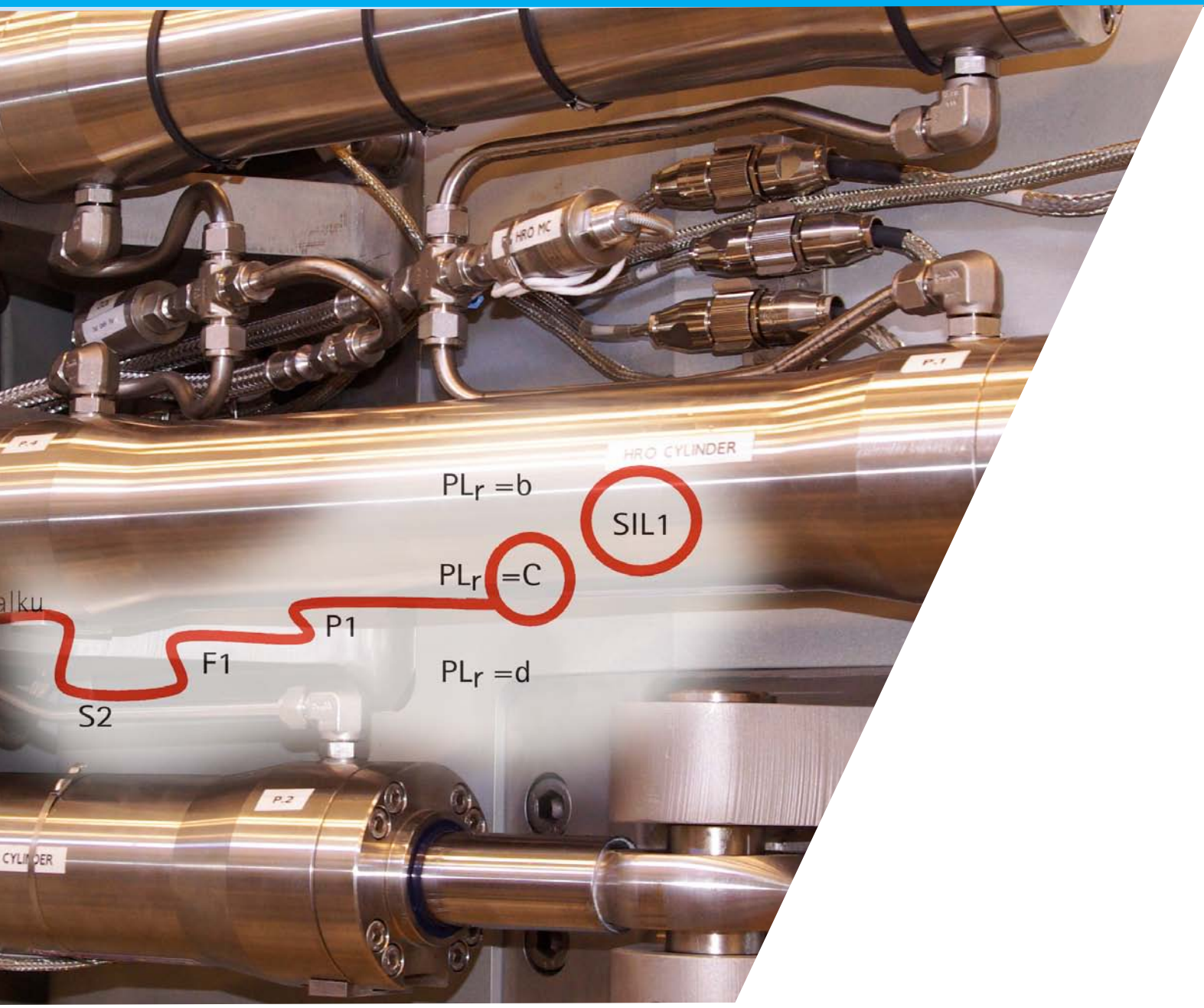
VTT TIEDOTTEITA 2485



Marita Hietikko, Timo Malm & Jarmo Alanen

Koneiden ohjausjärjestelmien toiminnallinen turvallisuus

Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen

VTT TIEDOTTEITA – RESEARCH NOTES 2485

Koneiden ohjausjärjestelmien toiminnallinen turvallisuus

Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen

Marita Hietikko, Timo Malm & Jarmo Alanen

ISBN 978-951-38-7298-4 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

Copyright © VTT 2009

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 7001

VTT, Bergsmansvägen 5, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 7001

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax + 358 20 722 7001

Marita Hietikko, Timo Malm & Jarmo Alanen. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen [Functional safety of machine control systems. Instructions and tools for the creation of standard safety process]. Espoo 2009. VTT Tiedotteita – Research Notes 2485. 75 s. + liitt. 14 s.

Avainsanat machines, functional safety, control systems

Tiivistelmä

Koneiden ja niiden ohjausjärjestelmien turvallisuusvaatimusten määrittelyvaiheessa tehdään ratkaisuja, joilla on vaikutusta koneen koko myöhempien elinkaaren vaiheiden turvallisuuteen. Turvallisuusvaatimusten määrittelyssä tehtyjen virheiden on havaittu olevan syynä suureen osaan tapaturmista.

