



SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Niko Myllykoski

Rautateiden turvalaitejärjestelmien toiminnallisen turvallisuuden varmistaminen rakennuttamisessa

Opinnäytetyö

Kevät 2021

SeAMK Tekniikka

Automaatiotekniikan tutkinto-ohjelma



SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Koneautomaatio

Tekijä: Niko Myllykoski

Työn nimi: Rautateiden turvalaitejärjestelmien toiminnallisen turvallisuuden varmistaminen rakennuttamisessa

Ohjaaja: Alpo Anttonen

Vuosi: 2021

Sivumäärä: 45

Tämä opinnäytetyö toteutettiin Welado Oy:lle, työn tilaajana toimi Väylävirasto. Welado on riippumaton rakennuttamisen suunnan näyttäjä ja monipuolisen asiantuntijuuden organisaatio. Opinnäytetyön tarkoituksena oli parantaa toiminnallisen turvallisuuden valvontaa rautateiden liikenteenohjausjärjestelmissä, erityisesti asetinlaitteiden rakentamisessa. Työssä käytettiin standardien määäämiä asetuksia toiminnallisen turvallisuuden parantamiseksi. Lisäksi hyödynnettiin asiantuntijoiden kokemusta kehityskohteiden selvittämiseksi. Työssä tarkennettiin myös standardien asetuksia ja määräyksiä prosessin varmistamiseksi.

Työn teoriaosuudessa esiteltiin käytetyt standardit. Lisäksi teoriassa käytiin läpi yleisesti toiminnallisen turvallisuuden valvontaa ja sen tarkoitusta. Rautateiden turvalaitteita esiteltiin myös teoriassa. Toiminnallisen turvallisuuden valvonnan tämänhetkistä tilannetta rautateiden ohjausjärjestelmissä tarkasteltiin myös teoriaosuudessa.

Lopussa käytiin läpi prosessi, joka saatiin kehitettyä toiminnallisen turvallisuuden parantamiseen rautateiden asetinlaitteiden rakentamiseen. Prosessilla pystytään varmistamaan toiminnallinen turvallisuus koko projektin aikana, eli hankkeen alusta loppuun. Tämä prosessi auttaa rakennuttajia tulevaisuudessa hankkeilla toiminnallisen turvallisuuden varmistamisessa.

¹ Asiasanat: Welado, toiminnallinen turvallisuus, rautatie, asetinlaite, ohjausjärjestelmä, standardi

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Automation Engineering

Specialisation: Machine Automation

Author: Niko Myllykoski

Title of thesis: Ensuring the Operational Safety of Railway Safety Equipment Systems in Construction

Supervisor: Alpo Anttonen

Year: 2021

Number of pages: 45

The thesis was carried by Welado Oy. The work was commissioned by the Finnish Transport Infrastructure Agency. Welado is a distinct indicator of construction and an organization of diverse expertise. The purpose of the thesis was to improve the control of operational safety of railway traffic control systems, especially in the construction of interlocking devices. The standards were used in the work to improve operational safety. In addition, the experience of experts was utilized to identify areas for development. The work also specified the regulations and provisions of the standards to ensure the process.

The theoretical part of the work dealt with the standards that were used. In addition, the theory generally reviewed the control of operational safety and its purpose. The current situation of operational safety control in railway control systems was also examined in the theoretical part. Railway safety devices were also introduced in theory.

In the end a process was reviewed which could be developed to improve operational safety in the construction of railway interlocking devices. The process can ensure operational safety through the project, from the beginning to the end of the project. This process will help developers with their future projects. In addition, possible further developments to ensure operational safety were considered at the end. The last section went through a summary and reflection on the thesis.

¹ Keywords: Welado, operational safety, railway, interlocking, control system, standard

SISÄLTÖ

Opinnäytetyön tiivistelmä	1
Thesis abstract	2
SISÄLTÖ	3
Kuva- ja kuvioluettelo.....	5
Käytetyt termit ja lyhenteet.....	6
1 JOHDANTO	8
1.1 Työn tausta	8
1.2 Työn tavoite	9
1.3 Työn rakenne	10
1.4 Welado Oy	10
2 TOIMINNALLISEN TURVALLISUUDEN VALVONTA.....	12
2.1 Toiminnallinen turvallisuus	12
2.2 Toiminnallisen turvallisuuden todentaminen ja arviointi	13
2.3 Ohjausjärjestelmien toiminnallinen turvallisuus	14
2.4 Toiminnallinen turvallisuus rautateillä	14
3 TURVALAITTEET	17
4 STANDARDIT	25
4.1 SFS-EN 50126	25
4.1.1 SFS-EN 50126-1.....	26
4.1.2 SFS-EN 50126-2.....	27
4.2 SFS-EN 50128	28
4.3 SFS-EN 50129	29
5 KEHITYSKOhteet TOIMINNALLISEN TURVALLISUUDEN VARMISTAMISEKSI.....	30
5.1 Kehityskohteet.....	30
6 PROSESSIN TOTEUTUS	32
6.1 Vaatimusten erittely.....	32

6.2 Riskianalyysi	32
6.3 Yhteys turvallisuusviranomaiseen	33
6.4 Turvallisuusvaatimusten määrittely.....	33
6.5 Suunnitelma vaatimusten määrittelyyn	34
6.6 Suunnittelu	35
6.7 Järjestelmän rakentaminen	35
6.8 Käyttöönottotarkastus.....	37
6.9 Käyttöönoton hyväksyntä	38
6.10Projektin valmistuminen	39
7 LOPULLINEN PROSESSI.....	40
8 YHTEENVETO JA POHDINTA.....	41
LÄHTEET	43

Kuva- ja kuvioluettelo

Kuva 1. Welado Oyj:n logo	11
Kuva 2. Toiminnallisen turvallisuuden elinkaari	13
Kuva 3. Syötteet turvallisuusohjelman rakentumiseen.....	15
Kuva 4. Jalasjärven laitetila	18
Kuva 5. Turvalaitekaappi	18
Kuva 6. Siemens DrS-asetinlaite	19
Kuva 7. Siemens Simis-C-alueasetinlaite, päätietokoneet.....	20
Kuva 8. Baliisi	21
Kuva 9. Opastin	22
Kuva 10. Simis-C-akselinlaskentapiste	23
Kuva 11. Westrace-akselinlaskentapiste	23
Kuva 12. Avainsalpalaitte.....	24
Kuva 13. Turvallisuusvaatimukset	34
Kuva 14. Järjestelmän rakentaminen.....	36
Kuva 15. Valmis prosessi.....	40
Kuvio 1. Käyttöönottotarkastusprosessi	38

Käytetyt termit ja lyhenteet

CSM	Euroopan rautatievirasto on valmistellut common safety methods (CSM) -nimellä tunnetun säädöksen, jossa esitetään prosessi rautatiealalla tapahtuvien turvallisuuteen liittyvien hankkeiden hallinta.
FAT	Factory acceptance test, tehdastestaus, jonka tarkoituksena on todentaa, että ohjelmisto ja laitteisto täyttävät niille asetetut vaatimukset.
ISA	Independent Safety Assessor, yhteisen turvallisuusmenetelmän (YTM) yhteydessä tarkoittaa riippumatonta arviointilais- tosta ja toimivaltaista henkilöä, organisaatiota tai yhteisöä, joka ottaa tehtäväkseen tutkia ja laatia todisteisiin perustuvan arvion siitä, täyttääkö järjestelmä asianmukaisesti sille asetetut turvallisuusvaatimukset.
JIRA	JIRA on tehtävienhallintaohjelmisto. Sen on kehittänyt Atlasian. Sen avulla huolehditaan, että osatehtävät tulevat suoritetuksi ja kokonaisuus valmistuu.
PL	Performance level, suoritustaso. Erillinen taso, jota käytetään määrittelemään turvallisuuteen liittyvältä ohjausjärjestelmän osien kyky suorittaa turvatoiminto ennakoitavissa olosuhteissa.
RAMS	RAMS on luotettavuuden, käytettävyyden, ylläpidettävyyden ja turvallisuuden lyhenne, jota käytetään yleisesti tekniikassa tuotteen tai järjestelmän luonnehtimiseksi.
SIL	Safety integrity level, turvallisuuden eheystaso. Standardien määrittelemä turvallisuustaso.

- SIT** System integration test, systeemi-integroititestausta, tarkoituksena on todentaa eri järjestelmien rajapinnat yhteen- toimivuuden varmistamiseksi.
- SAT** Site acceptance test, käyttöönottotestausta, tarkoitus on varmistaa turvalaitejärjestelmälle asetettujen vaatimusten toteuttaminen lopullisessa konfiguraatiossa sekä toiminta- ja asennusympäristössä sekä varmistua järjestelmän soveltuvuudesta asetettuun tehtävään.
- YTM** YTM-asetus on riskienhallintaa koskevaa yhteistä turvallisuusmenetelmää, josta on annettu asetus. Asetuksen tavoitteena on varmistaa, että rautatiejärjestelmässä tehtävät muutokset eivät heikennä sen turvallisuutta. Euroopan komission antama asetus, asetus koskee kaikkia rautatiejärjestelmän merkittäviä muutoksia.

1 JOHDANTO

Tässä luvussa käydään läpi opinnäytetyön tausta, tavoitteet ja rakenne. Lisäksi tässä luvussa kerrotaan opinnäytetyön toimeksiantajana toimivasta yrityksestä.

1.1 Työn tausta

Tämä työ käsittelee toiminnallisen turvallisuuden valvontaa rautateiden liikenteenohjausjärjestelmissä, erityisesti asetinlaitteiden rakentamiseen perustuen standardeihin. Aihealue on hyvin uusi ja kyseisestä aiheesta tarvitaan lisää tietoa, jotta voidaan parantaa rautateiden liikennöinnin turvallisuutta useiden vuosien ajaksi. Lisäksi tarkoituksena on suunnitella valvontasovellus tai -työkalu, jolla voidaan varmistaa toimiva ja turvallinen prosessi liikennöinnissä.

Turvallisuuden toteutuminen rautateilla vaatii monelta osa-alueelta onnistumista ja tietenkin yhteistyötä eri tahoilta. Rautateilla olevat tekniikat, jotka liittyvät turvallisuuteen, ovat kehittyneet runsaasti vuosien aikana. Tietotekniikkaan perustuvat turvallisuus-, hallinta- ja ohjausjärjestelmät ovat myös lisääntyneet merkittävästi vuosien varrella. (Katajala 2009, 2.)

Kaikkeen, mikä rautateilla liittyy turvallisuuteen järjestelmien hallinnassa ja toteutuksessa, kohdistuu eurooppalaisen lainsäädännön vaatimukset. Nämä vaatimukset on nimetty Rata-laiksi. Näiden erillisten vaatimuksien toteuttamiseksi on laadittu rautatiealan omat turvallisuusstandardit. Nämä standardit määrittelevät menetelmiä turvallisuuden toteutumiseksi.

