



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MIKA PIETIKÄINEN

STANDARDIN ISO 26262 ASETTAMAT VAATIMUKSET AJONEU-
VON TUOTEKEHITYKSEEN

Diplomityö

Tarkastaja: professori Jouni Kivistö-
Rahnasto

Tarkastaja ja aihe hyväksytty

Teknisten tieteiden tiedekuntaneu-
voston kokouksessa 1. helmikuuta
2017

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO

Konetekniikan koulutusohjelma

MIKA PIETIKÄINEN: Standardin ISO 26262 asettamat vaatimukset ajoneuvon tuotekehitykseen

Diplomityö, 59 sivua, 3 liitesivua

Elokuu 2017

Pääaine: Turvallisuustekniikka

Tarkastaja: professori Jouni Kivistö-Rahnasto

Avainsanat: ISO 26262, toiminnallinen turvallisuus, tuotekehitys

Ajoneuvojen monimuotoisuus ja kompleksisuus on kasvanut huomattavasti viimeisten vuosikymmenien aikana ja niihin on tullut paljon sähköisiä ja ohjelmoitavia komponentteja. Näillä komponenteilla on saatu lisättyä ajoneuvojen toiminnallista turvallisuutta, mutta vanhojen vaatimusten ja säädösten soveltaminen niihin on hankalaa. Uusia säädöksiä, kuten standardi ISO 26262, on kehitetty, jotta uusille sähköisille ja ohjelmoitaville järjestelmille tai turvallisuuskriittisille järjestelmille on yksityiskohtaisia vaatimuksia sekä hyväksymiskriteerejä.

Tämän opinnäytetyön tarkoituksena on tutkia standardia ISO 26262 ja kartoittaa sen asettamia vaatimuksia tuotekehitykseen. Tutkimuksen perusteella analysoidaan tarvittavia muutoksia kohdeyrityksen nykyiseen tuotekehitysprosessiin ja tarjotaan muutosehdotuksia standardin noudattamiseksi. Analysoinnissa käytetään apuna yrityksen suunnittelemaa jarrujärjestelmää, jonka avulla voidaan verrata toteutuneita suunnitteluperusteita standardin vaatimuksiin.

Työ jakaantuu kolmeen pääosaan. Ensimmäisessä osassa perehdytään työn taustalla olevaan teoriaan, kuten säädöksiin, tyyppihyväksyntään sekä lakeihin. Ensimmäisessä osassa perehdytään myös työssä tarkasteltavaan standardiin. Toisessa osassa kuvataan kohdeyrityksen tuotekehitysprosessia ja käytössä olevia suunnittelumalleja. Tässä osassa perehdytään myös työssä käytettävään jarrujärjestelmään. Kolmannessa osassa kuvataan analyysi, sen tuloksia sekä muutosehdotuksia löydetyille eroavuuksille.

Työn tuloksina löydettiin kohteita, jotka on muokattava, mikäli standardia ISO 26262 halutaan noudattaa. Kohteita löydettiin jokaiselta tarkasteltavalta osa-alueelta ja ne jakautuivat eri kriittisyystasoisille. Muutokset toteuttamalla yritys voi toimia standardin mukaisesti ja tuotekehitysprosessia saadaan paremmaksi sekä järjestelmällisemmäksi.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY

Master's Degree Programme in Mechanical Engineering

MIKA PIETIKÄINEN: Standard ISO 26262 requirements on product development of vehicles

Master of Science Thesis, 59 pages, 3 Appendix pages

August 2017

Major: Safety Engineering

Examiner: Professor Jouni Kivistö-Rahnasto

Keywords: ISO 26262, functional safety, product development

Diversity and complexity of vehicles has risen substantially in the last decades and the use of electrical and programmable components has become more common. These components have helped to raise the vehicles functional safety, but the use of old legislation is difficult with new components. New laws and standards, such as ISO 26262, have been compiled to give detailed requirements and approval criteria to these new safety related components.

The purpose of this theses is to study the ISO 26262 standard and analyze its requirements to product development. Based on this information required changes to the present product development process are analyzed. Change proposals are given to comply with the standards requirements. A host company developed brake system will be used in the analysis to compare current development practices with the standards' requirements.

The thesis is divided into three main parts. First, the theory such as vehicle directives, type approval and legislation are depicted. Thereafter, on the second part the host company's product development process and design principles are described. In the second part, the brake system is also illustrated thoroughly. In the third part the analyze, its results and given change proposals are described to found differences.

As the results of this thesis, some parts were found that need to be changed to comply with the standard ISO 26262. Changes were found on all analyzed sections and they were categorized based on their criticality. By carrying out the changes the company can comply with the standard and the product development process will be better and more systematic.

ALKUSANAT

Tämä diplomityö toteutettiin kohdeyrityksen halusta tutkia ja parantaa nykyisiä toimintatapoja. Diplomityön ohjaajana toimi yrityksen puolelta Anneli Hiltunen ja tarkastajana oli professori Jouni Kivistö-Rahnasto.

Haluan kiittää mahdollisuudesta tehdä työ mielenkiintoisesta aiheesta sekä kiittää kaikkia kohdeyrityksen edustajia joiden avulla työ on toteutettu ja jotka antoivat hyviä ohjeita ja kommentteja. Erityiset kiitokset Anneli Hiltuselle, joka toimi työn ohjaajana sekä antoi rakentavia kommentteja ja ohjeita. Haluan myös kiittää professori Jouni Kivistö-Rahnastoa työhön liittyvistä ohjeista sekä palautteista kirjoitusprosessin aikana. Lopuksi haluan kiittää perhettäni ja tyttöystävääni, jotka ovat olleet tukena opiskelujeni aikana.

Tampereella, 14.8.2017

Mika Pietikäinen

SISÄLLYSLUETTELO

1.	JOHDANTO	1
2.	TAUSTA JA TEORIA	3
2.1	Ajoneuvodirektiivit	3
2.2	Tyyppihyväksyntä	4
2.3	IEC 61508 – Toiminnallinen turvallisuus	5
2.3.1	Pääprosessit	5
2.3.2	SIL-eheystasot	7
2.4	ISO 26262 Road vehicles – Functional safety	8
2.4.1	Standardin pääprosessit	9
2.4.2	ASIL-luokitus	11
2.4.3	Tuotekehitys	12
2.4.4	Systemitaso	13
2.4.5	Laitetaso	13
2.4.6	Ohjelmistotaso	14
2.4.7	Tukiprosessit	14
3.	TYÖN KOHDE JA TUTKIMUKSEN OSATEHTÄVÄT	16
3.1	Työn kohde	16
3.2	Työn keskeiset osatehtävät	16
3.2.1	Nykyisen tuotekehityssyklin selvittäminen	17
3.2.2	Tarkasteltavan jarrujärjestelmän suunnittelun kuvaus	17
3.2.3	Nykytila-analyysi	18
3.2.4	Kohteiden priorisointi ja muutosehdotukset	18
3.3	Tuotekehityssykli ja yleinen tuotekehitysprosessi	18
3.3.1	Tuotekehityksen kulku	19
3.3.2	Iteraatiopohjainen kehityssykli	20
3.3.3	IMS-järjestelmä	21
3.3.4	Työpohjat	21
3.4	Ohjelmistokehitysprosessi	21
3.5	Jarrujärjestelmän kuvaus	24
3.5.1	Laitteisto	24
3.5.2	Ohjelmisto	25
3.5.3	Suunnittelussa noudatetut periaatteet	27
4.	NYKYTILA-ANALYYSI TOIMINNAN JA STANDARDIN VAATIMUSTEN VÄLILLÄ	29
4.1	Turvallisuuskulttuuri	29
4.2	Turvallisuuden erot ja uudet osiot	30
4.2.1	Käytännöt	30
4.2.2	Dokumentit	31
4.3	Laitteiston erot ja uudet osiot	32
4.3.1	Käytännöt	32

4.3.2	Arkkitehtuurikuvaukset ja systeemisuunnittelu	34
4.3.3	Dokumentit.....	36
4.4	Ohjelmistojen erot ja uudet osiot	37
4.4.1	Käytännöt.....	37
4.4.2	Arkkitehtuurikuvaukset ja systeemisuunnittelu	38
4.4.3	Testaus, verifiointi ja validointi	39
4.4.4	Dokumentit.....	40
4.5	Yleisiä muutoksia.....	41
4.5.1	Käytännöt.....	41
4.5.2	Dokumentit.....	42
4.5.3	Käytössä olevat ohjelmistot	42
5.	TULOSTEN TARKASTELU.....	44
5.1	Työn kohteiden selvitys	44
5.1.1	Tuotekehityssykli.....	44
5.1.2	Jarrujärjestelmä	45
5.2	Nykytila-analyysi	45
5.2.1	Turvallisuus.....	46
5.2.2	Laitteisto.....	47
5.2.3	Ohjelmistot.....	48
5.2.4	Yleiset osat.....	49
5.3	Muutoskohteiden priorisointi	50
5.4	Vaadittavat toimenpiteet	51
5.5	Muutosten aikataulutus	52
5.6	Tutkimuksesta saatu uusi tieto	53
5.7	Käytännön vaikutukset.....	53
5.8	Tulosten luotettavuus sekä käytettävyys.....	53
6.	JOHTOPÄÄTÖKSET	55
6.1	Turvallisuus.....	55
6.2	Standardin vaatimukset	55
6.3	Löydetyt eroavuudet.....	56
6.4	Standardin ulkopuoliset havainnot.....	56
	LÄHTEET.....	58

LIITE A: ASIL-Luokituksen määrittelyt

LYHENTEET JA MERKINNÄT

ABS	<i>Antilock Brake System</i> , lukkiutumattomat jarrut
ASIL	<i>Automotive Safety Integrity Level</i> , standardissa ISO 26262 käytettävä turvallisuuden eheystaso
IEC	<i>International Electrotechnical Commission</i> , kansainvälinen sähköalan standardointiorganisaatio, joka hallinnoi ja laatii sähkö- ja ohjelmistoalaan liittyviä standardeja
ISO	<i>International Organization for Standardization</i> , kansainvälinen standardointijärjestö, joka hallinnoi ja laatii standardeja
PL	<i>Performance Level</i> , Standardissa ISO 13849 käytetty menetelmä vaadittavan turvatoiminnon eheystason määrittelyyn
S/E/OE elementti	Sähköinen ja/tai Elektroninen ja/tai Ohjelmoitava Elektroninen elementti
SIL	<i>Safety integrity level</i> , standardissa IEC 61508 käytettävä eheystaso
Toiminnallinen turvallisuus	Toiminnallinen turvallisuus on tuotteen tai järjestelmän kokonaisturvallisuuden osa, joka riippuu systeemin tai komponenttien oikeasta toimivuudesta
TTY	Tampereen teknillinen yliopisto
QM	<i>Quality Management</i> , ASIL-luokituksen alin taso jolloin riski voidaan mitätöidä laaduntarkkailun avulla
Verifiointi	Verifiointilla varmistetaan, että suunniteltava tuote tai järjestelmä täyttää sille asetetut vaatimukset ja että se sopii käyttötarkoitukseensa

1. JOHDANTO

Sähköiset, elektroniset ja ohjelmoitavat elektroniset laitteet (S/E/OE) ovat kehittyneet nopeasti viimeisten vuosikymmenien aikana ja niiden käyttö on kasvanut monilla eri aloilla. Myös ajoneuvoteollisuudessa on otettu käyttöön yhä enemmän S/E/OE järjestelmiä, jotka auttavat ajoneuvon hallinnassa sekä lisäävät toiminnallista turvallisuutta. Toiminnallisella turvallisuudella tarkoitetaan turvallisuuden osa-aluetta, joka riippuu systeemin tai laitteen oikeasta toiminnollisuudesta annetuilla syötteillä. Vanhoja lakeja ja säädöksiä on hankala soveltaa S/E/OE järjestelmien toiminnalliseen turvallisuuteen, koska säädöksiä ja vaatimuksia laadittaessa S/E/OE elementtejä ei ollut laajassa käytössä, eikä niitä ole voitu huomioida säädöksiä laatiessa.

Uusien lakien, asetusten ja standardien tarkoituksena on tarjota S/E/OE laitteiden valmistajille ohjeita ja vaatimuksia turvallisen tason saavuttamiseksi. Laitekohtaisten säädösten ja vaatimusten avulla valmistajien on helpompaa varmentaa ja todentaa laitteiden sekä järjestelmien turvallisuus, koska niille on valmiiksi asetettu tarkat turvallisuusvaatimukset. Lakien ja standardien antamat vaatimukset on myös hyvä ottaa huomioon mahdollisimman aikaisessa vaiheessa tuotekehitystä, jolloin tarvittavat muutokset ovat helpompia sekä halvempia tehdä.

Ajoneuvojen komponenttien ja järjestelmien, kuten jarrujen ja ohjauslaitteiden valmistajilta vaaditaan aikaisempaa enemmän varmennuksia laitteiden turvallisuudesta. Omat turvallisuusselvitykset sekä vakuudet turvallisuustoimenpiteistä eivät riitä, vaan asiakkaat vaativat standardien noudattamista ja varmentamista. Standardeja noudattamalla valmistajat voivat osoittaa tuotteiden täyttävän vaaditut turvallisuustasot sekä olevan yleisellä teknologian tasolla. Standardeja noudattamalla voidaan myös saada markkinaetua kilpailijoihin sekä helpottaa vastuukysymyksissä osoittamaan laitteen toiminnollisuutta. Kohdeyrityksessä ei ole aiemmin tehty työn kaltaista tutkimusta, joten se toimii pohjana tarvittaville muutoksille sekä niiden aikatauluttamiselle.

Tämän työn päätavoitteena on saada tarkka kuvaus standardin ISO 26262 edellyttämistä lisäyksistä tuotekehitysprosessiin sekä niiden vaatimista muutoksista. Työssä keskitytään toimintaprosessien muutoksiin, eikä tarkastella mahdollisia laitteisiin liittyviä muutostarpeita. Tarkoituksena on perehtyä ajoneuvojen toiminnallisen turvallisuuden standardin ISO 26262 vaatimukseen tuotekehityksen osalta sekä heijastaa niitä nykyiseen toimintaan. Tässä diplomityössä vastataan kahteen tutkimuskysymykseen:

1. Mitä lisäyksiä ja muutoksia tuotekehitysprosessiin on tehtävä standardin noudattamiseksi?

2. Miten toimintaprosesseja on muutettava?

Lähtötilanteessa on nähtävissä tarve standardin noudattamiselle, jonka seurauksena standardin asettamia vaatimuksia kartoitetaan ja tarkastellaan kehitysmahdollisuuksia standardin osa-alueilla. Nykyiseen toimintaan perehdytään nykytila-analyysillä, jonka kohteena on yleinen tuotekehityssykli sekä ohjelmiston tuotekehitys. Nykytila-analyysissä käytetään apuna yrityksessä kehitettyä jarrujärjestelmää, koska se kuuluu standardin piiriin. Analyysin pohjalta laaditaan suunnitelma tarvittaville muutoksille ja niiden käyttöönotolle. Työ jakautuu kolmeen osatehtävään:

1. Nykyisen tuotekehityssyklin selvitys
2. Tarkasteltavan jarrujärjestelmän suunnittelun kuvaus
3. Nykytila-analyysi toimintaprosessien ja standardin vaatimusten välillä

Työssä keskitytään standardin ISO 26262 ensimmäiseen kuuteen osaan, koska ne sisältävät vaatimuksia tuotekehitykselle ja jälkimmäiset osat keskittyvät tuotantoon sekä käytöstä poistoon. Työ on rajattu, jotta tuotekehityksestä ja sen muutoksista saadaan tarkempi kuvaus.

2. TAUSTA JA TEORIA

Toiminnallinen turvallisuus on yksi osa laitteen tai systeemin kokonaisturvallisuutta, joka yleensä keskittyy S/E/OE ohjelmistoon. Toiminnallisen turvallisuuden tavoitteena on laskea riskit siedettävälle tasolle tunnistamalla vaaralliset tilanteet sekä olosuhteet ja estää niiden syntyminen (Functional safety). Toiminnallista turvallisuutta sisältävät laitteet ovat hyvin kriittisiä, koska niiden vikaantuminen voi estää järjestelmää menemästä turvalliseen tilaan vaaratilanteessa. (Foord et al. 2011)

Toiminnallisen turvallisuuden perustana on järjestelmällinen suunnittelu sekä toimien verifiointi ja dokumentointi. Jokaiselle kohdalle asetetaan tarkat vaatimukset edeltävistä toimista sekä mitä kyseisen kohdan jälkeen on oltava valmiina. Nämä toimet dokumentoidaan ja verifioidaan ohjeiden mukaan, jolloin minimoidaan systemaattisten vikojen mahdollisuus järjestelmässä tai komponentissa. Toiminnalliseen turvallisuuteen asetetut vaatimukset tulevat yleensä standardien sekä asetusten kautta. Näitä vapaaehtoisia vaatimuksia noudatetaan, koska niiden avulla on huomattavasti helpompaa todentaa ajoneuvon tai sen osan tyyppihyväksyntävaatimukset. Tyyppihyväksyntää vaaditaan direktiiveissä, joita vaaditaan markkinoille tuomiseksi. (Brown 2000)

Laitteiden ja systeemien monimutkaisuus sekä tarve toteuttaa useita turvallisuustoimenpiteitä hankaloittavat mahdollisten vaaratilanteiden selvittämistä sekä toiminnallisen turvallisuuden laatimista. S/E/OE laitteistoille on useita eri lakeja ja standardeja, joista ensimmäisiä on toiminnallisen turvallisuuden standardi IEC 61508. Monille aloille, kuten junateollisuuteen, lääketieteeseen sekä ajoneuvoteollisuuteen on kehitetty omia tarkempia standardeja tämän standardin pohjalta. Ajoneuvoteollisuuteen kehitetty standardi ISO 26262 on johdettu standardin IEC 61508 pohjalta. Kohdistettujen standardien käyttö on helpompaa ja niissä voidaan käsitellä kyseiseen teknologiaan liittyviä tunnetuimpia riskitekijöitä. (IEC 2015)

Ajoneuvojen toiminnallisessa turvallisuudessa on useita haasteita, joista monet aiheutuvat järjestelmien ja laitteiden kasvavasta monimutkaisuudesta. S/E/OE laitteilla muodostetaan erilaisia turvallisuustoimintoja, jolloin on mahdotonta testata ja määrittää kaikki mahdolliset vikaantumistavat. Järjestelmällinen ja laadukas suunnitteluprosessi takaavat, että vaaralliset vikaantumiset saadaan poistettua tai hallittua niiden esiintyessä. (International Electrotechnical Commission 2011)

2.1 Ajoneuvodirektiivit

Ajoneuvojen ja niiden osien valmistajien on noudatettava EU-alueella vallitsevia direktiivejä, jotta tuotteita voidaan tuoda myyntiin. Direktiivien vaikutusalue koskee vain EU-alueen markkinoita, mutta ne antavat hyvän pohjan myös sen ulkopuolelle tapahtuvaan

myyntiin. Direktiivit kattavat esimerkiksi ajoneuvojen ja niiden osien valmistusta, varustelua, rekisteröintiä sekä henkilö- ja tavaraliikennettä. Direktiivien kautta ajoneuvojen valmistajien täytyy tyyppihyväksyttää ajoneuvot sekä niihin suunniteltavat osat. Yrityksessä ajoneuvojen ja niiden järjestelmien suunnittelussa on alusta asti kiinnitettävä huomiota turvallisuuteen sekä toiminnallisten kohtien toimivuuteen mikä helpottaa tyyppihyväksynnän hakemista. (Liikenteen turvallisuusvirasto 2016)

Ajoneuvojen sekä niiden osien valmistajien kannalta tärkeimmät kohdat direktiiveissä ovat ajoneuvon rakennetta ja varusteita koskevia. Turvallisuuskriittisiin osiin vaikuttavia direktiivejä ovat esimerkiksi Asetus moottoriajoneuvojen ja niiden osien yleiseen turvallisuuteen liittyvistä tyyppihyväksyntävaatimuksista (661/2009) sekä Puitedirektiivi moottoriajoneuvojen ja niiden osien hyväksymisestä (2007/46/EY). Direktiivit antavat tarkennettuja ohjeita, kuinka valmistajien tulee toimia, jotta tuotteet voidaan hyväksyttää. Hyväksyntä toteutetaan yleisesti tyyppihyväksynnän avulla, jolle on erilaisia metodeja tuotteen laajuudesta sekä turvallisuuskriittisyydestä riippuen. (Liikenteen turvallisuusvirasto 2016)

2.2 Tyyppihyväksyntä

Tyyppihyväksyntä ei ole osa toiminnallista turvallisuutta, mutta tyyppihyväksyntää vaaditaan ajoneuvojen komponenteilta ja järjestelmiltä ennen kuin ne voidaan tuoda markkinoille. Tyyppihyväksynnän toteuttaa hyväksytty taho, joka tarkastaa, että tuotteelle asetetut turvallisuus, ympäristö sekä tuotannon vaatimukset täyttyvät. Komponenttihyväksynät sekä ajoneuvon kansallisen tyyppihyväksynnän Suomessa myöntää Trafí. Tyyppihyväksyntä vaaditaan direktiiveissä, joita on noudatettava ennen kuin uusi tuote voidaan tuoda markkinoille. Myös sotilaskäyttöön tulevat tuotteet, kuten ajoneuvot sekä erikoisajoneuvot on tyyppihyväksytettävä, mutta tällöin hyväksynnän suorittaa puolustusvoimien Pääesikunnan teknillinen tarkastusosasto. (Ajoneuvolaki 2002)

Vaadittava tyyppihyväksyntämenettely riippuu siitä, onko hyväksynnän kohteena komponentti vai koko ajoneuvo. Komponenttihyväksyntää voidaan hakea täyttämällä EY-direktiivin tai E-säännösten asettamat vaatimukset. Tyyppihyväksyntätesteissä tuotteen valmistaja on vastuussa hyväksyntämenettelyjen tekijöistä sekä vaatimustenmukaisuudesta. Tyyppihyväksynnässä käytetään testejä varmistamaan esimerkiksi jarrujen riittävä tehokkuus pysäyttämään ajoneuvo eri nopeuksista. Mikäli valmistaja on tehnyt omia testejä, joita käytetään apuna hyväksynnässä, niistä on tarjottava dataa, josta käy ilmi vaatimusten täyttyminen. (Puitedirektiivi 2007/46/EY)

Ajoneuvovalmistajat valmistavat yleensä useita prototyyppejä tyyppihyväksyntätestauksiin, jotta testaukset eivät viivästyä ajoneuvon tuomista markkinoille. Ajoneuvoista testataan esimerkiksi valojen toimivuus, jarrujen tehokkuus, ohjattavuus, törmäyksen aiheuttamat vahingot sekä pakokaasut. Järjestelmät voidaan testata ja hyväksyttää erikseen, joka helpottaa ja nopeuttaa tyyppihyväksyntää. Komponentteja ja järjestelmiä voidaan

tämän jälkeen käyttää ja myydä, mutta mikäli niiden toiminnallisuuteen tehdään muutoksia, tulee tyyppihyväksyntä tehdä uudelleen. (European Commission 2016)

2.3 IEC 61508 – Toiminnallinen turvallisuus

S/E/OE laitteiden toiminnalliseen turvallisuuteen alettiin kiinnittää huomiota 80-luvulla, kun niiden käyttö alkoi yleistyä. Laitteiden ja järjestelmien valmistajilla tai käyttäjillä ei ollut apuna kunnollisia standardeja tai lakeja joiden avulla toiminnallista turvallisuutta olisi voitu parantaa tai varmentaa järjestelmällisesti. Valmistajat sovelsivat muita standardeja ja lakeja, mutta suuri osa varmentamisesta ja turvallisuuden todentamisesta ei ollut validoitua puutteellisten vaatimusten takia. IEC 61508 standardia alettiin kehittää 80-luvun puolella välissä ja ensimmäiset osat siitä julkaistiin vuonna 1998. Standardi on tehty yleiskäyttöiseksi ja sen avulla toiminnallisen turvallisuuden perusvaatimukset saadaan täytettyä. Standardi on edelleen laajasti käytössä ja sitä käytetään pohjana toiminnallisen turvallisuuden määrittämiseksi tai tilanteissa joissa spesifejä standardeja ei ole saatavilla. (Exida 2006)

Standardissa on seitsemän osaa, joissa annetaan vaatimuksia S/E/OE laitteille ja systeemeille. Standardissa jaotellaan järjestelmien ja komponenttien turvallisuustasot SIL-eheystasojen avulla (safety integrity level). SIL-luokitus kertoo, kuinka hyvin riskejä on redusoitu turvallisuustoiminnoilla sekä mikä on laitteen tai systeemin hyväksyttävä vikaantumisväli. Standardissa on myös ohjeita sekä esimerkkejä sen noudattamiseen käytön helpottamiseksi. (Foord et al. 2011)

