFFR	Tolerable functional failure rate, hyväksyttävä toiminnallinen vikataajuus.
SIL	Turvallisuuden eheyden taso.
RAMS	Sisältää käsitteet reliability, availability, maintainability, safety eli toiminta-varmuus, käyttövarmuus, kunnossapidettävyys, turvallisuus.
SRAC	Safety related application condition, turvallisuuteen liittyvät käyttöehdot.
SAR	Turvallisuuden arviointikertomus.

1 Johdanto

Tämän opinnäytetyön tavoitteena on selventää turvalaitejärjestelmiin liittyvien turvallisuusperusteluiden (safety case) toimeksiantojen prosessia. Tarkoitus on antaa yleiskuva turvallisuusperusteluista ja toimista eikä mennä syvemmälle spesifin prosessin tai erilaisten turvallisuusperustelujen kuten sovellusten turvallisuusperustelujen eri elinkaaren vaiheisiin ja siihen liittyviin toimiin. Tämän johdosta standardissa EN 50126-1 käsitellyt RAMS-osatekijöiden, eli toimintavarmuuden, käyttövarmuuden, kunnossapidettävyyden ja turvallisuuden tarkastelu rajoitetaan turvallisuuteen liittyviin toimiin. Opinnäytetyön yhteydessä on tarkoituksena tuottaa osa turvallisuusperusteluihin liitettävien dokumenttien pohjista eli templateista. Opinnäytetyön toimeksiantajana toimii NRC Group Finland Oy.

Työssä käsitellään tarkemmin standardin EN 50129 mukainen turvallisuusperustelujen rakenne ja siihen liittyviä toimia. Aluksi opinnäytetyössä käsitellään yleisellä tasolla turvalaitteet ja turvallisuusperustelu, jonka jälkeen käydään tarkemmin läpi turvallisuusperustelun osia ja otsikoita, joiden alle dokumentaatio on velvoitettu luomaan. Turvallisuusjohtamisen prosessin yhteydessä käydään myös lyhyesti läpi YTM-asetuksen mukainen riskienhallintaprosessi.

Työn lopputuloksena luodaan standardien mukainen prosessikaavio, jonka perusteella projektit toteutetaan toiminnallinen turvallisuus huomioiden. Lisäksi luodaan dokumenttipohjat systemaattista turvallisuusperustelun laadintaa varten.

2 Turvalaitteet

Turvalaitteet ovat asetinlaitteisiin, suojastusjärjestelmiin, varoituslaitoksiin sekä junien kulunvalvonta-, kauko-ohjaus- ja laskumäkijärjestelmiin liittyvät laitteet. Yhdessä liikennöinnistä annettujen määräysten kanssa turvalaitteista koostuva turvalaitejärjestelmä varmistaa rautatien turvallisen liikennöinnin sekä muodostaa radan liikenteenvälityksen kapasiteetin. (1, s. 22.)

Väylävirasto määrittelee uusille turvalaitejärjestelmille turvallisuustason eurooppalaisen CENELEC-normiston mukaan. Yksittäisvian sattuessa turvalaitejärjestelmien täytyy olla

suunniteltu siten, että järjestelmä menee kontrolloidusti turvalliseen tilaan. Turvalaitejärjestelmien toiminnan on täytettävä vaadittu varmuusvaatimus, joka ilmaistaan EN-standardien mukaisina SIL-tasoina. Pääosin turvalaitteiden osalta käytetään SIL-tasoa 3 tai 4. (1, s. 22, 55.)

3 Safety case

Safety case eli turvallisuusperustelu sisältyy osana rautateiden turvalaitejärjestelmiin liittyviin toimeksiantoihin. Turvallisuusperustelu kuvaa toimeksiannon laadunhallintaa, turvallisuudenhallintaa sekä toiminnallisen ja teknisen turvallisuuden hallintaa standardien EN 50126, EN 50128, EN 50129 ja EN 50159 näkökulmasta. Lisäksi toimeksiannoissa vaaditaan riippumattoman arviointilaitoksen eli ISA:n lausunto siitä, että turvalaitejärjestelmätoimeksianto on viety läpi standardien EN 50126, EN 50128, EN 50129 ja EN 50159 osoittamalla tavalla.

Turvallisuusperustelun tavoite on johtaa ja esittää väite siitä, että käsiteltävä järjestelmä on turvallinen käyttää annetussa ympäristössä. Turvallisuusperustelun tulee sisältää kaikki tarvittava tieto, jotta voidaan tehdä päätelmä järjestelmän turvallisuudesta. Sen ei kuitenkaan tarvitse sisältää isoa määrää tietoa, mutta sen tulee viitata kaikkiin oleellisiin dokumentteihin, analyyseihin ja tuloksiin. (2, s. 4–5.)

Turvallisuusperustelujen tarkoituksena on lisäksi siteerata todisteita, joilla pystytään todistamaan, että käsiteltävä järjestelmä täyttää kaikki tarvittavat standardit ja lainsäädännöt. Sen tulee varmistaa, että avainhenkilöt ovat hoitaneet heille määritetyt vastuut, kaikki turvallisuusvaatimukset ja -tavoitteet on saavutettu sekä ovat sopivia käyttötarkoitukseensa, riskianalyysi on suoritettu oikein, jäännösriskin taso on siedettävä ja järjestelmän turvallisen toiminnan on tarkastanut riippumaton arviointilaitos. (2, s. 4–5.)

Jokainen turvallisuusperustelu koostuu neljästä osatekijästä:

1. Tarkoitukset tai vaatimukset: Turvallisuusperustelun täytyy tunnistaa ja esittää vaatimukset, jotka on täytettävä, jotta voidaan varmistua järjestelmän turvallisesta toiminnasta. (3, s. 154.)

2. Todisteet: Turvallisuusperustelun tulee esittää todisteet siitä, että vaatimukset järjestelmän turvallisesta toiminnasta ovat täytetty. (3, s. 154.)

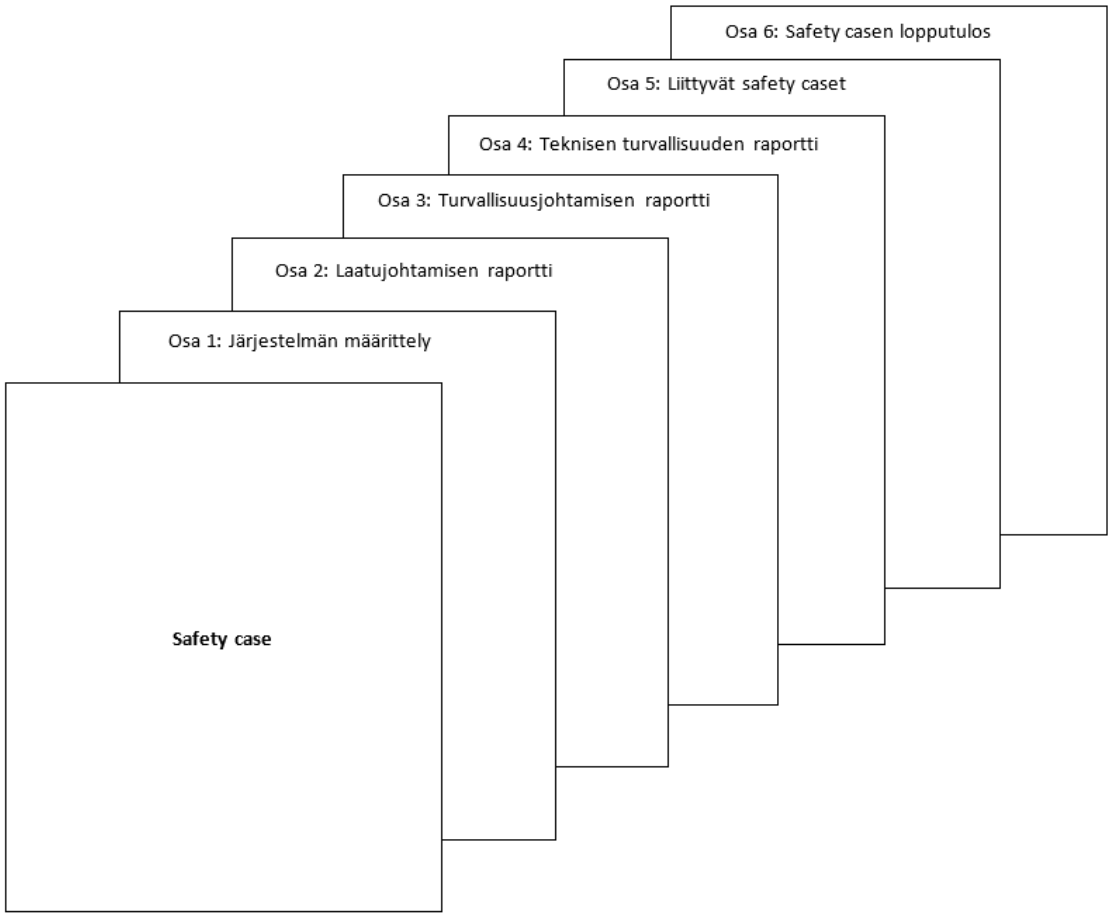
3. Argumentit: Turvallisuusperustelun tulee väittää, että tunnistetut vaatimukset ovat riittäviä esittämään, että järjestelmä on turvallinen olettaen, että kaikki vaatimukset on otettu käyttöön. (3, s. 154.)

4. Konteksti: Turvallisuusperustelun pitää määrittää järjestelmä toiminnallisessa kontekstissa. Näin ollen turvallisuusperustelun tulee tunnistaa ja rajata järjestelmän toiminnallinen ympäristö. Tämän pitää sisältää tekninen toiminnallinen rajaus järjestelmästä, joka toimii annetussa ympäristössä kaikissa olosuhteissa, oli se sitten normaali, heikentynyt tai hätätila. (3, s. 154.)

Turvallisuusperustelun idea ei ole pelkästään esittää matemaattiset ja tilastolliset todisteet vaan väitellä, kuten oikeussalissa.

Liian usein turvallisuusperustelujen luominen jätetään projektin loppuun johtuen siitä, että tarvitaan ymmärrys koko järjestelmän toiminnasta, ennen kuin voidaan aloittaa turvallisuusperustelun luominen. Tämä on osoittautunut kalliiksi ratkaisuksi ja voi johtaa järjestelmään, jota ISA-tarkastaja tai turvallisuusviranomainen ei hyväksy. On huomattavasti tehokkaampaa rakentaa turvallisuusperustelu vaiheittain lisäämällä siihen tietoa silloin, kun se tulee saataville projektin aikana. (4, s. 101–102.)

Kuvassa 1 on esitetty standardin EN50129 mukainen turvallisuusperustelun rakenne ja otsikot, joita opinnäytetyö mukailee sekä joiden alle turvallisuusperustelu kootaan. Standardin mukainen rakenne on laajalti käytetty ja luokiteltu hyväksi toimintatavaksi, mikä koskee turvallisuusperustelujen tuottamista. Sitä käytetäänkin laajalti myös standardin ulkopuolisissa tarkoituksissa. (3, s. 264.)