Tähän julkaisuun on kerätty KOTOTU-hankkeen (Koneiden ohjausjärjestelmien toiminnallinen turvallisuus) tulokset. Hankkeessa kehitettiin turvallisuussuunnittelun toimintamalli eli KOTOTU-prosessityökalu, jonka avulla koneiden ohjausjärjestelmien turvallisuuteen liittyvät riskit voidaan arvioida ja turvallisuusvaatimusten määrittely toteuttaa koneen ja sen ohjausjärjestelmän elinkaaren varhaisessa vaiheessa. Hankkeessa kehitettiin myös suunnittelijan työtä helpottava KOTOTU-laskentatyökalu, jonka avulla saavutettu turvallisuustaso (suoritustaso = PL) voidaan laskea ja arvioida standardin SFS-EN ISO 13849-1 mukaan. Työkalut soveltuvat ohjausjärjestelmien turvallisuuden suunnitteluun, arviointiin ja koulutukseen. Julkaisussa on kuvattu näiden työkalujen käyttö ja soveltaminen sovellusesimerkin avulla. Julkaisu antaa ohjeita myös muiden uusimpien koneiden ohjausjärjestelmien turvallisuutta käsittelevien standardien soveltamiseen.

Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen [Functional safety of machine control systems. Instructions and tools for the creation of standard safety process]. Espoo 2009. VTT Tiedotteita – Research Notes 2485. 75 p. + app. 14 p.

Keywords machines, functional safety, control systems

Abstract

In the specification phase of a machine and its control system such decisions are frequently made that affect the safety of all the later life cycle phases of the machine. Errors made in the definition of safety requirements are found out to be a reason for large amount of accidents.

This report includes results of the project "Functional safety of machine control systems" (KOTOTU). In this project a functional model for the safety design, i.e. KOTOTU process tool, was developed, which helps safety designers to assess safety risks and define safety requirements of a machine control system in the early phase of system life cycle. In addition, in this project a KOTOTU calculation tool was developed, which helps the designer for assessing and calculating the attained performance level (PL) according to ISO 13849-1 standard. These tools can be applied to control system safety design, evaluation and education. The use and application of these tools are described in this report with the aid of an example system. This report gives instructions also for the application of the newest control system safety related standards.

Alkusanat

Tähän julkaisuun on kerätty KOTOTU-hankkeen (Koneiden ohjausjärjestelmien toiminnallinen turvallisuus) tulokset. Hankkeen tavoitteena oli kehittää turvallisuussuunnittelun toimintamalli, jonka avulla koneiden ohjausjärjestelmien turvallisuuteen liittyvät riskit voidaan arvioida ja turvallisuusvaatimusten määrittely toteuttaa koneen tai järjestelmän elinkaaren varhaisessa vaiheessa. Tavoitteena oli myös kehittää suunnittelijan työtä helpottava työkalu, jonka avulla saavutettu turvallisuustaso voidaan arvioida ja joka antaa ohjeita myös uusimpien koneiden ohjausjärjestelmien turvallisuutta käsittelevien standardien soveltamiseen.

Hankkeen toteutukseen osallistuivat Jarmo Alanen, Marita Hietikko ja Timo Malm VTT:stä. Hanketta ohjasivat seuraavat asiantuntijat: Misa Tillaéus ja Mauri Lehtonen Raute Oyj:stä, Pekka Kämäräinen Metso Minerals Oy:stä, Reijo Laine, Pekka Pihola ja Eero Suomi Metso Paper Oy:stä, Lauri Ora ja Teemu Parkkinen Sandvik Mining and Construction Oy:stä, Hannu Lindfors Konecranes Oyj:stä, Sami Loukasmäki Exertus Oy:stä, Jari Hauta-aho ja Juha Liukkonen Siemens Oy:stä, Veikko Nuortio Cimcorp Oy:stä, Pasi Lehmusoksa, Risto Liukkonen ja Markus Karppi Patria Land & Armament Oy:stä, Petri Ylönen ja Terjo Kallioniemi Nekos Oy:stä, Heikki Joensuu ja Mikko Ristolainen ABB Oy:stä, Tapio Hyvölä Ruukki Productionista, Ilkka Tahvanainen Työsuojelurahastosta, Matti Sundquist Uudenmaan Työsuojelupiiristä (myöhemmin Sundcon Oy:stä) sekä Risto Tiusanen ja Helena Kortelainen VTT:stä.

Hankkeen kuluessa järjestettiin workshop, johon osallistui yli 30 yritysedustajaa ja jossa voitiin testata hankkeessa kehitettyä turvallisuussuunnittelun toimintamallia (KOTOTU-prosessityökalu) ja Excelillä toteutettua suoritustason laskentatyökalua (KOTOTU-laskentatyökalu) sekä antaa koulutusta toimintamallin ja työkalun käytöstä.

Kiitämme kaikkia hankkeeseen osallistuneita yhteistyöstä ja avusta.

Tämä tiedote on julkaistu Työsuojelurahaston tuella.

Sisällysluettelo

Symboliluettelo

B_{10d}	Keskimääräinen toimintajaksojen lukumäärä, johon mennessä 10 % komponenteista vikaantuu vaarallisesti
CCF	Common Cause Failure, yhteisvikaantuminen
DC	Diagnostic Coverage, diagnostiikan kattavuus
DC_{avg}	Keskimääräinen diagnostiikan kattavuus
FET	Field Effect Transistor, kanavatransistori
HAZOP	Poikkeamatarkastelu (Hazard and operability study)
HW	Hardware, laitteisto
MTBF	Mean time between failure, keskimääräinen vikaantumisväli
MTTF	Mean Time To Failure, keskimääräinen vikaantumisaika
$MTTF_d$	Mean Time To dangerous Failure, keskimääräinen vaarallinen vikaantumisaika
PFH_D	Probability of dangerous Failure per Hour, vaarallisen vikaantumisen todennäköisyys tuntia kohden
PL	Performance Level, suoritustaso
PL_r	Required Performance Level, vaadittava suoritustaso
S/E/OEJ	Sähköinen, elektroninen ja ohjelmoitava elektroninen järjestelmä
SFF	Safe Failure Fraction, turvallisten vikaantumisten osuus
SIL	Safety Integrity Level, turvallisuuden eheyden taso
SRCF	Safety-Related Control Function, turvallisuuteen liittyvä ohjaustoiminto
SRECS	Safety-Related Electrical Control System, turvallisuuteen liittyvä sähköinen ohjausjärjestelmä
SW	Software, ohjelmisto
VPA	Vikapuuanalyysi
VVA	Vika- ja vaikutusanalyysi