Standardin IEC 61508 ja sen johdannaisten tärkeä piirre on laitteilta ja systeemeiltä vaadittava turvallisuuselinkaari, joka toimii teknisenä viitekehysenä tarpeellisille toimenpiteille toiminnallisen turvallisuuden varmistamiseksi. Tämä elinkaari varmistaa, että turvallisuustoimenpiteet otetaan huomioon suunnittelussa, käyttöönotossa sekä normaalissa toiminnassa (IEC 61508 2011). Kun turvallisuus otetaan huomioon suunnittelun aikaisessa vaiheessa, voidaan erilaisia ratkaisuja ja vaihtoehtoja miettiä vapaammin. Tällöin myös yleensä saadaan huomattavasti parempi ratkaisu kuin analysoimalla ja miettimällä turvallisuustoimenpiteitä olemassa olevalle kappaleelle. (Foord et al. 2011)

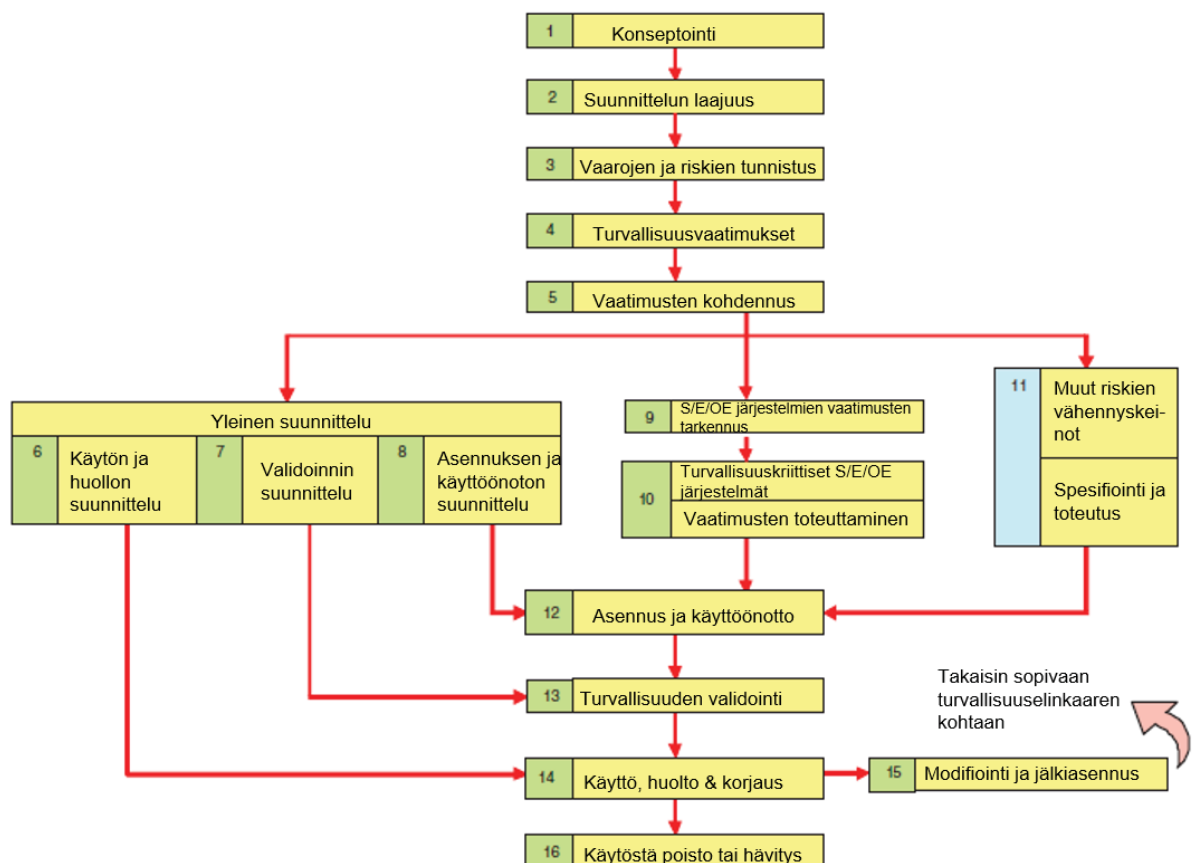
2.3.1 Pääprosessit

Standardissa tuotekehitysprosessi alkaa suunniteltavan tuotteen tai järjestelmän kuvauksella sekä turvallisuustöiden aloittamisella. Turvallisuustyöhön kuuluu turvallisuuselinkaaren aloitus, riskien analysointi sekä turvallisuusvaatimusten laatiminen. Näiden jälkeen suunnittelua jatketaan vaatimusten määrittelyllä, konseptoinnilla ja alustavalla suunnittelulla jossa hahmotellaan tulevaa tuotetta tai systeemiä sekä sen rajapintoja. Standardin IEC 61508 tapauksessa riskien arviointi tehdään käyttämällä SIL-eheystasoa, joka antaa järjestelmällä tai turvallisuuden kannalta kriittiselle osajärjestelmälle eheystason.

Järjestelmän tulee täyttää kyseisen eheystason asettamat vaatimukset, joten suunnittelussa on otettava eheystaso huomioon. (Foord et al. 2011)

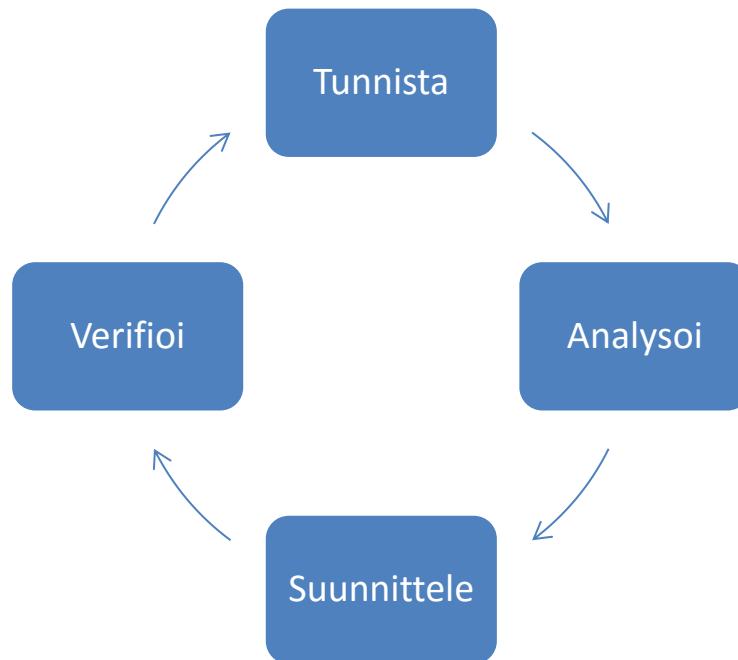
Tärkeimmät vaiheet turvallisuuskriittisten järjestelmien ja laitteiden suunnittelussa on suunnittelun jäsentäminen, tietojen kerääminen sekä koko turvallisuuselinkaaren analysointi hyvin varhaisessa vaiheessa (IEC 61508 2011). Tällöin voidaan eniten vaikuttaa laitteen turvallisuuteen sekä myös sen päivittämiseen ja muokkaukseen. Standardien ja lakien muutosten lisäksi myös teknologia kehittyy, jolloin myös turvallisuudesta vastaavia laitteita ja järjestelmiä saatetaan joutua muokkaamaan. (Foord et al. 2011)

Standardin mukainen prosessin sekä turvallisuuselinkaaren kuvaus on nähtävissä kuvassa 1. Kuvasta näkee alkusuunnittelun sekä turvallisuusselvityksien painotuksen. Kaikki nämä on oltava valmiina ennen varisnaista suunnittelua. Turvallisuusvaatimusten määrittelyn jälkeen kehitystä voidaan hajauttaa, koska kaikkiin kohtiin vaikuttavat samat vaatimukset. Riskejä voidaan edelleen pyrkiä löytämään ja vähentämään käyttämällä muita riskientunnistusmetodeja sekä analyysejä. Mikäli turvallisuusvaatimuksia täytyy muuttaa uusien analyysien tulosten perusteella, vaikuttaa muutokset myös muihin osa-alueisiin kuvan mukaisesti. (Foord et al. 2011)



Kuva 1 Turvallisuuselinkaaren kulku (Foord et al. 2011)

Turvallisuuselinkaari voidaan hahmottaa myös kuvan 2 tyyllisenä turvallisuussyklinä, jonka avulla tunnistetaan kaikki mahdolliset vaaratilanteet sekä tehdään tarvittavat toimenpiteet. Syklissä analysoidaan löydetyt tilanteet ja suunnitellaan jokaiseen paras mahdollinen ratkaisu. Tämän jälkeen varmistetaan, että tehdyt toimenpiteet poistivat vaaratilanteet tai laskivat sen riittävän alhaiselle tasolle. Tämän jälkeen sykli aloitetaan alusta ja etsitään lisää mahdollisia vaaratilanteita. Millään analyysillä ei voida löytää kaikkia mahdollisia vaaratilanteita, mutta syklisellä menetelmällä tilannetta tarkastellaan jatkuvasti ja uusia vaaratilanteita voidaan löytää. (Exida 2006)



Kuva 2 Turvallisuuselinkaaren sykli

Jokaisessa kuvan 1 mukaisessa elinkaaren kohdassa tulisi tarkastella tilannetta syklisen analysoinnin kautta ja kehittää paras mahdollinen ratkaisu ongelmaan. Syklisen ja järjestelmällisen etenemisen avulla voidaan varmistua ja verifioida, että tarpeelliset toiminnot on suoritettu suunnitellusti. (Brown 2000)

2.3.2 SIL-eheystasot

SIL-eheystasot määritetään jokaiselle S/E/OE elementille, jonka tarkoituksena on poistaa tai lieventää riskiä. Eheystasojen avulla varmistetaan, että turvallisuuden kannalta kriittiset järjestelmän osat täyttävät niille asetetut vaatimukset ja toimivat halutusti. SIL-eheystasot kertovat mikä on järjestelmän tai komponentin hyväksyttävä vikaantumisväli. Kriittisillä kohteilla on korkea SIL-eheystaso, koska niiden vikaantumisvälien on oltava mahdollisimman suuret. Suuremmille SIL-eheystasoilla tehtävät riskienvähennys sekä -torjumiskeinot ovat vaativampia kuin alemmilla luokituksilla. (Brown 2000)

Eheystasojen määrittämisessä voidaan käyttää esimerkiksi taulukon 1 mukaista, standardissa IEC-61058 esitettyä matriisia. Taulukon vasemmalla olevat prosentit kuvastavat kuinka suuri osa tapahtuvista vioista ei aiheuta kyseisen järjestelmän tai komponentin turvallisuustoiminnon menetystä. Laitteiston vikasietoisuudella kuvataan vähimmäismäärä vikoja, jotka voivat aiheuttaa turvatoiminnon menetyksen. Vikasietoisuutta kuvataan symbolilla N ja se määritetään kaavalla $N+1$ taulukon 1 mukaisesti. Mikäli turvallisuustoiminnon menetykseen johtavia vikoja on useampia, vaadittava SIL-eheystaso nousee. (IEC 61508 2011)

Taulukko 1 SIL-eheystasojen määrittäminen

Elementin turvallisten vikaantumisten osuus	Laitteiston vikasietoisuus		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Järjestelmän tai komponentin SIL-luokituksen määrittely alkaa normaalilla riskitarkastelulla jossa kerätään kaikki mahdollinen tieto, jonka pohjalta tarkastelu tehdään. Riskien tarkastelu ja analysointi voidaan tehdä usealla eri menetelmällä, mutta niissä on otettava huomioon vaaran tyyppi, tapahtuman todennäköisyys sekä mahdolliset seuraukset. Riskin laajuudesta ja turvallisuustoiminnon kriittisyyden perusteella sille annetaan SIL-luokitus, joka määrittelee siltä vaadittavaa dokumentointia ja verifiointia. (Germanicher Lloyd 2016)

2.4 ISO 26262 Road vehicles – Functional safety

Standardi ISO 26262, Ajoneuvojen toiminnallinen turvallisuus, on kehitetty ajoneuvojen turvallisuuskriittisten S/E/OE laitteiden ja järjestelmien kehitykseen ja tuotantoon. Standardi on suunniteltu ajoneuvojen sekä niiden komponenttien valmistajille. ISO 26262 käsittelee riskejä, jotka johtuvat S/E/OE laitteiden ja järjestelmien vikaantumisesta. Standardi on johdettu toiminnallisen turvallisuuden yleisstandardista IEC 61508. (ISO 26262 2011)

Ajoneuvoteollisuudessa toteutetaan kasvavassa määrin turvallisuustoimia S/E/OE laitteilla ja järjestelmillä. Toiminnallisen turvallisuuden perusstandardi IEC 61508 on kattava ja tarkka kokoelma ohjeita ja sääntöjä, mutta se soveltuu paremmin yksittäisten järjestelmien ja laitteiden tarkasteluun. Standardi ISO 26262 on kehitetty ajoneuvoteollisuuden jossa tuotantomäärät ovat erittäin suuria, jolloin tuotteiden ja järjestelmien suunnitteluun on kiinnitettävä erityisesti huomiota. Suurien erien korjaus ja muokkaaminen on kallista ja erittäin hankalaa, joten suunnittelu ja tuotanto on mietittävä tarkasti ennen valmistusta.

Standardin ohjeita ja perusidea voidaan käyttää myös muissa kuin ajoneuvoteollisuuden tuotteissa ja järjestelmissä. Tuotekehitykseen sekä organisaation toimintaan liittyvät ohjeet sekä vaatimukset ovat sovellettavissa moniin erilaisiin tilanteisiin ja ne antavat yleisperiaatteita toiminnalle.

2.4.1 Standardin pääprosessit

Standardissa on annettu tarkasti ohjeita ja sääntöjä koko tuotekehitysprosessiin sekä prosessien hallintaan. Sääntöjen ja ohjeiden lisäksi painotetaan turvallisuuskulttuurin luomista ja ylläpitoa. Turvallisuuden tulisi olla yksi toiminnan kriittisistä lähtökohdista jokaisessa osa-alueessa, jotta tuotteisiin ja järjestelmiin saadaan parhaat mahdolliset turvallisuusratkaisut. Standardissa on ohjeita organisaation turvallisuuskulttuurin arviointiin, joiden avulla voidaan arvioida ja myös tehdä muutoksia ja parannuksia toimintaan. Jos organisaatiossa ei ole toimivaa turvallisuuskulttuuria, turvallisuusnäkökulmat yleensä unohdetaan suunnittelussa. (ISO 26262 2011)

Standardin kymmenen osaa jakautuvat tuotekehitysprosessiin kuvan 3 mukaisesti. Standardin tuotekehitysprosessi etenee normaalin V-mallin mukaisesti konseptoinnin ja tuotannon kautta julkaisemisen jälkeisiin prosesseihin. Monet tuotekehityksen sisällä olevat prosessit koostuvat myös sisäkkäisistä V-malleista, kuten kohtien 5 ja 6 tuotekehitykset laite- ja ohjelmistotasolla.

Pääkohtina standardissa on toiminnallisen turvallisuuden hallintatoimenpiteiden suunnittelu, koordinointi ja seuraaminen. Kattavalla projektin hallinnoinnilla voidaan kattaa kaikki osa-alueet ja varmistaa, että tarvittavat toimenpiteet tulevat tehdyksi. Standardissa tuotteen turvallisuutta hallinnoidaan turvallisuuselinkaaren avulla, jonka suunnittelu aloitetaan jo konseptivaiheessa. Yksinkertaistettu turvallisuuselinkaari sekä sen pääkohdat näkyvät kuvassa 4. Standardin muut kohdat painottuvat turvallisuuselinkaaren käyttöön, joten sen suunnitteluun on alussa käytettävä tarpeeksi resursseja.

Standardi tarjoaa elinkaaren hallintaan erilaisia työkaluja ja ohjeita, kuten standardiin kehitetyn riskilähtöisen ASIL-luokituksen sekä vaatimuksia validoinnille ja varmennukselle. Varmennusten ja verifioinnin avulla voidaan varmistua, että tarvittavat toimenpiteet on tehty ja tuote on vaaditulla turvallisuustasolla. Standardi antaa myös vaatimuksia ja ohjeita alihankkijoiden ja toimittajien kanssa toimimiselle. Turvallisuuden takaamiseksi myös muualta hankittujen osien turvallisuudesta on varmistuttava, jotta kokonaistuotteen tai järjestelmän turvallisuus voidaan varmentaa. (ISO 26262 2011)

2.4.2 ASIL-luokitus

Standardiin ISO 26262 on kehitetty oma riskienarviointimenetelmä, joka käyttää ASIL-luokkia riskien jaotteluun. Riskejä arvioidaan kolmella eri perusteella joita ovat altistuminen (Exposure), kontrolloitavuus (Controllability) sekä mahdollisen tapaturman aiheuttamat vahingot (Severity). Altistuminen ja tapaturman vahingot ovat hyvin samantlaisia muiden riskienarviointimenetelmien kanssa, mutta kontrolloitavuus on ASIL-luokituksen oma kategoria. Kontrolloitavuudella määritetään kuinka helposti kuljettaja tai muut tiellä liikkujat voivat välttää vaarallisen tilanteen. Riskitilanteen määrittämiseen käytettäviä ohjetaulukoita on liitteessä A. (ISO 26262 2011)

Riskeille määritetään ASIL-eheystaso edellä mainittujen kategorioiden sekä taulukon 2 mukaisesti. ASIL-luokituksessa on viisi erilaista kategoriaa, jotka ovat *QM*, *A*, *B*, *C* sekä *D*. *QM* (Quality Management) tarkoittaa, että kyseiselle riskille ei tarvitse tehdä erityisiä toimenpiteitä vaan se voidaan poistaa laadunvalvonnan avulla. Luokkien *A-D* riskit vaativat lisää analysointia sekä dokumentointia normaaliin laadunvalvontaan verrattuna.

Taulukko 2 ASIL-luokituksen määrittäminen

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Jokaiselle tunnistetulle riskille määritetään ASIL-luokka, joka kuvaa kuinka turvallisuus-kriittinen kohde on. Esimerkiksi vakavaan vammaan tai kontrolloitavuuden menetykseen johtavat riskit ovat kriittisiä, joten ne ovat korkeammassa ASIL-luokituksissa. Tuote tai järjestelmä suunnitellaan luokituksen asetuksen jälkeen siten, että luokituksen asettamat vaatimukset täyttyvät. Riskejä voidaan jakaa edelleen osaelementteihin jolloin ei välttämättä tarvitse käyttää systeemin korkeinta ASIL-luokitusta. Jakoa voidaan käyttää, mikäli rinnakkaisilla elementeillä on eri eheystasot ja niiden turvallisuusvaatimukset eivät ole toisistaan riippuvaisia.

2.4.3 Tuotekehitys

Tuotekehitys kattaa tuotteen elinkaaren suunnittelun aloituksesta tuotantoon asti. Tuotekehitys jaetaan yleensä useampaan osa-alueeseen koska eri alueita voidaan kehittää rinnakkain ja prosessia on helpompaa hallita. Tuotekehityksen kulku on kuvan 3 mukaista ja varsinainen tuotekehitys tehdään kohtien 3-6 aikana. Konseptoinnin jälkeen tuotekehitys siirtyy systeemitason suunnitteluun, joka haarautuu edelleen osa- sekä ohjelmistotasolle. Kuvasta 3 nähdään myös tuotekehitysvaiheiden sisällä olevat V-mallit. Kehitystä jaetaan pieniin osiin, jotka toteutetaan myös omilla V-mallin kaltaisilla prosesseilla hallinnan helpottamiseksi ja jäsentämiseksi. (ISO 26262 2011)

V-mallissa suunnittelun luonne on erilaista sakaroiden yläosissa. Vasemman puoleisessa sakarassa suunnittelu keskittyy tuotteen tai järjestelmän määrittelyyn, konseptointiin ja ylätasoon suunnitteluun. Oikeanpuoleisessa sakarassa suunnittelu on valmista ja keskittyy validointiin, verifiointiin ja tuotantoon siirtymiseen. V-mallin sisäiset suunnittelusykliä noudattavat samaa periaatetta ja niistä siirrytään eteenpäin, kun tehdyt toiminnot ja työt on verifioitu.

2.4.4 Systeemitaso

Systeemitason kehitys sisältää validointia, ulkoisten toimien tehokkuuden tarkastelua, tuotannon ja toiminnan asettamia vaatimuksia sekä valmistuksen jälkeistä toiminnallista turvallisuutta. Validoinnissa tarkastetaan standardin ulkopuolisilla teknologioilla toteutettujen järjestelmien turvallisuus. Ulkopuolisia teknologioita ovat esimerkiksi hydrauliset ja mekaaniset toteutukset sekä sähköiset järjestelmät, jotka eivät lukeudu standardin piiriin. Ulkoisilla toimilla tarkoitetaan järjestelmiä, jotka vähentävät kehityksessä olevan tuotteen aiheuttamia riskejä. Tällaiset järjestelmät, kuten dynaaminen ajonvakautusjärjestelmä sekä run-flat rengas, vaikuttavat yleensä koko ajoneuvon turvallisuuteen. Standardin ulkopuoliset järjestelmät on myös tarkistettava, mikäli ne vaikuttavat suunniteltavien laitteiden toimintaan. (ISO 26262 2011)

Ennen systeemin jakoa laite- tai ohjelmistotasolle tekniset turvallisuusvaatimukset tarkennetaan ja tehdään alustavaa systeemisuunnittelua. Tämän suunnitelman pohjalta tehdään jako alisysteemeihin, joiden avulla kokonaissuunnittelua on helpompaa seurata sekä varmentaa turvallisuusvaatimusten täytyminen. Alisysteemien kehitys alkaa myös teknisten turvallisuusvaatimusten sekä systeemisuunnittelun kautta. Turvallisuusvaatimukseen kiinnitetään paljon huomiota, koska ajoneuvoteollisuudessa osia tuotetaan erittäin paljon, jolloin muutosten teko valmiisiin tuotteisiin on erittäin hankalaa. Alisysteemeihin jakamisen jälkeen kehitys jaetaan laite- sekä ohjelmistokehitykseen.

2.4.5 Laitetaso

Laitetason suunnittelu etenee samalla tavalla kuin systeemitason suunnittelu. Aluksi määritellään tarkasti turvallisuusvaatimukset, jonka jälkeen laitteistoa voidaan suunnitella. Turvallisuusvaatimusten määrittelyyn kuuluu kaikki laitteistovaatimukset, jotka vaikuttavat tuotteen turvallisuuteen. Tällaisia piirteitä ovat esimerkiksi ominaisuudet, jotka kontrolloivat sisäisiä vikoja sekä vikojen havainnointi ja niistä ilmoittaminen kuljettajalle.

Suunnittelussa on otettava myös huomioon, että laitteiston on oltava yhdenmukainen systeemin vaatimusten kanssa. Laitteistoarkkitehtuuri ei myöskään saa olla liian monimutkainen, koska se lisää virheiden mahdollisuutta. Monimutkaisuutta voidaan vähentää tekemällä laitteistosta modulaarinen, jolloin jokainen osa voidaan tarkastaa erikseen sekä lopuksi kokonaisuutena. Laitteiston vikaantumisessa on otettava huomioon myös ympäristötekijöitä kuten lämpötila, vesi ja pöly. Suunnittelun sekä vikatarkastelun laajuus riippuu systeemille asetetusta ASIL-luokituksesta. Korkeamman luokan vaatimukset ovat tarkempia ja vaativat laitteistolta tehokkaampia turvatoimia. Tällaisia turvatoimia ovat esimerkiksi laitteen siirtyminen turvalliseen tilaan sekä ilmoittaa kuskille vikatiloista salitussa aikavälissä. Analyyseissä käytettävät vikavälit sekä käytettävät arvot tulee perustua mittausdataan, käyttöstatiikkaan tai asiantuntijalausuntoihin. (ISO 26262 2011)

2.4.6 Ohjelmistotaso

Standardissa on useita vaatimuksia sekä sääntöjä ohjelmien laatimiseen sekä käytettäviin työkaluihin. Ohjelmistojen monimutkaistuessa sekä muuttuessa laajemmiksi on niihin käytettävä tarpeeksi resursseja, jotta ohjelmistojen turvallisuus vastaa sille asetettuja vaatimuksia. Ohjelmoinnissa käytetyt menet, ohjelmointikielet sekä työkalut tulee olla yhtenäiset koko ohjelmiston elinkaaren aikana ja olla yhteensopivat systeemin ja laitteiston kehityksen kanssa. Yhtenäisyyden avulla vältetään ohjelmistojen välisiltä yhteensopivuusongelmilta ja ohjelmien lähdekoodia on helpompaa lukea sekä muokata.