Kuva 1. Turvallisuusperustelun rakenne ja sen osatekijät (5, s. 43)

3.1 Järjestelmän määrittely

Järjestelmän määrittely on tärkeä dokumentti turvallisuusperustelun tuottamisessa. Sen tulee sisältää kuvaus järjestelmästä, sen toiminnallisuudesta ja tarkoituksesta, millä viitataan vaatimusten määrittelyyn ja muihin kuvaileviin dokumentteihin. Sen tulee kuvata järjestelmä ennen ja jälkeen muutoksen, sekä sen, miten muutoksen turvallisuus missäkin elinkaaren vaiheessa hallitaan. Siihen täytyy sisällyttää myös tuotteiden rakenne. Järjestelmän määrittelyn on tarkoitus olla enemmän kuin pelkkä osalistaus. Siinä tunnistetaan järjestelmän komponentit ja tapa, jolla ne ovat yhteydessä toisiinsa ja koko järjestelmään. Samaan aikaan määritellään kaikki rajapinnat, olivat ne sitten ulkoisia tai sisäisiä sekä mahdolliset viittaukset liittyvään dokumentaatioon. Rajapintojen tulee olla myös jäljitettävissä tuotteiden rakenteisiin. Järjestelmäkuvaukseen sisällytetään myös kuvaus

toimintaympäristöstä. Järjestelmän määrittelyssä seurataan EN-standardien mukaista elinkaarimallia, jota seuraamalla voidaan tuottaa riittävän kattava dokumentaatio, joka tukee hyväksyntämenettelyjä. (4, s. 107–108; 5, s. 43; 6, s. 13, 31.)

Toinen tapa määrittelyvaiheen lähestymiseen on miettiä, mitä tietoa tarvitaan turvallisuusperustelun rakentamiseen, jolloin aloitetaan turvallisesta järjestelmästä ja kuvataan ehdot, joilla järjestelmä on hyväksytysti turvallinen. Tällöin nähdään, että tarvitaan järjestelmän määrittely ja määritelmä hyväksytysti turvallisesta järjestelmästä. (4, s. 108.)

Vaarat riippuvat järjestelmän määrittelystä, erityisesti järjestelmän rajapinnoista. Vaarojen tunnistaminen ja vaikutusanalyysi suoritetaankin useasti eri vaiheissa. Rajapintojen tarkka määrittäminen on tärkeää vaara-analyysin ja turvallisuusperustelun luomisen tähden, eikä se ole ainoastaan rakentajan työ, sillä niiden määrittämiseen tarvitaan asiakkaan ja mahdollisesti muiden osallistujien yhteistyötä. Standardissa EN 50126 järjestelmän rajapintoihin sisältyvät rajapinnat fyysisen ympäristön kanssa, muiden teknologisten järjestelmien kanssa, ihmisten kanssa ja rajapinnat muiden rautateiden viranomaisten kanssa. (4, s. 108–109.)

3.2 Laatujohtamisen raportti

Laatujohtamisen raportin päävaatimus on se, että koko järjestelmän elinkaari on laatujohtamisjärjestelmän alaisuudessa. Laatujohtamisjärjestelmän tarkoitus on minimoida ihmisten virheiden todennäköisyydet ja parantaa prosessin tehokkuutta jokaisessa elinkaaren vaiheessa, ja näin ollen vähentää systemaattisten virheiden todennäköisyyttä. Laatujohtamisen raportin tulee ottaa kantaa kaikkiin aiheisiin, jotka ovat tärkeitä systemaattisten virheiden ehkäisyssä, kuten organisaation rakenteeseen sekä tarkastuksiin ja testauksiin. Laatujohtamisen raportti on pakollinen kaikille järjestelmätoimittajille, mutta dokumentaation laajuus riippuu turvallisuuden eheyden tasosta. Laatujohtamisjärjestelmällä on paljon yhtäläisyyksiä EN ISO 9001 -standardin laatujohtamisjärjestelmän vaatimusten kanssa ja mikäli rakennuttajalla on sertifioitu ISO 9001 -laatujärjestelmä tulee se mainita laatujohtamisjärjestelmän raportissa. (4, s. 13–14, s. 111–112.)

Laatujohtamisen raporttiin täytyy sisällyttää seuraavia asioita:

- organisaatiorakenne
- suunnittelun hallinta
- suunnittelun verifiointi ja katselmukset
- henkilöstön pätevyys ja koulutus
- tarkastukset ja testaukset
- laadun auditointi ja lisätoimet.

Rautatiemaailmassa on monia nimettyjä, standardisoituja ja säänneltyjä rooleja, jotka tulee määritellä projekti- ja laatusuunnitelmassa ja safety planissa yhdessä pätevyyksien kanssa. Oleelliset roolit ja niiden itsenäisyys tulee kirjata safety planiin ja ilmoittaa turvallisuuden arvioijalle. (4, s. 113.)

Suunnittelun hallinta alkaa kehityksellä yhdessä suunnittelun toimintojen ja dokumenttien hyväksynnän kanssa, se perustuu laadunvarmistukseen ja teknisiin perusteisiin. Sovelluksen suunnittelu hyödyntää useasti yleisiä sovelluksia, joita voidaan käyttää pohjana. Sovelluksen suunnittelu ei pääty suunnittelun mennessä tuotantoon, vaan suunnittelun hallinta koskettaa kaikkia laitteen tai tuotantoprosessin suunnittelun muutoksia. (4, s. 118–119.)

Suunnittelun verifioinnin ja katselmusten avulla saavutetaan laadukkaampia tuotteita, elinkaarikustannukset pienevät. Kun mahdolliset virheet tunnistetaan jo suunnittelun aikana, on virheet helpompi korjata kuin myöhemmissä vaiheissa. (4, s. 119.)

Laatujohtamisjärjestelmä mukailee siis suurilta osin ISO 9001 -laatujärjestelmää. Jos yrityksellä on jo ISO 9001 -sertifioitu laatujohtamisjärjestelmä, on suurin osa raportin toimista jo valmiiksi luotu ja hyväksyttävällä tasolla.

3.3 Turvallisuusjohtamisen raportti

Turvallisuusjohtamisen raportin sekä turvallisuusperustelun päätavoite on esittää määräystenmukaisuus kaikkien turvallisuusjohtamisprosessien kanssa koko järjestelmän elinkaaren ajan. Turvallisuusjohtamisjärjestelmä tähtää systemaattisten virheiden ja turvallisuusuhkien jäännösriskin minimoimiseen. Turvallisuusjohtamisen prosessi tulee liittää osaksi turvallisuuden elinkaarta. Prosessin suunnittelu ja validointi voidaan esimerkiksi esittää V-mallina, jossa järjestelmävaatimuksia käytetään järjestelmätestaukseen ja järjestelmän validointiin ja toiminnallisia turvallisuusvaatimuksia käytetään toiminnallisten testien luomiseen ja validointiin. Turvallisuusjohtamisen prosessin tulee toteutua pätevän turvallisuusorganisaation alaisuudessa. On myös tärkeää dokumentoida kyseisen organisaation itsenäisyys muusta organisaatiosta. (4, s. 14; 5, s. 26.)

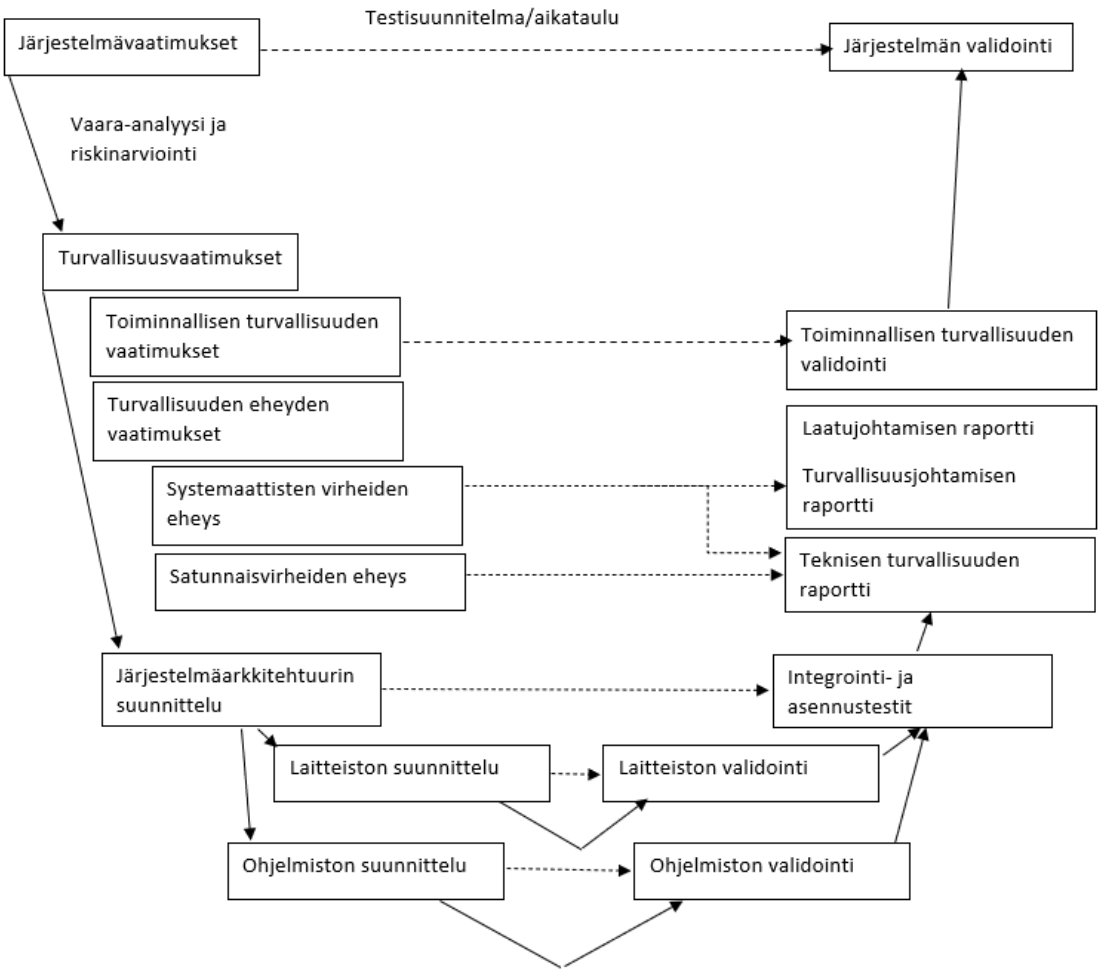
Standardin EN 50129 mukaan turvallisuusjohtamisen raporttiin tulee dokumentoida turvallisuustoimenpiteet, jotka on tehty, jotta voidaan varmistua tarpeellisesta turvallisuusjohtamisesta koko elinkaaren ajalta. Turvallisuusjohtamisen raporttiin tulee siis kirjata

- johdanto
- turvallisuuden elinkaari
- turvallisuusorganisaatio
- safety plan
- vaararekisteri
- turvallisuusvaatimukset
- järjestelmän/alijärjestelmän/laitteiston suunnittelu
- turvallisuuskatselmukset
- turvallisuuden verifiointi ja validointi

- turvallisuuden oikeutus
- toiminta ja huolto
- käytöstä poisto ja hävitys.

Turvallisuusjohtamisjärjestelmää tulee soveltaa kaikkiin turvallisuuteen liittyviin järjestelmiin. Riskiarvio ja vaarojen kontrolloimisen prosessi ovat aina pakollisia, kun tunnistetaan jokaisen eri toiminnon oikeaa SIL-tasoa. Tähän sisältyvät myös ne tapaukset, joissa analyysi ja arvio paljastavat, että toiminto voidaan luokitella turvallisuuteen liittymättömäksi. (5, s. 26.)

Kuvassa 2 esitetään turvallisuusjohtamisen prosessi, joka koostuu monista vaiheista ja toimista, jotka ovat linkittyneet yhteen turvallisuuden elinkaareksi. Turvallisuusjohtamisen prosessin tulee olla yhteneväinen järjestelmän elinkaaren kanssa. Turvallisuuden elinkaari voidaan esittää siten, että suunnitteluosa luetaan ylhäältä alas vaiheisena, jota seuraa integraatio ja validointi alhaalta ylös vaiheisena.



Kuva 2. Turvallisuuden elinkaari, jossa suunnitteluvaiheet vasemmalla ja validointivaiheet oikealla. (5, s. 27.)