1. Johdanto

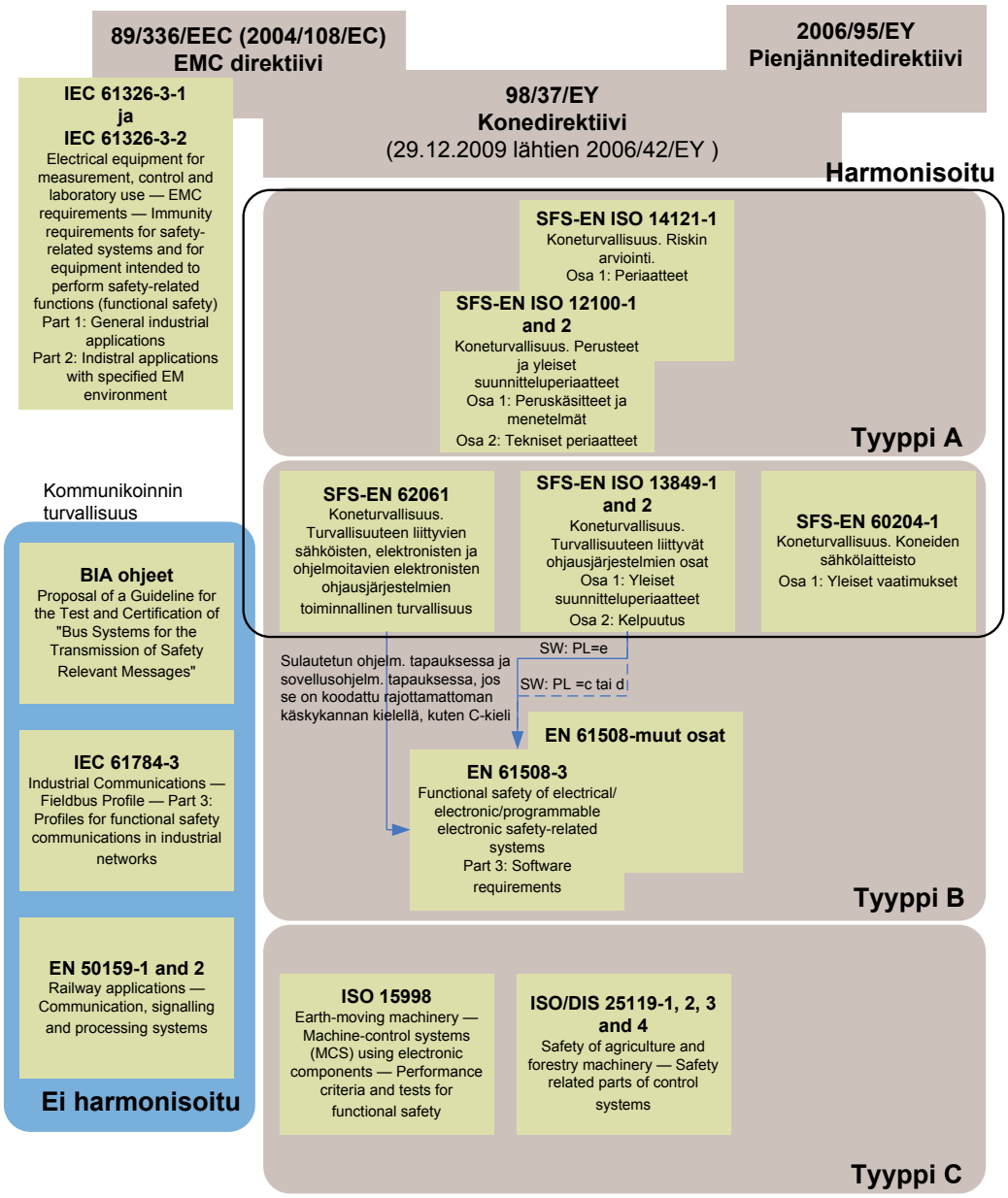
Julkaisussa keskitytään sähköisten, elektronisten ja ohjelmoitavien elektronisten järjestelmien (S/E/OEJ) toiminnalliseen turvallisuuteen. Erityisesti tarkastellaan turvallisuusprosessin alkupäätä, riskien arviointia ja ohjausjärjestelmien suunnittelua, jotta saavutettaisiin riittävä turvallisuuden taso. Ohjausjärjestelmän kelpuutusvaihe jää tässä yhteydessä vähemmälle tarkastelulle.

S/E/OE-järjestelmien turvallisuusstandardien kenttä on Euroopassa kohtuullisen selkeä, ja konedirektiivi ja sen alaiset harmonisoidut standardit tunnetaan yleensä hyvin. Konedirektiivin (Suomessa konepäätöksen/koneasetuksen) noudattaminen on pakollista, kun taas harmonisoitujen standardien noudattaminen on vapaaehtoista, mutta usein vaatimustenmukaisuus on helpompi osoittaa, kun noudatetaan asianomaisia harmonisoituja standardeja.