RAMS (Reliability, Availability, Maintainability, Safety) standardina tunnettu EN 50126 luettelee kaikki muutkin rautatietoimintaan kohdistuvat keskeiset standardit:

- Laatustandardit ISO 9000
- EN 50128, Rautatiesovellukset – Rautateiden ohjaus- ja turvasovelluksien hallinta
- EN 50129, Rautatiesovellukset – Turvallisuuteen liittyvät elektroniset ohjausjärjestelmät, Safety Case
- IEC 60050, sanasto 191 – Riippuvuus ja palvelun laatu

- IEC 61508, Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus
- Euroopan rautatievirasto on valmistellut Common Safety Methods (CSM) -nimellä tunnetun säädöksen, jossa esitetään prosessi rautatiealalla tapahtuvien turvallisuuden liittyvien hankkeiden hallintaan. (Katajala 2009, 2.)

Työ käsittelee rautateiden liikenteenohjausjärjestelmien toiminnallista turvallisuutta standardin IEC 61508 näkökulmasta. Alla on lueteltu standardeja, joita tässä työssä on käytetty tärkeimpinä lähteinä ja tukena:

- SFS-EN50126
- SFS-EN50128 (Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems)
- SFS-EN50129 (Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling)

Toimeksiantajana toimii Welado Oy. Asiakkaana ja työn tilaajana toimii Väylävirasto. Työn tilaaja haluaa kehittää toiminnallisen turvallisuuden valvontaa rautateiden liikenteenohjausjärjestelmissä. Lisäksi Welado Oy haluaa kehittää työstä mahdollisesti uuden palvelun yritykselle. Tarkoituksena on kehittää prosessi, jolla saadaan varmistettua toiminnallinen turvallisuus kaupalliseen liikenteeseen luovutettavilla järjestelmillä.

1.2 Työn tavoite

Tämän työn tavoitteena on:

- Selvittää toiminnallisen turvallisuuden valvonnan teoriaa
- Selvittää, miten kehitetään toiminnallisen turvallisuuden valvontaa
- Kehittää valvontasuunnitelma tai jonkinlainen prosessi, jota voidaan hyödyntää toiminnallisen turvallisuuden valvonnassa standardeja hyväksi käyttäen
- Kehittää uusi palvelu yritykselle

- Turvalaitejärjestelmän turvallisuuden toteutuminen. Prosessilla varmistettava sujuva hanke

1.3 Työn rakenne

Luvussa yksi käsitellään perusasiat työn taustasta, tavoitteista sekä yrityksestä. Tämän jälkeen siirrytään lukuun kaksi, jossa kerrotaan teoriaa toiminnallisen turvallisuuden valvonnasta rautateiden ohjausjärjestelmissä. Luvussa kolme käydään läpi rautateiden turvalaitteita. Luvussa neljä käydään läpi työssä käytettyjä standardeja ja niiden sisältö, eli kerrotaan tiivistetysti, mitä aihealueita ne käsittelevät. Nämä käytetyt standardit ovat saatavilla englanninkielisinä. Luvussa viisi käydään läpi toiminnallisen turvallisuuden kehityskohteita. Kuudennessa luvussa tarkastellaan ja suunnitella vaadittavia toimenpiteitä, joilla pystytään varmistamaan toimiva ja sujuva prosessi kokonaisuudessa uudella hankkeella. Luvussa seitsemän esitellään valmis prosessi. Luvussa kahdeksan käydään läpi yhteenvetoa ja pohdintaa työn kulusta ja lopputuloksesta.

1.4 Welado Oy

Welado on riippumaton rakennuttamisen suunnannäyttävä ja monipuolisen asiantuntijuuden organisaatio. Welado tarjoaa asiakkailleen kattavia asiantuntija-, rakennuttamis-, projektinjohto- ja valvontapalveluita. Toimistoja Weladolla on yhteensä 11 kpl. Päätoimipaikat sijaitsevat Oulussa, Kuopiossa, Tampereella, Helsingissä ja Örnsköldsvikissä (Ruotsi). Työntekijöitä Weladolla on noin 160. (Welado, [viitattu 30.3.2021].)

Weladon päätoimialat ovat:

- ratarakennuttaminen
- tie- ja katurakennuttaminen
- teollisuusrakennuttaminen
- Kiinteistörakennuttaminen

- Muut asiantuntijapalvelut. (Welado, [viitattu 30.3.2021].)

Weladon missiona toimii halu olla vastuullisena edelläkävijänä sekä olla turvallisen ja toimivan tulevaisuuden elinympäristön rakennuttaja. (Welado, [viitattu 30.3.2021].) Kuvassa 1 Welado Oyj:n logo.



Kuva 1. Welado Oyj:n logo. (Welado, [viitattu 30.3.2021].)

2 TOIMINNALLISEN TURVALLISUUDEN VALVONTA

Tässä luvussa käydään läpi toiminnallisen turvallisuuden valvontaa ja sitä, mitä se tarkoittaa. Tässä luvussa on myös tarkoitus tutustua toiminnallisen turvallisuuden valvonnan tämänhetkiseen tilanteeseen rautateillä. Lisäksi käydään läpi prosessia, joka sisältyy turvalaitteiden hankintoihin.

2.1 Toiminnallinen turvallisuus

Toiminnallisella turvallisuudella on tarkoitus suojata ihmisiä, omaisuutta ja ympäristöä. Lisäksi sillä pyritään varmistamaan se, että laite tai järjestelmä toimii oikein kaikissa mahdollisissa tilanteissa, ilman vaaroja. Toiminnallinen turvallisuus on osa kokonaisturvallisuutta. Se liittyy ohjelmoitavaan järjestelmään. Lisäksi se riippuu elektronisen turvallisuuteen liittyvien järjestelmien, teknologian järjestelmien sekä ulkoisten riskien vähentämisen oikeanlaisesta toiminnasta. (Sundquist 2010, 2–13.)

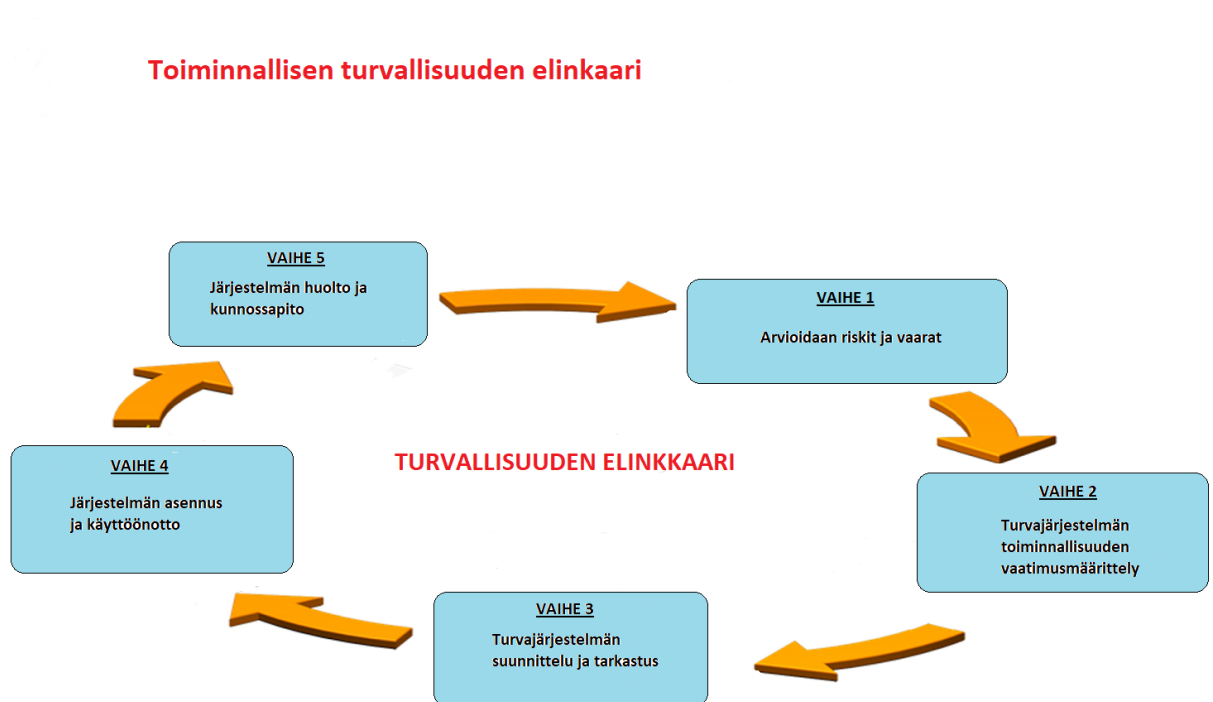
Turvallisuuden varmistamiseksi ei katsota riittäväksi vain testaustoimenpiteitä laitteille, koska järjestelmässä voi olla piileviä ja satunnaisia virheitä. Arvioidessa toiminnallista turvallisuutta kohteessa ensiksi kerätään turvallisuuteen liittyvistä järjestelmistä tai laitteista todistusaineistoa ja tarkastetaan ovatko laitteet vaatimusten mukaisia, ja ovatko ne turvallisia sekä onko riskien vähentämisen eteen tehty riittävästi. Arviointiprosessiin kuuluu myös suunnitelmallisuuden, turvallisuuden hallinnan, laitteiden soveltuvuuden ja turvallisuuden sekä toteuttajien pätevyyden arviointi. Arvioinnin päätteeksi tehdään vielä arviointilausunto, missä otetaan kantaa turva-automaatiojärjestelmän toiminnalliseen turvallisuuteen ja vaatimusten mukaisuuteen. (Tukes 2007, 13.)

Toiminnallinen turvallisuus on laaja käsite, mutta yksinkertaistettuna se tarkoittaa elinkaariajattelun mukaista toimintamallia, jossa jaetaan turvajärjestelmä tai turvalaite eri vaiheisiin koko elinkaarensa ajaksi. Kaikki lähtee vaatimusmäärittelystä, eli mitä toimintoja ja minkälaista vastetta laitteistolta vaaditaan. (Tukes 2007.)

Toiminnallisen turvallisuuden elinkaarella on viisi eri vaihetta:

1. Arvioidaan riskit tai vaarat

2. Turvajärjestelmän toiminnallisuuden vaatimusmäärittely
3. Turvajärjestelmän suunnittelu ja tarkastus
4. Järjestelmän asennus ja käyttöönotto
5. Järjestelmän huolto ja kunnossapito. (Tukes 2007.)



Kuva 2. Toiminnallisen turvallisuuden elinkaari (Tukes 2007.)