Ohjelmistoja suunniteltaessa sen arkkitehtuuri tulee kuvata ja suunnitella tarkasti ennen varsinaista koodin kirjoittamista. Ohjelmistoarkkitehtuurin tulee selittää ohjelmistokomponenttien suunnittelunäkökulmat kuten datan käsittelyjärjestys, datatyypit sekä komponenttien ja ohjelmiston ulkoiset rajapinnat. Arkkitehtuurissa määritellään myös dynaamisia suunnittelunäkökulmia, kuten ohjelmiston toiminnallisuutta, käyttäytymistä sekä tiedonkulkua ohjelmistokomponenttien välillä. (ISO 26262 2011)

Varsinaisen lähdekoodin suunnittelussa ja kirjoituksessa on otettava huomioon useita piirteitä, jotka vaikuttavat ohjelmiston kokonaisturvallisuuteen. Koodin tulisi olla yhdenmukaista ohjelmiston eri osien välillä sekä myös mahdollisimman yksinkertaista ja helpolukuista. Tällöin vältetään liiallisen monimutkaisuuden aiheuttamista virheistä. Lähdekoodi tulisi suunnitella siten, että sitä on helppoa testata ja modifioida tarpeiden mukaan.

Ohjelmistoturvallisuuteen asetettavat vaatimukset keskitetään jokaiseen ohjelmistopohjaiseen toimintoon jonka virhe voi aiheuttaa turvallisuuden menetyksen. Tällaisia toimintoja ovat esimerkiksi turvalliseen tilaan siirtyminen, vikojen havainnointi turvallisuuskriittisistä osista sekä vioista ilmoittaminen. Turvallisuusvaatimukset johdetaan systeemin spesifikaatiosta sekä turvallisuussuunnitelmasta.

2.4.7 Tukiprosessit

Standardin tukiprosessit jatkuvat kuvan kolme mukaisesti koko prosessin läpi. Tärkeimpiä kohtia tukiprosesseista ovat toimintojen verifiointi, varmennus sekä tehtyjen toimenpiteiden dokumentointi. Näitä toimenpiteitä vaaditaan jokaisessa kohdassa varmistamaan tuotosten täyttävän niille asetetut vaatimukset.

Verifioinnin avulla varmistetaan, että toimenpiteet vastaavat suunnitelmia ja vaatimuksia. Konseptointivaiheessa tarkastellaan, että rajapinnat ovat yhdenmukaisia, rajaehdot ovat oikein ja konsepti voidaan realisoida. Kehitysvaiheessa ja suunnittelussa verifioinnilla varmistetaan arkkitehtuurin, mallien sekä ohjelmistokoodin täyttävän suunnitelmissa asetetut vaatimukset.

Varmennuksessa voidaan käyttää erilaisia metodeja riippuen mitä toimenpidettä tai komponenttia tarkastellaan. Helpoin tapa on tehdä arviointi tai analyysi esimerkiksi tarkistuslistojen avulla. Tällaiset keinot sopivat varmistamaan esimerkiksi, että konseptointivaiheessa kaikki tarpeelliset kohdat on huomioitu. Vaativampia keinoja varmennukseen on käyttää simulointia tai tehdä testausta erillisillä testikappaleilla. Simulointi vaatii erillisen mallin luomista, jonka avulla voidaan testata tuotteen toimivuutta sen tulevassa ympäristössä. Simulointia käytetään yleensä tilanteissa, joissa varmennettava tuote on niin kallis, että on kannattavampaa laatia simulointimalli kuin testata erillisillä tuotteilla. Testikappaleita joudutaan yleensä tekemään useita kappaleita, sillä ne saattavat vahingoittua joissain testeissä siten, ettei niitä voida käyttää. Testausvaiheessa varmistetaan laitteiden toiminta aidossa tai aitoa vastaavassa ympäristössä.

Verifioitaessa ohjelmistojen arkkitehtuuria sekä suunnittelua on tarkastettava, millaisilla metodeilla verifiointi tehdään. Eri ASIL-luokituksen osille on suositeltavaa käyttää eri metodeja parhaan tuloksen saamiseksi sekä ajan säästämiseksi. Esimerkiksi ASIL A ja B -luokille riittää suunnitelmien läpikäynti ja arviointi, mutta luokat C ja D vaativat monipuolisempaa tarkastelua, kuten simulointia tai turvallisuuskriittisten kohtien suoritusjärjestyksen sekä tiedon kulkuun liittyviä analyysejä.

Dokumentoinnissa tulee käyttää koko prosessin ajan samoja sääntöjä, jotta dokumentit ovat helposti luettavissa sekä selkeitä. Säännöt ovat hyvin yleisiä ja ne sopivat myös standardin ulkopuoliseen dokumentointiin. Säännöissä painotetaan esimerkiksi dokumenttien selkeyttä, ytimekkyyttä sekä jaottelua. Dokumentoinnissa tulisi myös käyttää järjestelmiä, jotka sallivat dokumenttien muokkauksen ja ylläpitämisen.

Standardi ei anna tarkkoja vaatimuksia dokumenttien ulkomuodolle tai jäsentelylle, vaan painottaa dokumenttien sisältövaatimuksia. Standardi painottaa myös luomaan dokumentointistrategian koko turvallisuuselinkaarelle ja sen osa-alueille. Joitain ohjeita ja toimintaa helpottavia piirteitä on kuitenkin annettu, kuten päällekkäisyyksien poistamista dokumenttien välillä. Dokumentoinnin ja dokumentointistrategian luomisessa jätetään joissain piirteissä päätäntävalta yrityksille. Osa dokumentoinnin piirteistä ovat tilannekohtaisia, kuten riittävän dokumentointitason määrittäminen sekä kompleksisuus.

3. TYÖN KOHDE JA TUTKIMUKSEN OSATEHTÄVÄT

Organisaatiossa kehitetään raskaita kuljetusajoneuvoja sekä niihin liittyviä alijärjestelmiä ja tuotteita. Käytössä oleva tuotekehityssykli sisältää konseptointia, suunnittelun hajauttamista eri osa-alueisiin sekä tehtyjen toimintojen varmentamista. Tuoteistamisprosesseissa on projektijohtaja, joka on vastuussa projektin etenemisestä oikeaan suuntaan oikealla tahdilla. Projekteissa on mukana vastuusuunnittelijoita, turvallisuushenkilöstöä sekä muuta suunnitteluhenkilöstöä tarvittavilta osa-alueilta.

3.1 Työn kohde

Työn kohteena tarkastellaan nykyistä tuotekehityssykliä sekä jarrujärjestelmää ja verrataan niitä standardin ISO 26262 vaatimuksiin. Toimintojen tarkastelu toteutetaan haastattelemalla suunnitteluhenkilöstöä sekä tarkastelemalla tuotekehityksen dokumentteja. Vertailu toteutetaan nykytila-analyysin avulla tilanteen kartoittamiseksi. Analysointia on jaettu osatehtävien avulla, jotta kokonaisuutta on helpompaa hallita ja tulokset saadaan selvemmin esille.

3.2 Työn keskeiset osatehtävät

Työ on jaettu osatehtäviin helpottamaan ja selkeyttämään työn kulkua. Työssä käytettävät osatehtävät näkyvät kuvassa 5. Aluksi perehdytään nykyiseen tuotekehityssykliin sekä analyysissä käytettävään jarrujärjestelmään. Molempiin perehdytään haastattelemalla suunnittelupäälliköitä, suunnittelijoita sekä käyttämällä toimintoihin liittyviä dokumentteja. Analyysin avulla saadaan selville mitä tuotekehityksessä on tehtävä, jotta standardin vaatimukset täyttyvät.



Kuva 5 Työn osatehtävät

Osatehtävien lisäksi apuna käytetään johdannossa esitettyjä tutkimuskysymyksiä. Kysymyksien avulla saadaan vastaus työn päätavoitteeseen ja osatehtävien avulla työtä on jaettu pienempiin osa-alueisiin. Jokaisesta osatehtävästä on seuraavaksi kattavampi selitys sekä kuvaus, kuinka ne toteutetaan.

3.2.1 Nykyisen tuotekehityssyklin selvittäminen

Nykyisen tuotekehityssyklin selvittäminen on tärkeä osa työn onnistumisen ja laadukkaiden tulosten kannalta. Nykyisen toiminnan pohjalta tehdään analyysit standardin noudattamiseksi sekä ehdotetaan muutoksia, joten kartoitus on tehtävä kattavasti. Tuotekehityssykliä tarkastellaan erikseen tekniseltä- sekä ohjelmisto-osuuksilta. Jako on toteutettu, jotta molemmista saadaan mahdollisimman tarkka kuvaus. Tekninen toteutus ja ohjelmistojen luonti on jaettu erillisille osastoille, mikä helpottaa tarkastelua.

Tietoja tuotekehityksen kulusta kerätään haastatteleamalla molempien osa-alueiden vastuusuunnittelijaa avoimessa haastattelussa sekä tarkastelemalla tuotekehityksen dokumentteja sekä ohjeita. Dokumenttien lisäksi tuotekehityksen kulkua tarkastellaan valmiiden järjestelmien avulla perehtymällä niissä käytettyihin toimintatapoihin. Näiden tietojen avulla kasataan tarkka kuvaus nykyisestä tuotekehityksen tilanteesta.

3.2.2 Tarkasteltavan jarrujärjestelmän suunnittelun kuvaus

Jarrujärjestelmän suunnittelun kuvaus tehdään samalla tavalla, kuin tuotekehityssyklin selvitys. Tarkastelu toteutetaan suunnittelupäälliköiden haastatteluilla sekä dokumenttien

avulla. Jarrujärjestelmä sisältää ostettuja osia, yrityksen omaa suunnittelua sekä järjestelmään kehitettyjä ohjelmistoja, jotka kaikki otetaan huomioon tarkastelua tehdessä.

Jarrujärjestelmässä käytettyä tuotekehityssykliä ja suunnittelupäätöksiä käytetään apuna nykytila-analyysissä, joten järjestelmän tarkastelu on toteutettava mahdollisimman yksityiskohtaisesti. Mahdollisimman kattava tarkastelu myös varmistaa laadukkaat tulokset sekä suurimman hyödyn kohdeyritykselle.

3.2.3 Nykytila-analyysi

Nykytila-analyysiä tehdään jarrujärjestelmän avulla ja siinä käytettyjä suunnittelupäätöksiä ja toimenpiteitä verrataan standardin vaatimuksiin. Mikäli kaikkia standardin vaatimia kohtia ei ole käytetty jarrujärjestelmässä, käytetään tuotekehitykseen annettuja ohjeita ja dokumentteja mahdollisuuksien mukaan. Analyysiä tehdessä käydään läpi standardin osa-alueet ja verrataan nykyistä toimintaa standardin asettamiin vaatimuksiin.

Analyysiä laadittaessa vaikeimpia tekijöitä on varmistua, että kaikki standardin tuotekehitykseen vaatimuksia antavat kohdat otetaan huomioon. Parhaan tuloksen saamiseksi standardi käydään yksityiskohtaisesti läpi ja pyritään löytämään kaikki tuotekehitykseen ja toimintaan liittyvät vaatimukset.

3.2.4 Kohteiden priorisointi ja muutosehdotukset

Nykytila-analyysin pohjalta löydetyt muutoskohteet ja tarvittavat lisäykset jaetaan kolmeen kategoriaan, joissa numero 1-3 kuvastaa muutostarpeen kriittisyyttä. Kategorisoinnissa käytetty kolmiportainen jako sekä kategorioiden kuvaukset ja niiden merkitykset valittiin kohdeyrityksen edustajien kanssa. Kategorian 1 kohde on esimerkiksi tilanne, jossa nykyisessä toiminnassa on valmiiksi epäkohtia, jotka täytyy muokata standardin tuloksesta riippumatta. Kategoriassa 3 on kohteet, joita voidaan parantaa ja muokata, mutta tilanne ei ole niin kriittinen, että toimintoja täytyisi aloittaa heti.

Työn puitteissa kaikkia löydettyjä muutoskohteita ei tarkastella, vaan keskitytään kriittimpiin kohteisiin. Vähemmän kriittisten kohteiden tarkastelu riippuu kriittisten muutoskohteiden määrästä. Mikäli kriittisiä kohteita ei löydetä, voidaan vähemmän kriittisiin muutoksiin panostaa enemmän. Muutosehdotuksissa mietitään myös tarvittavien muutosten ja lisäysten aikataulutusta standardin noudattamiseksi.

3.3 Tuotekehityssykli ja yleinen tuotekehitysprosessi

Yleinen tuotteistamisprosessi sisältää tuotekehitystä, toteutusta ja ylläpitoa. Koko prosessin läpi kulkee myös tukiprosesseja, kuten vaatimusten ja konfiguraation hallintaa. Tuotekehityksen puolella vaaditaan enemmän vaatimusten, kuin konfiguraation hallitsemista,

mutta tuotteistamisen loppupäässä konfiguraation hallinta on suuremmissa osassa. Tuotteistamisen tuotekehitysosio on jaettu kahteen päävaiheeseen, konseptointiin ja suunnitteluun.

Toimintajärjestelmässä kuvattu tuotekehitysprosessi pohjautuu yleisesti käytössä olevaan V-malliin sekä iteraatiopohjaiseen toimintaan. Malliin on kuitenkin tehty pieniä muutoksia ja muokattu sitä omaan toimintaan sopivaksi. Tuotekehitysprosessiin on lisätty katselmointeja, baselineja ja virstanpylväitä, joiden avulla varmistetaan, että vaatimukset ja toimintojen dokumentointi ovat hallinnassa.

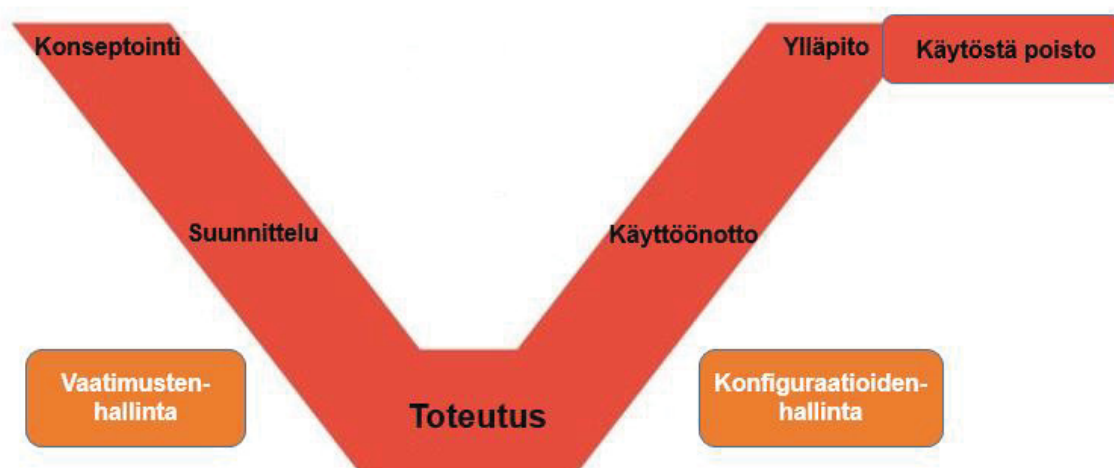
Katselmuksissa tarkoituksena on varmistua siitä, että toiminta vastaa projektin alussa sovittuja näkökulmia. Tuotekehitysprosessin alussa katselmuksissa varmistetaan, että asiakkaan vaatimukset ja tarpeet on ymmärretty ja niiden pohjalta tehdyt vaatimukset ovat riittävän hyvin määriteltäviä. Katselmuksia tehdään useita kertoja saman aliproessin aikana varmistamaan, että prosessi keskittyy alussa määritettyjen tarpeiden ja vaatimusten täyttämiseen. Katselmuksissa sisältävät myös vastuiden jakoa sekä tarkastuksia joissa varmistetaan, että toimenpiteet on hyväksytty ja prosessia voidaan jatkaa. Baselinet liittyvät katselmuksiin ja niiden tarkoituksena on dokumentoida jäljitettävästi hyväksytysti katselmoidut dokumentaatiot tai tuotteet. Tämän avulla seuraavaan vaiheeseen siirryttäessä on kiinteä lähtöpiste, jota vastaan toimintaa voidaan tarkastella. Osa baselineista on yhteisiä teknisen ja ohjelmistopuolen kanssa, koska niissä olevat kohdat liittyvät molempien suunnitteluun. Ennen seuraavaan vaiheeseen siirtymistä on kuitenkin prosessin virstanpylväiden kohdalla varmistettava, että kaikki toimenpiteet ja tuotokset on suoritettu hyväksytysti. Tarkasteluihin on laadittu valmiita pohjia, joiden avulla kaikki tarpeelliset kohdat tulevat tarkastelluiksi.

Tuotekehitysprosessin sisällä tekninen ja ohjelmistopuoli on jaettu suunnittelun helpottamiseksi erikseen. Molemmat noudattavat samoja tuotekehityksen sääntöjä ja ohjeita, mutta koska kehitys ja suunnittelu ovat teknisellä ja ohjelmistopuolella erilaista, on helppointa jakaa ne erilleen. Tällöin konseptivaiheessa määritellyt vaatimukset ja rajapinnat ovat entistä tärkeämmässä asemassa, jottei suunnittelussa ajauduta erilaisiin toimintoihin. Suunnittelun aikana kommunikointi on tärkeää ja on tiedettävä, millaisia ratkaisuja toinen puoli tekee, jotta myös omaa ratkaisua voidaan hioa paremmaksi. Katselmointien sekä baselinejen tärkeys nousee, kun tuotekehitystä on jaettu osiin.

3.3.1 Tuotekehityksen kulku

Käytössä oleva malli on jaettu kuuteen päävaiheeseen, jotka ovat: konseptointi, suunnittelu, toteutus, käyttöönotto, ylläpito sekä käytöstä poistaminen. Mallin selkeytetty versio näkyy kuvassa 6. Koko tuotteistamisprosessin läpi kulkee myös tukiprosesseja, kuten vaatimusten – ja konfiguraatioiden hallintaa. Vaatimusten hallinta tarvitaan enemmän alkupään kehityksessä ja loppupäässä konfiguraatioiden hallinta on tärkeämpää, koska vaa-

timuksiin on hankalaa vaikuttaa tuotannon aikana ja sen jälkeen. Kuvan 6 mallissa keskellä toteutusvaiheessa vaatimukset ja konfiguraationhallinta ovat samalla tasolla, jonka jälkeen konfiguraationhallinnan merkitys nousee suuremmaksi.



Kuva 6 Tuoteistamisprosessin malli

Standardin käyttämä malli, kuvassa 3, on suurelta osin samanlainen yrityksessä käytettävän mallin kanssa. Molemmista malleista käytetään iteraatiopohjaista kehitystä prosessien alakohtien sisällä. Myös standardin mallissa kehitystä on jaettu eri osiin suunnittelun helpottamiseksi ja selkeyttämiseksi. Standardissa esitetyssä mallissa tukiprosesseja on enemmän, koska siinä käsitellään myös prosessin aikana käytettäviä työkaluja sekä niiden kelpoisuusvaatimuksia.

3.3.2 Iteraatiopohjainen kehityssykli

Tuotekehityksen alkuvaiheessa konseptoinnissa ja suunnittelussa käytetään iteraatiopohjaista lähestymistapaa. Iteraatioissa työtä jaetaan pieniin kokonaisuuksiin, joiden toimituutta voidaan arvioida ja toistaa suunnittelua kunnes löydetään kriteerit täyttävä ratkaisu. Tällöin varmistetaan suunnittelun täyttävien vaatimukset pienemmässä mittakaavassa ennen laajempien kokonaisuuksien määrittelyä. Iteraatioiden aikana on myös helpompaa kerätä suunnitelmaan mielipiteitä muilta tahoilta ja ottaa ideat käyttöön seuraavassa kierroksessa. Ideoita voidaan yhdistellä keskenään ja lisätä seuraavan kierroksen tuotokseen ja jälleen heijastaa tulosta eri näkökulmista. Yleensä paras ratkaisu saadaan mahdollisimman monen tekijän avulla sekä useiden iteraatiokierrosten jälkeen.

Tarvittavien iteraatioiden määrä ja kehityksen kesto vaihtelee projektien välillä huomattavasti. Alussa laaditussa projektisuunnitelmassa tarkastellaan projektin laajuutta ja monimutkaisuutta, jonka avulla määritellään, kuinka paljon iteraatioita ja kehitystä tarvitaan. Uusien tuotteiden kehityksessä iteraatioita ja kehitystä tarvitaan enemmän, kuin vanhojen

tuotteiden muokkauksessa. Iteraatioita ja kehityksen edistymistä ohjataan projektinhallinnan prosesseilla.

3.3.3 IMS-järjestelmä

Yrityksessä on käytössä kaikille työntekijöille avoin toimintajärjestelmä IMS, johon on sijoitettu kaikki dokumenttipohjat, ohjeistukset, vaatimukset sekä työkalut tuotekehityksen jokaiseen kohtaan. Järjestelmässä on myös ohjeistusta ja prosessikuvauksia, joiden avulla tuotekehitystä voidaan viedä eteenpäin. Prosesseista on tarkat kuvaukset, joissa määritellään niiden etenemisjärjestys, jokaisen kohdan vastuhenkilöt sekä tarvittavat tuotokset. Järjestelmän avulla voidaan hakea vastausta kysymyksiin, miten yritys toimii ja minkälaista ohjeistusta toiminnassa on noudatettava.

Järjestelmä ei rajoitu vain tuotekehitykseen, vaan se kattaa koko yrityksen toiminnan ja prosessit. Järjestelmää on jaettu yrityksen eri liiketoimintojen välillä sen selkeyttämiseksi ja käytön helpottamiseksi. Liiketoiminnot pääsevät tarkastelemaan toisten prosessikuvauksia, joista voi hakea lisäinformaatiota sekä monipuolistaa omia prosesseja. Kaikkiin prosessikuvauksiin pääsy auttaa myös ongelmatilanteissa sekä yhteisessä työskentelyssä muiden liiketoimintojen kanssa.

3.3.4 Työpohjat

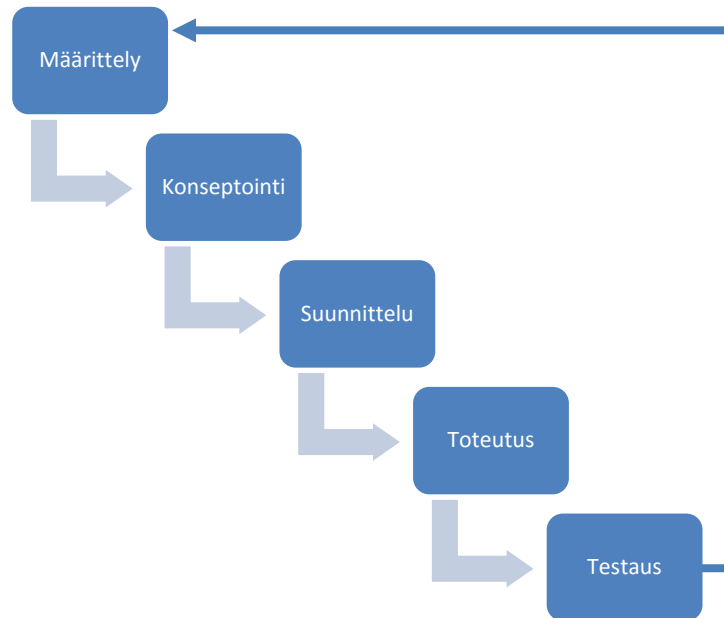
Tuotteistamisen suunnittelussa ja prosessien edetessä toimintaa ohjataan ja tarkastellaan erilaisten dokumenttien ja työpohjien avulla. Näillä varmistetaan tarpeellisten kohtien täytyminen sekä suunnittelun dokumentointi. Valmiiden työpohjien avulla yrityksen toimintatavat sekä prosessien kulku on helppoa sisäistää. Valmiit pohjat myös varmistavat tarpeellisten kohtien dokumentoinnin ja dokumenttien yhtenäisyyden projektien välillä. Työpohjat helpottavat myös vastuiden jakoa, sillä niissä on valmiiksi annettu jokaiseen osatehtävään tarvittavat vastuulliset henkilöt. Dokumentteja ja työpohjia on erilaisiin tilanteisiin, kuten uusien tuotteiden kehitykseen, vanhojen tuotteiden muokkaukseen sekä katselmuksiin.

Dokumenttien ja työpohjien lisäksi järjestelmässä on listauksia suunnittelua ohjaavaan materiaaliin sekä erilaisten suunnitelmien ja analyysien tekoon. Suunnittelua tukevia materiaaleja ovat esimerkiksi listaukset tuotesuunnittelussa noudatettavista laeista, olemassa olevia tuotedokumentteja sekä tarkastuslistoja. Näiden tukimateriaalien avulla on nopeaa tarkastaa yleisimpiä suunnittelupiirteitä.