3.3.1 Organisaatiorakenne

Turvallisuusjohtamisen prosessi toteutetaan sopivan turvallisuusorganisaation alaisuudessa, jonka henkilöstön tulee olla riittävän päteviä suorittamaan annetut työtehtävät. Oleellisille henkilöille suoritetaan sopivuuden arviointi, johon sisältyvät esimerkiksi teknisen tietämys ja sopiva koulutus. Myös järjestelmän kehittämiseen tai muuttamiseen määrätyistä henkilöistä ylläpidetään rekisteriä, ja soveltuva itsenäisyyden taso luodaan eri tehtävien välillä. Nämä järjestelyt koskevat kaikkia elinkaaren vaiheita. (5, s. 28.)

Aikaisissa järjestelmän elinkaaren vaiheissa yleiset vaatimukset roolien erillisyydestä ovat käytössä, jolloin verifioinnin suorittaa henkilö, joka ei ole ollut tekemisissä verifioitavien asioiden kanssa. Validoija ei saa myöskään olla ollut tekemisissä vaatimusten määrittämisen kanssa ja hänen tulee olla riippumaton projektinjohtajasta. Myöhemmissä elinkaaren vaiheissa projektin tiimi on määritelty ryhmäksi, joka koostuu tyypillisesti seuraavista henkilöistä: projektin johtajasta, suunnittelijasta, verifioijasta ja validoijasta. ISA on ulkopuolinen projektin tiimistä. Millä tahansa SIL-tasolla 1–4 ja perusyhtenäisyyden tasolla projektitiimin organisaatiorakenteen tulee noudattaa seuraavia vaatimuksia:

- Henkilö, joka on suunnittelija, ei voi olla saman järjestelmän, alijärjestelmän tai laitteiston verifioija.

- Henkilö, joka on suunnittelija, ei voi olla validoija.

- Validoijalle pitää antaa tarpeellinen itsenäisyys ja vastuu, jotta hän voi tehdä riippumattoman päätöksen.

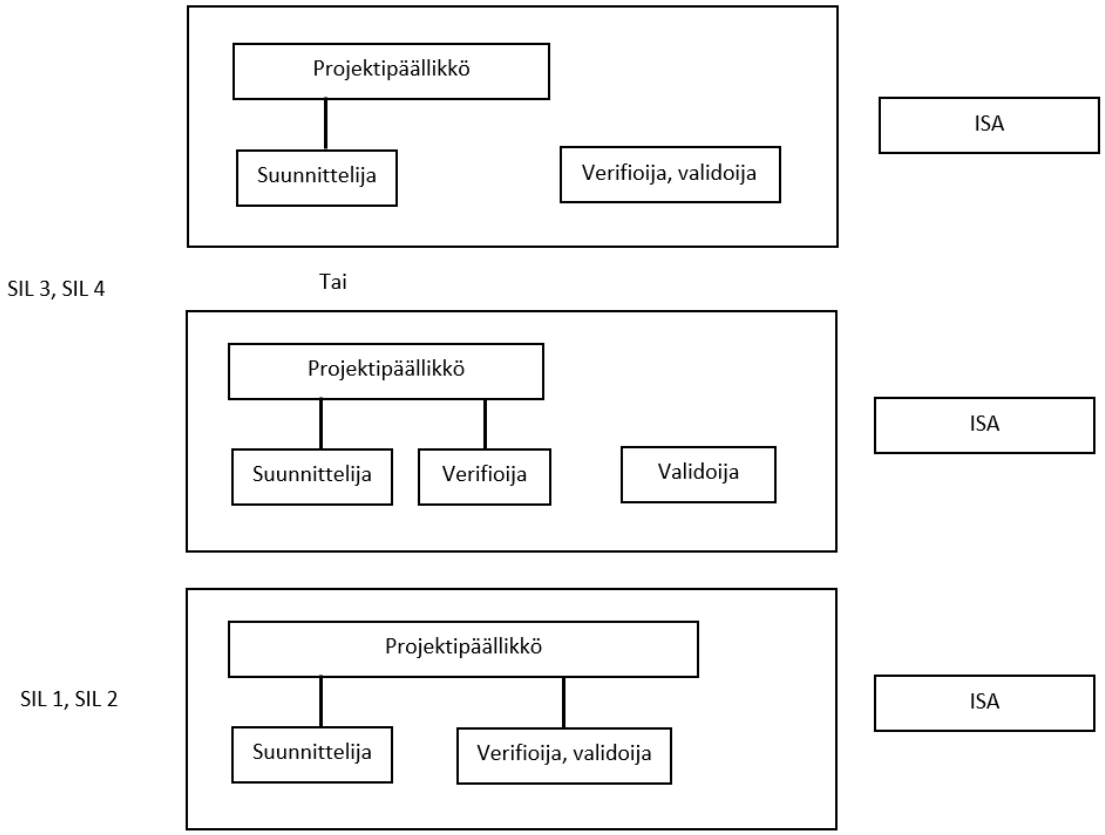
- Henkilö, joka on validoija, voi olla myös verifioija. Tässä tapauksessa, kuten kaikessa muussa kehitystyössä, turvallisuuden verifioinnin ja validoinnin tulokset tulee jonkun muun pätevän henkilön tarkastaa.

Lisäksi SIL 3- ja 4-tasoilla projektitiimin organisaatiorakenteen täytyy myös noudattaa seuraavaa vaatimusta.

- Validoija ei saa raportoida projektin johtajalle.

ISA ei saa raportoida projektin johtajalle, eikä saa olla osa projektitiimiä. Kuitenkin ISA voi olla osa sidosryhmän organisaatiota. (5, s. 28; 8, s. 18–19.)

Kuvassa 3 on esitetty, miten projektiorganisaatio rakentuu eri SIL-tasoilla.



Kuva 3. Roolien erillisyys eri SIL-tasoilla. (5, s. 29.)

3.3.2 Safety plan

Standardissa EN50129 sanotaan, että safety plan tulee luoda turvallisuuden elinkaaren aikaisissa vaiheissa, joskin yksityiskohtainen suunnittelu tehdään vasta myöhemmissä vaiheissa. Kyseinen suunnitelma määrittää turvallisuusjohtamisen organisaation, turvallisuuteen liittyvät toimet ja tavoitteet elinkaaren ajalta, ja sitä tulee tarkastella tietyin väliajoin. Safety plania päivitetään, jos peräkkäisiä muutoksia tai lisäyksiä tehdään alkuperäiseen järjestelmään. Jos mikä tahansa tällainen muutos tehdään, sen vaikutus turvallisuuteen arvioidaan alkaen sopivasta kohtaa turvallisuuden elinkaarta. Safety planin läpikäynnit tehdään sovituissa kohdin turvallisuuden elinkaarta, ja niiden tulokset dokumentoidaan. Mikä tahansa muutos tai lisäys järjestelmään on myös tarkastuksen alaisena. Safety plan ottaa kantaa kaikkiin järjestelmän, alijärjestelmän tai laitteiston näkökantoihin, liittyen myös laitteistoon ja ohjelmistoon. Safety planin pitää myös sisältää suunnitelman turvallisuusperustelun luomisesta, joka määrittelee turvallisuusperustelun

laajuuden, sen rakenteen, mahdolliset alemman tason turvallisuusperustelut, vastuussa olevat ihmiset sekä sen tekemisen aikataulun. Safety planin tulee sisältää tai referoida turvallisuuden verifiointisuunnitelmaa verifioimalla, että jokainen elinkaaren vaihe täyttää tietyt turvallisuusvaatimukset, jotka on määritelty edellisessä vaiheessa. Sen tulee myös sisältää tai referoida turvallisuuden validointisuunnitelmaa validoidakseen valmiin järjestelmän turvallisuuden vaatimusten määrittelyä vasten. (5, s. 29–30.)

3.3.3 Verifiointi ja validointi

Turvallisuuden verifioinnin laajuus, toiminnot ja metodit aina elinkaaren alkuvaiheista sen integrointiin asti täytyy suunnitella ja dokumentoida. Vaara-analyysit, testaus ja dokumenttien läpikäynti ovat turvallisuuden verifioinnin päätoimenpiteet. Turva-analyysit, testisuunnitelmat ja testien työselostukset turvallisuuden verifiointia varten täytyy verifioijan itse luoda tai verifioijan tulee käydä läpi ja hyväksyä ne. Luotuihin testisuunnitelmiin ja raportteihin sisällytetään, kenellä on vastuu testin määrittelystä ja toteutuksesta, versiointi sekä tulokset testeistä, joihin sisältyvät eroavaisuudet ennakoiduissa ja oikeissa tuloksissa. (5, s. 31–32.)

Turvallisuuden validoinnin tarkoituksena on esittää, että turvallisuuteen liittyvät vaatimukset on määritelty, toteutettu ja verifioitu ja että tarkastelussa oleva järjestelmä täyttää siihen liittyvät turvallisuuden tavoitteet ja se on sopiva sen suunniteltuun käyttöön määritellyssä ympäristössä. (5, s. 32.)

Turvallisuuden validoinnin laajuus, toiminnot ja metodit kaikissa oleellisissa elinkaaren vaiheissa tulee suunnitella ja dokumentoida. Validoija voi vaatia tai suorittaa analyysejä, testejä tai läpikäyntejä soveltuvissa turvallisuuden elinkaaren vaiheissa varmistaakseen, että määritellyt ominaisuudet ja turvallisuusvaatimukset on saavutettu. Vika-analyysit, testisuunnitelmat ja testipöytäkirjat turvallisuuden validointia varten tulee validoijan itse luoda tai validoijan tulee käydä ne läpi ja hyväksyä. Validoijan tulee varmistua siitä, että suunnittelun konseptit eivät ole vaarantuneet tuotannon, asennuksen huollon tai käytön aikana. Tähän päätelmään päästäkseen validoijan tulee käydä läpi vaatimukset, turvallisuuteen liittyvien menetelmien edellytykset ja varotoimet sekä auditoida näitä prosesseja. Validoijan tulee arvioida tuotannon, asennuksen, toimeksiantojen ja turvallisuuden verifioinnin prosesseja ja tehdä lausunto eri näkökulmista, kuten

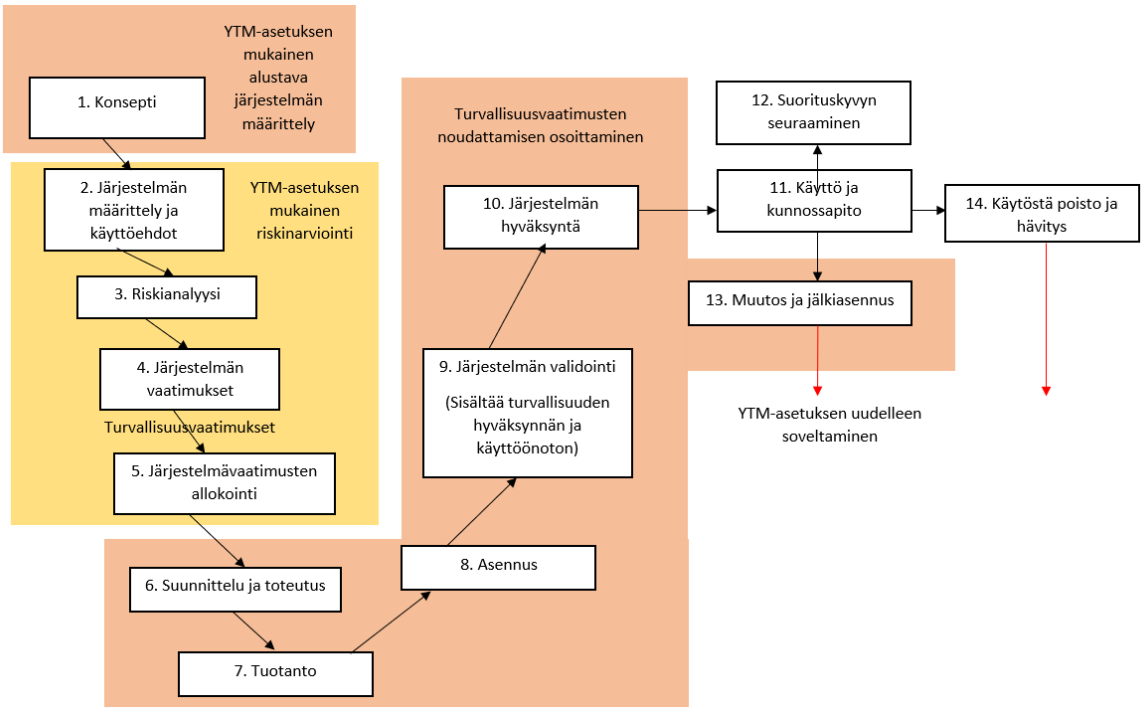
- dokumenttien vaatimusten yhdenmukaisuudesta
- suunnitelmien, raporttien ja toimitusten jatkuvuudesta
- kyseessä olevan järjestelmän turvallisuusvaatimusten täyttymisestä.