2.2 Toiminnallisen turvallisuuden todentaminen ja arviointi

Automaation turvajärjestelmien, turvalaitteiden tai laitekokonaisuuteen kuuluvan sähköisen, elektronisen tai ohjelmoitavan järjestelmän osan arvioinnissa ja toiminnallisen turvallisuuden todentamisessa on oltava perusteellinen, koska kyse on aina lopulta niin henkilö- kuin omaisuus- ja turvallisuudesta (Tukes 2007, 13).

Tästä syystä loppuarviointi on tehtävä asianmukaisesti asiakirjoihin, kuten esimerkiksi vaatimustenmukaisuusvakuutus, jonka avulla vakuutetaan loppukäyttäjälle, että laitteesta on olemassa sitä koskevat direktiivin mukaiset tekniset asiakirjat. Tietysti täytyy olla varmuus kokonaisuuden toimivuudesta. Arviointi tehdään yleensä laitteelle ja sovellukselle. (Tukes 2007, 13.)

2.3 Ohjausjärjestelmien toiminnallinen turvallisuus

Sähköisten/elektronisten/ohjelmoitavien järjestelmien toiminnallinen turvallisuus EN 61508 on turvallisuusperusstandardi, joka käsittelee käyttökohteesta riippumatta sähköisten, elektronisten ja ohjelmoitavien järjestelmien toiminnallista turvallisuutta. Se on keskeinen standardi ohjausjärjestelmien toiminnalliselle turvallisuudelle. SFS-EN 61508 -standardissa määritetään turvallisuusjärjestelmien vaatimukset laitteistoturvallisuudessa. (Hietikko, Malm & Alanen 2009,19.)

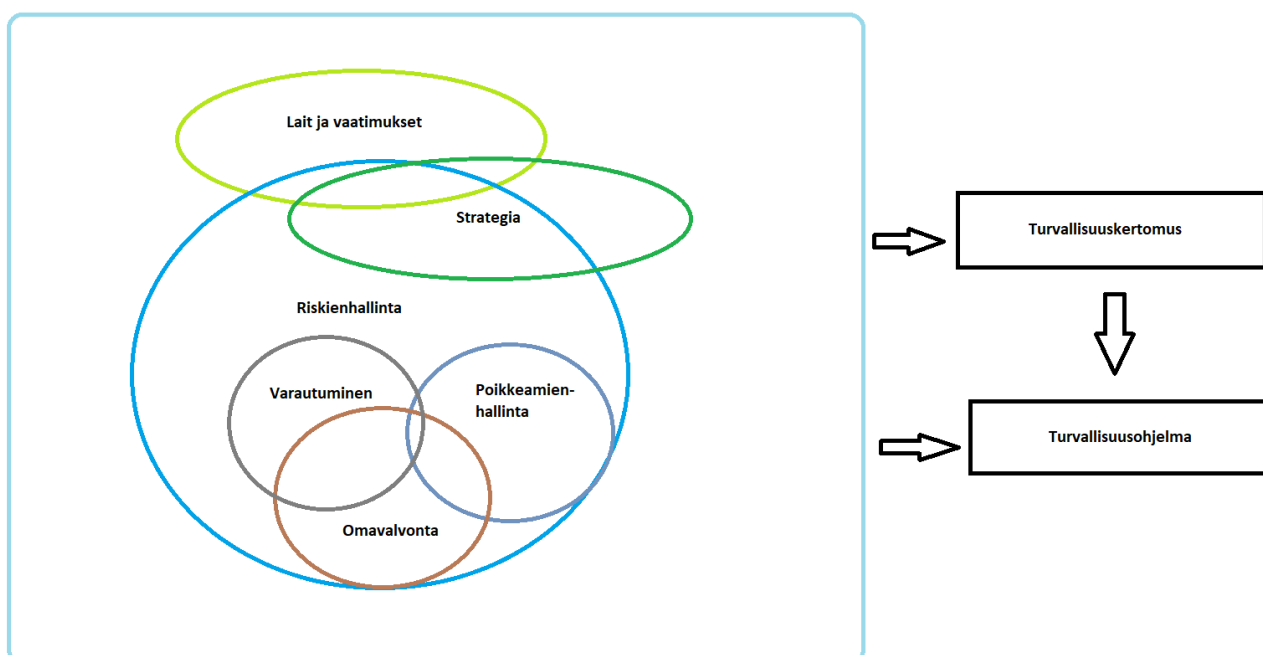
Standardissa ISO 13849-1 ohjausjärjestelmien turvallisuus luokitellaan suoritustason (PL) mukaan. Suoritustaso tarkoittaa sitä, miten hyvin ne toteuttavat turvatoiminnon ja selviävät erilaisista tilanteista. Mitä suuremmat riskit ohjausjärjestelmällä on, sitä korkeamman suoritustason se vaatii. (Hietikko, Malm & Alanen 2009,19.)

2.4 Toiminnallinen turvallisuus rautateillä

Toiminnallinen turvallisuus on osa riskienhallintaa rautateillä. Toiminnallisella turvallisuudella varmistetaan rautateillä järjestelmäteknisesti turvalaitejärjestelmien turvatoiminnoilla laitteiston toimivuus niin, että rataverkoilla on turvallista ja luotettavaa junien liikennöintiä. Rautateillä toiminnallinen turvallisuus kohdistuu ainoastaan tietokonepohjaisiin järjestelmiin. (Väylävirasto 2020d, 23.)

Rautateiden toiminnallinen turvallisuus perustuu lähtökohtaisesti vaarojen tunnistamiseen ja siihen, että riskit saadaan pienennettyä hyväksytylle tasolle turvalaitejärjestelmien turvatoiminnoilla. Toiminnallisesta turvallisuudesta huolehditaan osana turvalaitehankintoja ja kunnossapitoa. Rautateillä tehtävissä turvalaitehankinnoissa toiminnallisen turvallisuuden osalta noudatetaan turvalaitestandardien EN 50126, EN 50128, EN 50129 ja EN 50159

mukaisia menetelmiä. Rele pohjaisissa järjestelmissä noudatetaan standardia EN 50129 soveltuvien osien. (Väylävirasto 2020d, 23.)



Kuva 3. Syötteet turvallisuusohjelman rakentumiseen (Väylävirasto. 2020d.)

Toiminnallista turvallisuutta rautateillä selvitettiin kyselyllä. Kysely lähetettiin 23 asiantuntijalle. Kyselyssä asiantuntijoilta kysyttiin mitä toiminnallinen turvallisuus tarkoittaa, miten turvallisuus toteutuu projekteilla käytännössä, miten todetaan riittävän hyvää toiminnallista turvallisuutta projekteilla ja mitkä ovat merkittävimmät kehityskohteet. Kyselyyn vastasi 7 asiantuntijaa.

Kyselyssä selvisi, että projekteilla toiminnallinen turvallisuus toteutuu käytännössä siten, että ensin määritellään haluttu järjestelmä standardien mukaisilla toimilla ja tarkastuksilla. Lopuksi riippumaton taho arvioi turvallisuustodistelun. Yleisesti ottaen tämä on todettu hyvin toimivaksi projekteilla.

Kyselyssä myös tarkasteltiin erikseen turvalaiteprojekteja. Turvalaiteprojekteissa uuden asennettavan turvalaitteen on täytettävä tietty turvallisuustaso SIL3 tai SIL4. Laitetoimitajalta saatava tekninen ISA-dokumentaatio osoittaa tätä vaatimustenmukaisuuden toteutumista. Kun laite asennetaan uuteen ympäristöön ja kytketään kentällä oleviin

laitteistoihin ja kauko-ohjaukseen, suoritetaan käyttöönottotarkastukset. Käyttöönotossa käyttöönottotarkastaja tekee tarkastuksen, jossa tarkastetaan kaikki elementit ja kulku-
teiden toiminnallisuudet. Tällä varmistetaan, että laite toimii oikein ympäristössään. Tar-
kastajan havaitessa jotain vikaa, se kirjataan ylös ja mahdollisesti kyseiseen paikkaan
asennetaan liikenteen rajoite.

Kyselyssä selvitettiin käyttöönottotarkastuksien nykyistä käytäntöä. Käyttöönottotarkas-
tukset, jotka laitteelle tehdään, ovat monessa osassa. On olemassa FAT eli tehtaan
vastaanottotarkastus, SIT eli systeemi-integrointitestaus ja SAT eli käyttöönottotestaus,
näissä tarkastuksissa tarkastellaan laitteen toimivuutta. Esimerkiksi testivaihe on osa
tarkastusprosessia, testivaihe on liitetty uuteen asetinlaitteeseen, mutta se ei ole rauta-
tieverkossa, vaan irrallaan siitä. Testivaihteella laitetoimittaja voi tehdä jo ennen käyt-
töönottoa testejä. Vaihe on rautateillä turvallisuuskriittinen osa, sen testaukset etukä-
teen testivaihteella ennen käyttöönottoa varmistavat toiminnallista turvallisuutta käyt-
töönotossa.

Nykyistä riskienhallintaa selvitettiin myös kyselyn avulla. Projekteilla tehdään riskienhal-
lintaa mm. YTM, joka tarkoittaa yhteisiä turvallisuusmenetelmiä, joissa arvioidaan käyt-
töönoton ja käytön aikaisia riskejä ja suunnitellaan toimenpiteitä riskien pienentä-
miseksi/poistamiseksi. Toiminnalliseen turvallisuuteen liittyviä asioita ovat riskienhal-
linta, tekninen dokumentaatio, jossa osoitetaan, että laite on vaatimusten mukainen, lait-
teen testaaminen ja koekäyttö testivaihteessa, rajapintojen testaus / riskienhallinta, ja
käyttöönottotestit. JIRA-järjestelmän käyttö siten, että eri osapuolet saavat sieltä infor-
maatiota ominaisuuksista / ongelmista, on ollut toimiva. Myös tieto siitä, jos ongelma on
ratkaistu, menee järjestelmän kautta.

3 TURVALAITTEET

Tässä luvussa on tarkoitus tutustua hieman rautateiden turvalaitteisiin. Turvalaitteilla tarkoitetaan asetinlaitteisiin, suojausjärjestelmiin, varoituslaitoksiin, junien kulunvalvontaan, kauko-ohjaukseen ja laskumäkijärjestelmiin liittyviä laitteita. Nämä kaikki yhdessä muodostavat kokonaisuuden, jota kutsutaan turvalaitejärjestelmäksi. Järjestelmällä varmistetaan sujuva ja turvallinen liikennöinti. Turvalaitejärjestelmän tulee olla sellainen, että yksi järjestelmän vika johtaa koko turvalaitejärjestelmän hallitusti turvalliseen tilaan. (Liikennevirasto 2014, 22.)

Aina uutta järjestelmää rakentaessa on täytettävä Liikenneviraston määrittelemä turvalaitokselta vaadittu turvallisuustaso. Tämä turvallisuustaso on määritetty eurooppalaisen CENELEC:in mukaan. (Liikennevirasto 2014, 22.)