3.4 Ohjelmistokehitysprosessi

Ohjelmistokehitysprosessi on suurelta osin samankaltainen, kuin teknisen puolen kehitysprosessit. Kehitys kulkee standardin ISO 26262 mallin tavoin rajapintojen, rajoitusten sekä muiden piirteiden määrittelyllä konseptoinnin kautta suunnitteluun. Ohjelmistojen

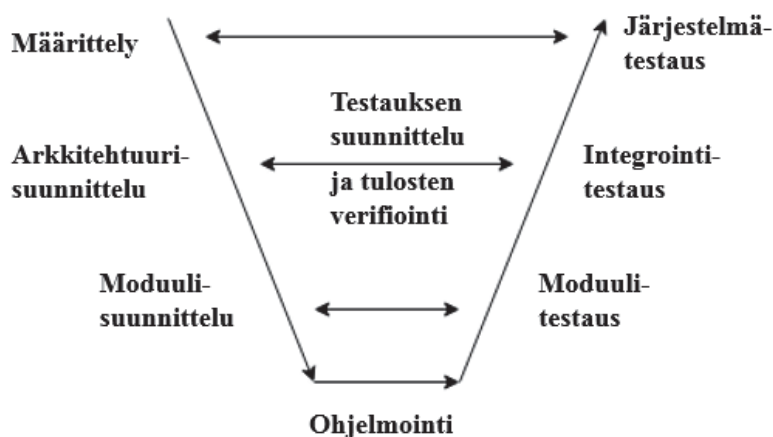
kehitys on iteraatiopohjaista, ja apuna käytetään erilaisia vaihejakomalleja, kuten kuvan 7 mukaista vesiputousmallia. Mallissa testauksen jälkeen palataan määrittelyyn, jolloin uusi iteraatiokierros aloitetaan. Vesiputousmallin lisäksi käytössä on muita malleja, mutta niiden pääprosessit ovat hyvin samankaltaisia. Käytettävän mallin valinta riippuu kehitettävän kohteen määrittelyistä.



Kuva 7 Vesiputousmalli

Ohjelmistokehityksessä erona teknisen osion kehitykseen on suurempi uudelleenkäyttöaste vanhoilla aliohjelmilla ja komponenteilla. Uudelleenkäytön määrä riippuu kuitenkin vanhojen ohjelmistojen suunnittelusta ja rajapinnoista. Vaikka vanhaa ohjelmakoodia ei voida käyttää, niin suunnitteluperiaatteita ja suunnitelmia voidaan hyödyntää uuden ohjelmakoodin teossa. Ohjelmakoodissa voidaan käyttää esimerkiksi samanlaisia keinoja virheiden havaitsemiseen sekä kriittisten toimintojen priorisoimisessa.

Erona ohjelmistokehityksessä on myös suurempi testausaste suunnittelun eri vaiheissa. Ohjelmoinnissa koodia testataan eri vaiheissa ja testaus vaatii huomattavasti enemmän resursseja kuin teknisellä puolella jossa komponentit yleensä suunnitellaan tarkkojen määritysten ja vaatimusten kautta. Ohjelmistokehityksessä jopa puolet resursseista voi kulua testaukseen ja siitä aiheutuvaan koodin muokkaukseen. Testaus tarkoittaa ohjelmoinnissa enemmän suunnitelmallista virheiden etsintää, kuin toimivuuden testautta. Ohjelmistojen testauksessa käytetään erilaisia metodeja, kuten kuvassa 8 olevaa testauksen V-mallia. (Ohjelmistotuotanto).



Kuva 8 Ohjelmistotestauksen V-malli (Ohjelmistotuotanto)

Ohjelmiston testaus on aina kompromissi resurssien ja tarvittavan luotettavuudesta saavutetun varmuuden välillä. Monimutkaisista ja laajoista ohjelmistoista ei saada kaikkia virheitä poistettua, mutta tarvittava luotettavuuden määrä tulee saavuttaa. Ohjelmoinnissa virheiden mahdollisuutta lisää ihmisten suuri vaikutus suunnitteluun ja toteutukseen. Ihmiset kirjoittavat koodin ja valitsevat käytettävät menetelmät, mitkä nostavat virheiden mahdollisuutta.

Ohjelmistopuolella työpohjat ja dokumentit ovat hieman erilaisia tekniseen puoleen verrattuna, mutta niiden käyttötarkoitus on sama. Työpohjien avulla varmistetaan, että kaikki vaaditut toimenpiteet tulevat dokumentoiduiksi ja tehdyksi vaaditulla tavalla. Dokumentteissa on myös valmiiksi listattu jokaiselle kohdalle tarpeellinen vastuuhenkilö, joka helpottaa vastuiden jakamista ja suunnittelun osittamista. Ohjelmistopuolen työpohjat ovat hieman erilaisia, koska ne perustuvat vanhoihin projekteista tulleisiin vaatimuksiin, kuten tiettyjen lakien ja standardien noudattamiseen. Projektivaatimusten pohjalta kehitettiin työpohjat ja niiden kautta ne otettiin laajempaan käyttöön. Dokumentteja on muokattu uusien lakien, asetusten ja kokemusten perusteella, jotta niistä saataisiin mahdollisimman paljon hyötyä ja ne olisivat helppokäyttöisiä.

Ohjelmistojen pohjana on käytetty standardia IEEE 12207 - System and software engineering. Standardi antaa kuvauksen vaadittavista prosesseista koko ohjelmiston elinkaarelle konseptoinnista käytöstä poistoon. Näitä kuvauksia ja ohjeita on käytetty työpohjien ja dokumenttien laatimisessa apuna. Standardin tarkkojen kuvausten ja vaatimusten takia ohjelmistopuolen dokumentit ovat tarkempia ja jäsennellympiä kuin teknisellä puolella. Teknisen puolen dokumentteja joudutaan kuitenkin käyttämään monenlaisissa tilanteissa erilaisille komponenteille, joten niissä on oltava joustavuutta. Standardi kattaa myös laadunvalvontaa, laatudokumentointia sekä laadunvalvontaprosesseja.

Työpohjissa on korostettu tärkeimpiä kohtia, kuten toiminnallisia vaatimuksia, joille on annettu prioriteetteja, esiehtoja ja todentamisohjeita. Prioriteeteissa on kuvattu missä mielestönnessä toimintoa implementoidaan ja sen on oltava valmiina. Esiehdoilla varmistetaan vaatimukset toiminnon toteutumiseen ja todentamisessa määritellään millä keinoilla toiminto voidaan todentaa. Todennuksessa voidaan käyttää esimerkiksi katselmointia, moduulitestausta tai järjestelmätestausta.

3.5 Jarrujärjestelmän kuvaus

Tarkasteluun on valittu jarrujärjestelmä, koska se on yksi uusimmista suunnitelluista järjestelmistä ja se sisältää ostokomponentteja sekä omaa suunnittelua teknisellä- ja ohjelmistopuolella. Jarrujärjestelmä on suunniteltu ja toteutettu esitetyn tuotekehityssyklin mukaisesti. Tarkastelua on jaettu mekaaniseen ja ohjelmisto osuuksiin sekä suunnittelussa noudatettuihin toimintaperiaatteisiin. Valittuja osa-alueita käytetään myös nykytila-analyysin tarkastelussa.

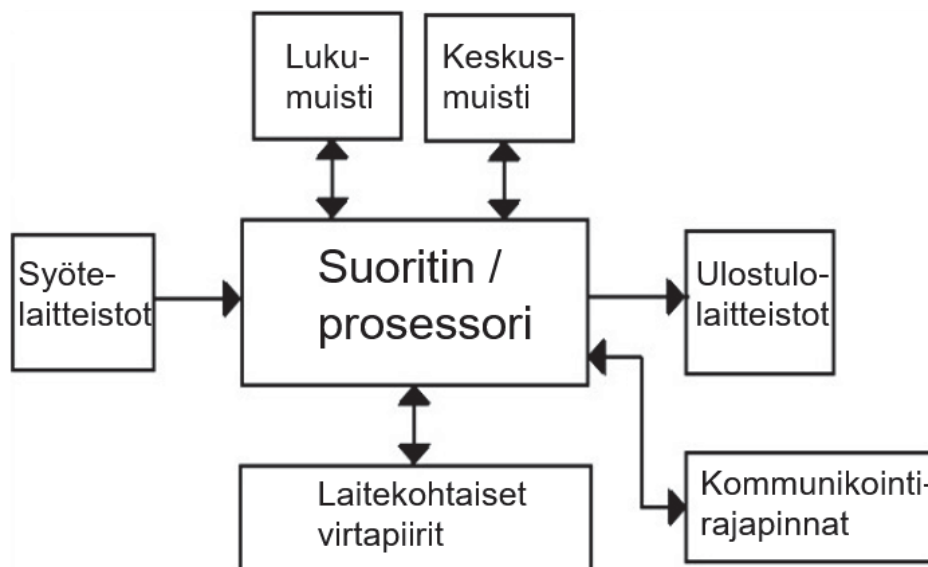
3.5.1 Laitteisto

Jarrujärjestelmän laitteisto-osuus koostuu ostokomponenteista, räätälöidyistä osista sekä kokonaan itse suunnitelluista osista. Ostokomponentteja järjestelmässä on hydrauliiikan vaatimat komponentit sekä jarrupalat, jarrupolkimet ja muut yleiset osat. Jarruyksikkö on suunniteltu ja räätälöity yhteistyössä toimittajan kanssa, jotta se sopisi ajoneuvon vaatimuksiin mahdollisimman hyvin. Omaa suunnittelua järjestelmässä on jarrulevyt sekä jarrusatulan ja jarrulevyjen kokoonpano. Kokonaisjärjestelmä on itse suunniteltu ja kasaminen sekä testaus toteutetaan itse.

Laitteistopuoli on jaettu alisysteemeihin joita ovat: jarrutus-, hydrauliiikka-, tarkkailusysteemi sekä ohjausyksikkö. Jarrutus- ja hydrauliikkasysteemit toteuttavat jarrutuksen suorittamalla tarkkailusysteemin sekä ohjausyksikön antamia käskyjä. Ohjausyksikön avulla annetaan käskyjä hydraulisille sekä sähkökomponenteille. Tarkkailusysteemi mittaa systeemin tilaa ja antaa kuskille tiedon, mikäli se havaitsee virheen. Mittausten avulla tarkkailusysteemi havaitsee, mikäli renkaat alkavat luistaa ja automaattisesti vähentää jarrutusta luistavilta renkailta tilanteen korjaamiseksi.

Jarrujärjestelmässä on erilaisia tapoja tunnistaa mahdollisia vikatilanteita. Antureilta tulevaa dataa tarkastellaan ja verrataan annettuihin raja-arvoihin. Mikäli mitatut arvot eivät ole annettujen arvojen sisällä, järjestelmä antaa kuskille varoituksen. Vikojen havainnoinnissa tarkastellaan esimerkiksi paine- ja lämpötila-antureita. Paineantureilla voidaan havaita alhaiset painetasot tai vikoja pumpussa ja hydrauliikkapiirissä. Mahdolliset vuodot havaitaan paine-eroina kahden yksikön välillä. Järjestelmä myös automaattisesti sulkee vuotavan yksikön. Vertaamalla renkaiden nopeuseroja toisiinsa nähden voidaan havaita ABS-toiminnon vikaantuminen.

Jarruissa oleva ohjainyksikkö toteuttaa myös ABS (antilock brake system) toiminnon, joka estää jarrujen lukkiutumisen. Ohjainyksikkö on toteutettu sulautettuna järjestelmänä, eli räätälöitynä toiseen järjestelmään sisällytettynä tietokoneohjattuna laitteistona. Sulautetun järjestelmän pääkomponentit ja karkea toimintatapa näkyy kuvassa 9.



Kuva 9 Sulautetun järjestelmän toiminta

Sulautetussa järjestelmässä suoritin tekee päätökset syötteiden, laitekohtaisten virtapiirien sekä kommunikointirajapintojen avulla. Syötteitä jarrujärjestelmässä ovat tarkkailu- ja ohjainsysteemit sekä käyttäjän antamat syötteet. Suorittimen tekemät päätökset ohjataan eteenpäin ulostulolaitteistoille, jotka toteuttavat käskyt. Jarrujärjestelmässä käskyjä toteuttavat jarrutus- ja hydraulikkayksiköt, jotka suorittavat varsinaisen jarrutuksen. Toimintaansa sulautettu järjestelmä tarvitsee luku- sekä keskusmuistia normaalin tietokoneen tavoin.

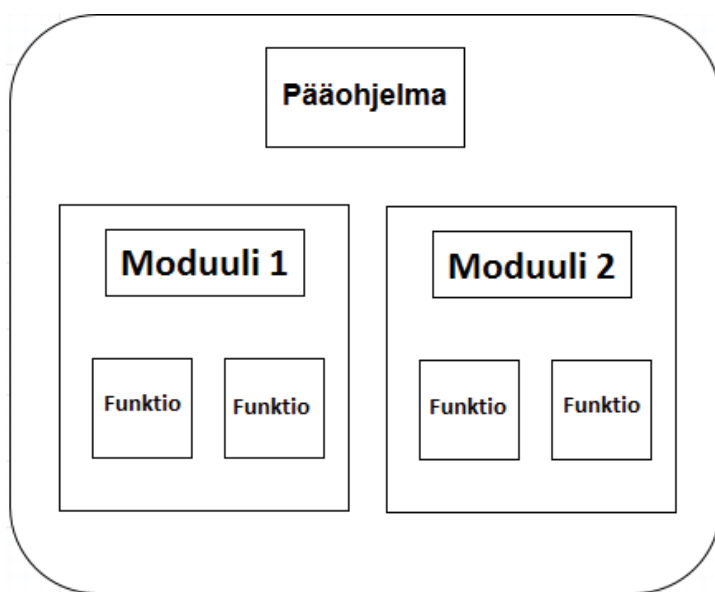
3.5.2 Ohjelmisto

Ohjelmistolla on kolme pääroolia: valvoa paineentuottoa jolla jarrutus saadaan aikaan, informoida käyttäjää havaituista vioista ja reagoida vikoihin ohjelmoituilla tavoilla. Jarrujärjestelmän ohjelmistot ovat kokonaan itse suunniteltuja ja niiden verifiointi ja validointi on myös toteutettu itsenäisesti. Ohjelmistoja tarkastellaan niissä noudatettujen suunnitteluperiaatteiden ja ohjeiden pohjalta sekä kuinka luotettavia ohjelmistot ovat. Tarkastelua toteutetaan ohjelmistojen määrittelyjen sekä vaatimusdokumenttien avulla, koska ohjelmakoodia tarkastelemalla ei nähdä käytettyjä suunnitteluperusteita ja menetelmiä.

Jarrujen ohjausjärjestelmään on laadittu kolme turvallista tilaa, johon jarrut siirtyvät erilaisissa vikatilanteissa. Vikatilanteita on sähkötön tila, kovien jarrujen tila sekä vähem-

män kriittisten vikojen tila. Kovilla jarruilla tarkoitetaan tilannetta, jossa ABS ei ole käytössä ja jarrutehoa ei kevennetä painon mukaan. Sähköttömässä tilassa jarruja voidaan käyttää mekaanisesti ajoneuvon hydrauliiikan avulla. Tarvittava painetaso jarrujen käyttöön saadaan mekaanisen latauksen avulla käyttämällä ajoneuvon dieselmoottoria. Dieselmoottori antaa tehoa hydraulipumpulle, joka lataa paineakkuja. Kuljettaja saa sähköttömästä tilasta varoitusilmoituksen jonka avulla tilanteeseen voidaan reagoida. Kovien jarrujen tilassa ohjainlaitteella on virtaa, mutta pyöräventtiileissä olevan vian takia ABS-toiminto ei ole käytössä ja jarrut voivat lukkiutua. Kuljettaja saa viasta ilmoituksen lisäksi keltaisen tai punaisen varoitusvalon vian kriittisyydestä riippuen. Vähemmän kriittisistä vioista ilmoitetaan keltaisella yleisvaroitusvalolla. Tällöin pyöräventtiileitä voidaan ohjata ja ABS -toiminto on käytössä.

Ohjelmistot on jaettu moduuleihin ja osajärjestelmiin, jotka helpottavat suunnittelua, verifiointia ja koodin kirjoittamista. Moduuleja on jaettu edelleen päämoduuleihin sekä alamoduuleihin helpottamaan monimutkaisimpia osia. Alimmalla tasolla moduuleissa on tehtäviä suorittavat funktiot. Kuvassa 10 on esitetty ohjelmistojen moduulijakoa yleisellä tasolla.



Kuva 10 Ohjelmiston moduulijako

Moduuleja voidaan ohjelmoida itsenäisesti tai pienissä ryhmissä jolloin kokonaisjärjestelmän valmistuminen on nopeampaa ja lopputulos on laadukkaampi. Moduulien muokaus on myös helpompaa, eivätkä muutokset heijastu muihin moduuleihin tai järjestelmän osiin, kun rajapinnat ja vaatimukset pidetään samoina. Moduulijaon avulla ohjelmoijat voivat keskittyä tiettyihin tarkempiin alueisiin järjestelmässä ja varmistaa niiden täytävän kaikki moduulille asetetut vaatimukset.

Ohjelmistojen toiminnallisuus on jaettu ylätasoon vaatimuksiin, jotka on edelleen hajautettu tarkemmiksi alatasoon vaatimuksiksi. Ylätasoon vaatimuksien todentaminen tehdään

täyttämällä kaikkien alatasojen vaatimukset. Vaatimukset liittyvät järjestelmän toimintaan, turvallisuuteen sekä vikojen havaitsemiseen. Jarrujärjestelmä on turvallisuuskriittinen osa ajoneuvoa, joten sen vaatimuksia ja turvallisuutta on määritelty kattavasti. Esimerkiksi ylätasoinen vaatimus: ohjausjärjestelmän pitää pystyä käyttämään siihen kytkettyjä antureita hajaantuu muun muassa vaatimukseen lukea jarrunesteen lämpötilaa, pinnankorkeutta ja ilmoittaa mikäli arvot ovat normien ulkopuolella. Toiminnallisia vaatimuksia on asetettu jokaiselle järjestelmän osalle joiden vikaantuminen voi aiheuttaa vikoja tai olla osana niiden syntymiseen.

Jarrujärjestelmässä on ei-toiminnallisia vaatimuksia, jotka vaikuttavat turvallisuuteen, käytettävyyteen sekä käyttöikään. Näitä ovat suorituskyky, turvallisuus ja suojaukset, ylläpidettävyys sekä yhteensopivuus. Ei-toiminnalliset vaatimukset on myös jaettu ylätasoinen vaatimukseen, jotka todennetaan alatasoinen vaatimusten kautta. Turvallisuutta on varmistettu esimerkiksi hidastamalla tiettyjen prosessien kiertoaikaa jolloin varmistetaan tarvittavat ajolohkot kriittisemmälle prosessille. Kaikki tarkasteltavat suureet eivät muutu yhden ohjelmakierron aikana ollenkaan tai muutokset ovat hyvin vähäisiä, joten ohjelmistojen tehtäessä tulee tietää mille prosesseille sallitaan hitaammat kiertajat. Esimerkiksi lämpötila on varsin hitaasti muuttuva suure, joten prosessoria on turhaa kuormittaa niiden liian tiheällä mittaamisella

Ohjelmistojen laatua ja toiminnallisuutta on varmistettu käyttämällä tunnettuja, laajasti käytössä olevia komponentteja sekä työkaluja. Koodia on myös ajettu simulaatioiden läpi tarkastaen, että se toimii oikeata ympäristöä vastaavassa tilanteessa. Ohjelmistojen teossa on käytetty MATLAB ohjelmiston tarjoamia malleja. MATLAB on laajasti käytössä oleva ohjelmisto, joten sen tarjoamien mallien voidaan olettaa olevan laadukkaita ja virheettömiä. Laadittujen ohjelmistojen laadusta varmistutaan verifioimalla ja varmentamalla sitä useissa kohdissa valmistusta. Koska ohjelmisto on jaettu erillisiin osiin ja moduuleihin, niitä voidaan testata itsenäisesti. Ohjelmiston toiminnallisuuden varmistamiseksi niihin on tehty erilaisia toimintoja, jotka varmistavat turvallisuuden täyttymisen. Esimerkiksi osa mitatusta datasta ajetaan suotimien läpi virheiden ja kohinan poistamiseksi. Muokkausten avulla saadaan tutkittava signaali jonka perusteella ohjelmisto voi tehdä muutoksia jarrutukseen. Ilman virheiden poistoa signaali voisi aiheuttaa viallisia muutoksia jarrutuksessa aiheuttaen vaaratilanteita.

3.5.3 Suunnittelussa noudatetut periaatteet

Jarrujärjestelmän suunnittelussa on käytetty työssä kuvattua tuotekehitysprosessia sekä työpohjia. Suunnitteluun on vaikuttanut useat eri lait, säädökset ja vaatimukset, koska kyseessä on turvallisuuteen kriittisesti vaikuttava järjestelmä. Ajoneuvolle asetetut vaatimukset, kuten käyttöympäristö, luotettavuus, huollettavuus sekä tarvittava suorituskyky ovat vaikuttaneet myös jarrujen kehitykseen. Järjestelmän turvallisuus on ollut keskeinen teema suunnittelun aikana, koska jarrujärjestelmä on turvallisuuden kannalta kriittinen osakokonaisuus ajoneuvossa.

Jarrujärjestelmä on tyyppihyväksytty, jonka pohjalta hyväksyntään vaadittava E-säännöstö on ollut tärkeä osa toiminnallisuuden suunnittelua sekä vaatimusten asettamista. E-säännöstön osa 13 ”Raskaan ajoneuvon jarrutus” kuvaa käyttötapauksia, vaadittavaa luotettavuutta sekä teho vaatimuksia jarruille. Säännöstö antaa myös vaatimuksia järjestelmän toiminnallisuuteen sekä testauksessa käytettäviin menetelmiin. Toiminnallisuudesta vaaditaan esimerkiksi, että käyttöjarrulla ja seisontajarrulla on oltava erilliset, toisistaan riippumattomat hallintalaitteet. Ottamalla säännöstön vaatimukset suoraan huomioon, ei järjestelmään tarvitse tehdä muutoksia suunnittelun jälkeen. Ajoneuvoja käytetään normaalisti maasto-olosuhteissa, mutta siirtymä kuljetaan yleisiä teitä pitkin, joten myös liikenneturvallisuuden vaatimuksia tulee noudattaa. Hyväksynnät nostavat jarrujärjestelmän luotettavuutta, koska sen toimintaa on varmennettu useilla eri tahoilla.

Testaus on kattava osa tyyppihyväksyntää ja sen kautta järjestelmälle voidaan antaa komponenttihyväksyntä. Fyysinen testaaminen on myös ainoa tapa varmistaa jarrujen toiminta oikeassa toimintatilanteessa. Tyyppihyväksynnässä vaadittavan testauksen lisäksi järjestelmälle on suoritettu laajamittaista testaamista yrityksen omasta aloitteesta. Testauksesta on laadittu suunnitelma, jossa on kuvattu testauksessa käytettävät laitteistot, tehtävä toimenpide, sen esiehdot sekä oletetut tulokset. Tällöin testauksen aikana voidaan tarkastella suunnitelmasta, miten järjestelmän tulisi toimia ja tehdä tarvittavia huomautuksia ja muutoksia oikean toiminnan perusteella. Testauksen avulla varmistetaan ohjelmistojen toiminta oikeassa konfiguraatiossa sekä laitteiston haluttu toiminta vikatilanteissa. Esimerkiksi käyttöjännitteen katketessa jarrujärjestelmän tulee ilmoittaa virheestä kuskille ja tehdä tarvittavat toimenpiteet, ettei vaaratilanteita aiheudu.

4. NYKYTILA-ANALYYSI TOIMINNAN JA STANDARDIN VAATIMUSTEN VÄLILLÄ

Nykytila-analyysiä tehdään käyttämällä esitettyjä jarrujärjestelmän osuuksia sekä toimintaperiaatteita ja verrataan niitä standardin ISO 26262 asettamiin vaatimuksiin. Tarkastelua on jaoteltu yleisemmän tason eroavuuksiin sekä muokkausta vaativiin osiin, joissa tarkastellaan syvemmin eri muutostarpeita. Mikäli jarrujärjestelmästä ei löydy kaikkia tarvittavia tarkastelukohteita, käytetään analyysissä suunnittelun yleisohjeita kyseiseen osa-alueeseen.

Aluksi tarkastelua tehdään yleisellä tasolla ja tarkastellaan turvallisuuskulttuuria sekä isompia kokonaisuuksia tunnistuen mahdollisia muutoskohteita tai puuttuvia osia. Tunnistettuja muutostarpeita käydään tämän jälkeen tarkemmin läpi ja esitetään tarpeellisia muutoksia sekä lisäyksiä toimintaan.