Kuvassa 1 on esitetty tärkeimmät ohjelmoitaviin järjestelmiin liittyvät standardit. Kuvassa ei ole mukana C-tyypin standardeista muut kuin tekeillä olevat kaksi sovelluskohtaista ohjausjärjestelmien turvallisuusstandardia: maansiirtokoneiden ISO 15988 ja maatalous- ja metsäkoneiden ISO 25119. Kuvasta puuttuu myös suuri joukko B-tyypin standardeja, jotka liittyvät sähköisiin ohjausjärjestelmiin (esim. valoverhoihin ja lähestymiskytkimiin liittyvät standardit). Kuvan 1 näkökulma on siis yksinomaan ohjelmoitavan automaation suunnasta.

Osa kuvan 1 standardeista on harmonisoituja, osaa ei vielä ole harmonisoitu ja osaa ei ilmeisesti harmonisoida myöhemminkään. SFS-EN ISO 14121-1 on jo harmonisoitu, ja se korvaa aiemmin käytössä olleen standardin EN 1050. Standardi EN 61508 ei ole harmonisoitu eikä sitä todennäköisesti harmonisoida myöhemminkään, mutta toisaalta siihen viitataan normatiivisena viitteenä esimerkiksi harmonisoidusta standardista SFS-EN ISO 13849-1. SFS-EN ISO 13849-1 standardin edeltäjä SFS-EN 954-1 ei ole enää harmonisoitujen standardien listalla, mutta sitä voi käyttää vielä vuoden 2009 marraskuun loppuun saakka.

Kommunikointijärjestelmiin liittyvistä kolmesta kuvassa 1 esitetyistä standardeista uusin on IEC 61784-3. Se on metodiltaan samankaltainen kuin BIA:n ohjedokumentti [FAET; FAEM III, BIA, 2000] ja samankaltainen kuin rautatiestandardi EN 50159. Kuvassa on esitetty myös pienjännitedirektiivin alainen standardi SFS-EN 60204-1, koska se on tässä yhteydessä relevantti. Samoin kuvassa on esitetty uusi toiminnallisen turvallisuuden EMC standardi IEC 61326-3, joka on julkaistu vuoden 2008 alussa.

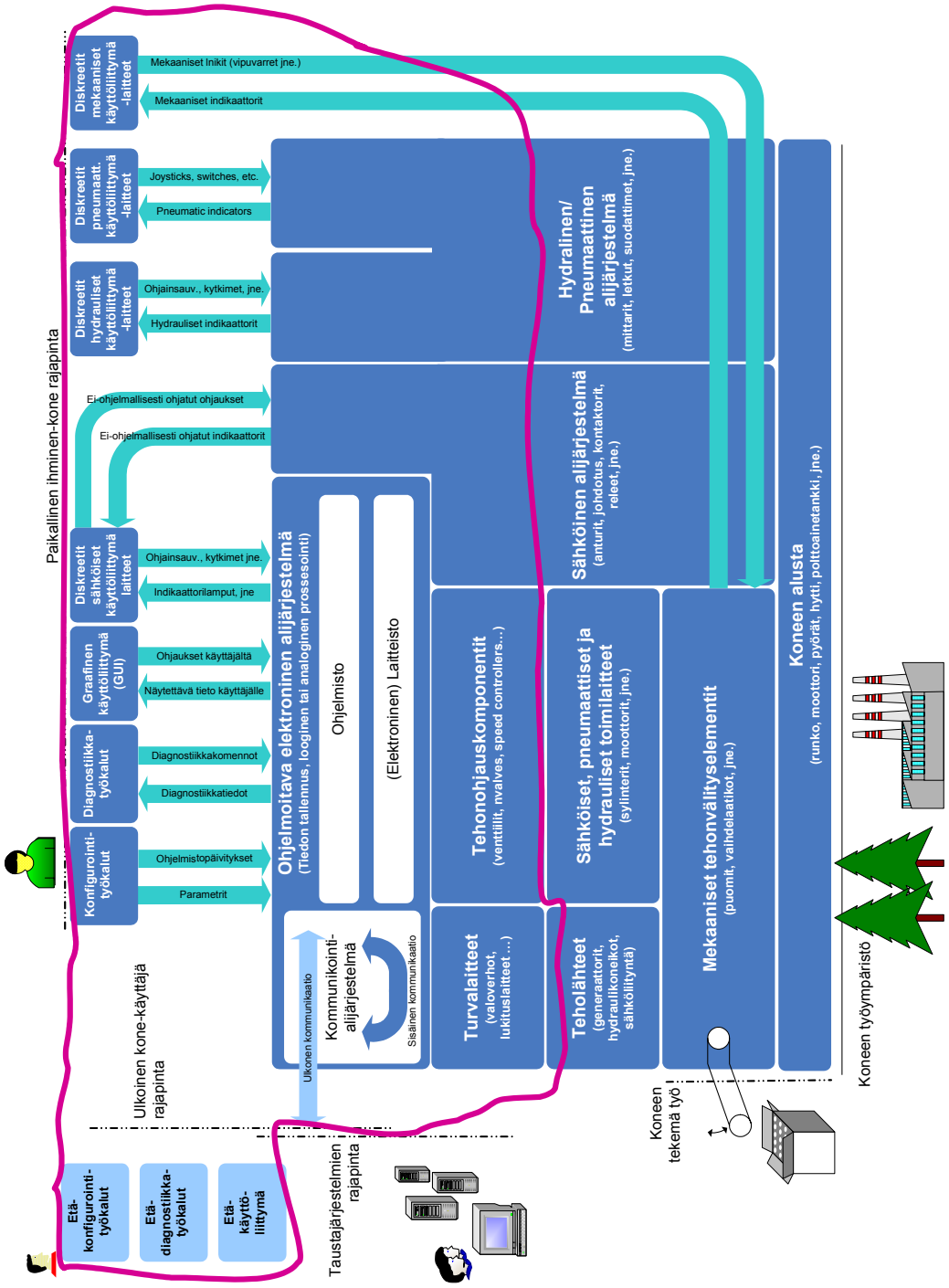


Kuva 1. Konedirektiivi ja sen alaiset ohjelmoitaviin järjestelmiin liittyvät standardit.