Seuraavassa muutamia turvalaitteita sekä esiteltyä laitetilaa. Turvalaitteet löytyvät ratateknisistä ohjeista (RATO) osasta 6.

Laitetila. Laitetilalla tarkoitetaan tilaa, jossa on sähkölaitteita. Laitetilalla tarkoitetaan mm. relehuonetta, asetinlaite-, tasoristeyslaite-, kuumakäynti-ilmaisilaitostilaa.

Laitetilojen lämpötilan on tärkeä pysyä optimaalisessa tasossa laitteiden toimivuuden kannalta. Aina uutta laitetta lisätessä tulee laitetilan jäähdytyskapasiteetti tarkasteltava uudelleen. (Väylävirasto 2020a, 8.)



Kuva 4. Jalasjärven laitetila

Turvalaitekaappi. Turvalaitekaappiin sijoitetaan turvalaitejärjestelmien komponentit, logiikat ja kaapeloinnit. Turvalaitekaappiin tulee kiinnittää tunnus, joka vasta suunnitelmassa olevaa tunnusta. (Liikennevirasto 2012c, 52.)



Kuva 5. Turvalaitekaappi

Asetinlaite. Asetinlaite on turvalaite, jota käytetään rautatieliikenteen ohjauksessa. Asetinlaitteita käyttää liikenteenohjaaja. Asetinlaitteella asetetaan keskitetysti yhdestä paikasta junan käyttämällä kulkutiellä olevat vaihteet oikeisiin asentoihin ja opastimet ajon salliviin asentoihin. Asetinlaite voi olla joko mekaaninen tai sähköinen. Asetinlaite voi olla myös kauko-ohjattu. Asetinlaitteet ovat tietokoneasetinlaitteita, releasetinlaitteita tai mekaanisia asetinlaitteita. Asetinlaitteella valvotaan junien sijaintia. Niiden avulla myös käännetään ja lukitaan vaihteita. Lisäksi niillä ohjataan opastimia. (Liikennevirasto 2014, 23–25.)



Kuva 6. Siemens DrS-asetinlaite



Kuva 7. Siemens Simis-C-alueasetinlaite, päätietokoneet

Kulunvalvonta (JKV). JKV:n tarkoitus on valvoa junien nopeuksia ja pysäyttää juna tarvittaessa vaaratilanteissa. Tämän järjestelmä koostuu radalle ja vetureihin asennetuista järjestelmistä. Juna saa tietoa radalle olevien baliisien kautta. Näillä tiedoilla saadaan mahdolliset nopeusrajoitukset sekä opastimien tilatiedot, eli onko junalla vapaa kulku raiteella. (Liikennevirasto 2012a, 19.)



Kuva 8. Baliisi

Opastimet. Opastimien tehtävänä on välittää kulkutieto näkyvällä valolla junalle. Opastimet sijaitsevat radan varrella. Opastimien sijoitus tapahtuu niin, että se on esteettömästi nähtävissä veturista. Opastimille on määritelty erilaiset näkemävaatimukset. Opastimia on olemassa erilaisia eri käyttötarkoituksiin. (Liikennevirasto 2014, 26.)



Kuva 9. Opastin

Akselinlaskija. Akselinlaskijoiden avulla lasketaan ohi kulkevien junien akseleita. Junan kulkiessa akselinlaskijan ohi on oltava sama määrä laskettuja akseleita sisään sekä ulos. Laskettujen akseleiden määrän ollessa sama junaradan osuus vapautuu seuraavalle. Laskenta tapahtuu magneetti- tai sähkökentän avulla. Junan vaihtaessa suuntaa pyörän ollessa laskentapisteen päällä on mahdollista, että laskenta menee sekaisin. (Liikennevirasto 2014, 180.)



Kuva 10. Simis-C-akselinlaskentapiste



Kuva 11. Westrace-akselinlaskentapiste

Avainsalpaite. Avainsalpalaitteen tehtävä on suojata vaihteen, pysäytyslaitteen tai raitteensulun varmistuslukon käyttöavainta. Asetinlaite välittää tiedon avainsalpalaitteelle, kun vaihteen kääntäminen on turvallista. Avainsalpaite on sijoitettava mahdollisimman lähelle kohdetta. (Liikennevirasto 2014, 63.)



Kuva 12. Avainsalpaite

4 STANDARDIT

Tässä luvussa käydään läpi työssä käytettyjä standardeja tiivistetysti. Työssä käytetyt standardit on vahvistettu englanninkielisinä ja ne ovat saatavissa ainoastaan englanninkielisinä. Työssä on tarkoitus hyödyntää näitä standardeja ja niiden määrittämiä rajoja toiminnallisen turvallisuuden valvonnassa rautateiden ohjausjärjestelmissä.

4.1 SFS-EN 50126

Standardi on jaettu kahteen osaan EN 50126-1 ja EN 50126-2. Tämä eurooppalainen standardi tarjoaa rautatieliikenteen haltijoille ja rautatieliikenteen toimittajille prosessin, jolla mahdollistetaan RAMS vaatimuksien mukainen toiminta. (SFS-EN 50126 2017, 3-4.)

RAMS-vaatimusten määrittely- ja esittelyprosessit ovat tämän standardin kulmakiviä. Tämä eurooppalainen standardi edistää yhteistä käsitystä ja lähestymistapaa RAMS vaatimuksien hallinnassa. (SFS-EN 50126 2017, 3-4.)

EN 50126 on osa standardin IEC 61508 rautatieliikennesovellusta. Tämän eurooppalaisen standardin vaatimusten täyttäminen yhdessä muiden sopivien standardien vaatimusten kanssa on riittävä sen varmistamiseksi, että standardin IEC 61508 lisävaatimuksia ei tarvitse osoittaa. (SFS-EN 50126 2017, 3-4.)

Turvallisuuden osalta EN 50126 ottaa turvallisuuden näkökulman toiminnallisella lähestymistavalla. (SFS-EN 50126 2017, 3-4.)

Rautatieliikenteen haltijat ja rautatieyritykset voivat soveltaa tätä standardia järjestelmällisesti rautatieliikenteen elinkaaren kaikissa vaiheissa kehittäessään rautatiekohtaisia RAMS-vaatimuksia ja saavuttaakseen näiden vaatimusten noudattamisen. Tämä standardin kehittämä järjestelmätason lähestymistapa helpottaa RAMS-vuorovaikutuksien arviointia rautatieliikenteen sovellusten elementtien välillä, vaikka ne olisivat luonteeltaan monimutkaisia. (SFS-EN 50126 2017, 3-4.)

Standardi edistää rautateiden sidosryhmien välistä yhteistyötä RAMS-vaatimuksien ja rautatieliikenteen kustannusten optimaalisen yhdistelmän. Standardin käyttöönotto tukee

Euroopan sisämarkkinoiden periaatteita ja helpottaa rautateiden yhteen toimivuutta Euroopassa. (SFS-EN 50126 2017, 3-4.)

4.1.1 SFS-EN 50126-1

SFS-EN 50126-standardin osa 1 käsittelee seuraavia seikkoja:

- RAMS-vaatimuksia
- RAMS-elinkaaren yleiset näkökohdat. Tämän osan ohjeita voidaan edelleen käyttää erityisten standardien soveltamiseen.
- Standardi määrittelee:
 - järjestelmän elinkaaren ja sen tehtäviin perustuvan prosessin RAMS-vaatimusten hallitsemiseksi
 - järjestelmällisen prosessin, joka on räätälöitävä tarkasteltavan järjestelmän tyyppin ja koon mukaan sekä RAMS-vaatimusten määrittelemiseksi ja osoittamiseksi niin, että nämä vaatimukset saavutetaan.
- Käsitellään rautatiejärjestelmän erityispiirteitä
- Mahdollistaa RAMS-elementtien välisten ristiriitojen hallinnan
- RAMS-vaatimusten määrittelyyn ja esittelyyn kaikilla rautatieliikennesovelluksilla ja niiden kaikilla tasoilla soveltuvien osien. Määrittelee suuret järjestelmät ja yksilöt ja näiden suurten järjestelmien yhdistetyt osajärjestelmät ja komponentin, mukaan lukien ne, jotka sisältävät ohjelmistoa; erityisesti:
 - uudet järjestelmät.
 - uusiin järjestelmiin, jotka on integroitu olemassa oleviin järjestelmiin, jotka on jo hyväksytty, mutta vain siinä laajuudessa ja sikäli kuin uutta järjestelmää ja uutta toiminnallisuutta integroidaan.
 - mahdollisuuksien mukaan jo olemassa olevien järjestelmien muutoksiin ja laajennuksiin, mutta vain siinä määrin ja siltä osin, kun olemassa olevia järjestelmiä muutetaan. Ei sovelleta mihinkään nykyisen järjestelmän muokkaamattomaan osaan.
- Sovelluksen elinkaaren kaikissa asiaankuuluvissa vaiheissa.
- Rautatieliikenteen haltijoiden ja rautatieyritysten käyttöön. (SFS-EN 50126-1 2017, 5.)

4.1.2 SFS-EN 50126-2

SFS-EN 50126-standardin osa 2 käsittelee seuraavia seikkoja:

- Ottaa huomioon turvallisuuteen liittyvät RAMS-elinkaaren yleiset näkökohdat
- Määrittelee menetelmät ja työkalut, jotka ovat riippumattomia järjestelmän todellisesta tekniikasta ja osajärjestelmistä.
- Tarjoaa:
 - standardin käyttäjälle ymmärrystä järjestelmän turvallisuudesta, joka on avainkonsepti standardissa.
 - menetelmät järjestelmän turvallisuusvaatimuksiin ja niiden eheysvaatimuksiin ja jakaa ne osajärjestelmiin.
 - menetelmät turvallisuuteen liittyvien elektronisten toimintojen turvallisuuden eheystasojen johtamiseen
- Tarjoaa ohjeita ja menetelmiä seuraaville alueille:
 - turvallisuusprosessi
 - turvallisuuden esittely ja hyväksyminen
 - roolien organisointi ja riippumattomuus
 - riskien arviointi
 - turvallisuusvaatimusten määrittely
 - toiminnallisten turvallisuusvaatimusten jakaminen
 - suunnittelu ja toteutus
- Tarjoaa tämän standardin käyttäjälle menetelmät turvallisuuden takaamiseksi, ottamalla huomioon järjestelmän ja sen vuorovaikutukset.
- Antaa ohjeita tarkasteltavan järjestelmän määrittelyssä, mukaan lukien järjestelmän rajapinnat ja vuorovaikutukset sen osajärjestelmiin tai muiden järjestelmien kanssa ja suorittaa riskianalyysin.
- Sovelluksen elinkaaren kaikissa asiaankuuluvissa vaiheissa.
- Rautatieliikenteen haltijoiden ja rautatieyritysten käyttöön. (SFS-EN 50126-2 2017, 6.)