Tarkastelut ja vertailu standardin esittämään malliin toteutettiin haastatteleamalla vastuuhenkilöitä sekä analysoimalla dokumentteja kattavimman tuloksen saamiseksi. Pelkkien dokumenttien avulla ei saada tarkinta kuvausta, koska useasti käytössä on menetelmiä ja tapoja joita ei ole kirjallisina ohjeina tai käytäntöinä.

4.1 Turvallisuuskulttuuri

Suurin osa standardin esittämistä turvallisuuskulttuurin vaatimuksista on valmiiksi olemassa, mutta toteutustavat ja toimintojen nimeäminen ovat erilaisia. Joissain kohdissa vaatimukset ovat osittain toteutettuja, jolloin ne voidaan muokata standardin mukaisiksi pienillä muutoksilla. Esimerkiksi standardissa esitetty turvallisuuselinkaaren suunnittelu on käytössä hieman erilaisena tuotekehityksen alkupäässä sekä tuotteen käyttöönotossa, mutta tuotteen elinkaaren loppua ei suunnitella. Tuotteille tehdään jatkoprosesseissa täydentäviä turvallisuustöitä, joissa määritellään esimerkiksi tuotteen käytöstä poistoa. Jatkoprosessien turvallisuustyötä voidaan liittää alkuperäiseen turvallisuussuunnitelmaan, jolloin se on lähempänä standardin vaatimuksia.

Suurimpia eroja nykyisessä turvallisuuskulttuurissa ja standardin mallissa on suuri riippuvuus henkilöstöstä. Useat piirteet, kuten toiminnallisen turvallisuuden poikkeamien ilmoitus turvallisuusvastaavalle sekä turvallisuuspoikkeamien tehokas ratkaisu ovat henkilöriippuvaisia. Yrityksessä on prosessi, jonka avulla laatu poikkeamista voidaan ilmoittaa vastuussa oleville henkilöille, mutta se ei sovellu kaikkien poikkeamien ilmoittamiseen. Pelkkien sanallisten ohjeiden avulla työntekijät eivät välttämättä muista raportoida tarvittavista poikkeamista ja löydetyistä virheistä tai tieto ei kulje vastuussa oleville tahoille. Laatuongelmien ilmoitusprosessia voidaan muokata ja laajentaa sopimaan myös muihin

poikkeamiin. Tällöin uutta prosessia ei tarvitse luoda eikä jalkauttaa uusia prosesseja toimintatapoihin.

Henkilöriippuvaisissa järjestelmässä joitain löydettyjä virheitä saattaa jäädä huomioimatta inhimillisten virheiden tai tietämättömyyden takia. Prosessityylisessä järjestelmässä on helppoa ja selkeää jäljittää toimintoja ja niiden tekijöitä tarvittaessa. Henkilöriippuvaisessa järjestelmässä jäljitettävyyden ja dokumentoinnin takaaminen riippuvat työtä tekevästä henkilöstä.

Standardissa painotetaan suunnittelua turvallisuusnäkökulmista, mutta joissain tapauksissa aikataulut ja resurssit saattavat aiheuttaa tilanteen, jossa kaikkia haluttuja toimintoja ja analyysejä ei voida toteuttaa päätösten tueksi. Turvallisuuskriittisissä järjestelmissä ja komponenteissa kuitenkin painotetaan turvallisuutta ja toiminnot suunnitellaan turvallisuuden näkökulmasta. Tällaisia ovat esimerkiksi ohjaukseen ja jarruihin liittyvät järjestelmät ja komponentit. Normaaleissa kappaleissa ja järjestelmissä testausta ja laadunvalvontaa saatetaan joutua jättämään vähemmälle resurssien ja aikataulujen takia. Näitä toimintoja painotetaan kuitenkin enemmän, mikäli kyseessä on turvallisuuskriittinen toiminto tai järjestelmä.

4.2 Turvallisuuden erot ja uudet osiot

Kaikkia standardin vaatimia käytäntöjä, dokumentteja sekä varmennusmetodeja ei ole nykyisessä toiminnassa. Nämä toiminnot tulee ottaa käyttöön, jotta standardin vaatimukset täyttyvät. Osa toiminnoista parantaa toimintaa myös yleisellä tasolla nostamalla niiden tarpeellisuutta ja muutosten kannattavuutta.

Analyysin avulla tunnistettuja muutoskohteita on jaoteltu niiden tarkastelun selkeyttämiseksi. Osa löydettyistä muutoskohteista kuuluu useaan eri kategoriaan ja saattavat sisältää muokkauksen lisäksi myös uusia osioita, mutta niitä ei ole lueteltu uudelleen uusissa tuotekehityksen osissa. Tällaisissa tapauksissa jako on toteutettu sen mukaan, vaatiiko toimenpide enemmän muokkausta vai uusia osia.

4.2.1 Käytännöt

Turvallisuuteen keskittyviä muutoskohteita on runsaasti, koska standardi painottaa turvallisuuskeskeistä lähestymistapaa. Nykyiset toimintatavat täyttävät keskeiset turvallisuusvaatimukset, mutta kaikkia standardin piirteitä ei ole toteutettu vaaditulla tavalla tai ne ovat osittain toteutettuja. Turvallisuustyöhön liittyvää resursointia tulee parantaa, koska työkuorma ei ole tasaista työntekijöiden kesken. Suuri osa työstä kasaantuu muutamalle henkilölle, jolloin töiden laatu voi kärsiä mahdollisten kiireiden tai usean työn samanaikaisuuden takia. Turvallisuuspuolella toimintaan ja käytettäviin menetelmiin tehdään kehitysehdotuksia, mutta niiden suunnittelu ja toteutus eivät ole systemaattista.

Suunnittelemalla kehityksiä pidemmälle aikajaksolle sekä muuttamalla toimintaa systemaattisemmaksi saadaan standardin vaatimukset täytettyä kehityksen osalta.

Standardissa käytettyä turvallisuuden konseptia ei ole täysin nykyisessä toiminnassa, mutta osia siitä on valmiiksi käytössä. Nykyisessä turvallisuussuunnitelmassa on määriteltä tarpeelliset riskianalyysit ja riskien arvioinnit, mutta esimerkiksi toiminnalliseen turvallisuuteen ei oteta erikseen kantaa. Suunnitelmassa käytetään standardin vaatimusten tavoin alustavia arkkitehtuurimääräyksiä sekä suunnitellaan millä toimenpiteillä turvallisuus saavutetaan. Standardin asettamat vaatimukset ovat lisättävissä nykyiseen toimintaan pienillä muutoksilla prosessisuunnitelmiin ja muokkaamalla tarvittavat dokumentit baselineihin.

Käytössä olevilla turvallisuusvaatimuksilla ei ole omia yksittäisiä tunnistusmetodeja niiden jäljittämiseksi. Vaatimusten merkkaaminen selkeästi ja yksilöidysti helpottaa niiden tunnistamista ja niihin viittaamista dokumenteissa. Vaatimusten laatimiseen ei ole selkeitä ohjeita joilla varmistuttaisiin niiden olevan toteutettavissa sekä tilanteeseen sopivia. Turvallisuusvaatimusten määrittely ja hallinta ovat myös tapauskohtaista ja ne riippuvat projektissa määritellyistä vaatimuksista sekä niiden laatijoista. Vaatimuksista tulisi laatia esimerkkejä sekä valmiita pohjia joiden avulla ne on helpompaa kohdistaa. Ohjeistuksen avulla varmistutaan myös vaatimusten yhdenmukaisuudesta tekijästä riippumatta.

Muutosten hallinnassa ja varmennuksessa käytettävät prosessit eivät ole standardin tasolla. Muutoksista laaditaan vaatimuksia ja analysoidaan muutosten vaikutuksia toimintaan, mutta turvallisuusnäkökulmia ei painoteta tarpeeksi analyysijä tehtäessä. Muutosten vaikutuksia toiminnalliseen turvallisuuteen ei myöskään kartoiteta. Muutostenhallintaprosessia tulee kokonaisuudessaan tarkentaa ja tarkastella muutoksia yksityiskohtaisemmalla tasolla. Dokumentoinnissa muutosten vaikutukset, päätöksiin johtaneet syyt sekä päätöksistä vastaavat henkilöt tulee tuoda selkeästi esille. Muutosprosessi koskee kaikkia suunnittelun osa-alueita, joten sitä käsitellään tarkemmin yleisissä muutoskohteissa.

Turvallisuustoimintojen validoinnissa tulee standardin vaatimusten mukaisesti käyttää toiminnallisen turvallisuuden vaatimuksista johdettuja kriteereitä. Nykyisessä toteutuksessa turvallisuuden validointi ei perustu täysin toiminnallisen turvallisuuden vaatimukseen vaan ne johdetaan muista vaatimuksista. Käyttämällä toiminnallisen turvallisuuden vaatimuksia validoinnissa voidaan selkeämmin varmistua niiden täyttymisestä sekä suunniteltujen toimenpiteiden riittävydestä.

4.2.2 Dokumentit

Turvallisuuteen liittyviä dokumentteja tehdään kattavasti ja suurin osa niistä saadaan standardin piiriin muutosten avulla. Konseptointivaiheessa laaditaan tarkka kuvaus rajauksista, ympäristöstä, vaikuttavista laeista ja standardeista, mutta turvallisuuspuolta ei

tuoda tarpeeksi esille. Konseptissa ei oteta huomioon seurauksia vikatiloissa tai tunnetuissa vikatiloissa. Tällöin samoja vanhoja vikoja voi joutua tuotteeseen, tai suunnitelmia joudutaan muokkaamaan suunnittelun loppupäässä.

Käytössä olevia analyyseja joudutaan muokkaamaan standardin noudattamiseksi, koska nykyisessä toiminnassa standardia ei vielä noudateta. Standardin omat ajoneuvo kohtaiset, taulukossa 2 esitetyt vaatimukset ja luokitukset puuttuvat, mutta ne voidaan lisätä analyyseihin. Kaikkiin analyysipohjiin ei tehdä muutoksia, koska yrityksessä suunnitellaan myös järjestelmiä, jotka eivät ole standardin piirissä. Käytössä olevia analyysejä tulisi myös yhtenäistää, jotta niistä saatavat tulokset ovat paremmin vertailukelpoisia ja selkeämpiä.

Toimittajien kanssa tehdään yhteistyötä ja räätälöidään joitain komponentteja ajoneuvoon sopiviksi. Nykyisessä toiminnassa kaikkia standardin vaatimia dokumentteja ja todennuksia toiminnoista ei ole käytössä. Toimittajien tulisi raportoida ennen toimitusta, mikäli tuotteissa huomataan poikkeamia tai on riski, ettei projektisuunnitelmassa pysytä. Yhteistyönä tehtävistä komponenteista tulee laatia dokumentit joista käy ilmi molempien yritysten vastuulliset henkilöt sekä vastuiden jako suunnittelun aikana. Raportoinnin ja dokumentoinnin avulla yritys voi valmistautua muutoksiin ja tehdä tarvittavia toimenpiteitä niiden pohjalta. Käytössä oleviin dokumentteihin voidaan tehdä tarvittavat lisäykset vastuiden jaosta sekä käytettävistä virstanpylväistä.

4.3 Laitteiston erot ja uudet osiot

Laitteiston tarkasteluun on otettu jarrujärjestelmän komponentit, jotka täyttävät standardin vaatimukset. Tällaisia ovat turvallisuuskriittiset sähköiset -, elektroniset - ja ohjelmoitavat järjestelmät. Työssä ei tarkastella mekaanisia osia, mutta myös niiden kestävyyttä ja vikavälejä on laskettu sekä otettu huomioon suunnittelussa. Nykytilassa standardin asettamia ASIL-luokkiin viittaavia vaatimuksia ja toimintoja ei ole toteutettu, koska standardin vaatimukseen perehdytään työn avulla. Näitä vaatimuksia ei käsitellä työssä, koska ne vaativat järjestelmälle ASIL-luokitusta ennen jatkotarkastelua.

Nykyisessä toimintamallissa ei ole erillistä osiota systeemitason suunnittelulle, joten sitä tarkastellaan laitteisto- ja ohjelmistosuunnittelun ohessa. Systeemisuunnittelusta vastaa osittain samat vastuuhenkilöt, joten sitä voidaan tarkastella samaan aikaan laitteiston ja ohjelmiston kanssa. Systeemisuunnittelu antaa ylätasoa vaatimuksia laitteistolle ja ohjelmistolle joita tarkennetaan laitteiston- ja ohjelmiston suunnittelussa.

4.3.1 Käytännöt

Laitteisto- ja systeemisuunnittelussa noudatetaan useassa kohtaa standardin vaatimuksia suoraan tai pienillä eroavaisuuksilla. Järjestelmän turvallisuustoiminnot on otettu tarkasti

huomioon ja ne täyttävät suoraan standardin asettamia vaatimuksia. Järjestelmä esimerkiksi siirtyy turvalliseen tilaan ja sulkee viallisen osan pois käytöstä, mikäli se vikaantuu. Järjestelmä havaitsee myös piileviä vikoja, kuten antureiden vikaantumista tai johtojen katkeamista. Antureista aiheutuvat piilevät viat huomataan antureiden kahdentamisen avulla vertaamalla niiden antamia signaaleja. Anturivikoja havaitaan myös, mikäli anturi ilmoittaa viasta, vaikka tilanne on raja-arvojen sisällä.

Jotkin standardin vaatimat prosessit ovat toteutettuna, mutta niitä ei ole erikseen määritelty toimintaohjeisiin. Standardin vaatimukseen kuuluu integraatiotarkastelua ja verifiointia, kun laitteisto- ja ohjelmistoelementtejä liitetään toisiinsa ja elementtejä liitetään systeemiin. Nykyisissä prosesseissa systeemejä tarkastellaan aina uusien osien liittämisen jälkeen, mutta toimintaa ei ole kuvattu prosesseihin tai vaatimuksiin. Vaatimukset voidaan kuitenkin helposti lisätä toimintaan ja prosessikuvauksiin, koska ne toteutuvat jo käytännön kautta. Pieniä lisäyksiä ja tarkennuksia tulee lisätä, mutta pääprosessi ja toiminta ovat valmiina.

Integraatiovaiheessa tehtävien tarkastelujen lisäksi järjestelmille tehdään erilaisia testauksia järjestelmä- sekä ajoneuvotasolla. Turvallisuuskriittisille järjestelmille, kuten jarruille, tehdään laajempaa testaamista. Jarrujärjestelmän testausta on kuvattua kattavammin sen kuvauksen yhteydessä luvussa 6. Testausta suunniteltaessa ja tehtäessä ei ole valmiiksi listattu mahdollisia vikaantumistapoja tai mitä toimintoja voi mennä vikaan. Testauksesta saadaan suurempaa hyötyä, mikäli sitä suunnitellaan tarkemmin ja mietitään mahdollisia vikatilanteita ennen testaamista. Tällöin vikatilanteiden purkaminen on nopeampaa ja testaamista voidaan jatkaa. Muokkaamalla testaamista järjestelmällisemmäksi sekä lisäämällä sen suunnitelmallisuutta saadaan standardin vaatimukset täytettyä.

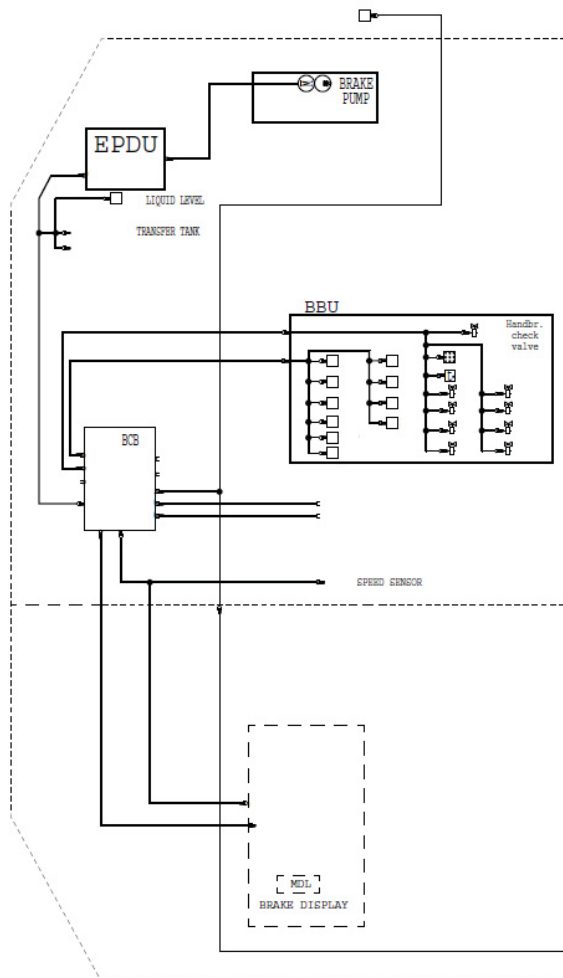
Laitteistolle ja systeemille asetetut vaatimukset eivät ole selkeästi jäljitettävissä tai yksilöllisesti tunnistettavissa. Kaikkia noudatettavia toimintoja ei myöskään ole kirjattu vaatimukseen. Mikäli vaatimuksia ei ole kirjattu, niiden täyttymistä ei voida varmentaa tai analysoida niiden vaikutusta muihin järjestelmän osiin. Kirjaamattomat vaatimukset eivät välity kaikille järjestelmän parissa työskenteleville jolloin päätöksiä saatetaan tehdä väärin perustein. Tämä luo turvallisuuden muutoksissa kuvattuja haittoja, kuten yhdenmukaisuuden puutetta vaatimusten kesken. Ulkopuolisilta toimittajilta tulevien laitteiden asettamia systeemivaatimuksia ei myöskään analysoida tai tarkastella laajamittaisesti. Vaatimusten laatimiseen ja analysointiin on laadittava selkeät prosessit, joiden avulla kaikille niiden kanssa työskenteleville on selkeää, kuinka niitä laaditaan ja validoidaan.

Turvallisuusanalysejä tehtäessä tarkastellaan suurimmaksi osaksi vain järjestelmän pysäyttäviä, single-point, virhetilanteita. Noudatettavan E-säännösten vaatimuksista muutamia usean vian, multiple-point, tilanteita on myös otettu tarkasteluun. Standardin vaatimuksissa on tarkastella molempia tapauksia ja laatia niiden todennäköisyyksille kvanti-

tatiivisia arvioita. Nykyisiä analyysejä voidaan laajentaa tarkastelemaan laajemmin useamman vian tilanteita sekä antaa niille kvantitatiivinen arvio. Arviointiin on ensin kerättävä riittävä määrä dataa, jonka perusteella arviointi on luotettavaa.

4.3.2 Arkkitehtuurikuvaukset ja systeemisuunnittelu

Standardissa käytetään arkkitehtuurikuvauksia systeemisuunnittelun tukena koko prosessin aikana. Arkkitehtuuria hahmotellaan suunnittelun alkuvaiheessa ja sitä tarkennetaan suunnittelun edetessä. Arkkitehtuurikuvauksen avulla vaatimuksia voidaan kohdentaa elementteihin ja analysoida niiden täyttymistä. Nykyisessä toiminnassa arkkitehtuurikuvauksia ei laadita systeemisuunnittelun ohessa. Kuvausten teko toteutetaan myöhemässä vaiheessa, kun komponentit ja suunnittelu on jo suurimmaksi osaksi toteutettu. Kuvasta 11 nähdään jarrujärjestelmästä tehty arkkitehtuurikuvaus, joka on standardin vaatimusten mukaisesti sähkökaaviotasolla.



Kuva 11 Arkkitehtuurikuvaus sähkökaaviotasolla

Myöhemmässä vaiheessa tehtävät kuvaukset poistavat monia niiden antamia hyötyjä, koska ne eivät ole tukena suunnittelun aikana. Ilman arkkitehtuurikuvausta valittua systeemijakoa on myös hankalaa analysoida, koska kokonaisuudesta ei ole selkeää kuvausta josta nähdään riippuvuudet osasysteemien välillä. Analysointimahdollisuuden puuttuessa systeemisuunnitelman optimointi ja tarkastaminen ovat hankalaa ja joitain toimintoja saatetaan joutua muokkaamaan suunnittelun jälkeen. Turvallisuus- ja muiden vaatimusten kohdentaminen ja validointi ovat työläämpiä toteuttaa ilman kuvauksia, koska riippuvuudet ja rajapinnat tulee selittää sanallisesti tai alemman tason kuvasten avulla. Projektin ulkopuolisille henkilöille on hankalaa saada selkeä kuvaus suunnittelussa olevasta järjestelmästä ja valintakriteereistä ilman arkkitehtuurikuvauksia ja kaavioita. Arkkitehtuurikuvausten tekoon tulisi panostaa enemmän, koska ne tarjoavat paljon hyötyä suunnitteluvaiheessa. Aikaisessa vaiheessa arkkitehtuurin panostaminen vähentää huonojen päätösten tekoa ja vähentää työntekijöiltä kuluvaan aikaan perehtyä systeemin toimintaan.

Systeemisuunnittelussa laitteistoa ja ohjelmistoa on standardin vaatimusten tapaan jaoteltu alasysteemeihin, joiden avulla ylätason vaatimuksia voidaan todentaa. Standardissa jakoa jatketaan elementtitasolle jolloin vaatimusten kohdentaminen ja varmentaminen ovat selkeämpiä ja helpompia laatia. Nykyisessä toimintamallissa jakoa ei jatketa elementtitasolle, joten testaaminen on suoritettava suurempina kokonaisuuksina. Alemman tason tarkastelussa hyötynä on yksityiskohtaisempi ja tarkempi testaaminen jolloin voidaan helpommin huomata virheitä elementissä. Selkeä elementtijako helpottaa tuotekehitystä ja suunnittelua, koska kokonaisuuden tarkastelu on systemaattisempaa ja tarkempaa. Nykyistä prosessia voidaan muokata jatkamaan pidemmälle ja jakaa alasysteemejä elementtitasolle jolloin sen hyödyt saadaan suunnitteluun. Elementtijakoa voidaan käyttää myös järjestelmän julkaisun jälkeisiin piirteisiin, kuten modifiointiin tai käytöstä poistoon. Näitä piirteitä ei oteta huomioon nykyisen systeemisuunnittelun aikana. Julkaisun jälkeisten toimintojen huomioon ottaminen suunnittelun aikana nopeuttaa modifiointien tekoa ja helpottaa tuotannon jälkeistä suunnittelutyötä.

Suunniteltaessa ja valittaessa järjestelmän laitteistoja ja komponentteja niiden vaatimuksia ei järjestelmällisesti vertailla toisiinsa tai ajoneuvon kanssa. Vaikka komponentit täyttäisivät ajoneuvon asettamat vaatimukset voivat ne olla keskenään epäsoivia esimerkiksi erilaisen käyttöjännitteen tai datan kulun suhteen. Laitteiston ja ohjelmiston rajapinnassa luotetaan ohjaintoimittajan dokumentaatioon ja siellä annettuihin tuloksiin ja dataan. Laitteisto tulee luotettavalta ulkoiselta valmistajalta, mutta sen toiminta normien ylittävissä tilanteissa olisi hyvä tietää käytettävän ajoneuvokonfiguraation kanssa, jotta toimintaa vikatilanteissa voidaan ennustaa paremmin. Vikatilanteissa toiminta voi olla konfiguraatiokohtaista ja vaikuttaa eri tavalla erilaisiin komponentteihin.

Suunnitteluvaiheiden lopussa ennen tuotantoon siirtymistä standardissa vaaditaan katselmus, jossa tarkastetaan, että kaikki vaaditut toiminnot ja dokumentit on tehty. Katselmuksessa tarkastetaan toiminnallisen turvallisuuden arviointi ja muiden turvallisuustoimenpi-

teiden hyväksyty validointi. Dokumentti toimii samalla koosteena tehdyistä toimenpiteistä, koska siihen kasataan käytettyjen tuotteiden versiot, konfiguraatiot sekä referenssit liittyviin dokumentteihin. Nykyisessä toimintamallissa tuotantoon siirtymisestä ei laadita erillisiä tarkastusdokumentteja tai katselmuksia. Hyväksymismenetelmä voidaan luoda osaksi muutos- tai konfiguraatiohallintaa, jolloin myös muutosten tarkastelu ja validointi saadaan osaksi toimintaprosesseja. Muutosten analysointiin ja validointiin tarvittavia prosesseja on kuvattu yleisissä parannuksissa, koska se koskee kaikkia osa-alueita.

4.3.3 Dokumentit

Systeemi- ja laitteistosuunnittelussa tehtävät dokumentoinnit kattavat osittain standardin vaatimukset, mutta joitain muutoksia on myös tehtävä. Systeemikuvausten laatimiseen ja dokumentointiin ei ole kuvauksia tai ohjeita, joten ne eivät ole yhtenäisiä tai järjestelmällisesti laadittuja. Alemman tason tarkat menetelmät ja niiden kuvaukset ovat yhtenäisiä ja järjestelmällisesti laadittuja, koska niistä on tarkat spesifikaatiot. Ylemmän tason toimintaa tulee parantaa ja laatia ohjeistuksia kuvausten tekoon, jotta niiden laatua saadaan parannettua standardin vaatimalle tasolle. Osaa tehtävistä systeemikuvauksista, kuten arkkitehtuurikuvauksia on siirrettävä aikaisempaan vaiheeseen suunnittelussa. Nykyisessä toiminnassa kuvausten teko jätetään suunnittelun jälkeiseen vaiheeseen jolloin siitä ei saada hyötyä ja kuvauksia ei voida analysoida. Tarkemman tason kuvauksia voidaan tehdä myöhäisessä suunnitteluvaiheessa, kun valitut komponentit ja elementit ovat tiedossa.