Turvallisuuden validointiraportin tulee esittää johtopäätökset, jotka perustuvat validoinnin tuloksiin ja kertoa, onko käsittelyssä oleva järjestelmä sopiva sen suunniteltua käyttöä varten määrätyssä ympäristössä koskien turvallisuutta. (5, s. 32–33.)

3.3.4 Järjestelmän elinkaari ja YTM-asetuksen mukainen riskienhallinta

Järjestelmän elinkaari voidaan erottaa selkeästi eri vaiheiksi, joiden aikana suoritetaan eri toimet ja toimenpiteet. Kaikki elinkaaren toimenpiteet on tärkeä dokumentoida. Jos tätä ei tehdä, elinkaaren prosesseille ja toimille ei voida saavuttaa tarvittavaa näkyvyyttä, eikä arvioija pysty verifioimaan, että standardia on seurattu. (9, s. 58.)

Kuvassa 4 on esitetty järjestelmän elinkaari yhdessä YTM-asetuksen mukaisen riskienhallinnan toimien kanssa.

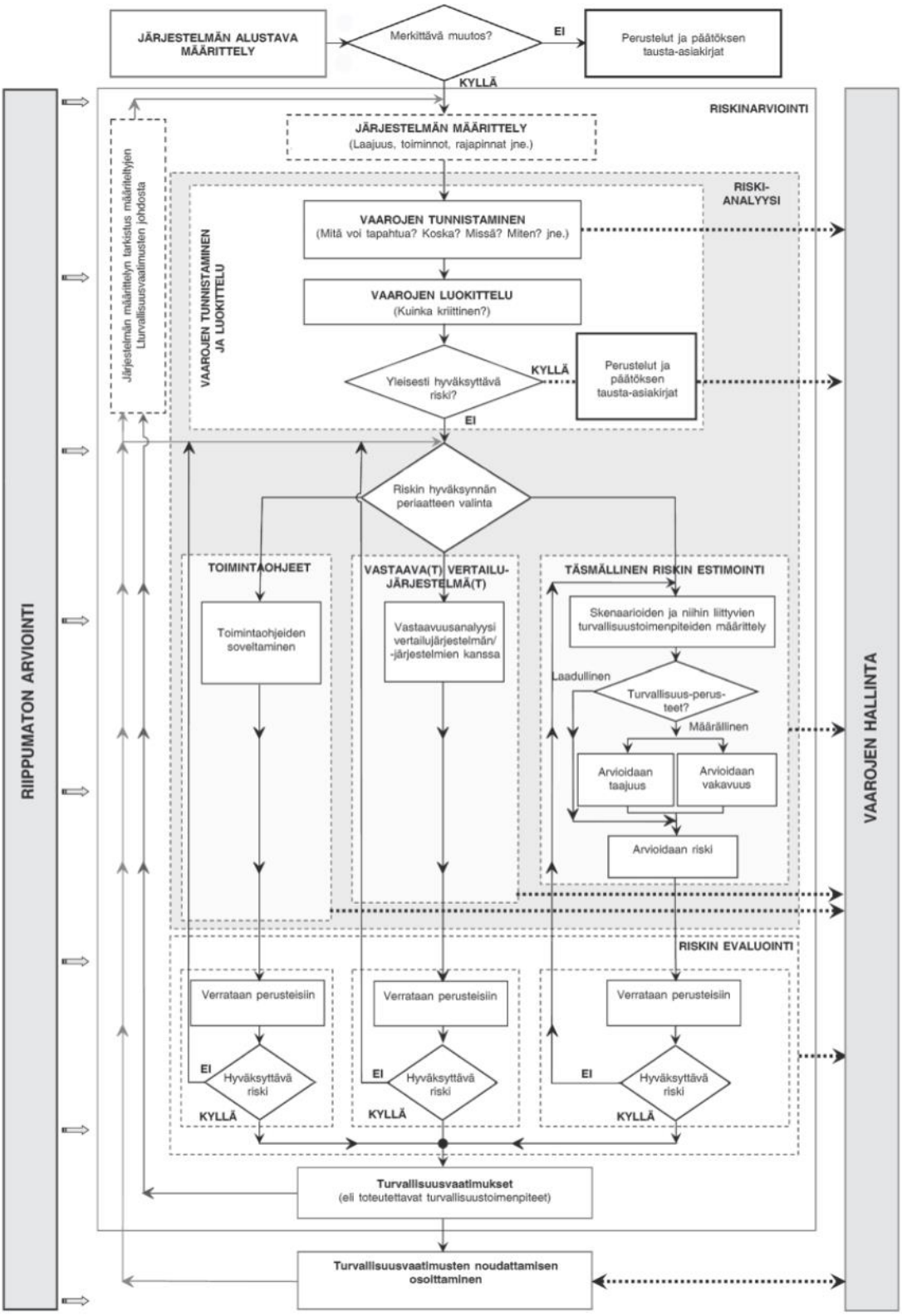


Kuva 4. Järjestelmän elinkaarta kuvaavat vaiheet 1–14 ja YTM-asetuksen mukaisen riskienhallinnan toimia laatikot elinkaaren vaiheiden ympärillä. (11, s. 33.)

YTM-asetuksen mukainen riskienhallinnan prosessi voidaan esittää yhdessä standardin EN 50126-1 järjestelmän elinkaaren kanssa. Järjestelmän elinkaari alkaa konseptivaiheesta ja päättyy mahdolliseen käytöstä poistoon.

YTM-asetus eli riskienhallintaa koskeva yleinen turvallisuusmenetelmä on Euroopan komission antama asetus. Asetus edellyttää turvallisuuteen liittyvien riskien hallintaa muutoksissa, joissa järjestelmän turvallisuus muuttuu merkittävästi. Tarkoituksena on se, että rautatiejärjestelmään tehtävät muutokset eivät voi heikentää sen turvallisuutta. (10, s. 8.)

Kuvassa 5 on esitetty YTM-asetuksen mukainen riskienhallinta ja toimenpiteet, joita suoritetaan sen aikana.



Kuva 5. YTM-asetuksen mukainen riskienhallinta ja sen toimet. (10, liite 1)

3.3.4.1 Järjestelmän alustava määrittely

Kuvassa 5 esitetään koko YTM-asetuksen mukainen riskienhallintaprosessi. Järjestelmän alustava määrittely vastaa järjestelmän elinkaaren vaihetta konsepti. Järjestelmän alustavassa määrittelyssä luodaan tarkasteltavan kohteen, sen rajojen ja vaikutuspiirin alustavaa kuvausta ja tarkoituksena on esittää, miten muutos vaikuttaa järjestelmään eli mikä kohde ja sen tilanne ovat muutoksen jälkeen. Alustavan määrittelyn pohjana voidaan käyttää esimerkiksi kohteen hankesuunnitelman kuvausta. Järjestelmän alustavaa määrittelyä päivitetään tarvittaessa projektin aikana, ennen kuin se korvataan järjestelmän määrittelyllä. (10, s. 12; 11, s. 22.)

Järjestelmän alustavan määrittelyn jälkeen suoritetaan muutoksen merkittävyyden arviointi. Arvioitaessa muutosta tarkastellaan sitä, että onko muutoksella vaikutusta rautatiejärjestelmän turvallisuuteen. YTM-asetuksen mukaisen riskienhallintaprosessin soveltaminen voidaan päättää, mikäli on selkeästi osoitettavissa, ettei turvallisuus vaarannu muutoksen takia. Jos järjestelmän muutoksella on pienikin vaikutus turvallisuuteen, sovelletaan riskienhallintaprosessia. Muihin muutoksiin liittyviä riskejä tulee kuitenkin hallita Väyläviraston rautatietoimintojen turvallisuusjohtamisjärjestelmän mukaisesti. (10, s. 12–13, 15.)

Mikäli asiantuntija-arvion avulla saadun muutoksen merkittävyyden arvioinnin perusteella muutos on merkittävä, tulee turvallisuuteen vaikuttavat muutoksen arviointia jatkaa. Arviointia jatkettaessa tarkastellaan muutosta seuraavien kriteerien pohjalta:

- kumuloituvuus
- uutuusaste
- muutoksen monimutkaisuus
- vian vaikutus
- seurattavuus
- peruutettavuus.

Päätös muutoksen merkittävyydestä dokumentoidaan aina ja arviointi säilytetään, jotta päätöksen perusteluja voidaan tarkastella. (10, s. 13.)

3.3.4.2 YTM-asetuksen mukainen riskinarviointi

Kuvan 4 järjestelmän elinkaaren vaiheiden 2–5 aikana suoritetaan YTM-asetuksen mukainen riskinarviointi. Kuvassa 5 näkyvät riskinarvioinnin toimet, jotka alkavat järjestelmän määrittelystä ja päättyvät ennen turvallisuusvaatimusten noudattamisen osoittamista. Ensimmäinen riskianalyysin vaihe on vaarojen tunnistaminen, joka perustuu järjestelmän määrittelyyn. Tunnistetut vaarat luokitellaan sen mukaan, onko muodostuva riski yleisesti hyväksyttävä vai ei. Yleisesti hyväksyttävien riskien vaaroja ei tarvitse analysoida enempää, joskin näiden vaarojen yhteyteen täytyy kirjata perustelut, miksi ne ovat yleisesti hyväksyttäviä. Kaikki tunnistetut vaarat kirjataan vaararekisteriin ja vaaroja tunnistetaan lisäksi koko hankkeen ajan. Riskit voidaan luokitella yleisesti hyväksyttäviksi, kun riski on niin pieni, ettei ole järkevää toteuttaa ylimääräisiä turvallisuustoimenpiteitä. Eli käytetään ALARP-periaatetta. Arviointi tehdään rautatiejärjestelmään ja riskienhallintaan liittyvän kokemuksen perusteella. (10, s. 16–17.)

Kun riskianalyysin tuloksena riskiä ei voida luokitella yleisesti hyväksyttäväksi, jatketaan riskianalyysin toimia valitsemalla sopiva riskin hyväksynnän periaate. Näitä ovat toimintaohjeet, vertailujärjestelmät ja riskin estimointi. Tarkoituksena on käyttää sopivia toimenpiteitä, jotta vaaroista aiheutuva riski saadaan pienennettyä hyväksyttävälle tasolle. (10, s. 20.)

Toimintaohjeet ovat kirjallisia sääntöjä ja määräyksiä, joita sovelletaan riskien hallinnassa. Toimintaohjeita ovat esimerkiksi EN-standardit, viranomaisten määräykset ja Väyläviraston yleiset ohjeet. Mikäli toimintaohjeiden mukaisen toiminnan jälkeen vaarasta aiheutuva riski ei ole edelleenkään hyväksyttävällä tasolla, jatketaan riskianalyysiä ja käytetään lisäksi jotain muuta riskin hyväksynnän periaatetta. (10, s. 21.)