4.2 SFS-EN 50128

SFS-EN 50128-standardi on osa vastaavien standardien ryhmää. Standardi keskittyy menetelmiin, mitä on käytettävä ohjelmistojen tuottamiseksi, jotka täyttävät näiden laajempien näkökohtien asettamat turvallisuusehtojen vaatimukset. (SFS-EN 50128 2017, 7.)

Standardi asettaa joukon vaatimuksia, joita kaikkien rautateiden ohjaus- ja suojaussovelluksiin tarkoitettujen turvallisuuteen liittyvien ohjelmistojen kehittämisen, käyttöönoton ja ylläpidon on täytettävä. Siinä määritellään organisaatorakennetta, organisaatioiden välistä suhdetta ja vastuunjakoa koskevat vaatimukset, jotka liittyvät kehitys-, käyttöönotto- ja ylläpito toimiin. Kriteerit henkilöstön pätevyydelle ja asiantuntemukselle annetaan myös tässä eurooppalaisessa standardissa. (SFS-EN 50128 2017, 7.)

Standardin keskeinen käsite on ohjelmistojen turvallisuuden eheyden taso. Standardi koskee viittä ohjelmiston turvallisuuden eheystasoa, joissa 0 on alin ja 4 korkein taso. Mitä suurempi riski ohjelmistoviasta johtuu, sitä korkeampi on ohjelmiston turvallisuuden eheystaso. (SFS-EN 50128 2011, 7.)

Standardi on yksilöinyt tekniikat ja toimenpiteet ohjelmistojen turvallisuuden eheyden viidelle tasolle. Vaaditut tekniikat ja toimenpiteet ohjelmistojen turvallisuuden eheystasoille 0–4 on esitetty standardin liitteen A normatiivisissa taulukoissa. Tässä versiossa vaaditut tekniikat tasolle 1 ovat samat kuin tasolle 2, ja vaaditut tekniikat tasolle 3 ovat samat kuin tasolle 4. Standardi ei anna ohjeita siitä, mikä ohjelmistojen turvallisuuden eheys on sopiva tietyille riskille. Tämä päätös riippuu monista tekijöistä, mukaan lukien sovelluksen luonteesta, siitä missä määrin muut järjestelmät suorittavat turvallisuustoimintoja, sekä sosiaalisista ja taloudellisista tekijöistä. (SFS-EN 50128 2017, 7.)

Standardien EN 50126-1 ja EN 50129 soveltamisalaan kuuluu määrittellä prosessi, jolla määritetään ohjelmistoille osoitetut turvatoiminnot. SFS-EN 50128-standardi määrittelee tarvittavat toimenpiteet näiden vaatimuksien saavuttamiseksi. (SFS-EN 50128 2017, 7.)

4.3 SFS-EN 50129

SFS-EN 50129 standardia sovelletaan turvallisuuteen liittyviin sähköisiin järjestelmiin (mu-
kaan lukien osajärjestelmät ja laitteet) rautateiden merkinantosovelluksissa. Standardi kos-
kee yleisiä järjestelmiä sekä järjestelmien erityissovelluksia. (SFS-EN 50129 2017, 7-8.)

Standardia sovelletaan vain järjestelmien toiminnalliseen turvallisuuteen. Sitä ei ole tarkoi-
tettu käsittelemään muita turvallisuuden näkökohtia, kuten työterveyttä ja henkilöstön turval-
lisuutta, vaikka toiminnallisen turvallisuuden järjestelmillä voi selvästi olla vaikutusta henki-
löstön turvallisuuteen. Järjestelmäsuunnittelussa on muitakin näkökohtia, jotka voivat vai-
kuttaa myös työterveyteen ja -turvallisuuteen ja niitä tämä asiakirja ei kata. (SFS-EN 50129
2017, 7-8.)

Standardia sovelletaan turvallisuuteen liittyvän elektronisen järjestelmän elinkaaren kaikkiin
vaiheisiin. (SFS-EN50129 2017, 7-8.)

5 KEHITYSKOhteet TOIMINNALLISEN TURVALLISUUDEN VARMISTAMISEKSI

Tässä luvussa on tarkoitus käydä läpi merkittävimpiä kehityskohteita toiminnallisessa turvallisuudessa. Kehitysideat ja kohteet selvisivät kyselyssä, joka pidettiin alan asiantuntijoiden keskuudessa. Vastauksia kyselyssä saatiin hyvin ja kehityskohteet olivat juuri sellaisia mitä tässä opinnäytetyössä on tarkoitus lähteä kehittämään.

5.1 Kehityskohteet

Suurimmiksi kehityskohteiksi nousivat kyselyn perusteella:

- Turvallisuusprosessin luominen
- Erillinen valvoja toiminnallisen turvallisuuden varmistamiseksi
- Asian tiedostaminen omaksi kokonaisuudeksi
- Toimijoiden tietämys ja osaaminen
- Testivaiheen kehitys.

Turvallisuusprosessin luominen nousi esille tutkimuksessa. Turvallisuusprosessilla tarkoitetaan teknisten toimenpiteiden toteuttamista vaaditun turvallisuuden eheystason mukaisiksi järjestelmän, laitteiston ja ohjelmiston osalta. Tällä prosessilla saataisiin enemmän varmuutta kokonaisuudessa toiminnallisen turvallisuuden varmistamiseksi.

Erillinen valvoja toiminnalliselle turvallisuudelle nousi myös esille kyselyssä. Tällaista valvojan roolia on kaavailtu jo pidemmän ajan, mutta varsinaista valvojan roolia ei ole. Valvoja voisi toimia laitetoimittajarajapinnassa ja auttaa yhteistyössä projektin maaliin viemisessä. Tällainen rooli varmasti tulevaisuudessa tulee erikseen hankkeille, mutta lähtökohtaisesti tällä hetkellä sellaista ei ole. Valvoja tarvitsisi laajan koulutuksen rautateiden rakentamisesta ja lisäksi suurta ammattitaitoa turvalaitteista.

Tällä hetkellä YTM-riskienhallinta on keskittynyt käyttöönoton ja käytön aikaisiin riskeihin. Tekninen ISA huolehtii puolestaan laitteen vaatimusten mukaisuuden osoittamisesta. Käyttöönottotarkastaja huolehtii näiden jälkeen, että käyttöönotettu laite täyttää sille asetetut vaatimukset. Yhtenä kehityskohteena tutkimuksessa nähtiin toiminnallisen turvallisuuden ymmärtäminen omaksi kokonaisuudeksi.

Yksi merkittävistä kohteista oli eri toimijoiden tietämys ja osaaminen. Tämä asia ilmeni jo opinnäytetyön alussa, sillä aihe on niin uusi, että siitä ei ole käytännön kokemusta ja osaamista kertynyt tarpeeksi alan ammattilaisille. Toimijoiden tulisi kehittää osaamistaan standardien vaatimuksista ja niiden mukaisten prosessien ja menettelyiden luomisesta sekä vaatimusten mukaan toimimisesta. Tähän sisältyy myös kaikkien standardien edellyttämien vaatimusten mukaisten suunnitelmadokumenttien ja ohjeistusdokumenttien järjestelmällistä tekemistä. Lisäksi muutoksia pitää pystyä hallitsemaan.

Testivaiheen kehitys nousi myös esille kyselyssä. Testivaiheeseen ehdotettiin uusia vaiheita, jotka sisältäisivät myös monipuolisempia testejä eivätkä vain normaaleja testejä. Tämä jälkeen pystyttäisiin kertomaan, onko laitteella tarvetta laajemmalle testille mahdollisten ilmenneiden puutteiden osalta.

Tämän opinnäytetyön tarkoitus on lähteä kehittämään prosessia, joka vastaa toiminnallisen turvallisuuden kehittämiseen jokaisella osa-alueella. Näin pystyttäisiin parantamaan toiminnallista turvallisuutta kokonaisuudessa.

6 PROSESSIN TOTEUTUS

Tässä luvussa on tarkoitus tarkastella ja suunnitella vaadittavia toimenpiteitä, joilla pystytään varmistamaan toimiva ja sujuva prosessi kokonaisuudessa uudella hankkeella. Tämän prosessin avulla on tarkoitus kehittää toiminnallista turvallisuutta rautateillä. Suomessa ei tällä hetkellä ole olemassa tällaista prosessia, jolla toiminnallinen turvallisuus saadaan parannettua korkeammalle tasolle. Tämän luvun alaotsikot ovat siinä järjestyksessä, millä toimiva prosessi saadaan aikaiseksi.

6.1 Vaatimusten erittely

Vaatimusten erittelyssä huomioidaan järjestelmävaatimusten määrittely (SIL4). Määrittelyssä tulee huomioida asetinlaitteiden vaatimukset, kohdemaata ja muut tarvittavat toimenpiteet sekä niiden huomioiminen. Traficom, määrittelee mitä vaatimuksia tulee noudattaa hankkeella. Suomessa vaatimusten erittelyssä hyödynnetään ratateknisiä ohjeita. Lisäksi käytetään asetinlaitteille määrättyjä ohjeistuksia. (Väylävirasto 2020b, 27.)

Vaatimusten erittelyn avulla pystytään varmistamaan, että uuden järjestelmän rakentaminen vastaa annettuja määräyksiä. Määräyksiä toteuduttua pystytään varmentamaan toiminnallista turvallisuutta jo hankkeen alussa.

6.2 Riskianalyysi

On tehtävä riskianalyysi, joka kattaa järjestelmän kehittämisprosessin ja varautuu mahdollisiin riskeihin. Riskianalyysissä on käytävä koko prosessi läpi ja suunnitella mahdolliset toimenpiteet riskien välttämiseksi. Lisäksi sen tulee sisältää valmistelusuunnitelma validointia varten ja sen tulee täyttää vaadittu turvallisuuden eheystaso. Nämä asiat on määritelty standardissa EN 50128. Näiden asioiden varmistuttua voidaan todeta riskianalyysi tehdyksi. (SFS-EN 50128 2017, 56.)

Riskianalyysillä pystytään parantamaan toiminnallista turvallisuutta jo ennen varsinaisia rakennusvaiheita. Sen avulla minimoidaan mahdolliset riskit jo ennen niiden tapahtumista. Riskianalyysi on perustana toiminnallisen turvallisuuden valvonnalle.

6.3 Yhteys turvallisuusviranomaiseen

Riskianalyysin jälkeen otetaan yhteyttä turvallisuusviranomaiseen (Traficom). Tämä taho on vastuussa siitä, että turvallisuuteen liittyvät järjestelmät noudattavat lakisääteisiä turvallisuuden vaatimuksia. Mikäli turvallisuusviranomainen hyväksyy esityksen, päästään etenemään seuraavaan vaiheeseen. Jos järjestelmät eivät noudata lakisääteisiä vaatimuksia tulee, ne korjata säännösten mukaisiksi. (SFS-EN 50128 2017, 13.)