Koska tämä tiedote rajoittuu ohjausjärjestelmien turvallisuuteen, on tarpeen määritellä, mikä on koneen ohjausjärjestelmä. SFS-EN 62061 -standardin mukaan se on: "*Järjestelmä, joka reagoi esimerkiksi prosessista, muista koneen osista, käyttäjältä tai ulkoisista ohjauslaitteista tuleviin tietoihin ja joka saa aikaan lähtötiedot, joiden avulla kone saadaan toimimaan tarkoitetulla tavalla.*"

Ohjausjärjestelmä sisältää antureita, releitä, solenoidiventtiilejä, asemantuntoelimiä, ohjelmoitavia kontrollereita, kommunikointijärjestelmiä, käyttöliittymälaitteita, moottorinohjausyksiköitä, kaksinkäsinhallintalaitteita, painetunnistimia, lukituslaitteita, jne.

Kuvassa 2 on esitetty yleispätevä malli koneesta; ohjausjärjestelmän osuus on siinä rajattu käsivaraisviivalla.



Kuva 2. Yleispätevä malli koneesta; ohjausjärjestelmän osuus rajattu käsivaraisviivalla.

2. Vaatimusmäärittely

Suuri osa turvallisuuskriittisistä virheistä tehdään vaatimusmäärittelyvaiheessa; joidenkin tutkimusten mukaan (esim. [Chambers et al. 1999 ja HSE 2003]) vaatimusmäärittelyvirheiden osuus ohjausjärjestelmästä johtuviin vaaratilanteisiin on ollut luokkaa 40–44 %. Siksi tässä luvussa annetaan ohjeita systemaattiselle turvallisuusvaatimusten määrittelylle.

Turvallisuusvaatimukset ovat osa koko järjestelmän vaatimusmassaa. Niiden keruu ja käsittely ei periaatteessa poikkea normaalista vaatimusmäärittelyprosessista; tutut työkalut ja menetelmät sopivat myös turvallisuusvaatimusten kartoitukseen ja hallintaan. Yleisestä vaatimusmäärittelyprosessista löytyy runsaasti kirjallisuutta ja ohjeita, esimerkiksi VTT:n julkaisu [Parviainen et al. 2003] toimii hyvänä yleiskatsauksena vaatimusmäärittelyprosessiin, tosin vain ohjelmistojen näkökulmasta. IEEE on julkaissut standardin [IEEE Std 1233 1998], jossa annetaan ohjeita koko järjestelmän vaatimusmäärittelyjen tekemiseksi. IEEE 1233 esitellään tarkemmin kohdassa 2.6. Vaatimusmäärittelyyn liittyvät prosessit on kuvattu myös systeemitekniikan standardissa [ISO/IEC/IEEE 15288 2008] ja sitä vastaavassa ohjelmistotekniikan standardissa [ISO/IEC/IEEE 12207 2008].

Tässä julkaisussa keskitytään pelkästään ohjausjärjestelmien turvallisuusvaatimuksiin.

2.1 Turvallisuusvaatimusten määrittely

Vaatimusmäärittelyprosessin päätehtävät ovat:

- vaatimusten keruu
- vaatimusten analyysi (vaatimusten arviointi ja formulointi suunnittelijoiden ymmärtämään, usein mitattavaan, muotoon)
- vaatimusten tarkentaminen ja kohdentaminen (kohdennus laitteistoon, ohjelmistoon, osajärjestelmiin, jne.)
- vaatimusten esittäminen (suunnittelijoille ja tilaajalle; eri esitysmuotoja tullaan mahdollisesti tarvitsemaan)
- vaatimusten todentaminen ja kelpuuttaminen
- vaatimusten hallinta (identifiointi, luokittelu, versionhallinta ja jäljitettävyys).

Näitä tehtäviä ei kuvata tässä yhteydessä tarkemmin, vaan lukijaa pyydetään etsimään tietoa mainituista asioista seuraavista julkaisuista (VTT-julkaisu, IEEE 1233, ISO/IEC/IEEE 15288 ja ISO/IEC/IEEE 12207).

Vaatimusmäärittely ajatellaan yleensä, ehkä harhaanjohtavastikin, tuotekehitysprosessin alkupään tehtäväksi. Todellisuudessa vaatimuksia syntyy koko tuotteen elinkaaren ajan, varsinkin suunnitteluvaiheessa, mutta esimerkiksi myös testausvaiheessa ja käyttöönoton jälkeen kenttäpalautteen perusteella.