Vertailujärjestelmät ovat aiemmin hyväksyttyjä järjestelmiä tai muutoksia, ja ne ovat vastaavanlaisia kuin arvioinnin kohteena oleva järjestelmä. Vaatimuksena vertailujärjestelmällä on, että sillä on samanlaisia toiminnallisuuksia ja rajapintoja sekä sitä käytetään samankaltaisessa ympäristössä. Jos arvioinnin kohteena oleva järjestelmä poikkeaa

vertailujärjestelmästä, tulee riskin evaluoinnin esittää, että käsiteltävä järjestelmä saavuttaa vähintään saman turvallisuustason kuin vertailujärjestelmä. Jotta turvallisuustaso saavutetaan, täytyy mahdollisesti käyttää lisäksi toista vertailujärjestelmää tai toista riskin hyväksynnän periaatetta. (8, s. 26–27.)

Täsmällisen riskin estimointia käytetään silloin, kun kahdella muulla riskin hyväksynnän periaatteella ei voida varmistua riskin olevan hyväksyttävällä tasolla. Riskin estimointia voidaan esimerkiksi käyttää silloin, kun arvioitava järjestelmä on aivan uusi. Estimointi voidaan tehdä määrällisesti tai laadullisesti. Riskin estimointimenetelmiä ovat esimerkiksi HAZOP-poikkeamatarkastelu ja VVA eli vika- ja vaikutusanalyysi. Estimoinnin esittämisessä on hyvä käyttää Väyläviraston riskimatriisia (liite 1). Riskimatriisilla kuvataan riskin suuruus vaaratilanteen esiintymistodennäköisyyden ja sen seurausten vakavuuden yhdistelmänä. (10, s. 22; 12, s. 21.)

Riskin evaluoinnissa riski voidaan lukea hyväksytyksi, kun on perusteellisesti sovellettu vertailujärjestelmien tai toimintaohjeiden toimenpiteitä. Riskin estimointia käyttäessä hyväksyntä tulee tehdä selkein perustein. Väyläviraston riskimatriisissa (liite 1), on esitetty luokittelu riskin hyväksyttävyydelle. YTM-asetuksen mukainen riskienhallintaprosessi on iteratiivinen, riskin suuruuden arviointi suoritetaan uudelleen tarvittaessa, ja tällöin otetaan huomioon aiemmin tehdyt riskien pienentämisen toimenpiteet. Hyväksyttävä riskitaso voidaan myös määritellä numeerisesti tapauksissa, joissa toimintahäiriö voi aiheuttaa tuhoisia seurauksia. Tällöin niihin sovelletaan luotettavuusvaatimusta, jolloin häiriön esiintymistaajuus voi olla enimmillään 10^-9 häiriötä toimintatuntia kohden. Tällaisia järjestelmiä ovat esimerkiksi turvalaitteet. Riskianalyysin tuloksena saadut hyväksyttävät riskitasot, joilla on luotettavuusvaatimus, siirretään teknisille järjestelmille. (8, s. 28; 10, s. 22–23.)

3.3.4.3 Turvallisuusvaatimusten noudattamisen osoittaminen

Kuvan 4 järjestelmän elinkaaren vaiheiden 6–10 aikana suoritetaan turvallisuusvaatimusten noudattamisen osoittaminen. Ennen turvallisuushyväksyntää Väyläviraston täytyy näyttää, että riskien arviointiin perustuvat turvallisuusvaatimukset täyttyvät. Täyttyminen todennetaan vaararekisterin avulla, johon on dokumentoitu YTM-asetuksen tarpeelliset vaiheet alusta alkaen. Rekisteristä selviävät riskinarvioinnin eri toimien tulokset, ja

kaikki vaadittavat turvallisuusvaatimukset ja toimenpiteet, joilla riskit saadaan hyväksyttävälle tasolle. YTM-asetus vaatii myös riskienhallintaprosessien soveltamisesta yhteenvetoraportin. (10, s. 26–27.)

3.3.5 Vaatimusten jakaminen toiminnoille

Riskin arvioinnin tuloksena saadaan järjestelmän turvallisuusvaatimukset. Kyseiset vaatimukset voidaan joko sisällyttää erilliseen turvallisuusvaatimusten määrittelyyn tai sisällyttää järjestelmävaatimusten määrittelyyn erillisinä turvallisuusvaatimuksina. Turvallisuusvaatimusten määrittelyssä otetaan kantaa esimerkiksi turvallisuuteen liittyviin toimintoihin, hyväksyttäviin riskitasoihin, turvallisiin tiloihin ja rajapintoihin sovittamiseen. Turvallisuusvaatimukset tulee luokitella toiminnallisiksi, teknisiksi tai kontekstuaalisiksi. Riskianalyysin jälkeen toiminto voidaan määritellä turvallisuuteen liittyväksi ja sille voidaan määrätä toiminnallisen turvallisuuden vaatimuksia, joita on esimerkiksi turvallisuuteen liittyvän toiminnon odotettu toiminta vikatilanteessa. (8, s. 33–34.)

Tekniset turvallisuusvaatimukset ovat yhteydessä järjestelmän tekniseen suunniteluun ja implementointiin. Tekniset turvallisuusvaatimukset voidaan johtaa olosuhteista ja mahdollisista uhista, jotka käytetty teknologia voi aiheuttaa, kun taas kontekstuaaliset turvallisuusvaatimukset kattavat toiminnalliset ja kunnossapidolliset turvallisuusvaatimukset. (8, s. 35.)

Turvallisuuden eheyden taso liittyy turvallisuuteen liittyvän järjestelmän kykyyn saavuttaa vaadittu toiminto. Mitä korkeampi eheyden taso, sitä suuremmalla todennäköisyydellä se saavuttaa vaaditun toiminnon. Eheyden taso sisältää sekä systemaattisten että satunnaisvirheiden eheyden. Satunnaisvirheiden eheys voidaan saavuttaa tuotteiden suunnittelulla ja satunnaisvirheiden eheys perustuu pääosin laatujohtamisen, turvallisuusjohtamisen ja organisaatioiden toimenpiteisiin. SIL-tasoja käytetään ainoastaan toiminnallisen turvallisuuden vaatimuksille. (8, s. 34–36.)

Kun riskienhallintatoimien jälkeen saadaan järjestelmän turvallisuusvaatimukset, jaetaan ne alijärjestelmille sekä komponenteille. Turvallisuuteen liittyvien vaatimusten jakamisen prosessia kutsutaan vaarojen hallinnaksi. Se sisältää mahdollisten vaarojen arvioinnin ja

turvallisuuden eheyden vaatimusten jakamisen turvallisuuteen liittyville toiminnoille. Alkuaan turvallisuuden eheyden vaatimukset, joita kuvataan järjestelmätasolla varmuusvikataajuutena jokaiselle vaaralle, linkitetään määritetylle toiminnalliselle kokoonpanolle, jonka määrittää valittu järjestelmäarkkitehtuuri, näin ollen ne pystytään muuttamaan toiminnoille hyväksyttäviksi toiminnallisiksi vikataajuuksiksi. Varmuusvikataajuudet jaetaan kausaalianalyysillä käyttämällä erilaisia toimintatapoja kuten vikapuuanalyysiä. Monien toimintojen yhdistelmän tapauksessa varmuusvikataajuus jaetaan alemmille vaaroille ja niiden hyväksyttävät toiminnalliset vikaantumistaajuudella viimeisille itsenäisille toiminnoille. Tämä on taso, jossa kaksi tai useampi toimintoa kontrolloi samaa vaaraa, mutta ovat molemmat täysin itsenäisiä. (8, s. 36–38.)

Kun vaatimukset ovat saatu johdettua turvallisuuteen liittyville toiminnoille, luodaan malli, joka täyttää määritetyt toiminnalliset vaatimukset ja turvallisuusvaatimukset. Erityisesti laitteiston ja ohjelmiston välinen suhde tulee huolellisesti määritellä ja rajapintoihin tulee käyttää erityistä huomiota. Jos tässä vaiheessa huomataan järjestelmäarkkitehtuurista johtuvia uusia vaaroja, johdetaan näistä vaaroista uusia vaatimuksia niiden hallitsemiseen ja ne jaetaan olemassa oleville järjestelmille tai komponenteille. (7, s. 62.)

3.3.6 Turvallisuuden eheyden taso

Toiminnon turvallisuuden eheyden taso eli SIL-taso ottaa kantaa eri asioihin, joista jokainen on tarpeellinen, jotta voidaan varmistua vaatimusten täyttymisestä. Laskennallinen turvallisuustaso on vain yksi asia turvallisuuden eheystasosta, joka tulee täyttää. Turvallisuuden eheyden tasoon kuuluu myös laadulliset puolet, joihin kuuluvat laatu-, turvallisuusjohtaminen ja tekniset turvallisuustoimenpiteet. Mitä tiukemmat määrälliset vaatimukset, jotka ilmaistaan hyväksyttävänä toiminnallisena vikaantumistaajuudella ovat, sitä tiukemmat myös laadulliset vaatimukset tulevat olemaan. Turvallisuuden eheys vaatii, että laadulliset toimenpiteet korreloidaan hyväksyttäviin toiminnallisiin vikaantumistaajuuksiin. (8, s. 39–40.)

TFFR on tavoite toiminnon turvallisuuden eheydelle ja se liitetään SIL-tasoon tai peruseheyteen. Kuvassa 6 on esitetty eri SIL-tasoilta vaadittu vikaantumistaajuus.

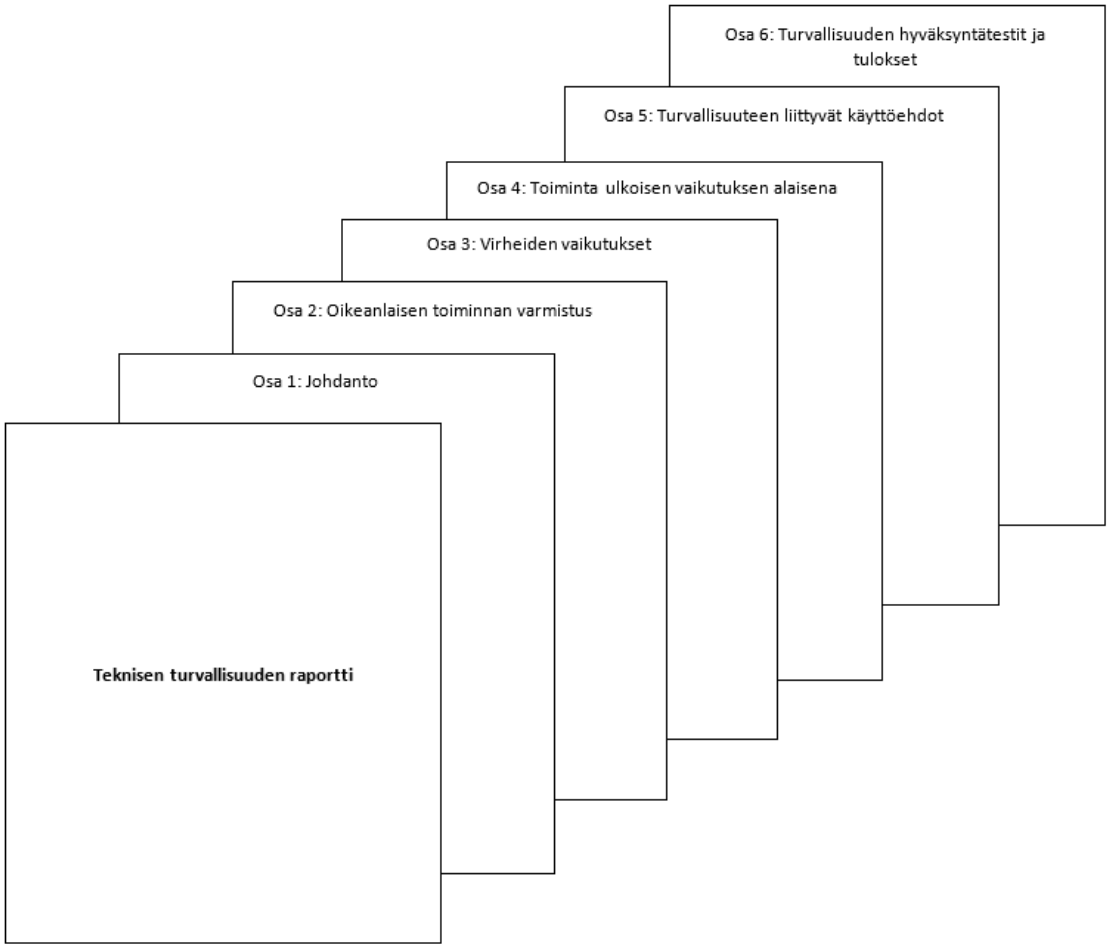
TFFR Per tunti ja toiminto	SIL-taso
$10^{-9} \leq TFFR < 10^{-8}$	4
$10^{-8} \leq TFFR < 10^{-7}$	3
$10^{-7} \leq TFFR < 10^{-6}$	2
$10^{-6} \leq TFFR < 10^{-5}$	1

Kuva 6. SIL-tasot ja niitä vastaavat toiminnon turvallisuuden eheyden vaatimukset. (5, s. 76.)