Tässä vaiheessa tulee myös ottaa huomioon muutoksen merkittävyyden arviointi. Tällä tarkoitetaan ehdotetun muutoksen vaikutusta turvallisuuteen. Arvioidaan, onko muutos rautatiejärjestelmään turvallisuuden kannalta merkittävä. Arvion tekee muutoksen ehdottaja ja siinä käytetään YMT-asetuksessa esitettyjä perusteita ja asiantuntijoiden arvioita. (Väylävirasto 2020c, 12.)

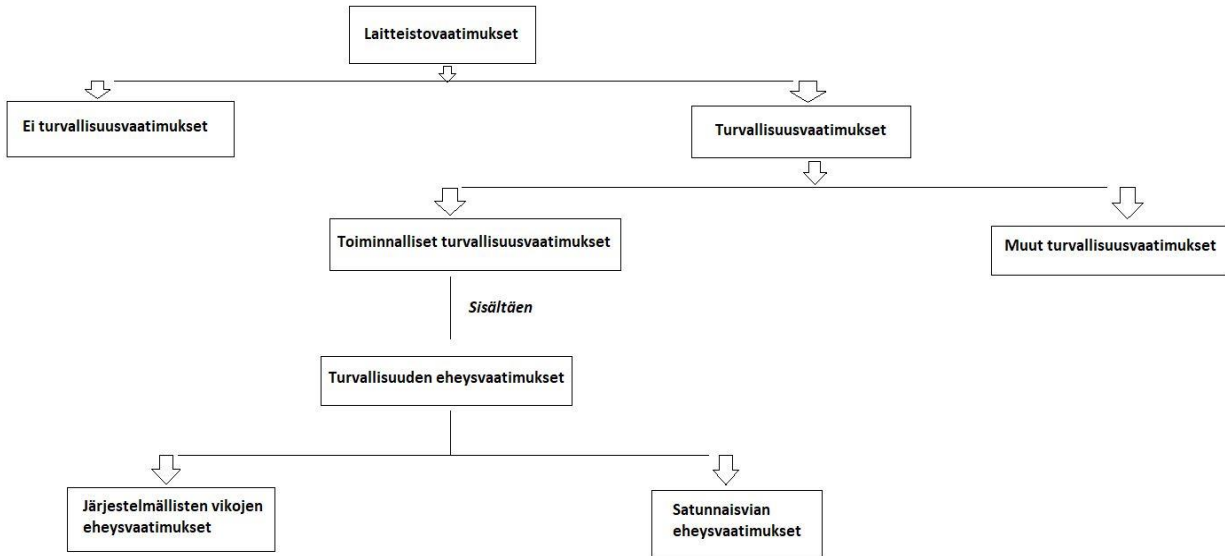
6.4 Turvallisuusvaatimusten määrittely

Järjestelmän turvallisuusvaatimukset erittelevät kaikki osa-alueet erilleen ja määrittävät niille turvallisuuden eheystason. Tarvittaessa oletukset, jotka tukevat turvallisuusvaatimusten määrittelyä, on yksilöitävä turvallisuuteen liittyvinä käyttöolosuhteina tulevaa järjestelmän elinkaaritehtävien käyttöä, huoltoa ja käytöstä poistoa varten. (SFS-EN 50126-1 2017, 60.)

Vaatimusmäärittelyä voidaan tarkastella kahdessa osassa

- Vaatimukset, jotka eivät liity turvallisuuteen
- Vaatimukset, jotka liittyvät turvallisuuteen

Turvallisuuteen liittyviä vaatimuksia kutsutaan turvallisuusvaatimuksiksi. Toiminnalliset turvallisuusvaatimukset kuvaavat todellisia turvallisuuteen liittyviä toimintoja, jotka täytyy suorittaa. Toiminnallisten turvallisuusvaatimuksien tulee kattaa turvallisuuden eheysvaatimukset, jotka määrittelevät kunkin turvallisuuteen liittyvän toiminnon edellyttämän turvallisuuden eheystason. (SFS-EN 50129 2018, 62.)



Kuva 13. Turvallisuusvaatimukset (SFS-EN 50129 2018, 63.)

Vaatimusten määrittelyn avulla pystytään varmistamaan toiminnallista turvallisuutta etukäteen. Toiminnallisen turvallisuuden varmistamiseksi vaatimusten määrittelyllä on suuri rooli. Näiden vaatimusten määrittelyllä varaudutaan tarvittavaan turvallisuuden eheystasoon (SIL).

6.5 Suunnitelma vaatimusten määrittelyyn

Suunnitteluperusteet on asiakirja, johon on koottu hankkeen tilaajan asettamat tavoitteet ja lähtökohdat. Lisäksi siihen on koottu suunnittelua ohjaavat tekniset asiat, joista on tehty päätöksiä joko aiemmissa suunnitteluvaiheissa tai ennen varsinaisen suunnittelutyön aloitusta. Ensimmäiset suunnitteluperusteet hankitaan esiselvitysvaihetta varten. Suunnitteluperusteissa annetaan kuvaus hankkeen tavoitteista ja reunaehdoista. Ratahankkeiden suunnitteluperusteita on kuvattu tarkemmin väylähankkeiden suunnitteluperusteissa. Suunnitteluperusteiden tarkoitus ohjata hankkeen suunnittelua. (Liikennevirasto 2011b, 2–22.)

Rautateillä yleissuunnitteluvaiheessa noudatetaan Liikenneviraston antamia ohjeita suunnitteluperusteiden laatimiseksi. Tarvittaessa suunnitteluperusteisiin tehdään muutos- tai poikkeamaselvityksiä. Suunnitteluperusteet laatii hankkeesta vastaava projektipäällikkö. Laatija vastaa siitä, että on käytetty eri alojen asiantuntemusta suunnitteluperusteiden laatimisessa. Suunnitteluperusteet hyväksytään esittelyssä. (Liikennevirasto 2011b, 2–22.)

Tarkalla suunnitelmavaatimusten määrittelyllä varmistetaan ennen suunnittelua vaadittavat kriteerit suunnitteluun. Määrittelyn tarkoitus on osana suurta kokonaisuutta varmistaa toiminnallinen turvallisuus ennen suunnitteluvaihetta, jolloin suunnittelu saadaan sujuvasti läpi.

6.6 Suunnittelu

Rakentamissuunnittelu on osa rakentamista. Rakentamissuunnitelma määrittelee vaadittavat toimenpiteet, sijainnin, mitoituksen ja järjestelmän rakenteen. Suunnitelma määrittelee myös käytettävät rakennusaineet sekä laatuvaatimukset. Suunnitelmassa tulee esittää työn lopputulos sekä toteutus. (Ratahallintokeskus 2008, 65.)

Rakentamissuunnitelman on täytettävä tietyt vaatimukset:

- Sen perusteella pitää pystyä tehdä tarvittavat päätökset ja hyväksynät teknisistä, toiminnallisista ja taloudellisista asioista.
- Sen pitää olla riittävän yksiselitteinen ja yksityiskohtainen asiakirjaksi.
- Suunnitelmasta pitää saada tarvittavat tiedot työ- ja laatusuunnitelmaa ja rakentamista varten. (Ratahallintokeskus 2008, 65.)

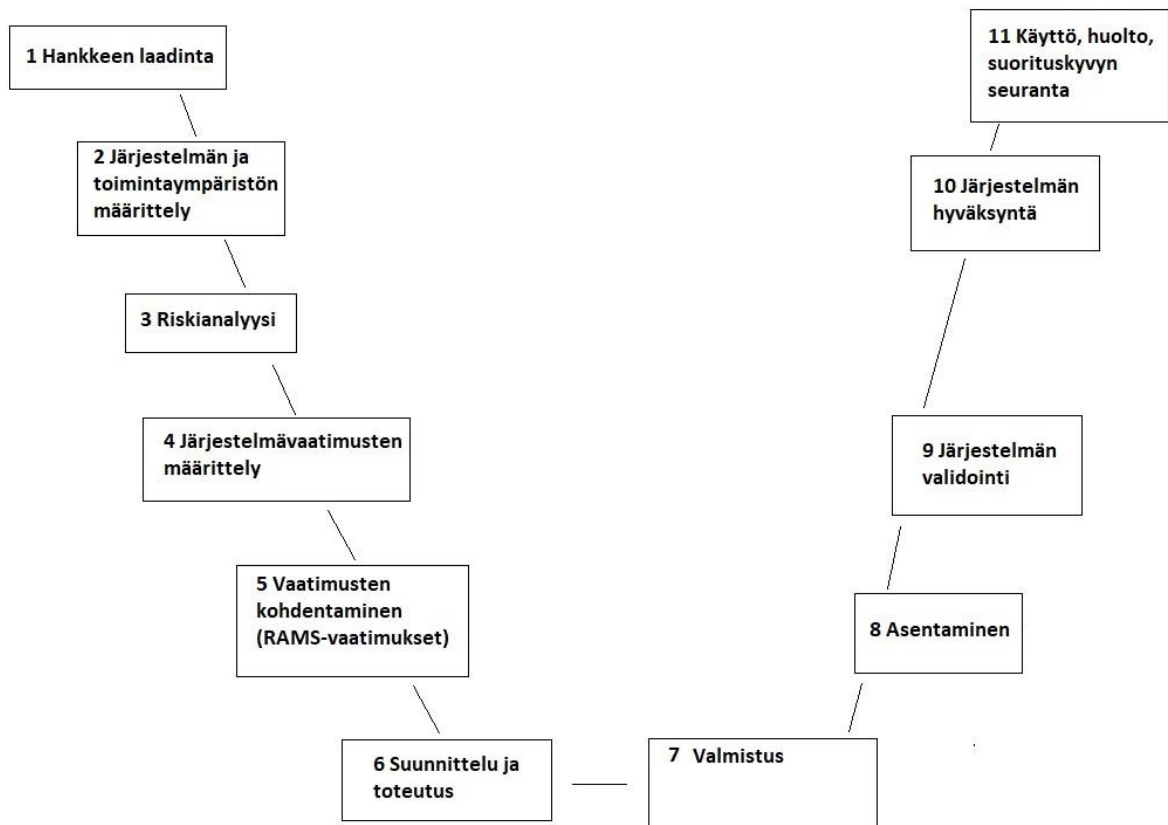
Näiden vaatimuksien avulla ja rakentamissuunnitteluohjeiden perusteella varmistetaan turvallinen rakentaminen. Turvallisesti suoritettu rakentaminen puolestaan varmistaa toiminnallisen turvallisuuden toteutusta hankkeella. Suunnittelulla on merkittävä rooli toiminnallisen turvallisuuden valvonnassa. Hyvällä suunnittelulla minimoidaan mahdolliset riskit rakentamisen aikana sekä järjestelmän käyttöönotossa.