Vaatimus ja suunnitelma on käytännössä vaikea erottaa toisistaan, vaikka niillä periaatteessa on selkeä seuraavanlainen merkitysero. Vaatimus on vastaus kysymykseen 'mitä', ja suunnitelma taas on vastaus kysymykseen 'miten'. Esimerkiksi, jos vaatimuksena on, että *liikkeen ohjaus ei saa jäädä päälle, kun ohjauslaite vapautetaan*, järjestelmäsuunnittelija päättää toteuttaa vaatimuksen sallintakytkimellä[1]. Hän ei kuitenkaan määrittele sallintakytkintä tarkkaan, vaan tekninen määrittely jää seuraaville suunnittelutasoille. Täten seuraavalle suunnittelutasolle asetetaan vaatimus: "*Ohjaussauvassa on oltava sallintakytkin"*. Vaatimukset ja suunnittelupäätökset menevät siis ketjuna: vaatimus → suunnitelma = vaatimus → suunnitelma = vaatimus … → suunnitelma → toteutus.

Tällaisessa ketjussa jäljitettävyys katoaa helposti. Suunnitteludokumenteissa ei yleensä ole viitteitä, että mitkä vaatimukset kyseinen suunnitelma täyttää. Kun on kyse turvallisuusvaatimuksista, jäljitettävyyden vaatimus korostuu juridisistakin syistä: on pystyttävä osoittamaan, mikä suunnitelman osa toteuttaa tietyn konedirektiivin (koneasetuksen) tai sen alaisen harmonisoidun standardin vaatimuksen tai riskianalyysin perusteella vaaditun turvallisuustoimenpiteen, ja miten vaatimus on kelpuutettu.

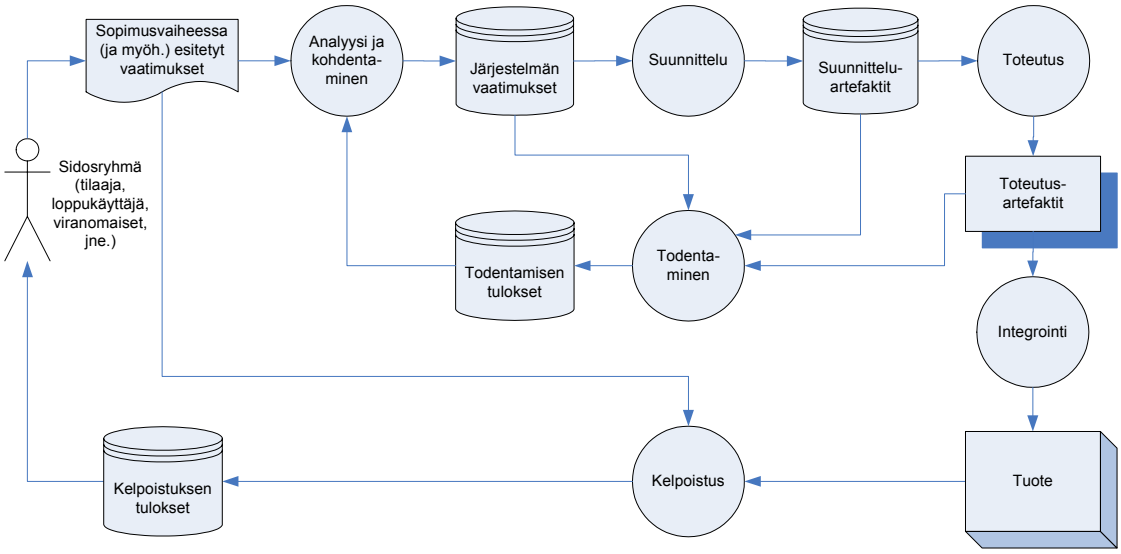
Turvallisuusvaatimusten lähteet ovat ainakin:

- koneasetus
- riskianalyysit
- turvallisuusstandardit, erityisesti koneasetuksen alaiset harmonisoidut standardit
- aikaisemmat kokemukset, esim. vahinkotilastot
- asiakas
- komponentti- tai laitevalmistaja
- viranomainen
- toteuttava tekninen organisaatio (suunnittelu ja testaus)
- loppukäyttäjät
- kenttäpalaute (esim. kunnossapidosta).

Vaatimusten hallintaa tukevia kaupallisia ja avoimen lähdekoodin työkaluja on tarjolla runsaasti. Vaatimuksia voi periaatteessa hallita toimisto-ohjelmillakin tai yleisillä tietokantatyökaluilla, mutta versionhallinnan, jäljitettävyyden ja työryhmäkäytön tarpeen takia varsinaiset vaatimushallintatyökalut ovat järkevämpi valinta.

Kuvan 3 kaaviossa on tuotekehityksen prosessimalli esitetty niin, että tuotekehitys-prosessin iteratiivinen luonne näkyy siinä selkeämmin kuin perinteisessä V-mallissa.

[1] Kansanomaisesti: kuolleenmiehenkytkin.



Kuva 3. Järjestelmäkehityksen prosessimalli.

Suunnittelu tapahtuu siis iteratiivisesti silmukassa: *vaatimukset – suunnittelu – todentaminen – analyysi – uudet ja tarkemmat vaatimukset – suunnittelu…* Vaatimukset tarkentuvat ja kohdentuvat jokaisella kierroksella. Myös uusia vaatimuksia voi syntyä tai vaatimuksia voidaan poistaa.

Prosessimallin iteratiivinen luonne on tärkeä riskianalyysien kannalta: riskianalyysejä ei tehdä pelkästään projektin alkuvaiheessa, vaan periaatteessa jokaisella kierroksella, eli riskianalyysi on osa todentamisprosessia. Riskianalyysissä syntyneet ehdotukset korjaaviksi toimenpiteiksi (eli riskin pienentämiskeinoiksi) talletetaan todentamistulosten tietovarastoon. Analyysin (tässä: riskin evaluoinnin) jälkeen korjaavien toimenpiteiden ehdotuksista muodostetaan uusia tai muutettuja vaatimuksia.