3.4 Teknisen turvallisuuden raportti

Teknisen turvallisuuden raportti sisältää tekniset todisteet järjestelmän turvallisuudesta, ja se on pakollinen. Sen laajuus ja sitä tukevan tiedon laajuus riippuu jälleen vaaditusta turvallisuuden eheyden tasosta. Teknisen turvallisuuden raportti sisältää periaatteet, joilla varmistutaan suunnittelun turvallisuudesta. (4, s. 14.)

Kuvassa 7 on esitetty teknisen turvallisuuden raportin rakenne ja otsikot, joiden alle se täytyy koota.



Kuva 7. Teknisen turvallisuuden raportin rakenne ja otsikot. (5, s.45)

3.4.1 Johdanto

Johdannossa luodaan kokonaiskuva mallista, joka sisältää yhteenvedon teknisistä turvallisuusperiaatteista, joihin turvallisuus nojaa ja kuinka laajalti järjestelmän väitetään olevan turvallinen tähän dokumenttiin verraten. Tässä vaiheessa tulee myös osoittaa, mitä standardeja on käytetty mallin teknisen turvallisuuden pohjana. (5, s. 45.)

3.4.2 Oikeanlaisen toiminnan varmistus

Standardin EN 50129 mukaan oikeanlaisen toiminnan varmistuksen tulee sisältää kaikki tarpeelliset todisteet, jotta voidaan esittää järjestelmän oikeanlainen toiminta virheettömässä tilassa määriteltyjen käyttö- ja turvallisuusvaatimusten mukaisesti. Siihen sisältyy

järjestelmäarkkitehtuurin kuvaus, rajapintojen määrittely, järjestelmävaatimusten ja turvallisuusvaatimusten määrittelyn täyttäminen sekä laitteiston ja ohjelmiston oikeanlaisen toiminnan varmistaminen. (5, s. 45.)

Järjestelmäarkkitehtuurin kuvauksessa luodaan yleinen kuva järjestelmän mallista, jotta pystytään esittämään selkeä kuva sen käyttämistä toimenpiteistä ja tekniikoista. Ohjelmisto- ja laitteistosuunnittelussa on kuvattava staattiset ja dynaamiset suunnittelunäkökohdat. Staattisia osia ovat esimerkiksi järjestelmän rakenne sekä hierarkiatasot ja datatyypit ja niiden ominaisuudet. Dynaamisia taas ovat toiminnallisuus ja käyttäytyminen sekä komponenttien välinen datavirta. (4, s.168–169; 5, s. 46.)

Rajapintojen määrittelyssä ensimmäisenä määritellään kaikki sisäiset ja ulkoiset rajapinnat. Ihmisten ja koneiden välisten rajapintojen määrittelyssä otetaan huomioon kolme erilaista rajapintaa. Operaattorin rajapinnoissa kuvataan mekanismit, joilla järjestelmää käytetään operaattoreiden ja suunnitteluhenkilöstön toimesta. Konfiguraation rajapinnoissa kuvataan prosessit, jotka tekninen henkilöstö suorittaa järjestelmän konfiguroimiseksi tietylle rautatielle tai sovellukselle. Kunnossapidon rajapinnoissa kuvataan huoltohenkilöstön rajapinnat, kun he suorittavat eri tason huoltoja. Järjestelmän rajapinnat jaetaan sisäiseen ja ulkoiseen. Sisäiset rajapinnat määrittävät järjestelmän sisäisten asioiden väliset toiminnalliset ja fyysiset rajapinnat. Ulkoiset rajapinnat määrittelevät järjestelmän ja ulkoisten asioiden väliset toiminnalliset ja fyysiset rajapinnat. Ennen kaikkea turvallisuusperustelun tulee määritellä termit toiminnallinen elementti ja fyysinen elementti. Lisäksi sen tulee määritellä kaikki toiminnalliset ja fyysiset elementit järjestelmässä sekä kaikkien sisäisten elementtien väliset rajapinnat. (4, s. 173–174.)

Järjestelmävaatimusten ja turvallisuusvaatimusten määrittelyn täyttämisessä suurin työ on jo tehty osana laatujohtamisen- ja turvallisuusjohtamisen raporttia. Kuitenkin informaatio siitä, miten kyseiset vaatimukset on täytetty, tulee sisällyttää oikeanlaisen toiminnan varmistukseen. Tähän voi liittyä väitteitä ja löytöjä, jotka liittyvät suunnitteluperusteisiin ja ratkaisuihin, analyyseja ja vastaavia laskelmia, testispesifikaatioita, määrityksiä sekä validointia. (4, s. 174–175.)

Laitteiston ja ohjelmiston oikeanlaisen toiminnan varmistamisessa kuvataan laitteisto-arkkitehtuurin osalta, kuinka se saavuttaa vaaditun turvallisuuden eheyden tason, vaatimusten määrittelyn sekä asiaankuuluvien standardien mukaisesti luotettavuuden, saatavuuden, ylläpidettävyyden ja turvallisuuden osalta. Ohjelmiston oikeanlainen toiminta osoitetaan noudattamalla standardin EN 50128 vaatimuksia. Tarkoitus on varmistua siitä, että elinkaariprosessit ja niiden tuotokset ovat sellaisia, että ohjelmisto on määritellyllä turvallisuuden eheyden tasolla ja se on sopiva sen tarkoitettua käyttöä varten. Ohjelmiston arviointia varten tarvittavat dokumentit ovat järjestelmän turvallisuusvaatimusten määrittely, ohjelmiston vaatimustenmäärittely ja mahdolliset muut tukevat arviointia tukevat dokumentit. Standardissa EN 50129 mainitaan muutama asia, joihin tulee kiinnittää erityistä huomiota:

- Laitteiston ja ohjelmiston välinen riippuvuus. Ohjelmiston laitteistovaatimukset tulee dokumentoida.

- Täytyy dokumentoida, että laitteisto täyttää kaikki asiaankuuluvat laitteistovaatimukset.

- Toimintojen järjestys. Suorittaessaan toimintojaan, ohjelmistojärjestelmällä on yksi tai useampi ennalta määritetty toimintajakso. Näiden täytyy olla dokumentoitu esimerkiksi käyttämällä sekvenssikaavioita.

- Omatestit ja tilan seuranta. Suunnittelut testit täytyvät olla suoritettuina, ja niiden pitää osoittaa, että omatestit on suoritettu onnistuneesti ja tilan seuranta toimii tarkoitetusti.

- Tiedonkeruutekniikat. Turvallisuusperustelun tulee esittää todisteet siitä, että järjestelmädata on testattu ja todettu oikeaksi, kaikki anturit toimivat oikein vaaditusti ja järjestelmä lukee tiedot oikein.

- Negaatiomenetelmät. Kuinka järjestelmä menee turvalliseen tilaan virheen jälkeen. Negaatio koostuu kahdesta osasta, virheen tunnistamisesta ja turvalliseen

tilaan menemisestä. Turvallisuusperustelun tulee ottaa kantaa siihen, että määritetyt turvalliset tilat ovat oikeasti turvallisia, ja mekanismit, joilla päästään turvalliseen tilaan toimivat.

Arviointiprosessi tuottaa kolme dokumenttia, jotka ovat ohjelmiston arviointisuunnitelma, ohjelmiston arviointiraportti ja ohjelmiston arvioinnin verifiointiraportti. (4, s. 176–179.)

3.4.3 Virheiden vaikutukset

Virheiden vaikutuksissa esitetään, että järjestelmä pysyy määrätyissä turvallisuusvaatimuksissa satunnaisen laitteistovirheen sattuessa. Koska systemaattinen virhe voi olla vielä olemassa, laatu- ja turvallisuusjohtamisprosesseista huolimatta tulee tämän osion esittää, mitkä tekniset toimenpiteet on tehty, jotta pienennetään tästä johtuva riski hyväksyttävälle tasolle. Osiossa tulee esittää myös, että järjestelmässä olevat virheet, joilla on pienempi SIL-taso kuin kokonaisjärjestelmällä, eivät voi pienentää kokonaisjärjestelmän turvallisuutta. (5, s. 48.)

Standardi EN 50129 velvoittaa käyttämään seuraavia otsikoita:

- Yksittäisten virheiden vaikutukset

Täytyy varmistua siitä, että järjestelmä täyttää THR-arvonsa yhden satunnaisen vian sattuessa. Täytyy myös varmistua siitä, että SIL 3 ja 4 järjestelmät pysyvät turvallisina minkä tahansa yksittäisen virheen vaikutuksen aikana. (4, s. 180.)

- Yksittäisten virheiden tunnistaminen

Ensimmäinen yksittäinen virhe, joka voi olla vaarallinen yksittäin tai yhdistettynä toiseen virheeseen, tulee tunnistaa ja turvallinen tila pakottaa tarpeeksi lyhyessä ajassa, jotta täytetään määritelty laskennallinen turvallisuuden tavoite. (4, s. 183.)

- Tunnistamisen jälkeiset toimet

Ensimmäisen virheen tunnistamisen jälkeen järjestelmän tulee mennä tai jatkaa turvallisessa tilassa olemista. Turvalliseen tilaan tulee päästä tarpeeksi lyhyessä ajassa, jotta täytetään määritetty turvallisuuden tavoite. (4, s. 184.)

- Useiden virheiden vaikutukset

Useat samanaikaiset viat, jotka voivat olla vaarallisia joko suoraan tai yhdistettynä myöhempään vikaan tulee tunnistaa ja turvallinen tila pakottaa tarpeeksi lyhyessä ajassa. Sopivaa käytäntöä, kuten vikapuuanalyysia käyttäen, tulee esittää useiden vikojen vaikutukset. (4, s. 185.)

- Puolustus systemaattisia virheitä vastaan

Laatu- ja turvallisuusjohtamisen toimien lisäksi, joita käytetään ihmisten virheiden minimoimiseen, tekniset toimenpiteet on toteutettava sellaisina, että jos vaarallinen systemaattinen vika olisi olemassa, niin se olisi kohtuudella käytännössä mahdollista estää luomasta hyväksymätöntä riskiä. (4, s. 186.)