6.7 Järjestelmän rakentaminen

Järjestelmän rakentamisessa tulee ottaa huomioon monia asioita. Muutoksia tehtäessä tulee huomioida, että ne eivät vaikuta turvalaitoksen osaan, jolla liikennöintiä suoritetaan sillä hetkellä. Lisäksi poistuvat turvalaitteet tulee peittää ja poistaa käytöstä niille asetettujen

määräyksien mukaan. Uuden järjestelmän toimintaa on tarkasteltava muutetulta osalta turvalaitteiden käyttöönotossa vaatimusten mukaan. (Liikennevirasto 2014, 186.)

Standardissa SFS-EN 50126-1 (2017, 25-36.) on määritelty, miten uuden järjestelmän rakentamisen tulee edetä. Alla olevassa kuvassa on esitetty, miten rakentaminen etenee. Vaiheiden sisältö on kuvattu standardissa SFS-EN 50126-1 tarkemmin.



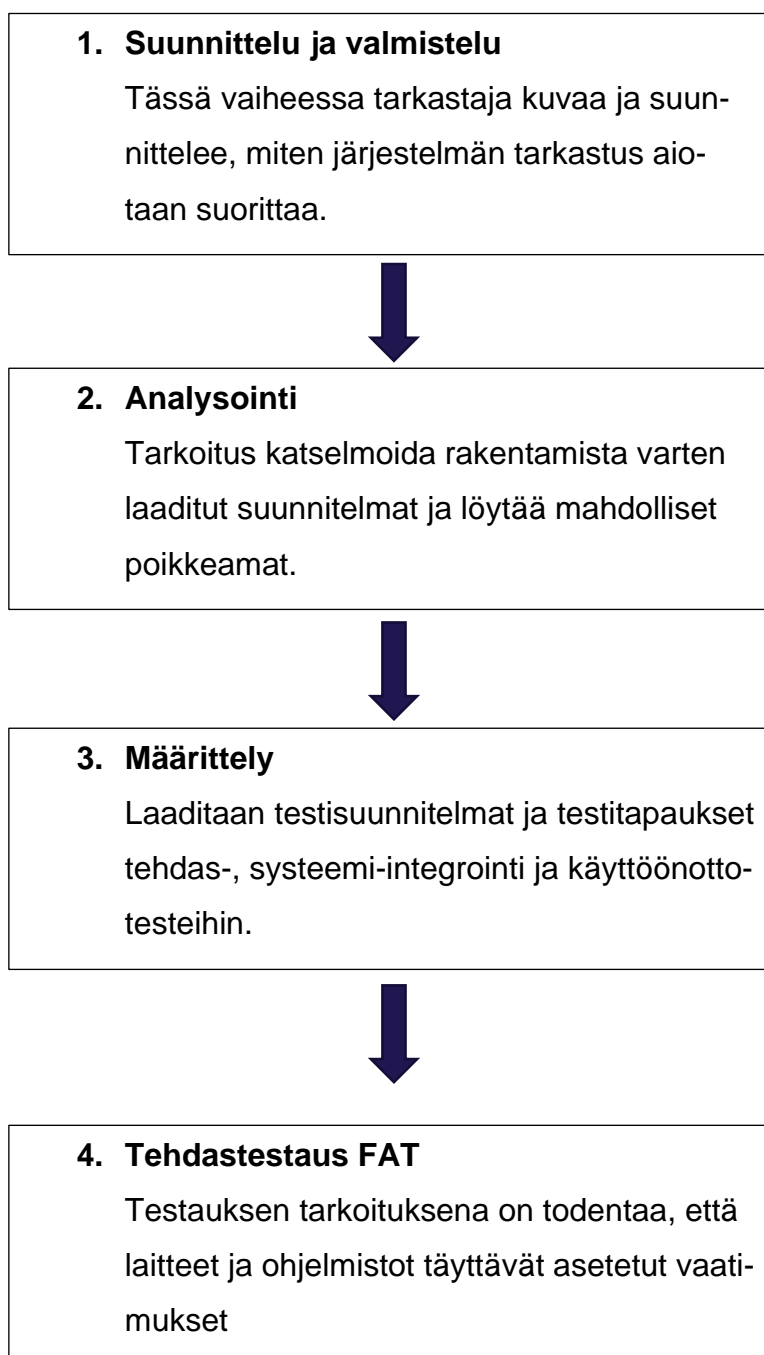
Kuva 14. Järjestelmän rakentaminen (SFS-EN 50126-1 2017, 35.)

Rakentamisen aikana toiminnallinen turvallisuus varmistuu hyvin suunnitellun rakentamisen myötä. Liikennöinti tulee myös huomioida rakentamisvaiheessa, sillä turvalaitteita on käytössä jatkuvasti. Rakentamisvaiheessa toiminnallinen turvallisuus nousee vahvasti esille ja rakentamisen valvonta tulee suorittaa asianmukaisesti. Tällä varmistetaan sujuva ja turvallinen rakentaminen ilman liikennöinnin vaarantamista. Valvonnalla varmistetaan, että

rakentaminen suoritetaan annettujen ohjeiden ja suunnitelmien mukaan. Jatkuva dokumentointi työvaiheista helpottaa toteutuksen tarkistamista.

6.8 Käyttöönottotarkastus

Käyttöönottotarkastus koostuu seitsemästä eri vaiheesta. Turvalaitejärjestelmien käyttöönottotarkastus on kuvattu prosessina. Jokainen prosessi on kuvattu erikseen ja ne sisältävät lähtömateriaalit ja lopputuotteet. Alla on listaus prosessin eri vaiheista ja niiden sisällöstä. Nämä eri vaiheet ovat kuvattuna tarkemmin Liikenneviraston ohjeissa. (Liikennevirasto 2012b, 10–18.)





Kuvio 1. Käyttöönottotarkastusprosessi (Liikennevirasto 2012b, 10-11.)

Käyttöönottotarkastuksella varmistetaan sujuva ja turvallinen liikennöinti rautateillä ennen luovutusta. Tällä prosessilla varmistetaan myös toiminnallista turvallisuutta ja riskien hallintaa jo ennen poikkeamien tapahtumista. Lisäksi mahdolliset viat järjestelmästä saadaan selville näillä testauksilla. Mahdolliset puutteet pystytään korjaamaan hyvissä ajoin.

6.9 Käyttöönoton hyväksyntä

Käyttöönottotarkastuksen jälkeen siirrytään käyttöönoton hyväksyntäprosessiin. Tämän prosessin tarkoitus on varmistaa teknisten järjestelmien vaatimustenmukaisuus ja riskienhallinnan toimenpiteiden ja todenteiden toteuttaminen. Tässä vaiheessa myös todetaan

toiminnallisen turvallisuuden hallinnan eteneminen. Käyttöönoton hyväksynnän jälkeen voidaan hakea käyttöönottolupaa. (Väylävirasto 2020b, 19–20.)

Käyttöönoton hyväksynnän vaatimukseen kuuluu toiminnallisen turvallisuuden varmistaminen. Mikäli käyttöönotto hyväksytään, voidaan todeta, että toiminnallinen turvallisuus on toteutunut sille vaadittavilla tasoilla koko hankkeen aikana.

6.10 Projektin valmistuminen

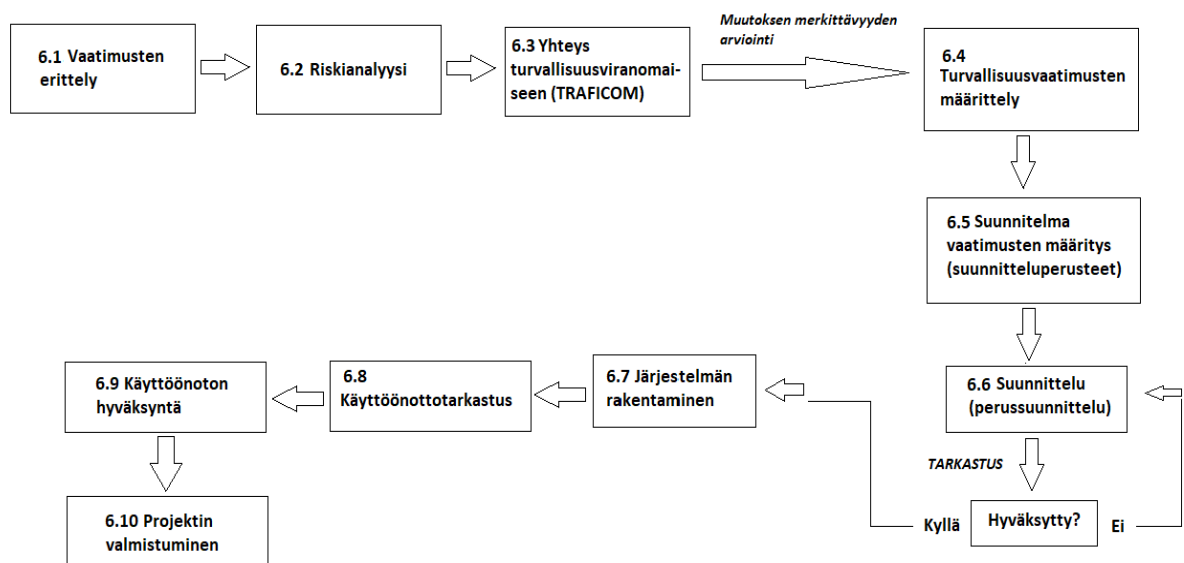
Projektin valmistuttua haetaan uudelle järjestelmälle käyttöönottolupaa. Käyttöönottolupa haetaan Liikenteen turvallisuusvirastolta käyttöönottolupalomakkeella. Tämän lomakkeen liitteenä tulee olla vaadittavat dokumentit, jotka on esitetty Väyläviraston osajärjestelmien käyttöönottolupamenettelyssä. Näiden dokumenttien avulla pystytään arvioimaan kohteen vaatimustenmukaisuus ja turvallisuus. Liikenteenturvallisuusvirastolla on oikeus pyytää lisäselvityksiä hankkeeseen liittyen. Mikäli hanke on monivuotinen ja sisältää useita vaiheita, voidaan käyttöönottolupaa hakea osajärjestelmälle. (Liikennevirasto 2013, 12.)

Projektin valmistuttua toiminnallisen turvallisuuden valvonta jatkuu koko järjestelmän elinkaaren ajan. Toiminnallisen turvallisuuden valvontaa tulee suorittaa niin kauan kuin järjestelmä on käytössä. Näin varmistetaan turvallinen liikennöinti järjestelmän elinkaaren aikana.