Käytössä olevassa validointisuunnitelmassa käytetään E-säännöstöstä johdettuja vaatimuksia, jotka ovat samantyyllisiä standardin kanssa. Validointisuunnitelma sisältää esimerkiksi tuotteen konfiguraation, hyväksymiskriteerit sekä ympäristökriteerien tarkastelun. Validointisuunnitelmaan on myös sisällytetty järjestelmän verifiointia. Validoinnista laaditaan oma raportti josta käy ilmi mitä vaatimuksia on hyväksytty ja hylätty. Raportissa ei ole eritelty erikseen turvallisuuteen liittyviä vaatimuksia, koska kaikki kohdat käsitellään validoinnin jälkeen läpi. Validointisuunnitelma saadaan standardin piiriin pienillä muutoksilla käytettäviin testitapauksiin, jotka tulee valita järjestelmän ASIL-luokituksen mukaisesti. Näitä vaatimuksia järjestelmä ei voi vielä täyttää, koska sille ei ole määritetty ASIL-luokitusta.

Nykyisessä toiminnassa on piirteitä, jotka täyttävät standardin vaatimukset, mutta toimintaa ei ole kuvattu omana prosessinaan. Järjestelmän pysäyttäviä vikoja on analysoitu ja tarkastelujen pohjalta on tehty suunnittelutoimenpiteitä niiden estämiseksi. Järjestelmään on esimerkiksi valittu kestävämpiä tai turvallisuuden kannalta parempia osia. Näitä valintoja ei ole dokumentoitu nykyisessä toiminnassa, mutta valinnoista voidaan laatia dokumentointia, jossa analysoidaan osavalintoja ja päätöksiä. Tällöin suunnittelun jälkeen on mahdollista tarkastaa osavalintoihin vaikuttaneet päätökset ja toiminnot sekä validoida niiden riittävyys.

4.4 Ohjelmistojen erot ja uudet osiot

Ohjelmistojen kohdalla tarkasteluun on valittu yrityksen itse tekemiä ohjelmistoja ja koodia. Tarkastelussa ei oteta kantaa ulkoisilta toimijoilta ostettuihin ohjelmistoihin tai laitteiden mukana tulleeseen koodiin. Yleisesti järjestelmien ohjelmistoja ei tehdä kokonaan alusta asti vaan käytetään valmiita ohjaimia ja muita komponentteja, joita räätälöidään toimintaan sopivaksi. Toimintoihin lisätään myös turvallisuuspiirteitä ja varmistetaan laitteiden keskinäinen toimivuus. Nämä muutokset ja lisäykset kuuluvat kuitenkin standardin piiriin ja niitä verrataan standardin vaatimuksiin.

Systemisuunnittelu koskee laitteiston lisäksi ohjelmistojen suunnittelua ja toteutusta, joten sitä tarkastellaan soveltuvin osin. Tarkastelussa keskitytään vain ohjelmistoihin liittyviin osioihin eikä laitteiston puolella käytyjä osa-alueita tarkastella uudelleen, mikäli ne eivät vaikuta ohjelmistosuunnitteluun. Jotkin piirteet, kuten arkkitehtuurikuvaukset koskevat molempia osioita, mutta tarkastelua tehdään vain ohjelmistokehityksen näkökulmasta.

4.4.1 Käytännöt

Ohjelmistosuunnittelu otetaan suunnittelun alusta asti huomioon turvallisuuskriittisissä ja komplekseissa järjestelmissä. Muissa tapauksissa ohjelmiston kehitys aloitetaan viimeistään ensimmäisiä teknisiä spesifikaatioita laadittaessa. Ohjelmistosuunnittelun alkua, kuten vaatimusten määrittelyä, tehdään yhteistyönä laitteistopuolen kanssa. Ohjelmisto- ja laitteistosuunnittelussa on yhteisiä rajapintoja ja ne vaikuttavat samoihin toimintoihin, joten vaatimusten määrittämisessä ja alkusuunnittelussa tarvitaan molempia osapuolia. Vaatimusten laatiminen laitteistosuunnittelun kanssa varmistaa, että molemmilla suunnittelupuolilla on samat lähtökohdat ja loppuvaatimukset järjestelmälle.

Ohjelmistojen ja järjestelmien suunnittelussa on valmiiksi useita piirteitä, joita myös standardissa vaaditaan. Ajoneuvojen pitkän käyttöiän takia elinkaari ja ohjelmistojen muokattavuus otetaan huomioon suunnittelussa alusta asti standardin asettamien vaatimusten tavoin. Modifiointi, muokattavuus ja ylläpidettävyys ovat aina vaatimuksina ohjelmistoja suunniteltaessa. Standardin vaatimusten mukaisesti käytettävät metodit, ohjelmointikielet ja työkalut on valittu yhteensopiviksi koko kehityksen kanssa. Näiden valintojen avulla voidaan myös helpottaa ylläpidettävyyttä ja nostaa ohjelmistojen laatua. Valitsemalla projektiin sopivimmat ohjelmointikielet ja työkalut voidaan minimoida virheiden määrää ja varmistua ohjelmistojen olevan muokattavissa vuosien päästä. Esimerkiksi yrityksessä ohjelmistopuolelle valittu MATLAB ohjelmisto on käytössä maailmanlaajuisesti, joten sen toimivuutta on testattu ja virheitä minimoitu. Laajasti käytössä olevia ohjelmistoja myös päivitetään ja ylläpidetään säännöllisesti eikä niiden käytöstä poisto ole todennäköistä.

Varsinaista koodia kirjoittaessa käytettävät metodit ja käytännöt ovat nykyisessä toiminnassa standardin vaatimusten mukaisia. Standardissa annetut suositukset riippuvat järjestelmän ASIL-luokituksista, mutta yrityksen nykyisessä toiminnassa ohjeistuksia noudatetaan kaikissa ohjelmistoissa, koska ASIL-luokitukset eivät ole vielä käytössä. Mikäli joitain huonoja menetelmiä, kuten globaaleja muuttujia, joudutaan käyttämään koodia tehtäessä, niille tarjotaan perusteluja. Perusteluissa kuvataan syyt menetelmän käytölle, tarkastelut sen vaikutuksista sekä vaihtoehtoisten menetelmien huonot puolet.

Ohjelmistopuolella tulee tehdä muutoksia resursointiin ja toimintakäytäntöihin, jotta voidaan varmistua standardin vaatimusten täyttymisestä. Joissain tapauksissa vain yksi henkilö tekee järjestelmän koodin ja kaikki siihen liittyvät oheisprosessit. Tällöin arkkitehtuurikuvaukset ja suunnitelmat eivät välttämättä tule tehdyksi tai eivät ole kunnolla validoituja. Yhden henkilön tekemänä ohjelmistoista voi jäädä alemman tason testausta pois, kuten moduuli- ja integrointitestaukset. Tällöin valmiiseen ohjelmistoon voi jäädä huomattavasti enemmän virheitä ja niiden poistaminen on työläämpää. Muiden työntekijöiden on myös hyvin hankalaa nähdä tehtyjä suunnittelupäätöksiä tai ohjelmiston kulkua ilman kattavaa alkupään suunnittelua ja kuvauksia. Useammalla työntekijällä ja pidemmillä aikatauluilla voitaisiin parantaa ohjelmistojen laatua ja varmistaa, että alkupään suunnitteluun ja kuvausten tekoon on riittävästi aikaa.

Vähiten lisäresursseja vaativa tapa muokata toimintaa olisi suunnittelutöiden ja koodin kirjoittamisen hajauttaminen useammalle työntekijälle. Työntekijöille annettaisiin yksittäisiä osia prosessista, kuten arkkitehtuurin kuvaaminen tai moduulijaon laatiminen. Tällöin varmistutaan työn dokumentoinnista ja se voitaisiin validoida helpommin. Seuraava työntekijä näkisi nopeasti ja selkeästi suunnittelupäätökset ja voi jatkaa työskentelyä järjestelmän parissa. Moduulijaon avulla saadaan myös parannettua testaamista ja ylläpidettävyyttä. Hajauttaminen saattaisi kuitenkin aluksi hidastaa toimintaa ja vaatisi hieman lisäresursseja kuten aikaa ja henkilöstöä. Näillä toimilla voidaan kuitenkin huomattavasti vähentää loppupäässä tehtäviä lisätöitä.

4.4.2 Arkkitehtuurikuvaukset ja systeemisuunnittelu

Ohjelmistopuolella käytetään laitteistopuolen tavoin arkkitehtuurikuvauksia suunnittelun apuna. Ohjelmistoarkkitehtuurin kehityksessä huomioidaan standardin asettamia turvallisuusvaatimuksia, kuten ohjelmistokomponenttien vuorovaikutusta, rajapintoja, datan kulkemista sekä prosessointijärjestyksiä. Arkkitehtuurin pohjalta ohjelmistoille laaditaan tarkempi suunnitelma, tekninen määritelmä, jossa määritellään yksityiskohtaisemmin ohjelmiston osien toimintaa. Teknisen määritelmän laatiminen riippuu järjestelmän laajuudesta ja kompleksisuudesta. Yksinkertaisimmille järjestelmille ja ohjelmistoille ei laadita erillistä teknistä määritelmää, koska arkkitehtuurikuvaus riittää kuvaamaan toimintaa. Mikäli ohjelmisto on laadittu MATLAB mallien avulla, sen muodostama kuvaus on myös riittävä yksikertaisemmille järjestelmille.

Arkkitehtuurikuvaukset auttavat suunnittelussa ja ohjelmistojen moduulijaossa. Ohjelmistojen suunnittelussa, samoin kuin laitteistopuolella, arkkitehtuurikuvausten teko ei ole riittävän suunnitelmallista tai järjestelmällistä. Joissain projekteissa kuvausten ja suunnitelmien tekoon panostetaan, mutta toiminta on henkilö- sekä projektiriippuvaista. Arkkitehtuurikuvausten puuttuminen aiheuttaa laitteistopuolella kuvattuja ongelmia, kuten vaikeampaa vaatimusten kohdentamista sekä suunnitelmien todentamista. Puutteelliset arkkitehtuurikuvaukset sekä alkupään suunnittelut näkyvät kasvavana työmääränä suunnittelun edetessä. Arkkitehtuurien tekoon ja yleiseen suunnitteluun ei aina haluta kuluttaa paljoa resursseja, koska halutaan tuloksia ja testattavia järjestelmiä mahdollisimman nopeasti. Myös ohjelmistopuolella arkkitehtuurien ja teknisten määrittelyjen tekoon tulisi varata enemmän aikaa ja resursseja, jotta ne voidaan tehdä laadukkaasti. Tällöin niistä saadaan eniten hyötyä ja niitä voidaan käyttää suunnittelun ja validoinnin tukena prosessin aikana.

Systemisuunnittelun avulla on otettu huomioon useita turvallisuustoimintoja, joiden avulla varmennetaan ja seurataan ohjelmiston toimintaa. Jarrujärjestelmän suunnittelussa on painotettu turvallisuustoimintoja, koska kyseessä on turvallisuuskriittinen järjestelmä. Ohjelmistojen suoritusajoja ja kiertoajoja seurataan, jotta voidaan varmistaa prosessoreilla olevan tarpeeksi vapaata aikaa. Tällä varmistetaan, että prosessori pystyy käsittelemään kiireellisiä turvallisuustoimenpiteitä niiden ilmetessä. Järjestelmässä myös käytetään staattista muistinvarausta jolloin ei ole vaaraa liiallisesta muistinkäytöstä. Staattista muistinkäyttöä suositetaan myös standardin antamissa suunnitteluohjeissa.

Ohjelmisto- ja laitteistosuunnittelussa käytetään samaa rakennehyväksyntää, jonka tarkoituksena on tarkastaa laitteiston ja ohjelmiston toimivuus sekä vaatimusten täyttyminen. Tässä suunnitteluvaiheessa ohjelmistosta ei kuitenkaan ole valmiina kuin tarkka tekninen määrittely sekä hieman aloitettua koodia, joten ohjelmiston toimivuutta ei voida varmentaa. Ohjelmiston ja laitteiston suunnittelu ja toteuttaminen ovat hyvin erilaisia prosesseja, joten niissä tulisi olla erilaiset hyväksyntäprosessit. Ohjelmistoja yleensä testataan ja tarkastellaan kirjoittamisen yhteydessä, koska niissä on suurempi riski inhimillisiin virheisiin. Laitteistopuolella osia ja järjestelmiä suunnitellaan yleensä tarkkojen spesifikaatioiden avulla ja tulosten varmentaminen on mahdollista vain lopussa. Projektin kulkuun voisi lisätä kohdan, jonka avulla varmistutaan, että järjestelmän kaikki osa-alueet ovat valmiita testaukseen. Lisäys voisi olla katselmus tai kevyempi tarkastus. Testivalmiuskatselmus olisi helppoa laatia prosessikulkuun ja sen avulla saataisiin myös dokumentoitua validointi testaushyväksynnälle.

4.4.3 Testaus, verifiointi ja validointi

Osa toiminnoista täyttää standardin asettamat vaatimukset, mutta projektikohtaisista käytännöistä riippuen niitä ei aina noudateta. Ohjelmistoturvallisuuden vaatimuksissa keskitytään standardin vaatimusten tavoin ohjelmistopohjaisiin toimintoihin joiden virheet voivat aiheuttaa teknisen turvallisuuden menetyksiä. Vaatimuksia määriteltäessä otetaan

huomioon olemassa olevat systeemikuvaukset, konfiguraatiot sekä rajapinnat. Vaatimusten laatiminen on kuitenkin henkilö- sekä projektiriippuvaista ja vaatimusten validointiin tai verifiointiin ei oteta kantaa niiden tarkastamista laadittaessa. Esimerkiksi turvallisuuden validoinnissa käytettävät hyväksyntäkriteerit johdetaan joissain tapauksissa standardin tapaan toiminnallisen turvallisuuden vaatimuksista. Kaikissa projekteissa ei kuitenkaan toimita näin, mutta projektikuvauksiin voidaan muokata vaatimus käytettävistä validointimenettelyistä, jolloin toiminnassa ei ole vaihtelua ja standardin vaatimukset saadaan täytettyä.

Nykyisessä toiminnassa monet verifioinneissa ja varmennuksissa tehtävät toiminnot riippuvat työskenneltävän järjestelmän tai laitteiston monimutkaisuudesta. Käytössä olevat menetilat ovat samanlaisia standardin esittämien toimintojen kanssa. Tällaisia ovat esimerkiksi katselmukselut, läpikulkutarkastelut, prototyypit, testaus ja simulaatiot. Katselmuksia toteutetaan jokaisessa projektissa ja niissä käydään läpi järjestelmän toiminnallisia vaatimuksia ja järjestelmän toimintaa. Jokainen tehty ohjelmisto myös testataan ajoneuvossa oikealla käyttökonfiguraatiolla. Uutena tarkastelumenetelmänä on otettu testikäyttöön staattinen kooditarkastelu, joka on myös standardin esittämässä menetelmässä. Standardin toimintamallissa vaihtoehtoista tulee valita sopivimmat toiminnot työskenneltävän järjestelmän tai laitteiston ASIL-luokituksen perusteella. Nykyisessä toiminnassa verifiointimenetelmät määritetään suunnitteluvaiheessa testaus- ja verifiointisuunnitelmiin.

Ajoneuvossa testaamisen lisäksi ohjelmistoa tarkastellaan eri tavoin koodin kirjoittamisen aikana sekä sen valmistuttua. Suunnittelun alkuvaiheessa laaditaan testaus suunnitelma, jossa määritellään vaadittavat verifiointimenetelmät riippuen ohjelmiston kompleksisuudesta. Valmiita moduuleja sekä osakokonaisuuksia testataan integraatiovaiheessa mahdollisimman pieninä osina ennen niiden liittämistä suurempaan järjestelmään. Tällöin havaitaan helpommin virheitä, jotka johtuvat osakokonaisuuksien rajapinnoista tai liitoksista. Mikäli järjestelmän kompleksisuus on hyvin alhaisella tasolla, integraatiotestaus jätetään yleensä tekemättä. Suuri osa koodin tarkastelusta painottuu kuitenkin lopputarkastuksiin ja katselmuksiin. Loppuvaiheessa tehtävien katselmusten avulla on hankalaa tarkastaa koodia yksityiskohtaisesti ja järjestelmällisesti, koska ohjelmistot voivat olla rivimääriltään hyvin mittavia. Komplekseista ohjelmistoista ei katselmuksissa voida tarkastaa kuin yleistä toimivuutta sekä suunnitteluvaihtojen kelpoisuutta resurssirajoitusten takia.

4.4.4 Dokumentit

Ohjelmistopuolen dokumenteissa on kuvattu standardin vaatimusten mukaisesti järjestelmä, johon koodia tehdään. Kuvauksessa on esimerkiksi ympäristö, rajapinnat, toiminnot, varmennuskeinot sekä kuinka turvallisuus on otettu huomioon. Järjestelmäkuvausessa on myös määritelty missä kohtaa suunnittelua ja toteutusta vaatimukset varmenneetaan sekä mitä menetelmiä varmennuksessa käytetään. Dokumentit eivät suoraan tarvitse suuria muutoksia, mutta niihin voidaan tehdä joitain pieniä lisäyksiä. Esimerkiksi lisäys

käytettävistä validointimenetelmistä voidaan lisätä dokumentteihin, jolloin kaikissa projekteissa käytettäisiin samoja menetelmiä.

Dokumenttien avulla voidaan helposti tehdä pieniä muutoksia toimintaan. Ohjelmistopuolella seurataan suunnitteludokumenteissa olevaa järjestystä, joten niihin voidaan tehdä lisäyksiä ja muokkauksia, jotka päätyvät helposti toimintaan. Dokumenttien muokkauksen lisäksi on tehtävä koulutusta ja opastusta uusista kohdista. Kaikkia muutoksia ei kannata tehdä suoraan, vaan lisäillä niitä hiljalleen, jotta työntekijät ehtivät sisäistää muutokset sekä niiden tarkoitukset.

4.5 Yleisiä muutoksia

Yleiset käytännöt keskittyvät koko tuotekehityssykliin ja koskevat kaikkia käsiteltyjä osa-alueita. Jokaisesta tarkastelualueesta löytyi yleisiä parannuksia, joiden avulla voidaan selkeyttää ja parantaa toimintaa. Muutoksia on tehtävä esimerkiksi alkupään suunnitteluun, dokumentointiin sekä käytössä oleviin ohjelmistoihin.

Jotkin kuvatuista muutoksista ja parannuksista on selitetty tarkemmin osatarkasteluissa, vaikka ne vaikuttavat myös yleisesti kaikkiin alueisiin. Esimerkiksi arkkitehtuurikuvausten teko vaikuttaa kaikkiin osiin hieman eri tavalla, joten ne on kuvattu yksityiskohtaisemmin laitteiston ja ohjelmiston tarkasteluissa.

4.5.1 Käytännöt

Tuotekehitykseen liittyy useita käytäntöjä ja ne täyttävät valmiiksi osittain standardin vaatimukset. Pienten muutosten ja lisäysten avulla nykyisiä käytäntöjä voidaan muokata standardin piiriin. Yleisistä käytännöistä muokkausta tarvitaan esimerkiksi prosessien seurantaan. Nykyisessä järjestelmässä prosesseja seurataan, mutta turvallisuusnäkökulmat, verifiointi sekä varmennus eivät ole standardin vaatimalla tasolla. Prosessien seuranta tulee tarkentaa ja tehdä tarvittavat verifiointit turvallisuuteen liittyville osille kehityksen edetessä, jotta standardin vaatimukset saadaan täytettyä. Lisäysten avulla voidaan myös reagoida nopeammin prosessissa tapahtuviin muutoksiin, koska kuvaukset ovat tarkempia ja dokumentointi kattavampaa.

Tärkeä huomio analyysiä tehtäessä oli, että kaikki työntekijät eivät käytä yrityksen yleistä IMS-toimintajärjestelmää. Järjestelmään on kasattu tuotekehitysprosessin kulku sekä vaatimuksia ja dokumenttimalleja. Noudattamalla näitä ohjeita ja seuraamalla järjestelmän mallia tulisi alkupään suunnittelu paremmin toimintaan ja kuvauksia laadittaisiin nykyistä paremmin. Toimintajärjestelmään täytyy silti tehdä muokkauksia, kuten erottaa systeemis suunnittelu erilliseksi osa-alueeksi. Muokkauksia tehtäessä järjestelmää voitaisiin muokata helpommin käytettävämmäksi sekä suunnata sitä enemmän työntekijöiden käyttöön sopivaksi.

Jokaisella tuotekehityksen alueella tarvitaan parannusta alkupään suunnitteluun ja järjestelmäkuvausten laatimiseen. Alkupään suunnittelussa voidaan vaikuttaa päätöksiin ja tehtäviin toimintoihin huomattavasti helpommin ja nopeammin, joten suunnitelmia ja päätöksiä tulisi analysoida ja validoida nykyistä enemmän. Kattavat kuvaukset myös auttavat muita projektin ulkopuolisia henkilöitä ymmärtämään järjestelmän kulkua ja siihen vaikuttavia tekijöitä tekstimuotoisia dokumentteja helpommin.

4.5.2 Dokumentit

Nykyisessä toimintatavassa turvallisuuteen liittyviä dokumentteja ja tuotoksia ei kasata projektikohtaisesti samaan paikkaan, vaan kaikki dokumentit laitetaan tuotetiedonhallintajärjestelmään. Standardissa esitetään käytäntöä, jossa kaikki turvallisuuteen liittyvät dokumentit kasataan tiettyyn paikkaan niin sanottuun ”turvallisuussalkkuun” josta ne löydetään helposti tarvittaessa. Kyseistä käytäntöä ei ole nykyisesti käytössä, joten sellainen on laadittava standardin vaatimusten täyttämiseksi. Tällainen menettely auttaa dokumenttien arkistointia ja löytämistä, joten se tuo lisäarvoa myös ilman standardin noudattamisvaatimuksia.

Nykyisessä toimintatavassa muutoksista ei tehdä tarkkoja analyyskejä vaan keskitytään yleisemmällä tasolla niiden vaikutuksiin. Standardin vaatimaa tarkkaa muutosanalyysiä ei ole, joten niistä on laadittava uutta dokumentointia. Muutosanalyysi tehdään tilanteessa, jossa muokataan olemassa olevaa järjestelmää tai kappaletta. Muutosten tunnistamisen lisäksi laaditaan vaikutusanalyysi, jossa tunnistetaan ja kuvataan suunnitellut muokkaukset tuotteeseen, ympäristöön, rajapintoihin tai toiminnallisiin tilanteisiin. Muokkausten lisäksi analyysissä tulee arvioida muutosten vaikutukset järjestelmään tai kappaleeseen. Mahdolliset vaikutukset toiminnalliseen turvallisuuteen tulee arvioida ennen muutosten tekoa. Mikäli toiminnalliseen turvallisuuteen tulee muutoksia, tulee ne ottaa huomioon riskianalyysissä sekä turvallisuusvaatimuksissa. Kaikkiin muokattaviin dokumentteihin on tehtävä selkeät merkinnät mitä kohtia on muutettu, mikä on edellisen version tunnistustapa sekä kuka on tehnyt kyseiset muutokset. Selkeiden analyysien ja dokumenttien avulla varmistetaan muutosten systemaattinen suunnittelu, kontrollointi sekä dokumentointi. Muutosprosessin lopuksi muutosalueen vastuuhenkilön tulee tarkastaa analyysien tulokset ja vaikutukset tuotteeseen ja hyväksyä tai hylätä muutos sen aiheuttamien vaikutusten perustella.

4.5.3 Käytössä olevat ohjelmistot

Osa turvallisuustöissä käytössä olevista ohjelmistoista on lisenssipohjaisia, mutta kaikille turvallisuustöitä tekeville ei ole saatavilla lisenssejä. Esimerkiksi käytössä olevaa suunnitteluohjelmistoa käytetään vikapuuanalyysien laatimisessa. Ohjelmistoon on vain muutamia lisenssejä, joten kaikki turvallisuustöitä tekevät eivät pääse tarkastelemaan alkupe-

räisiä tiedostoversiota. Lisenssipohjaisilla ohjelmistoilla voi syntyä tilanne jossa uusimpia versioita dokumenteista ei ole saatavilla ja töitä on tehtävä vanhojen versioiden pohjalta. Vanhoja versioita käytettäessä tiedot voivat olla virheellisiä, joka johtaa vääristyneisiin analyysien tuloksiin.