3.4.4 Toiminta ulkoisen vaikutuksen alaisena

Tämä kohta esittää, että järjestelmän vaatimustenmäärittelyssä määriteltyjen ulkoisten vaikutusten alaisina toimiessa järjestelmä jatkaa sen määriteltyjen toiminnallisten vaatimusten ja turvallisuusvaatimusten täyttämistä. Turvallisuusperustelu on siis pitävä ainoastaan näiden rajojen sisällä, jotka on määritelty järjestelmän vaatimustenmäärittelyssä. Turvallisuus ei ole taattu näiden rajojen ulkopuolella, ellei ylimääräisiä erikoistoimenpiteitä suoriteta. Kuitenkin, kunhan se on kohtuullisesti toteutettavissa, turvallisuuteen liittyvät järjestelmät tulee suunnitella siten, että ne pysyvät turvallisina, vaikka operoidaan ulkoisen vaikutuksen alaisena määriteltyjen rajojen ulkopuolella. Menetelmät, joilla kestetään määriteltyjä ulkoisia vaikutuksia, tulee kokonaisuudessaan esittää ja perustella. Vaikutukset, jotka tulee ottaa huomioon ovat: (5, s. 49–50.)

- ilmastolliset olosuhteet.

- mekaaniset olosuhteet.

- korkeus
- sähköiset olosuhteet
- suojautuminen luvattomalta käytöltä.

3.4.5 Turvallisuuteen liittyvät käyttöehdot

Suurin osa turvallisuusperustelun väitteistä kohdistuu tuotteen sisäisiin piirteisiin. Lisäksi on olemassa tunnistettuja vaaroja, joiden vaatimuksia ei pysty itse tuotteen sisäisillä ominaisuuksilla pienentämään, vaan tiettyjen vaatimusten noudattaminen tuotteen käytön aikana on pakollista, jotta kyseiset vaarat saadaan siedettävälle tasolle. Nämä vaatimukset ovat turvallisuuteen liittyviä käyttöehtoja (SRAC). Ne ovat dokumentoitava turvallisuusperusteluun ja luovutettava tuotteen käyttäjälle. SRAC:it sisältävät ehdot, joita tulee noudattaa tuotteen käytön aikana turvallisuuteen liittyvistä syistä, jotta vaaroilta vältytään. Ehtojen noudattaminen on käyttäjän vastuulla. On kuitenkin turvallisuuden kannalta vaarallista, jos käyttäjä ei täytä SRAC:ien vaatimuksia. Esimerkiksi käyttäjä ei ymmärrä, miksi SRAC:ien ohjeet ovat tarpeen turvallisuuden kannalta. (13, s. 32–33.)

Usein on mahdollista päättää, voiko muodostettu SRAC ratkaista välttämällä SRAC:ia kokonaan. Tällaiset SRAC:it, jotka olisi voitu välttää, voivat tarkoittaa suuria ponnisteluja ylemmällä järjestelmätasolla. Vältettävät SRAC:it voivat olla myös tarpeettomia ja vaatia kohtuuttomuuksia käyttäjiltä, kun vaadittu järjestelmän tai tuotteen turvallinen käyttö on erittäin laaja ja rajoittava tai jos SRAC:it ovat vaikea tulkita ja niiden määrä hallitsemattoman suuri. Tällä tavoin SRAC:it voivat estää tuotteen tuomista markkinoille. SRAC:it, joilla ei ole todellista merkitystä turvallisuuden kannalta, vaikeuttavat ja haittaavat kohteen käyttöä tarpeettomasti. Siksi tarvitaan lähestymistapoja, jotka tukevat SRAC:ien luomista selkeillä ja tarkoilla kuvauksilla niiden sisällöstä ja selkeyttä niiden turvallisuuden merkityksellisyydestä sekä päätöksiä, missä tapauksissa SRAC:it ovat tarpeellisia ja missä tapauksissa niitä pitäisi välttää ja niiden noudattaminen ilman suuria ponnisteluja on mahdollista. (13, s. 33.)

SRAC:it sisältävät useita etuja tuotteen elinkaaren aikana. Niillä varmistetaan tuotteen turvallinen käyttö määräämällä vaatimuksia, jotka takaavat järjestelmän turvallisen käytön. SRAC:it ovat tärkeitä antamaan käyttäjille selkeät turvallisuuteen liittyvät ohjeet. Näin ollen SRAC:it ovat välttämättömiä turvallisuuden kannalta. (13, s. 33.)

3.4.6 Turvallisuudenhyväksynnän testit ja tulokset

Kaupallisen käytön ja koekäytön aloittamisen edellytys on edeltävien vaiheiden arviontien ja tarkastusten suorittaminen hyväksytysti. Kaupallinen käyttö ja koekäyttö voidaan aloittaa, kun suunnittelun, rakentamisen ja käyttöönoton on todettu olevan vaatimustenmukaisia. Väyläviraston päätöksellä aloitetaan koekäyttö ja kaupallinen käyttö, jos projektille on myönnetty rakentamisenaikainen käyttölupa. Traficom voi kuitenkin vaatia, että kaupallinen käyttö alkaa vasta, kun projekti on saanut Traficomilta käyttöönottoluvan. (6, s. 21.)

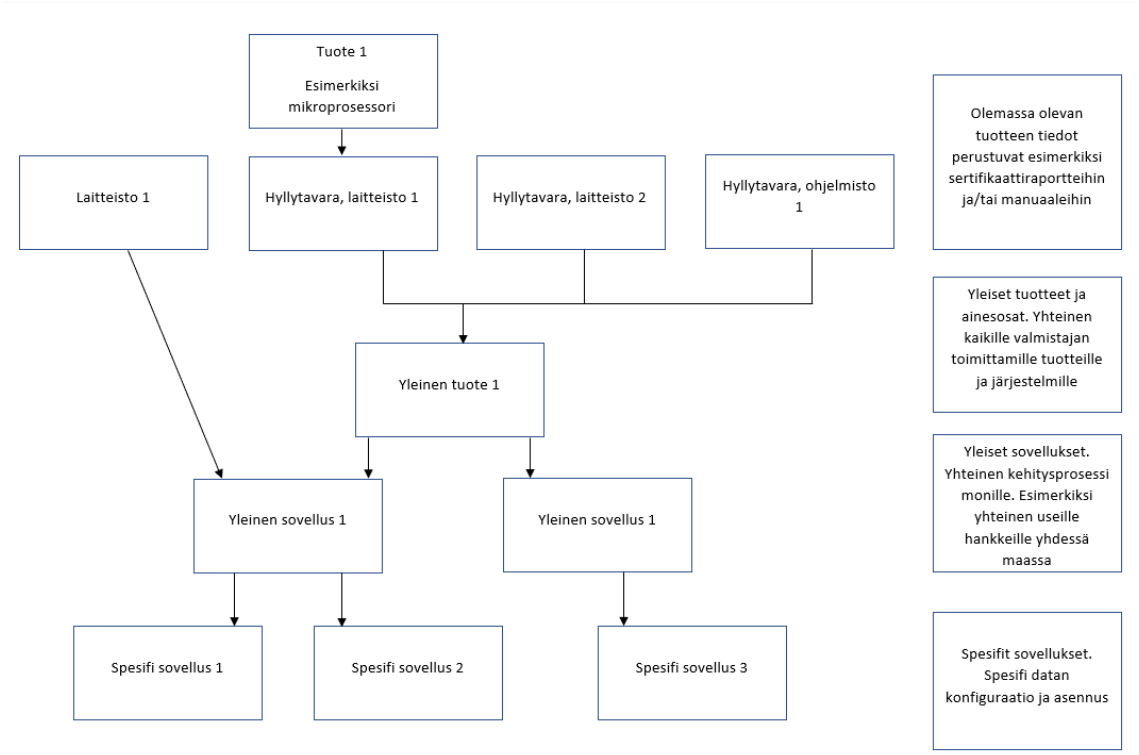
Kaupallisten ehtojen sekä RAMS-vaatimusten eli toimintavarmuuden, käyttövarmuuden, kunnossapidettävyyden sekä turvallisuuden täyttymistä seurataan, kun kaupallinen käyttö on aloitettu. RAMS-vaatimusten toteutumista seurataan tehostetusti koekäyttövaiheessa, ja vaiheen pituus on sovittu Väyläviraston kanssa. Jos teknisiä tai toiminnallisia muutoksia tehdään koekäyttövaiheessa turvalaitejärjestelmään, joka on koekäyttöönotettu, täytyy teknisiä asiakirjoja täydentää. Koekäyttövaihe voidaan todeta hyväksytysti päättyneen, kun Väylävirasto myöntää hakemuksesta ”teknisen käyttöluvan valtion rataverkolle”. Tällöin vaatimusten on todettu täyttyvän. (6, s. 21–22.)

3.5 Liittyvät turvallisuusperustelut

Rajoitukset, oletukset, hyväksyntätila ja mahdollinen käytön rajoittaminen tai turvallisuuteen liittyvien toimintojen ehdot, jotka mainitaan kyseisissä turvallisuusperusteluissa, kootaan yhteen tai kommentoidaan tässä luvussa. Liittyvät turvallisuusperustelut varsinkin yleisen tuotteen tasolla voivat viitata olemassa olevien tuotteiden sertifikaatteihin tai esimerkiksi ”suoraan hyllyltä ostettaviin” ohjelmisto- tai laitteistokomponentteihin, sillä kyseiset sertifikaatit itsessään perustuvat dokumentoituihin todisteisiin. (4, s. 201.)

Yleensä turvallisuusperustelu sisältää viittauksia yleisen tuotteen tai sovelluksen turvallisuusperusteluihin. Liittyvien tuotteiden ja sovellusten versio tulee raportoida. Jos on olemassa eroja tai ristiriitaisuuksia, tarvitaan perustelu eroille tai ylimääräinen verifiointi ja validointi pitää tehdä. Usein mahdolliset käytön rajoitukset ja oletukset mainitaan liittyvissä turvallisuusperustelussa, mutta niitä ei toisteta johtopäätöksissä. Hyväksynnän tila tulee mainita ja liittyviin turvallisuuden hyväksynnän raportteihin tulee viitata. (4, s. 203.)

Kuvassa 8 esitetään erilaisten turvallisuusperustelujen käyttäminen yhdessä olemassa olevien tuotteiden kanssa.



Kuva 8. Yleisen tuotteen, sovelluksen sekä spesifisen sovelluksen suhde ja miten niitä voidaan käyttää yhdessä olemassa olevien tuotteiden kanssa. (4, s.204)

3.6 Turvallisuusperustelun lopputulos

Lopputuloksena vedetään yhteen kaikki todisteet, joita edellisissä turvallisuusperustelun osissa on esitetty, väitetään, että kyseinen järjestelmä on riittävän turvallinen, määriteltyjen käyttöehtojen alaisuudessa. Tarkoitus on esittää pääargumentit järjestelmän turvallisuudesta ja esittää, miten järjestelmän turvallisuus peilautuu aiemmin käsiteltyihin laatujohtamisen, turvallisuusjohtamisen ja teknisen turvallisuuden raportteihin. Päätelmän tulee ilmaista, täyttävätkö tekniset ominaisuudet turvallisuuden vaatimukset ja onko niihin liittyvien turvallisuusperustelujen asettamat ehdot otettu riittävästi huomioon. (4, s. 206.)