7 LOPULLINEN PROSESSI

Tässä luvussa käydään läpi lopullinen tulos prosessista. Luvussa kuusi esitetty prosessin toteutus on tiivistetty tässä luvussa esitettyssä kuvassa 10. Kuvassa 10 esitetyt laatikot on merkitty numerojärjestyksessä luvun 6 mukaisesti. Jokaisen laatikon kuvaaman prosessin liityntäpinnat toiminnallisen turvallisuuden varmistamiseksi on kuvattu luvussa kuusi. Tämä valmis prosessi on suunniteltu ja rakennettu asiantuntijoiden haastattelujen, standardien ja nykyisten käytäntöjen perusteella.

Tällaista prosessia ei ole aiemmin kehitelty rautateiden asetinlaitteiden rakentamiseen. Hankkeilla on olemassa tietty kaava, mutta toiminnallisen turvallisuuden varmistaminen on niissä heikosti esillä. Tällä prosessilla varmistetaan uuden järjestelmän toiminnallinen turvallisuus koko järjestelmän elinkaaren ajalle. Hankkeen edetessä vaihe vaiheelta pystytään todentamaan toiminnallinen turvallisuus uudelle järjestelmälle.



Kuva 15. Valmis prosessi

8 YHTEENVETO JA POHDINTA

Tämän työn tavoitteena oli kehittää toiminnallisen turvallisuuden valvontaa rautateiden ohjausjärjestelmien rakentamisessa. Lisäksi pyrittiin kehittämään prosessi, jolla pystytään varmentamaan toiminnallisen turvallisuuden eteneminen uusilla hankkeilla. Alun teoriaosuudessa käytiin läpi yleisesti toiminnallisen turvallisuuden valvontaa rautateiden ohjausjärjestelmissä. Teoriaosuudessa tutustuttiin myös tässä työssä käytettyihin standardeihin sekä asiantuntijoiden näkemyksiin toimivan prosessin luontiin. Varsinaisen valmiin prosessin valmisteluun käytettiin apuna standardien määräämiä asetuksia sekä tällä hetkellä voimassa olevia määräyksiä. Valmis prosessi on suunniteltu vaadittavien määräyksien mukaan. Kaikki käytetyt määräykset löytyvät erilaisista asetuksista. Nämä määräykset on myös samalla tiivistetty tässä opinnäytetyössä. Lopputulokseksi saatiin toimiva prosessi, joka varmistaa toiminnallisen turvallisuuden uusilla hankkeilla.

Yritys pystyy jatkossa hyödyntämään tätä opinnäytetyötä uusilla hankkeilla. Tätä prosessia käyttämällä varmistetaan toiminnallinen turvallisuus hankkeen jokaisessa vaiheessa. Lisäksi yritys pystyy hyödyntämään opinnäytetyön teoriaosuutta uusien hankkeiden valmisteluun, koska tässä työssä määräykset ja asetukset on tiivistetty yhdeksi kokonaisuudeksi. Ne ovat helposti löydettävissä tästä työstä. Yrityksen asiakkaat saavat varmistuksen siitä, että toiminnallinen turvallisuus on otettu huomioon hankkeen jokaisessa vaiheessa.

Tulevaisuudessa olisi mielenkiintoista selvittää, miten prosessi toimii käytännössä uusilla hankkeilla ja saadaanko konkreettisia tuloksia aikaiseksi. Toiminnallisen turvallisuuden valvonta on myös haasteellinen, koska siitä ei kokemusta ole saatu kerättyä vielä tarpeeksi. Toiminnallisen turvallisuuden tarkempi tutkiminen mahdollisesti olisi myös mielenkiintoista jatkoa ajatellen. Tulevaisuutta ajatellen mahdollisesti toiminnallisen turvallisuuden valvontaa voisi lähteä kehittämään sille tehdyn sovelluksen avulla.

Työn teoriaosuus oli helposti selvitettävissä sillä standardit ja muut lähteet sisälsivät paljon tietoa asioista, jotka liittyvät toiminnallisen turvallisuuden valvontaan. Aiheen kuitenkin ollessa hyvinkin uusi aiheutti omia ongelmiaan prosessin kehittämiseen. Tällaista prosessia ei Suomessa ole, joten jatkossa tapahtuva kehitys on mahdollista. Olisi varmasti ollut mielenkiintoista testata tätä prosessia käytännössä ja analysoida saatuja tuloksia tähän

opinnäytetyöhön. Tätä pohjaa on kuitenkin helppo kehittää tulevaisuudessa paremmaksi käytännön oppien kautta.

Opinnäytetyön yhtenä tarkoituksena oli kehittää mahdollisesti valvontasovellus tai -työkalu, jolla olisi voitu valvoa toiminnallisen turvallisuuden valvontaa. Tämä osa kuitenkin jäi opinnäytetyöstä pois, koska prosessin suunnittelu todettiin paremmaksi vaihtoehdoksi. Prosessi itsessään toimii tietynlaisena työkaluna, jolla varmistetaan toiminnallisen turvallisuuden valvontaa rautateiden ohjausjärjestelmissä. Hankkeen edetessä prosessin mukaisesti ja sen määräyksiä hyödyntäen varmistetaan toiminnallinen turvallisuus.

Rakennuttajan näkökulmasta tällä prosessilla helpotetaan uusien hankkeiden valmisteluja. Prosessi myös helpottaa urakoitsijaa ja tilaajaa. Hankkeen mennessä prosessin mukaan varmistetaan toiminnallinen turvallisuus jokaisella osa-alueella.

LÄHTEET

Hietikko, Malm & Alanen. 2009. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. [www-dokumentti]. [Viitattu 22.12.2020]. Saatavissa: <https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2009/T2485.pdf>

Karllson, E. 2020. Regional Manager. Welado Oy. Kokous 10.2.2020.

Katajala, M. 2009. Onko monimutkaistuva rautatieympäristö uhka turvallisuudella? Esi-
telmä RATA 2010 seminaarissa. [www-dokumentti]. [Viitattu 26.11.2020]. Saatavissa:
http://www.safetyadvisor.fi/Download/Matti_Katajala_RATA2010.pdf

Liikennevirasto. 2011a. Tie- ja ratahankkeiden suunnitelmien käsittelyohje. [www-doku-
mentti]. Saatavissa: https://julkaisut.vayla.fi/pdf3/lo_2011-25_tie_ja_ratahankkeiden_web.pdf

Liikennevirasto. 2011b. Väylähankkeiden suunnitteluperusteiden menettelykuvaus. [www-
dokumentti]. [Viitattu 4.3.2021]. Saatavissa: https://www.doria.fi/bitstream/handle/10024/121823/lo_2011-24_978-925-255-062-0.pdf?sequence=1&isAllowed=y

Liikennevirasto. 2012a. Ratatekniset ohjeet (RATO) osa 10 Junien kulunvalvonta JKV. [www-dokumentti]. [Viitattu 15.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf3/lo_2012-09_rato10_jkv_web.pdf

Liikennevirasto. 2012b. Turvalaitejärjestelmien käyttöönottotarkastusohje. [www-doku-
mentti]. [Viitattu 17.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf3/lo_2012-07_turvalaitejarjestelmien_kayttoonottotarkastusohje_web.pdf

Liikennevirasto. 2012c. Varoituslaitoksen tekniset toimitusehdot. [www-dokumentti]. [Vii-
tattu 14.4.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf3/ohje_2012_varoituslaitosten_tekniset_web.pdf

Liikennevirasto. 2013. Rautateiden osajärjestelmien käyttöönotto-ohje. [www-dokumentti]. [Viitattu 17.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf3/lo_2013-24_rautateiden_osajarjestelmien_web.pdf

Liikennevirasto. 2014. Ratatekniset ohjeet (RATO) osa 6 Turvalaitteet. [www-dokumentti]. [Viitattu 11.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf8/lo_2014-07_rato6_web.pdf

Ratahallintokeskus. 2008. Radan suunnitteluohje. [www-dokumentti]. [Viitattu 16.3.2021].
Saatavissa: https://julkaisut.vayla.fi/pdf4/rhk_b20_radan_suunnitteluohje.pdf

- SFS-EN 50126-1. 2017. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process. Helsinki: Suomen standardisoimisliitto.
- SFS-EN 50126-2. 2017. Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Systems Approach to Safety. Helsinki: Suomen standardisoimisliitto.
- SFS-EN 50128. 2011. Railway Applications – Communication, signalling and processing systems – Software for railway control and protection systems. Helsinki: Suomen standardisoimisliitto.
- SFS-EN 50129. 2018. Railway Applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. Helsinki: Suomen standardisoimisliitto.
- Sundquist, M. Ei päiväystä. Toiminnallinen turvallisuus. [www-dokumentti]. [Viitattu 26.11.2020]. Sundcon Oy. Saatavissa: https://www.automatioseura.fi/site/assets/files/1431/iec61508_m_sundquist1.pdf
- Teknologian tutkimuskeskus VTT. 2009. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. [www-dokumentti]. Saatavissa: <https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2009/T2485.pdf>
- TUKES. 2007. TUKESOPAS. [www.dokumentti]. Turvatekniikan keskus. [Viitattu 21.12.2020]. Saatavissa: <https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0>
- Väylävirasto. 2021. Rautatieohjeet. [www-dokumentti]. Saatavissa: https://julkaisut.vayla.fi/pdf7/rautatieohjeet_web.pdf
- Väylävirasto. 2020a. Radan laitetilojen sähköliittymien hankinta ja tekninen toteuttaminen. [www-dokumentti]. [Viitattu 11.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf11/vo_2020-31_radan_laitetilojen_web.pdf
- Väylävirasto. 2020b. Turvalaitejärjestelmien hyväksyntäprosessit. [www-dokumentti]. [Viitattu 16.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf11/vo_2020-47_turvalaitejarjestelmien_hyvaksyntaprosessit_web.pdf
- Väylävirasto. 2020c. YTM-Asetuksien mukainen riskienhallinta rautatiejärjestelmässä. [www-dokumentti]. [Viitattu 16.3.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf11/vo_2020-52_ytm-asetuksen_mukainen_web.pdf

Väylävirasto. 2020d. Rautatietojärjestelmien turvallisuusjohtamisjärjestelmä käsikirja (RTJJ). [www-dokumentti]. [Viitattu 5.1.2021]. Saatavissa: https://julkaisut.vayla.fi/pdf11/rtjj_kasikirja_5.10.2020.pdf

Väylävirasto. 2019. Ratasuunnitelma. [www-dokumentti]. Saatavissa: https://julkaisut.vayla.fi/pdf11/vo_2019-03_ratasuunnitelma_sisalto_web.pdf

Welado. Ei päiväystä, yritys. [Verkkosivu]. Helsinki: Welado. [Viitattu 30.3.2021] Saatavissa: <https://www.welado.fi/yritys/>