Dokumentit ja muut tuotokset siirretään työntekijöiden toimesta tuotetiedonhallintaohjelmistoon. Ohjelmistossa olevilla dokumenteilla on yksittäiset numerot, joiden perusteella niitä tai niiden vanhempia versioita voidaan hakea. Haku voidaan toteuttaa myös dokumenttikuvausten avulla, mutta kuvausten teossa ei ole käytössä yhteisiä ohjeistuksia, joten dokumenttien löytäminen voi olla hankalaa ilman numeroa. Ohjelmiston heikkoutena on, ettei dokumenttiversioiden välillä tehtyjä muutoksia ole näkyvissä. Muutokset kirjataan dokumenttikuvaukseen, mutta kuvausten tekeminen on henkilöriippuvaista eikä tehtyjä muutoksia aina päivitetä tai selitykset ovat puutteellisia. Joissain tapauksissa muutoksia kirjataan myös itse dokumentin sisään, mutta se on henkilöriippuvaista. Dokumentteja käyttävien on hankalaa tietää dokumenttia lukematta, kuinka paljon siihen on tehty muutoksia. Kuvausten tekoon tulisi tehdä tarkemmat ohjeistukset ja varmistaa, että kaikki käyttävät samanlaisia ohjeita. Ohjelmistossa voisi olla myös sisäänrakennettuna ohjeistukset kuvausten tekoon, jolloin erillisiä ohjeita ei tarvitse etsiä kuvauksia tehdessä.

5. TULOSTEN TARKASTELU

Tuloksia on jaoteltu osatehtävien ja analyysin tulosten perusteella. Tarkastelun tuloksina löydettiin kohteita, jotka on muokattava standardin vaatimusten saavuttamiseksi. Näiden lisäksi löydettiin yleisiä kehityskohteita, jotka hyödyttävät toimintaa, vaikka standardia ei otettaisi käyttöön. Löydetyt kohteet on kategorioitu niiden kriittisyyden mukaan ja niiden saavuttamiseksi on annettu parannusehdotuksia.

Tuloksia tarkastellessa esille on nostettu vain suurimpia muutoksia ja lisäyksiä. Kaikkien pienempien muutosten listaaminen ja analysointi on mahdotonta toteuttaa työn puitteissa. Keskittymällä suurimpiin ja tärkeimpiin muutoksiin voidaan niille tarjota vaadittavia muutostoimenpiteitä, priorisointia sekä aikataulutusta.

Kaikkia standardin vaatimuksia on paikoitellen hankalaa noudattaa, koska niille ei anneta mittasuhteita tai esimerkkejä. Tällöin päätävältä on yrityksellä ja käytännössä toimintaa ei välttämättä tarvitse muokata ollenkaan. Esimerkiksi standardin ohjelmistosuunnittelun ohjeissa mainitaan tiettyjen toimintojen olevan huonoja, eikä niitä tulisi käyttää laajasti. Tätä ei määritellä selkeämmin, joten yritys voi itse päättää missä määrin on sopivaa käyttää kyseistä toimintoa. Tällaisiin piirteisiin kiinnitetään kuitenkin huomioita ja pyritään minimoimaan niiden käyttö.

5.1 Työn kohteiden selvitys

Kohteita selvitettiin tarkastelemalla dokumentteja ja toimintajärjestelmää sekä haastatteleamalla vastuuhenkilöitä. Tarkasteltavat alueet ovat hyvin laajoja, joten niistä valittiin työn kannalta tärkeimmät kohdat ja perehdyttiin niiden sisältöön. Tarkasteluissa on keskitytty tuotekehitykseen ja suunnittelun alkupäähän työn rajausten takia.

Tarkastelun aluksi perehdyttiin yleiseen tuotekehitykseen toimintajärjestelmän kautta, jolla saatiin yleiskuvaa nykyisestä suunnitteluprosessin kulusta. Tuotekehitykseen perehtymisen jälkeen tarkasteltiin yksityiskohtaisemmin jarrujärjestelmää ja siinä tehtyjä suunnittelupäätöksiä. Näiden jälkeen nykyistä tuotekehitystä verrattiin standardin vaatimukseen ja kuvattiin tarvittavat muutokset.

5.1.1 Tuotekehityssykli

Tuotekehityssykliin perehtymisessä käytettiin suurimmaksi osaksi toimintajärjestelmässä olevia dokumentteja ja ohjeistuksia, koska niiden avulla saatiin kattava kuvaus tuotekehityksen kulusta. Järjestelmää käyttämällä saatiin myös sama kuvaus, joka kaikilla työntekijöillä on käytössä. Tuotekehitystä tarkasteltiin erillisesti laitteistopuolelta sekä ohjelmistopuolelta, koska ne ovat toiminnassa jaettu erillisiksi suunnittelupuoliksi.

Tuotekehityssyklin kuvausten perusteella saa selkeän käsityksen missä järjestyksessä toimituksia tehdään sekä mitä dokumentteja vaaditaan ennen siirtymistä virstanpylvästä eteenpäin. Tarkasteltavan tuotteistamisprosessin kuvaukset ja dokumentit ovat helppolukuisia ja hyvin jäsennettyjä mikä lisää niiden käytettävyyttä. Tuotekehityksen kuvauksiin ja dokumenttipohjiin tulee joitain muutoksia standardin takia, mutta niiden perustat voidaan pitää samana. Järjestelmässä olevat työpohjat ovat kuitenkin suurimmaksi osaksi ylätasen dokumentteja, eikä niitä voida täysin hyödyntää normaalissa suunnittelutyössä.

5.1.2 Jarrujärjestelmä

Jarrujärjestelmän tarkastelu jaettiin laitteisto- ja ohjelmistopuoleen erillisen suunnittelun ja työn selkeyttämisen takia. Tarkastelu toteutettiin suunnitteludokumenttien avulla sekä haastattelemalla molempien suunnittelupuolien vastuusuunnittelijoita. Haastattelujen avulla saatiin lisätietoa suunnittelussa käytetyistä perusteista sekä piirteistä joita ei ole dokumentoitu.

Järjestelmää koskevista dokumenteista on nähtävissä yrityksen osaaminen suunnitella sekä toteuttaa monimutkaisia ja kriittisiä järjestelmiä. Yrityksellä on pitkä kokemus tuotelähtöisestä suunnittelusta, joka näkyy selkeissä ja hyvin jäsennetyissä dokumenteissa ja tuotekuvauksissa. Ylemmän tason suunnittelussa ja kuvausten teossa on kuitenkin parannettavaa ja niiden käyttöä tulee laajentaa. Ylätasen kuvauksen auttavat suunnittelussa sekä validoinnissa ja standardi painottaa niiden käyttöä suunnittelun aikana. Kuvauksia on olemassa järjestelmille, mutta ne ovat laadittu hyvin myöhäisessä vaiheessa suunnittelua. Yrityksellä on tietotaitoa tehdä kyseisiä kuvauksia ja dokumentteja, joten pienellä lisäresursoinnilla ne voidaan ottaa laajempaan käyttöön tuotekehitysprosessiin.

5.2 Nykytila-analyysi

Analyysin pohjana toimivat tarkastelut tuotekehityssyklistä sekä jarrujärjestelmästä. Jarrujärjestelmän suunnittelussa noudatettuja periaatteita verrattiin standardin asettamiin vaatimuksiin ja kuvattiin tarvittavat muutokset. Vertailu toteutettiin pääpainoisesti haastatteluilla, koska niiden avulla saatiin paras mahdollinen kuvaus nykyisestä toiminnasta. Analyysi on tehty mahdollisimman kattavasti, koska työn pääpaino on analyysin tuloksissa ja tarvittavien muutosten tarkastelussa.

Nykytila-analyysin tuloksina saatiin muutoskohteita standardin noudattamiseksi. Muutoskohteita löydettiin jokaisesta tarkastellusta osa-alueesta. Löydetyt muokkauskohteet parantavat ja selkeyttävät toimintaa myös yleisellä tasolla standardin täyttämisen lisäksi. Esimerkiksi muutosanalyysien lisääminen ja henkilöriippuvuuden vähentäminen auttavat muokkaamaan toimintaa selkeämmäksi ja lisäämään dokumentointia.

5.2.1 Turvallisuus

Nykytila-analyysin avulla saatiin selkeä kuvaus turvallisuuskulttuurin tilanteesta sekä yleisestä turvallisuuden tasosta. Turvallisuustoiminnoissa pääkohdat ovat hyvällä tasolla, mutta pieniä muutoksia ja lisäyksiä on tehtävä, jotta standardin vaatimukset saadaan täytettyä. Muutosten laajuus vaihtelee pienistä lisäyksistä sekä toimintojen yhdistämisestä kokonaan uusien osioiden luomiseen. Suurin osa muokkauksista on kuitenkin pieniä ja helppoja toteuttaa.

Turvallisuuskulttuurissa kaikkia yritystä koskevia piirteitä ei voida selkeästi määrittää, koska standardi jättää päätäntävaltaa toimintojen toteutukseen. Esimerkiksi vaatimukset turvallisuuskulttuurin ylläpitämisestä ja kehittämisestä eivät anna vaatimuksia millä tasolla toiminnan tulee olla. Yrityksessä on kuitenkin valmiiksi mietitty turvallisuuspiirteitä ja tehty turvallisuuskulttuurin eteen työtä sekä mietitty kehityskohteita.

Yksi suurimmista tarvittavista muutoksista turvallisuuskulttuuriin on standardin esittämän turvallisuuselinkaaren käyttöönotto. Elinkaaren luominen vaatii nykyisten toimintojen yhdistämistä sekä muokkaamista. Esimerkiksi nykyisessä toiminnassa tuotteelle tehtävät lisäanalyysit käytöstä poistoa koskien tulee lisätä normaaliin analysointiin ja turvallisuustyöhön. Konfiguraatiohallinta on myös nykyisessä toimintamallissa vähäistä, mutta sitä voidaan parantaa turvallisuuselinkaaren käyttöönotolla. Turvallisuuselinkaari tulee ottaa käyttöön jokaisessa suunnittelualueessa ja validoida suunnittelupäätöksiä sen avulla. Muokkausten avulla turvallisuuselinkaari tulee muokata helppokäyttöiseksi, jotta kaikki suunnittelun osa-alueet voivat käyttää sitä ja tarkastaa järjestelmään kohdistuvat turvallisuusvaatimukset. Näiden muutosten avulla suurimmat turvallisuuskulttuurin erot saadaan poistettua standardin ja nykyisen toiminnan välillä.

Jarrujärjestelmää tarkasteltaessa kävi ilmi, että turvallisuusvaatimuksilla ei ole standardin vaatimia yksilöllisiä tunnistusmetodeja joiden avulla niitä voidaan hakea tai viitata niihin. Vaatimusten laatiminen on projekti- ja henkilöriippuvaista, joten vaatimuksissa saattaa olla huomattavasti eroa projektien välillä. Vaatimusten laatimisesta tulisi kehittää ohjeistuksia tai järjestelmä, jonka avulla niille voidaan antaa yksilölliset tunnistusmenetelmät. Tällöin vaatimuksiin voidaan viitata helpommin ja niiden kanssa työskentely on selkeämpää.

Pienempiä muutoksia, joita löytyi haastattelujen ja dokumenttien tarkastelun ohessa on esimerkiksi analyysien muuttaminen sekä uusien analyysien luominen. Nykyisiä analyysipohjia voidaan hyödyntää ja tehdä niihin pieniä lisäyksiä, jotta ASIL-luokitukseen liittyvät muutokset saadaan turvallisuusanalyysiin. Myös muita olemassa olevia toimintoja ja dokumentteja voidaan käyttää tai muokata sopimaan standardin vaatimukseen, joka vähentää vaadittavaa työmäärää.

5.2.2 Laitteisto

Analyysissä tarkasteltiin laitteiston lisäksi samanaikaisesti systeemisuunnittelua, koska sillä ei ole omaa kohtaa yrityksen toimintamallissa. Systeemisuunnittelulle tulisi laatia oma prosessi toimintamalliin, koska sillä on suuri vaikutus tuotekehityksen kulkuun sekä muihin kehitysvaiheisiin. Systeemisuunnittelulla varmistetaan ylemmän tason suunnitelmien ja kuvausten olevan valmiina, kun siirrytään laitteiston ja ohjelmistojen suunnitteluun.

Yksi työn tärkeimpiä muutoskohteita on tuotekehityksen alkupäähän sijoittuvan suunnittelun muuttaminen ja kehittäminen. Tarkasteluissa ja haastatteluissa tuli ilmi, että suunnittelun alussa ei panosteta standardin kuvaaman systeemisuunnittelun osa-alueisiin, kuten arkkitehtuurikuvauksiin ja moduulijakoihin. Ilman ylemmän tason suunnittelua päätöksiä ja valintoja on hankalaa validoida ja vaatimuksia ei voida kohdentaa. Projektin parissa työskentelevät joutuvat perehtymään hyvin tarkasti käsiteltävään järjestelmään, jotta sen toiminnasta, rajapinnoista ja muista toiminnoista saadaan selkeä kuvaus. Kattavilla arkkitehtuurikuvauksilla ja selkeillä moduulijaoilla järjestelmän yleinen toiminta nähdään selkeästi ja tarvittaessa voidaan tarkastella syvemmin yksittäisten moduulien toimintaa.

Haastattelujen aikana huomattiin, että arkkitehtuurikuvauksia tekevillä henkilöillä ei ole selkeää ohjeistusta tai esimerkkejä, kuinka laatia kuvauksia ja moduulijakoja. Kuvauksia tehdään vanhojen projektien perusteella ja muokataan niitä omien kokemusten perusteella. Tämän takia kuvaukset eivät ole järjestelmällisesti laadittuja tai yhtenäisiä tekijöiden ja projektien kesken. Yhtenäisemmin ja aikaisemmassa vaiheessa tehtyjen kuvausten hyödyt näkyisivät suunnittelun loppupäässä. Tällöin muutoksia ei tarvitse enää tehdä tai miettiä järjestelmän toimintaa, koska kaikki on validoitu jo aikaisemmassa vaiheessa. Ylemmän tason suunnitteluun tulee panostaa huomattavasti enemmän ja se vaatii muutoksia, jotta standardin vaatimukset saadaan siltä osin täytettyä. Muutokset auttavat huomattavasti tuotekehityksessä myös yleisellä tasolla, joten niiden muokkaaminen on priorisoitu korkealle.

Analyysissä löydettiin jarrujärjestelmästä myös pienempiä muutoskohteita, kuten integraatiotarkastelun sekä verifiointin puuttuminen dokumentoinnista. Kyseiset tarkastelut tehdään laitteistolle, mutta nykyisessä toiminnassa niitä ei dokumentoida. Luomalla näille dokumentointipohjat ja päivittämällä ne toimintajärjestelmään saadaan standardin vaatimukset tältä osin täytettyä. Jarrujärjestelmään valittujen komponenttien taustalla olevat syyt ja päätökset eivät myöskään ole näkyvillä tai dokumentoitu. Valintaperusteet voidaan lisätä olemassa oleviin dokumentteihin, jolloin muutosten jalkauttaminen on helpompaa.

Uutena lisäyksenä laitteiston suunnitteluun tulee lisätä tuotantoon siirtymistä edeltävä katselmus. Tämän tarkastuksen avulla varmistetaan, että kaikki vaadittavat toimenpiteet

on tehty ja validoitu ennen valmistuksen aloittamista. Tarkastukseksi riittää esimerkiksi pienimuotoinen katselmus jossa on jokaisen suunnittelualueen vastuuhenkilöt tarkastamassa dokumenttien validointi ja vaatimusten täyttyminen.

5.2.3 Ohjelmistot

Jarrujärjestelmän ohjelmistoja analysoitaessa tarkasteluun valittiin laitteistosuunnittelun tavoin myös systeemisuunnittelua. Systeemisuunnittelua parantamalla ohjelmistojen suunnittelua voidaan selkeyttää ja muokata järjestelmällisemmäksi. Systeemisuunnitteluun kohdistuvat muutokset ovat hyvin samankaltaisia ohjelmistojen ja laitteiston suunnittelussa.

Ohjelmistosuunnittelun näkökulmasta arkkitehtuuri- ja systeemikuvauksia tulisi laatia aikaisemmassa vaiheessa suunnittelua, jotta ohjelmistoja voidaan helpommin jakaa moduuleihin. Ohjelmakoodin kirjoittaminen ja koodin tarkastaminen ovat huomattavasti helpompaa toteuttaa moduulitasolla kuin laatia suoraan yksi iso kokonaisuus. Selkeä moduulijako myös tukee esitettyä menetelmää, jossa työtä hajautetaan useammalle työntekijälle. Hajauttamisen avulla kuvausten teko selkeytyy, testaamista saadaan helpotettua ja toiminnot dokumentoidaan. Jarrujärjestelmää tarkasteltaessa kävi ilmi, että sen toteutus ei ole moduulipohjainen tai hajautettuna toteutettu, mikä on hankaloittanut koodin läpikäyntiä ja virheiden etsimistä.

Nykyisessä toimintamallissa laitteisto- ja ohjelmistosuunnittelulle on käytössä samat hyväksyntämenettelyt ja tarkastukset. Esimerkiksi testaushyväksyntää haettaessa laitteistopuolella suunnittelut on tehty ja prototyyppejä on valmiina. Ohjelmistopuolella on yleensä valmiina vasta tekninen määrittely ja joitain koodin osia. Hyväksyntä ja tarkastusmenettelyt tulisi standardin vaatimusten mukaan laatia laitteistolle ja ohjelmistoille erikseen, koska niiden valmistusprosessit ovat hyvin erilaisia.

Testausmenettelyihin täytyy tehdä muutoksia, jotta standardin vaatimukset saadaan täytettyä. Suurin tarkasteluissa löydetty muutos testauksessa koskee alemman tason testausta, kuten moduulien sisäistä ja välistä testausta. Alimman tason testausta tehdään nykyisessä toiminnassa vähäisesti joissain projekteissa, mutta se on hyvin tärkeää koodin laadun varmistamiseksi. Virheiden havaitseminen ja korjaaminen ovat hankalampia toteuttaa, mikäli niiden etsiminen keskitetään vain valmiiseen koodiin. Nykyisessä toimintamallissa tarkastelu painottuu loppukatselmuksiin, joissa ei voida käydä koko koodia läpi järjestelmällisesti ja yksityiskohtaisesti. Staattinen koodin tarkastelu voidaan myös ottaa isommaksi osaksi toimintaa, mikäli tarkasteltavasta järjestelmästä jää hyvät kokemukset ja se nähdään hyödyllisenä.

Testausta ja yleistä koodin kirjoittamista voidaan helpottaa hankkimalla lisää lisenssejä MATLAB ohjelmistoon. Kyseisen ohjelmiston avulla voidaan helposti testata ja tarkastaa koodia kirjoittamisen aikana. Ohjelmistoon on sisäänrakennettu tarkastustoimintoja,

kääntäjä sekä yleisiä ohjeita koodin kirjoittamiseen. Lisenssit ohjelmistoon ovat kalliita, mutta niiden antamat hyödyt testaamiseen ja suunnittelun jälkeisiin muutoksiin tulisi arvioida. Ottamalla huomioon suunnittelun jälkeiset muutokset sekä virheiden korjaaminen, lisenssien hankkiminen voi olla hyvin kannattavaa.

Ohjelmistosuunnittelussa, kuten muissa osa-alueissa, on paljon pieniä muutoksia, jotka saadaan standardin vaatimusten tasolle vähäisillä resursseilla. Useat vaadittavat muutokset ovat jo olemassa, mutta niitä noudatetaan vain tietyissä osissa toimintaa. Siirtämällä nämä vaatimukset koskemaan kaikkea toimintaa, saadaan standardin vaatimukset helposti täytettyä ilman lisäresursseja.

5.2.4 Yleiset osat

Monet tarkasteluissa ja haastatteluissa löydettyistä muutoksista koskevat standardin esittämään ASIL-luokitukseen liittyvien lisäysten tekemistä. Esimerkiksi turvallisuussalkun luominen tai laitteistosuunnittelussa olevaan validointisuunnitelman testitapauksiin tulee lisätä ASIL-luokituksiin liittyvät tapaukset. Tarvittava muutos ei ole kovin suuri, mutta samankaltaisia pieniä muutoksia on useita, minkä takia kaikkien tarvittavien kohtien muokkaaminen vaatii aikaa ja useita työntekijöitä.

Yksi tärkeimpiä jarrujärjestelmän tarkastelussa löytyneistä muutoskohteista on alkupään suunnittelun puute. Järjestelmällisen ja systemaattisen suunnittelun avulla tuotekehityksen alkuvaiheessa voidaan laatia tarkemmat ja selkeämmät kuvaukset suunniteltavasta tuotteesta tai järjestelmästä. Tarkempien kuvausta avulla suunnittelua on helpompaa jatkaa ja validoida. Tämä myös helpottaa muita työntekijöitä hahmottamaan suunnitelmia ja liittymään tarvittaessa projektiin. Panostamalla enemmän tuotekehityksen alkupäähän saadaan useita muutoskohteita poistettua. Alkupään suunnittelulla voidaan estää monia työssä esille tulleita ongelmakohtia, kuten arkkitehtuurikuvausten puutetta sekä vaatimusten kohdentamista.

Alkupään suunnittelu vaikuttaa jokaiseen tarkastelussa olleeseen osa-alueeseen sekä muihin V-mallissa esitettyihin kohtiin. Tämän takia alkupään suunnittelu on erittäin kriittinen kohta tuotekehityksessä ja sen parannukseen tulee käyttää resursseja. Selkein tapa toteuttaa muutos on jakaa systeemisuunnittelu omaksi osa-alueeksi, joka toteutetaan ennen muiden suunnittelujen aloittamista. Lähes kaikki tarvittavat toiminnot ovat jo olemassa, mutta ne tulee kerätä samaan paikkaan ja tehdä niistä ohjeistuksia. Tällöin varmistutaan systeemisuunnittelun dokumentoinnista ja verifioinnista.

Jarrujärjestelmää tarkastelemalla sekä suorittamalla haastatteluja löydettiin tärkeä huomio henkilöstön toimintatavoissa. Vain harva suunnittelija käytti olemassa olevaa IMS toimintajärjestelmää normaalissa työskentelyssä. Henkilöstö käytti samoja toimintatapoja kuin vanhoissa projekteissa, eikä ennen työn aloittamista tarkastettu järjestelmästä prosessin vaatimuksia tai mahdollisia muutoksia. Mikäli järjestelmää käytettäisiin enemmän

ja siellä olevaa prosessikuvausta seurattaisiin, tuotekehityksen alkupään suunnitteluun kiinnitettäisiin enemmän huomiota. Järjestelmän käyttöastetta voitaisiin myös saada nostettua muokkaamalla siitä selkeämpi ja kohdistamalla sitä enemmän suunnittelijoiden arkkikäyttöön sopivaksi. Vanhojen toimintatapojen muokkaaminen vaatii myös johdon tuen, jotta järjestelmän käyttö otetaan osaksi normaalia toimintaa.

5.3 Muutoskohteiden priorisointi

Muutoskohteita löytyi jokaiseen prioriteetti-alueeseen, mutta suurin osa muutoskohteista on kategoriassa kolme. Esimerkiksi aiemmin kuvattu validointisuunnitelman muutos ASIL-eheystason perusteella kuuluu kategoriaan kolme. Muutos on pieni, eikä se ole kriittisimpien joukossa standardin käyttöönoton kannalta, joten sen prioriteetti on alhainen. Kaikkia luokan kolme muutoksia ei ole listattuna taulukkoon, jotta luettavuus ja selkeys eivät heikkene. Esitetyt tapaukset ovat suuntaa antavia ja kuvaavat minkälaisia muutoksia prioriteetti-alueeseen on sisällytetty. Prioriteetti-alueen yksi ja kaksi muutoskohteet ovat kaikki listattuna taulukkoon, koska ne ovat kriittisempiä ja tulisi suorittaa ennen muita muutoksia. Prioriteetti-alueen sisällä muutoskohteita ei ole lajiteltu erikseen kriittisyyden mukaan, vaan kaikki kohteet oletetaan yhtä tärkeiksi. Muutoskohteiden priorisoinnit ovat kerättyinä taulukkoon 3.