4 ISA-tarkastus

Riippumaton turvallisuusarvioija tai -tiimi on riippumaton henkilö tai toimija, joka on nimitetty suorittamaan turvallisuuden arviointi. Turvallisuuden arvioinnin pohjana käytetään standardeja EN 50126, 50128, 50129 ja 50159. Standardin EN 50129 mukaan arvioijan tehtävänä on arvioida, ovatko suunnitteluviranomainen ja validoija luoneet tuotteen, joka täyttää määritellyt vaatimukset ja muodostaa tuomio siitä, onko tuote sopiva sen tarkoitettuun käyttöön. Turvallisuuden näkökulmasta riippumattoman turvallisuuden arvioinnin on annettava arvio järjestelmän turvallisuudesta, sen toiminnasta ja käytöstä. Turvallisuusarviointi voidaan suorittaa turvallisuusperustelun perusteella. Riippumaton turvallisuusarviointi koostuu yleensä turvallisuus- ja laadunvarmistustoimien seurannasta ja sellaisten asioiden osoittamisesta, joita on parannettava. Työn tuloksena on raportteja, joissa on päätelmät ja suosituksia hyväksymisprosesseista ja käyttöehdoista. Tutkittavat järjestelmät ja laitteet rajoitetaan niihin osiin, joihin liittyy turvallisuustoiminto. (4, s. 59–60.)

Turvallisuusarvioija voi olla myös YTM-asetuksen arvioija joissain projekteissa. Turvallisuuden arviointi koskee päätöstä, jonka mukaan kaikki turvallisuuden ehdot on täytetty. Jotta voitaisiin tehdä päätös järjestelmän turvallisuudesta, on tarpeen ottaa huomioon sekä järjestelmä että sen kehitysprosessi. Turvallisuusarvioijan toimiin tulee aina sisältyä läpikäynnit turvallisuusvaatimusten määrittelyjen sopivuudesta, tuotteen kyvystä täyttää kyseiset vaatimukset, turvallisuus- ja laatuorganisaatiosta sekä turvallisuusprosesseista,

jossa tärkeimmät elementit ovat safety plan, vaararekisteri ja turvallisuusperustelu. Turvallisuusarvioinnin suorittamiseen liittyvät toimet ovat pääasiassa asiakirjojen ja tietojen tarkastuksia, turvallisuuteen liittyviä auditointeja, turvallisuustarkastuksia, suunnitteluanalyysejä ja testaustoimien todistamista. Näiden toimien tulokset dokumentoidaan turvallisuuden arviointikertomukseen. Turvallisuuden arviointikertomuksella tarkoitetaan sekä YTM-ISAn yhteenvetoa riskienhallintaprosessin vaatimustenmukaisuudesta, että EN-ISAn yhteenvetoa järjestelmätoteutusprosessin EN-standardien vaatimustenmukaisuudesta. (4, s. 51–52; 6, s. 13.)

5 Yhteenveto

Opinnäytetyön tarkoituksena oli luoda standardien mukainen prosessikaavio, jonka perusteella projektit toteutetaan toiminnallinen turvallisuus huomioiden. Lisäksi tarkoituksena oli luoda dokumenttipohjat systemaattista turvallisuusperustelun laadintaa varten.

Työlle asetetut tavoitteet saavutettiin, joskin aihe oli pakko rajata koskemaan ainoastaan standardin EN 50129 mukaista safety case -työskentelyä. Mahdollista olisi ollut esimerkiksi ottaa mukaan myös järjestelmän elinkaaren tarkempi tutkiminen, joka olisi tosin vaatinut RAMS-osatekijöiden huomioon ottamista, ja näin lisännyt työtaakkaa huomattavasti tai ohjelmistoihin liittyvän standardin EN 50128 tarkempaa huomioimista.

Hankalaa työn tekemisestä teki sen, ettei safety case työskentelyyn ole olemassa valmiita ohjeita. Opinnäytetyössä läpi käydyt standardit osaltaan antavat raamit, joiden sisään turvallisuusperustelu pitää koota, joskin paljon jäi omalta osaltani toivomisen varaan erinäisille tarkennuksille. Standardit eivät kuitenkaan taivu aina samalla tavalla käytännön asioihin. Kaikkeen taipuvaa ohjetta onkin mahdotonta luoda, sillä projektit, joihin turvallisuusperusteluja tarvitaan, voivat olla esimerkiksi kokonaan uuden järjestelmän luomista tai vanhan muuttamista, jotka eroavat luonteeltaan täysin toisistaan.

Opinnäytetyön tuloksena tehtyjen dokumenttien ja kaavioiden hyödyntäminen näkyy toivottavasti tulevaisuudessa systemaattisempana turvallisuusperustelujen laadintana.

Opinnäytetyön tarkoitus on myös antaa jonkinlainen käsitys turvallisuusperustelujen luomisesta ja mitä siihen vaaditaan esimerkiksi projektin henkilöstöltä tai mitä arviointilaitos voi mahdollisesti vaatia yritykseltä.

Tutkimusta voisi jatkaa esimerkiksi käymällä ensin läpi toiminnallisen turvallisuuden kattostandardin IEC 61508 osatekijät läpi, joiden alle rautatieturvallisuuden standardit EN 50xxx kuuluvat. Näin ollen saisi laajemman kuvan prosesseista ja siitä, mitä toiminnallisella turvallisuudella ylipäätään tarkoitetaan ja miten se voidaan saavuttaa.

Lähteet

1 Väylävirasto. 2014. Ratatekniset ohjeet (RATO) osa 6 Turvalaitteet. PDF-tiedosto. Luettu 15.1.2021. https://julkaisut.vayla.fi/pdf8/lo_2014-07_rato6_web.pdf.

2 Maguire, Richard. 2006. Safety Cases and Safety Reports: Meaning, Motivation and Management.

3 Lucic, Ivan. 2015. Risk and Safety in Engineering Processes.

4 Myklebust, Thor; Stålhane, Tor. 2018. The Agile Safety Case.

5 SFS-EN 50129:2018, Railway Applications. Communication, signalling and processing systems. Safety related electronic systems for signalling. Helsinki: Suomen Standardisoimisliitto.

6 Väylävirasto. 2020. Turvalaitejärjestelmien hyväksyntäprosessit. PDF-tiedosto. Luettu 26.1.2021. https://julkaisut.vayla.fi/pdf11/vo_2020-47_turvalaitejarjestelmien_hyvaksyntaprosessit_web.pdf.

7 SFS-EN 50126-1:2017, Railway Applications. The specification and Demonstration of Reliabilty, Availability, Maintainability and Safety (RAMS). Part 1: Generic RAMS Process. Helsinki: Suomen Standardisoimisliitto.

8 SFS-EN 50126-2:2017, Railway Applications. The specification and Demonstration of Reliabilty, Availability, Maintainability and Safety (RAMS). Part 1: Systems Approach to Safety. Helsinki: Suomen Standardisoimisliitto.

9 Smith, David J.; Simpson, Kenneth G. L. 2016. The Safety Critical Systems Handbook : A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance.

10 Väylävirasto. 2020. YTM-asetuksen mukainen riskienhallinta rautatiejärjestelmässä. PDF-tiedosto. Luettu 14.2.2021. https://julkaisut.vayla.fi/pdf11/vo_2020-52_ytm-asetuksen_mukainen_web.pdf.

11 European Railway Agency. 2009. Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation. PDF-tiedosto. Luettu 26.2.2021. https://www.era.europa.eu/sites/default/files/activities/docs/collection_of_ra_ex_and_some_tools_for_csm_en.pdf.

12 Väylävirasto. 2020. Ohje riskienhallinnan menetelmistä. PDF-tiedosto. Luettu 1.3.2021. https://julkaisut.vayla.fi/pdf11/vo_2020-51_ohje_riskienhallinnan_web.pdf.

13 Rabe, Gerd; Buth, Bettina; Seyfarth, Till. 2009. Computer Safety, Reliability, and Security, 28th International Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18.

Väyläviraston riskimatriisi

Väyläviraston riskimatriisin avulla aiheutuvan riskin suuruus voidaan määritellä, ja se voidaan esittää todennäköisyyden ja seurausten vakavuuden yhdistelmänä. Riskimatriisin tuloksena saadaan lukuarvo 1–5, joka kuvaa riskien todennäköisyyttä ja niiden seurausten vakavuutta, jossa 1 on pienin ja 5 suurin.

Väylävirasto
Trafikledsverket

RISKIMATRIISI / RISKIN MERKITTÄVYYDEN ARVIOINTI

	TAPAHTUMAN SEURAUSTEN VAKAVUUS				
Vahinkolaji	**1 Erittäin lieviä / vähäisiä**	**2 Lieviä / vähäisiä**	**3 Vakavia / kohtalaisia**	**4 Suuria**	**5 Erittäin suuria**
Henkilövahinko	Erittäin lieviä loukkaantumisia, sairausloma alle 1 vrk	Lieviä loukkaantumisia, sairausloma alle 14 vrk	Vakavia loukkaantumisia, sairausloma yli 14 vrk	Kuolemantapauksia	Useita kuolemantapauksia
Omaisuusvahinko	Erittäin vähäisiä omaisuus- tai liiketoimintavahinkoja	Vähäisiä omaisuus- tai liiketoimintavahinkoja	Kohtalaisia omaisuus- tai liiketoimintavahinkoja	Suuria omaisuus- tai liiketoimintavahinkoja	Erittäin suuria omaisuus- tai liiketoimintavahinkoja
Toiminnallinen haitta	Haittaa suunnittelun/urakoiden toteutusta Erittäin lieviä vaateita	Haittaa suunnittelun/urakoiden toteutusta Lieviä vaateita	Haittaa suunnittelun/urakoiden toteutusta Kohtalaisia vaateita	Hanke viivästyy kuukauden Suuria vaateita	Hanke viivästyy useita kuukausia Erittäin suuria vaateita
Liikennevahinko	Ei liikennevahinkoa, vain liikennehaittaa	Vähäisiä liikennevahinkoja	Kohtalaisia liikennevahinkoja	Suuria liikennevahinkoja	Erittäin suuria liikennevahinkoja
Ympäristövahinko	Erittäin vähäisiä ympäristö-vahinkoja tai haittaa, erittäin helposti korjattavissa	Vähäisiä ympäristö-vahinkoja, lievää haittaa, helposti korjattavissa	Kohtalaisia ympäristövahinkoja / haittaa, korjattavissa	Suuria ympäristövahinkoja, huomattavaa ja laajaa haittaa, korjattavissa	Erittäin suuria ympäristö-vahinkoja, vakavaa pitkävaikutteista haittaa, vaikeasti korjattavissa

TAPAHTUMAN TODENNÄKÖISYYS
5 Erittäin yleinen Esiintyy ainakin 10 kertaa vuodessa
4 Yleinen Esiintyy ainakin kerran vuodessa
3 Satunnainen Esiintyy ainakin kerran 10 vuodessa tai esiintyy ainakin kerran hankkeen toteutusaikana
2 Harvinainen Esiintyy ainakin kerran 100 vuodessa tai esiintyy ainakin kerran hankkeen käytön aikana
1 Erittäin harvinainen Esiintyy harvemmin kuin kerran 100 vuodessa Teoreettinen, ei tiedetä tapahtuneen rakentamisen tai käytön aikana

	1 Erittäin lieviä/vähäisiä	**2 Lieviä/vähäisiä**	**3 Kohtalaisia**	**4 Suuria**	**5 Erittäin suuria**
5 Erittäin yleinen	Vähäinen	Kohtalainen	Merkittävä	Sietämätön	Sietämätön
4 Yleinen	Merkityksetön	Vähäinen	Kohtalainen	Merkittävä	Sietämätön
3 Satunnainen	Merkityksetön	Vähäinen	Kohtalainen	Kohtalainen	Merkittävä
2 Harvinainen	Merkityksetön	Merkityksetön	Vähäinen	Kohtalainen	Merkittävä
1 Erittäin harvinainen	Merkityksetön	Merkityksetön	Merkityksetön	Vähäinen	Kohtalainen

TOIMENPIDELUOKAT	
Sietämätön	Välittömät toimenpiteet
Merkittävä	Toimenpiteet meneillään olevassa suunnitteluvaiheessa
Kohtalainen	Toimenpiteet suunniteltava
Vähäinen	Seurataan
Merkityksetön	Ei tarvita toimenpiteitä