Taulukko 3 Muutoskohteiden priorisointi

Muutos-priori-teetti	Kehityskohde
1	Systeemisuunnittelun erottaminen, arkkitehtuurikuvaukset, ohjelmistosuunnittelun hajauttaminen, ohjelmistokoodin kattavampi tarkastelu valmistuksen aikana, tuotekehitysprosessin seuranta IMS-järjestelmästä
2	Turvallisuuselinkaari, turvallisuusvaatimusten yksilöiminen, muutosanalyysit, tehdyn työn dokumentointi
3	Pienemmät yleismuutokset ja lisäykset eri osa-alueilla: ASIL-luokitukseen liittyvät muutokset, integraatiotarkastelun ja verifioinnin lisääminen dokumentointiin, tuotantokatselmus, käytössä olevien ohjelmistojen muokkaus

Kaikki korkeimman muosprioriteetin kohteet liittyvät yleiseen toimintaan eivätkä ole suoranaisesti standardikohtaisia. Kohteet löytyivät standardia tarkastelemalla, mutta ne ovat yleisiä tuotekehitykseen liittyviä muutoksia, eivätkä standardin painottamia turvallisuuskohteita. Nämä toiminnot tulisi muokata ensimmäiseksi, koska ilman niitä joitain

alemman prioriteetin muutoksia on hyvin hankalaa tehdä nykyiseen järjestelmään. Laadukkaalla alkupään suunnittelulla voidaan helpottaa turvallisuustyön tekemistä ja varmistaa laitteiden ja järjestelmien laatu sekä turvallisuus. Muutokset tulisi tehdä toimintaan standardista riippumatta tuotekehitysprosessin parantamiseksi. Käytössä olevat muutosresurssit tulisi kohdistaa ensisijaisesti kategorian yksi ja kaksi muutoksiin ja näiden jälkeen keskittyä pienempien muutosten toteuttamiseen.

5.4 Vaadittavat toimenpiteet

Yksittäisille parannusehdotuksille on kuvattu tarkkoja ratkaisuvaihtoehtoja niiden esittelyn yhteydessä nykytila-analyysissä. Tärkeimpiä muutoskohteita on otettu esille myös tämän luvun yhteydessä ja esitetty niille parannusehdotuksia. Tässä kappaleessa kuvataan myös toimenpiteitä ja muutoksia, joita ei ole tuotu muussa yhteydessä esille.

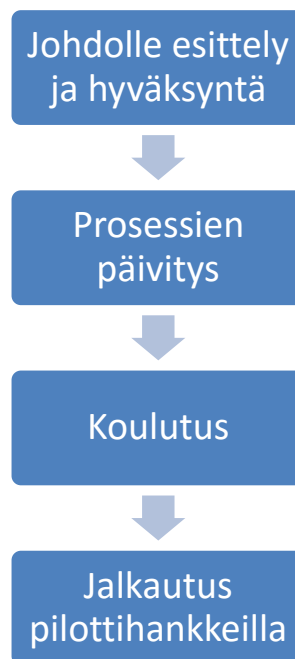
Tärkein vaadittava piirre muutosten teolle on johdon tuki ja kannustus. Ilman kattavaa ja selkeää tukea johdolta, muutokset eivät ajaudu osaksi normaalia toimintaa ja työskentelyä. Johdon tulee uskoa muutosten hyötyyn ja kannattavuuteen sekä saada työntekijät vakuuttuneeksi tästä. Omalla esimerkillä ja uskomalla muutoksiin johto saa työntekijät pysymään paremmin uudessa toimintatavassa sekä estettyä työntekijöiden palaamisen vanhoihin työskentelytapoihin.

Useissa kohtaa haastatteluissa sekä jarrujärjestelmää tarkasteltaessa ilmeni tilanteita, joissa standardin vaadittavia piirteitä oli suoritettu, mutta niitä ei ollut dokumentoitu. Tällaisia tilanteita oli esimerkiksi testaamisessa sekä toimintojen verifiointissa. Kaikki mahdollisesti tarpeelliset varmennukset ja testaukset tulisi dokumentoida, jotta niihin voidaan viitata ja tarkastaa tiedot tulevaisuudessa. Tehtyjen toimintojen dokumentoinnin lisääminen ei vaadi paljoa resursseja, koska ainoana lisäyksenä ne tarvitsevat dokumenttipohjat. Yrityksessä on käytössä useita erilaisia työpohjia, joita voidaan käyttää apuna ja luoda uudet pohjat samantyyllisiksi.

Muutosten toteuttamiseksi vaaditaan myös resursseja kuten henkilöstöä ja aikaa. Monet muutokset voidaan kuitenkin tehdä normaalin toiminnan ohessa ja päivittää toimintajärjestelmään muutosten valmistuttua. Tällöin työskentelyä ei tarvitse muuttaa suoraan tai keskeyttää muutosten takia. Muutosten tekoon tulisi saada henkilöstöä jokaiselta osa-alueelta johon muutos vaikuttaa. Esimerkiksi systeemisuunnittelun erottaminen erilliseksi osa-alueeksi vaatii työntekijöitä laitteisto, ohjelmisto sekä turvallisuuspuolelta. Tämän avulla varmistutaan, että muutos on kaikille osa-alueille sopiva ja kohdistuu tarpeellisiin piirteisiin.

5.5 Muutosten aikataulutus

Muutosten käyttöönottoon vaadittavaa aikataulua suunniteltiin yhdessä yrityksen edustajien kanssa. Aikataulutukseen ei määritelty tarkkoja toteutumisaikoja muutosten käyttöönottoon, koska niiden noudattaminen saattaisi olla hankalaa ja ne voisivat haitata lopputulosta. Muutosten käyttöönotossa tulee panostaa koulutukseen ja muutosten jalkauttamiseen, joiden toteutumista tarkkojen aikataulujen noudattaminen saattaisi häiritä. Aikataulutukseen valittiin menetelmä, joka perustuu muutosten toimeenpanemiseksi vaadittavaan tapahtumaketjuun. Tapahtumaketju on jaettu neljään osaan, jotka on esitetty kuvassa 12.



Kuva 12 Muutosten toteuttamiseksi vaadittava tapahtumaketju

Muutosten toimeenpano tulee aloittaa esittelemällä muutosehdotukset johtoryhmälle, joka hyväksyy muutokset ja päättää missä laajuudessa ne otetaan käyttöön. Johtoryhmä myös valitsee vastuuhenkilöt, jotka valmistelevat tarvittavat muutokset ja varmistavat niiden käytön valituissa projekteissa.

Aluksi prosessikuvaukset ja dokumenttipohjat päivitetään toimintajärjestelmä IMS:iin, jolloin työntekijät voivat tukeutua siellä oleviin kuvauksiin toimintojen muuttuessa. Kun muutokset ovat näkyvillä, voidaan aloittaa työntekijöiden koulutus ja perehdyttäminen uusiin menetelmiin. Koulutuksen jälkeen muutoksia jalkautetaan sisäisillä pilottihankkeilla, joilla voidaan varmistaa uusien menetelmien käyttö ja tarvittaessa muokata prosessikuvauksia ja dokumentteja palautteiden pohjalta. Muutoksia on tuotava toimintaan hiljalleen, jotta voidaan varmistua niiden korvaavan vanhat toiminnot. Tämä vaatii useita sisäisiä hankkeita, ennen kuin muutoksia voidaan viedä normaaleihin asiakashankkeisiin.

5.6 Tutkimuksesta saatu uusi tieto

Tutkimuksen aikana saatiin tietoa yrityksen tuotekehitysprosessin kulusta sekä siinä olevista kehitysmahdollisuuksista. Osa ehdotetuista kehityskohteista oli havaittu, mutta niiden muokkaamiseksi ei ollut valmiita ehdotuksia. Tutkimuksessa löydettiin myös uusia kehityskohteita, jotka havaittiin tarpeellisiksi.

Uutta tietoa tutkimuksessa on kohteet, joita ei ollut ennen tunnistettu sekä kaikille muutostyökohteille tarjotut kehitysehdotukset. Tämä on myös yritykselle erittäin tarpeellista ja käytännöllistä, koska resurssit voidaan keskittää vain muutosten tekoon ja käyttöönottoon. Muutosten tunnistaminen laajoista prosesseista on työlästä ja aikaa vievää, joten tutkimuksesta saadut tiedot auttavat huomattavasti toiminnan kehitystä.

Yrityksen kannalta uudeksi tiedoksi voidaan laskea myös varmistuminen siitä, että toiminta on yleisesti hyvällä tasolla ja täyttää suuren osan standardin vaatimuksista. Tutkimuksen kaltaista yleistarkastelua ei ollut ennen tehty, joten sen avulla saatiin varmuutta toiminnan laatuun.

5.7 Käytännön vaikutukset

Kohdeyrityksen kannalta tutkimuksen tulokset aiheuttavat analysointia ja pohdintaa siitä, missä laajuudessa muutoksia otetaan toimintaan. Toimintamalleja ja prosesseja tulee muokata sekä lisätä toimintojen dokumentointia. Muutosten jälkeen tilannetta on tarkasteltava uudelleen ja analysoitava ovatko tehdyt muutokset sopivia vai tarvitseeko toimintaa muuttaa edelleen. Muutosten käyttöönotto on iteratiivista toimintaa, jossa palautteiden ja käyttökokemusten perusteella toimintoja muokataan sopiviksi.

Tutkimuksen tuloksista voidaan tehdä laajempia, toimialakohtaisia suosituksia. Vanhoissa suunnitteluyrityksissä on kannattavaa aika ajoin käydä prosesseja läpi ja tarkastella voitaisiinko niitä optimoida ja kehittää. Tämä aikaväli voi olla muutamia vuosia ja sitä voidaan tihentää tai harventaa esimerkiksi suunnittelijoiden palautteen perusteella. Monesti on helppoa pitäytyä vanhoissa tavoissa ja prosesseissa, eikä niitä katsota kriittisesti kehitysten kannalta. Suunnittelua ja sen tukiprosesseja muokkaamalla voidaan kuitenkin huomattavasti optimoida toimintaa ja saavuttaa suuria hyötyjä. Tästä syystä toimintoja tulisi tarkastella ja miettiä mahdollisia kehityskohteita.

5.8 Tulosten luotettavuus sekä käytettävyys

Saatujen tulosten luotettavuudesta sekä uskottavuudesta voidaan varmistua sillä, että kaikki vastuusuunnittelijat olivat samaa mieltä muutostarpeista sekä löydettyistä puutteista tuotteistamisprosessissa. Haastatellut suunnittelijat myös vahvistivat muutostyökohteet ja kokivat muutosehdotukset positiiviseksi ideaksi, jotka tulisi ottaa käyttöön. Lähes

kaikki haastateltavat myös painottivat muutosten tarvitsevan selkeyttä ja ohjeistusta, jotta niiden jalkautus tuotteistamisprosessiin olisi mahdollisimman nopeaa.

Tulosten käytöstä ja vahvistamisesta voidaan varmistua tekemällä jatkotarkasteluja sovitun ajankohdan jälkeen, jolloin voidaan tarkastella onko tuotteistamisprosessi parantunut ja uudet muutokset jalkautettu toimintaan. Mikäli muutoksilla saadaan hyviä tuloksia, voidaan myös muita osa-alueita toiminnasta tarkastella samalla tavalla ja käyttää nykyistä analysointia pohjana. Tällöin kaikkea alkutyötä sekä suunnittelua ei tarvitse tehdä uudelleen, vaan voidaan keskittyä muutoskohteiden tunnistukseen ja parannusehdotusten miettimiseen.

6. JOHTOPÄÄTÖKSET

Työn tarkoituksena oli saada tarkka kuvaus standardin ISO 26262 aiheuttamista lisäyksistä ja muutoksista tuotekehitysprosessiin. Tarkastelu toteutettiin nykytila-analyysillä, jossa tarkasteltiin nykyistä tilannetta standardin asettamiin vaatimuksiin. Apuna käytettiin yrityksen suunnittelemaa jarrujärjestelmää, koska se täytti standardin vaatimukset ja on suunniteltu nykyisten ohjeiden avulla. Analyysiä tehtäessä käytettiin myös tutkimuskysymyksiä ja osatehtäviä, joiden avulla tarkastelua saatiin selkeytettyä ja jäsennettyä. Vastaavaa analyysiä ei ollut ennen tehty, joten työn avulla saatiin kartoitettua myös yleisiä muutoskohteita toiminnassa.

Suurin osa muutoksista kohdistui yleiseen toimintaan, mutta kohteet löydettiin tarkastelemalla standardia ja vertaamalla sen vaatimuksia yrityksen toimintamalleihin. Standardin vaatimia yksityiskohtaisempia vaatimuksia on hankalaa toteuttaa nykyiseen toimintamalliin ennen yleisten muutosten käyttöönottoa. Muutosten hyödyllisyyttä voi olla hankalaa mitata tai todentaa ennen niiden käyttöönottoa. Haastattelujen aikana pääsuunnittelijat kuitenkin kannattivat muutosten tuomista toimintaan ja tiedostivat olemassa olevat tuotekehitysprosessin puutteet. Ehdotettujen muutosten luotettavuutta ja hyödyllisyyttä nostaa myös niiden painotus standardissa sekä muissa lähteissä.

6.1 Turvallisuus

Työn aikana saatiin varmistus yrityksen toiminnan sekä tarkasteltavan jarrujärjestelmän olevan turvallisuusnäkökulmasta hyvällä tasolla. Turvallisuustoimintoihin on panostettu eri osa-alueilla ja suunnitellut tuotteet ovat laadukkaita ja turvallisia. Yrityksen toiminta turvallisuuskriittisellä alalla vaatii, että tuotteet ovat turvallisia ja suunniteltu vaatimaan käyttöön. Yrityksen järjestelmät ja tuotteet ovat laajasti testattuja ja hyväksytyt useissa eri testeissä turvallisuuden todentamiseksi.

Toimintaan on tehtävä joitain muutoksia, jotka lisäävät turvallisuuden tasoa ja auttavat varmentamaan järjestelmän vaatimuksia. Näiden muutosten, kuten turvallisuuselinkaaren avulla järjestelmän toimintoja ja turvallisuutta on helpompaa varmentaa asiakkaille, koska vaadittavat kuvaukset ja toimenpiteet ovat dokumentoituina. Turvallisuuselinkaaren avulla myös muissa suunnittelun osa-alueissa olevat turvallisuusvaatimukset ja verifiointit on helpompaa todentaa, koska ne on johdettu elinkaaren pohjalta.

6.2 Standardin vaatimukset

Standardi asettaa paljon vaatimuksia turvallisuuteen liittyville toiminnoille, koska sen pääkohde on ajoneuvojen toiminnallinen turvallisuus. Näiden avulla varmistetaan suun-

niteltavan järjestelmän tai laitteen olevan turvallinen ja laadukkaasti toteutettu. Vaatimuksia annetaan myös muille toiminnoille kuten suunnitteluprosessin etenemiselle sekä toimintojen verifiointille ja dokumentoinnille. Yleisten toimintojen avulla varmistetaan, että suunnittelun perusosat ovat hyvällä tasolla, jonka jälkeen standardikohtaisia sekä turvallisuuteen liittyviä vaatimuksia voidaan helpommin lisätä toimintaan.

Joidenkin vaatimusten varmentaminen on hankalaa, koska niille ei anneta vertailukohtia tai esimerkkejä. Tällaisissa tilanteissa yrityksen on tehtävä itse päätös missä määrin vaatimusta noudatetaan ja esimerkiksi sanallisesti selittää vaatimuksen täyttyminen ja suunnittelupäätökset sen taustalla. Standardissa olisi hyvä olla selkeitä esimerkkejä tällaisista tilanteista, jotta sitä noudattavat tahot voisivat selkeästi osoittaa täyttävänsä tietyt vaatimukset. Epäselkeät vaatimukset voivat pahimmassa tapauksessa aiheuttaa sekaannuksia sekä väärää informaatiota.

6.3 Löydetyt eroavuudet

Kriittisimmät muutoskohteet löytyivät systeemisuunnittelusta ja tuotekehityksen alkupäähän liittyvistä toimenpiteistä. Mitä alemmalle tasolle suunnittelussa mentiin, sitä vähemmän muutoksia löytyi. Alatason suunnittelussa käytössä on tarkkoja raja-arvoja ja rajauksia, jotka helpottavat suunnitelmien tekemistä. Joitakin alemman tason muutoksia kuitenkin löytyi, kuten ohjelmistopuolella puuttuva alatason testaaminen. Pääsuunnitteli-joilla oli tiedossa osa puutteista, mutta resurssipuutosten takia asioihin ei ole ehditty puuttua halutulla tavalla. Työntekijöillä ei myöskään ole ollut aikaa suunnitella parannuksia ja muutoksia toimintaan normaalien töiden ohella.

Löydetyt muutoskohteet ja niille esitetyt parannusehdotukset tulee käydä kohdeyrityksen kanssa läpi ja miettiä millä panostuksella ne ovat toteutettavissa. Ehdotettuja ideoita tulee analysoida ja pohtia voiko niitä parantaa edelleen tai mikäli niiden kautta keksitään uusia muutostapoja. Muutosten analysoinnissa tulee olla mahdollisimman laajasti eri osa-alueiden henkilöstöä paikalla, jotta voidaan varmistua muutosten sopivan jokaiseen toimintaan.

6.4 Standardin ulkopuoliset havainnot

Analyysiä ja tarkastelua tehtäessä tehtiin havaintoja ja löydettiin muutoskohteita, jotka eivät kuulu standardin vaatimukseen, mutta parantavat toimintaa. Standardin ulkopuolisia havaintoja tehtiin suurimmaksi osaksi vastuuhenkilöiden haastatteluiden aikana, jolloin tuli ilmi joitain epäkohtia toiminnassa.

Ohjelmistoa koskevia turvallisuusvaatimuksia, menetelmiä ja valintoja katselmoitaessa mukana on turvallisuushenkilöitä, jotka validoivat toimintoja. Turvallisuushenkilöstöllä ei kuitenkaan ole kohdennettua osaamista esimerkiksi elektroniikasta tai ohjelmoinnista, joten kaikkiin toimintoihin ei saada asiantuntevaa validointia. Katselmoinneissa luotetaan

paikalla olevien ohjelmoinnista vastuussa olevien henkilöiden kyvystä selittää järjestelmän toimintaa, jotta sitä voidaan analysoida. Turvallisuushenkilöstössä olisi hyvä olla eri osa-alueilla tarkempaa asiantuntemusta, jotta voitaisiin helposti validoida toimintoja katselmuksien ja muiden tarkastusten aikana. Tällöin turvallisuustyötä tekevät voisivat myös helpommin kyseenalaistaa tehtyjä suunnitteluperusteita ja tarjota vaihtoehtoisia ratkaisuja.

Haastattelujen ja tarkastelun aikana huomattiin, että kommunikointi on paikoitellen heikkoa eri osa-alueiden välillä. Hankittaessa komponentteja ja osia ostopuoli ei kommunikoi turvallisuuspuolen kanssa ja tarkasta mitä mahdollisia dokumentteja tarvitaan turvallisuuden varmistamiseksi. Dokumentteja voi olla hankalaa saada jälkikäteen ja se hidastaa turvallisuustyön tekemistä.

Kommunikointipuutoksia tapahtuu myös suunnittelun aikana löydetyt epäkohdat ja kysymykset tuotekehitysprosessia koskien pidetään oman suunnittelualueen sisällä. Suunnittelun aikana tapahtuvia turvallisuushavainnoiteja tai vikoja ei välttämättä välitetä turvallisuusvastaavalle tai laadita tapahtumasta selvitystä, joka olisi yleisesti näkyvillä. Ilmoitusten laatimisesta ei ole olemassa omaa prosessia, joka takaisi dokumentoidun ilmoituksen. Nykyisessä toiminnassa ilmoitus on henkilöriippuvaista ja se tehdään sähköpostin välityksellä.

LÄHTEET

Brown, S. (2000). Overview of IEC 61508 – Design of electrical/electronic/programmable electronic safety-related systems. Institution of Electrical Engineers. Computing & Control Engineering Journal, Vol. 11(11).

DG Internal Market, Industry, Entrepreneurship and SMEs. Technical harmonisation in the EU. (2016). [WWW]. European Commission. [viitattu: 18.11.2016]. Saatavissa: https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu_en

EUR-Lex. (2007). Puitedirektiivi – puitteiden luomisesta moottoriajoneuvojen ja niiden perävaunujen sekä tällaisiin ajoneuvoihin tarkoitettujen järjestelmien, osien ja erillisten teknisten yksiköiden hyväksymiselle - 2007/46/EY. Euroopan parlamentti ja neuvosto

European committee for standardization. (2015). Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat – EN ISO 13849. Suomen Standardoimisliitto

IEC 61508 Overview Report. (2006). Exida.

Ajoneuvolaki. (2002). Finlex.

Foord, A.G., Gulland, W.G., Howard C.R. (2011). Ten years of IEC 61508; Has it made any difference?. IChemE. Symposium series No. 156. s. 232-237.

Safety Integrity Level (SIL) Studies. (2016). [WWW]. Germanischer Lloyd. [viitattu: 10.11.2016]. Saatavissa: <http://docplayer.net/20886220-Safety-integrity-level-sil-studies-germanischer-lloyd-service-product-description.html>

Haikala, I., Märijärvi, J. (2004). Ohjelmistotuotanto. Talentum.

Hietikko, M., Malm, T., Alanen, J. (2009). Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. VTT

Honkanen, T. (2015). Toiminnallisen turvallisuuden vaatimukset ja soveltaminen. Metropolia Ammattikorkeakoulu. Insinööriyö

Functional safety. (2015). [WWW]. IEC. [viitattu: 1.11.2016]. Saatavissa: http://www.iec.ch/about/brochures/pdf/technology/functional_safety.pdf

International Electrotechnical Commission. (2011). Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus – IEC 61508. Suomen Standardoimisliitto.

International Organization for Standardization. (2011). Road vehicles – Functional safety – ISO 26262. Suomen standardoimisliitto

EU-Säädökset. (2016). [WWW]. Liikenteen turvallisuusvirasto Trafi. [viitattu: 19.12.2016]. Saatavissa: <http://www.trafi.fi/tieliikenne/saadokset/eu-saadokset>

LIITE A: ASIL-LUOKITUKSEN MÄÄRITYKSET

	Class of severity (see Table 1)			
	S0	S1	S2	S3
Reference for single injuries (from AIS scale)	<ul style="list-style-type: none"> — AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related 	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	<ul style="list-style-type: none"> — Bumps with roadside infrastructure — Pushing over roadside post, fence, etc. — Light collision — Light grazing damage — Damage entering/exiting parking space — Leaving the road without collision or rollover 	<ul style="list-style-type: none"> — Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with very low speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with very low speed — Rear/front collision with another passenger car with very low speed — Collision with minimal vehicle overlap (10 % to 20 %) — Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) without passenger compartment deformation 	<ul style="list-style-type: none"> — Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with low speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed — Rear/front collision with another passenger car with low speed — Pedestrian/bicycle accident while turning (city intersection and streets) 	<ul style="list-style-type: none"> — Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with medium speed — Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed — Rear/front collision with another passenger car with medium speed — Pedestrian/bicycle accident (e.g. 2-lane road) — Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) with passenger compartment deformation

		Class of probability of exposure in operational situations (see Table 2)			
		E1	E2	E3	E4
Frequency of situation		Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples	Road layout	—	— Mountain pass with unsecured steep slope	—	—
	Road surface	—	— Snow and ice on road	— Wet road	—
	Nearby elements	—	—	— In tunnel — In car wash — Traffic congestion	—
	Vehicle stationary state	— Stopped, requiring engine restart (at railway crossing) — Vehicle being towed — Vehicle during jump start	— Trailer attached — Roof rack attached	— Vehicle being refuelled — Vehicle on a hill (hill hold)	—
	Manoeuvre	—	— Evasive manoeuvre, deviating from desired path	— Overtaking	— Starting from standstill — Shifting transmission gears — Accelerating — Braking — Executing a turn (steering) — Using indicators — Manoeuvring vehicle into parking position — Driving in reverse

Driving factors and scenarios		Class of controllability (see Table 3)			
		C0	C1	C2	C3
		Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm
Examples	Situations that are considered distracting	— Maintain intended driving path	—	—	—
	Unexpected radio volume increase	— Maintain intended driving path	—	—	—
	Warning message - gas low	— Maintain intended driving path	—	—	—
	Unavailability of a driver assisting system	— Maintain intended driving path	—	—	—
	Faulty adjustment of seat position while driving	—	— Brake to slow/stop vehicle	—	—
	Blocked steering column when starting the vehicle	—	— Brake to slow/stop vehicle	—	—
	Failure of ABS during emergency braking	—	—	— Maintain intended driving path	—
	Headlights fail while night driving at medium/high speed on unlighted road	—	—	— Steer to side of road or brake to stop.	—
	Motor failure at high lateral acceleration (motorway exit)	—	—	— Maintain intended driving path	—
	Failure of ABS when braking on low friction road surface while executing a turn	—	—	—	— Maintain intended driving path, stay in lane
	Failure of brakes	—	—	—	— Brake to slow/stop vehicle
	Incorrect steering angle with high angular speed at medium or high vehicle speed (steering angle change not aligned to driver intent)	—	—	—	— Maintain intended driving path, stay in lane
	Faulty driver airbag release when travelling at high speed	—	—	—	— Maintain intended driving path, stay in lane — Brake to slow/stop vehicle