2.2 Uuden koneasetuksen vaatimukset

Uusi koneasetus VNa 400/2008 [Koneasetus VNa 400/2008] (uusi konedirektiivi 2006/42/EY [Konedirektiivi 2006/42/EY]) astuu ilman siirtymäkautta voimaan 29.12.2009. Koneiden turvallisuusvaatimukset on lueteltu sen liitteessä 1. Ohjausjärjestelmiä koskevat vaatimukset ovat liitteen 1 kohdassa 1.2, mutta niitä on myös sovelluskohtaisissa täydentävissä vaatimuksissa, jotka löytyvät liitteen 1 luvuista 2–6. Vaatimukset eivät poikkea radikaalisti edellisestä konedirektiivistä, mutta joitakin muutoksia on toteutettu: esimerkiksi harmonisoitujen standardien vaatimuksia on nostettu koneasetuksen puolelle. Tämä aiheuttaa muutospaineen myös harmonisoiduille standardeille. Päivitetyt versiot harmonisoiduista standardeista eivät välttämättä ole vielä valmiina uuden koneasetuksen astuessa voimaan, joten standardeja joudutaan alkuvaiheessa sopeuttamaan uuteen tilanteeseen.

Koneasetuksen vaatimukset ovat enimmäkseen yleisellä tasolla, mutta joukossa on yksityiskohtaisiakin vaatimuksia. Seuraavassa on esimerkkejä liitteen 1 vaatimuksista; ensimmäinen kuvaa yleisen tason vaatimuksia ja jälkimmäinen yksityiskohtaisempaa vaatimusta. Molemmat ovat koneasetuksen liitteen 1 kohdasta 1.2.1.

”Ohjausjärjestelmät on suunniteltava ja rakennettava sellaisiksi, että ne estävät vaaratilanteiden syntymisen. Ennen kaikkea ne on suunniteltava ja rakennettava sellaisiksi, että

— ne kestävät tarkoitetut käyttörasitukset ja ulkoiset vaikutukset,
— ohjausjärjestelmän laitteisto- tai ohjelmistovika ei aiheuta vaaratilanteita,
— virheet ohjausjärjestelmän logiikassa eivät aiheuta vaaratilanteita,
— …”

”Langattomassa ohjauksessa on aikaansaatava automaattinen pysäytys, jos oikeita ohjaussignaaleja ei saada tai jos yhteys menetetään.”

Jälkimmäinen vaatimusesimerkki on samalla myös esimerkki vaatimuksesta, joka on nostettu uuteen koneasetukseen vanhan konedirektiivin alaisesta harmonisoidusta standardista (SFS-EN ISO 12100-2:2003, kohta 4.11.8).

Koneasetuksen kaikkia koneita koskevat ohjausjärjestelmävaatimukset on kategorisoitu seuraavasti:

- ohjausjärjestelmien turvallisuus ja toimintavarmuus
- ohjauslaitteet
- käynnistäminen
- pysäyttäminen
- ohjaus- tai toimintatapojen valinta
- tehonsyötön häiriöt.

Sovelluskohtaisista vaatimuksista tulee vielä lisää kategorioita, kuten esimerkiksi liikkuminen ja jarruttaminen.

Koneasetuksen vaatimukset ovat lähtökohta turvallisuusvaatimuksille. Ne toimivat (ovat toimineet) pohjana myös harmonisoitujen standardien tekijöille. Valitettavasti vaatimusten jäljitettävyydestä ei ole pidetty huolta eli harmonisoitujen standardien vaatimuksien yhteydessä ei ole kerrottu, mistä koneasetuksen vaatimuksista kyseisen standardin vaatimukset periytyvät.

Konedirektiivi vaatii lisäksi, että koneenrakentaja laatii teknisen rakennetiedoston, joka sisältää mm. koneen yleiskuvauksen, piirustukset, riskin arvioinnin asiakirjat sekä jäljennöksen koneen ohjeista (ks. tarkempi luettelo konedirektiivin liitteestä VII).

2.3 Riskin arviointi

Uusi koneasetus VNa 400/2008 vaatii, kuten myös aikaisempi konedirektiivi, että riskin arviointi on aina tehtävä. Uuden koneasetuksen liitteen 1 luvussa 1 on kirjattu seuraava vaatimus:

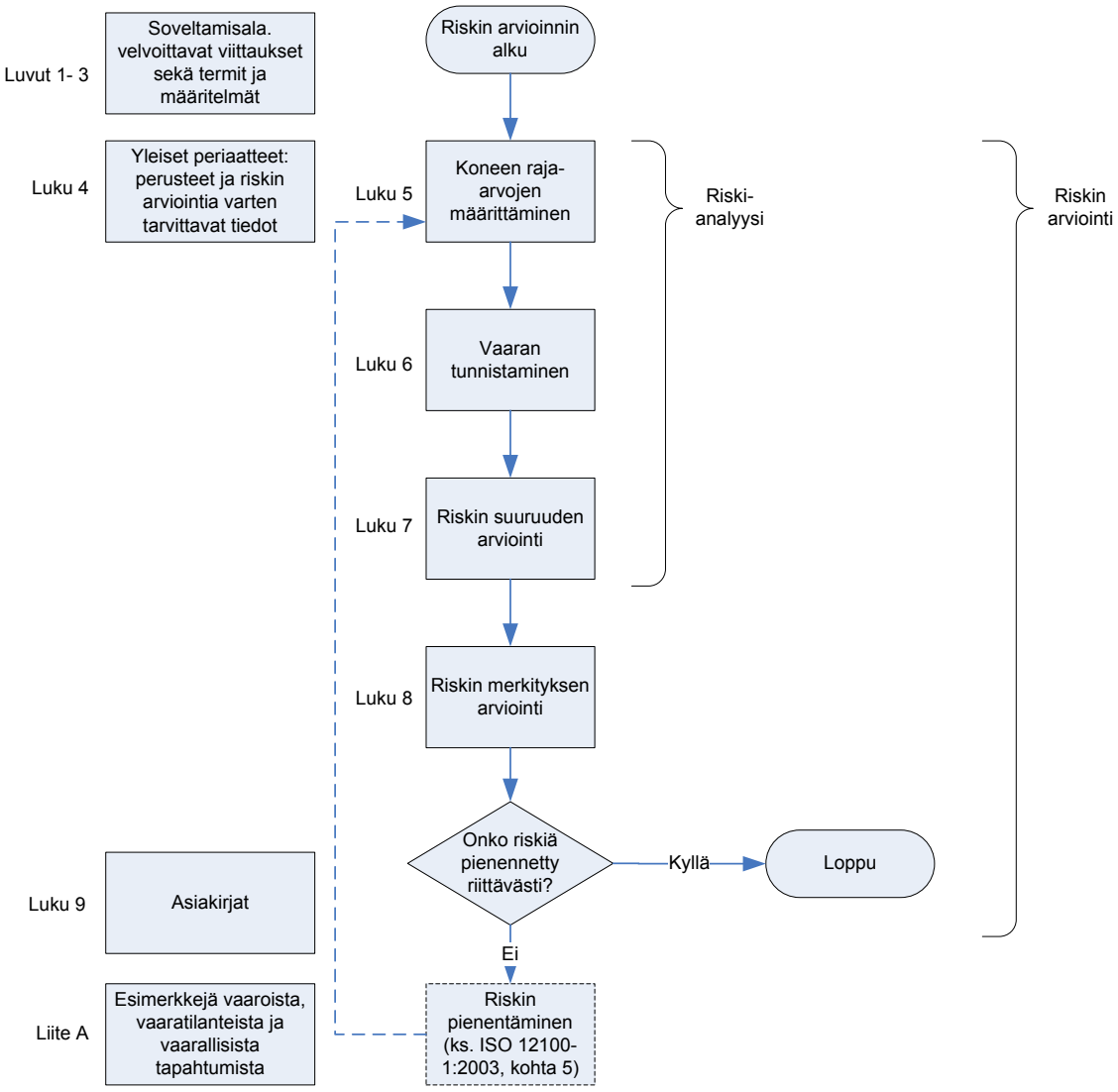
> ”Koneen valmistajan tai tämän valtuutetun edustajan on varmistettava, että tehdään riskin arviointi, jotta koneeseen sovellettavat terveys- ja turvallisuusvaatimukset voidaan määrittää. Kone on sen jälkeen suunniteltava ja rakennettava ottaen huomioon riskin arvioinnin tulokset.”

Riskin arviointia tehdään koko tuotekehitysprosessin ajan sitä mukaa, kun tieto järjestelmästä kasvaa. Riskin arvioinnin seurauksena syntyy joukko (riskin suuruuden perusteella priorisoituja) korjausehdotuksia. Niille tehdään jälkiseuranta eli ne analysoidaan. Analyysin perusteella muodostetaan uusia, kyseiseen sovellukseen liittyviä, turvallisuusvaatimuksia. Korjausehdotukset eivät siis sellaisenaan ole turvallisuusvaatimuksia, vaan niiden toteutustapa vs. jäännösriski arvioidaan eli tehdään riskin evaluointi, kuten standardi ISO 14121-1 esittää. Korjausehdotuksia voidaan siis myös hylätä tai muuttaa. Jäljitettävyys on tässäkin tärkeää: on pystyttävä osoittamaan, miten riskianalyysissä havaitut riskin pienentämistarpeet on viety suunnitteluun, ja miten toteutus on lopulta testattu. Jälkiseurantadokumentaatiossa täytyisi olla myös perustelut, jos korjausehdotus on hylätty tai se on toteutettu toisin kuin riskianalyysissä on ehdotettu.

2.3.1 SFS-EN ISO 14121 ja SFS-EN ISO 12100-1

Riskin arvioinnin standardi ISO 14121 on kaksiosainen; osa 1 [SFS-EN ISO 14121-1 2007] on varsinainen standardi ja osa 2 [ISO/TR 14121-2 2007] on tekninen raportti, jossa annetaan ohjeita ja esimerkkejä ISO 14121-1:n käyttöön.

ISO 14121-1 kuvaa mallin, miten riskin arviointi koneille tehdään. Se koostuu kuvan 4 mukaisesta sisällöstä.



Kuva 4. ISO 14121-1 -standardin sisältö.

Koska ISO 14121-1 -standardista on olemassa edellä mainittu soveltamisopas (tekninen raportti ISO 14121-2), ISO 14121-1 -standardin soveltamista yleisellä tasolla ei tässä yhteydessä käsitellä tarkemmin, mutta luvussa 3 esitellään standardin sovellusesimerkki (luvun 3 turvallisuusprosessin toimintamalli on suunniteltu ISO 14121-1 -standardin mukaisesti).

ISO 12100-1 -standardin [SFS-EN ISO 12100-1 2004] sisältö limittyy suurelta osaltaan ISO 14121-1 -standardin kanssa. Näitä standardeja ollaan yhdistämässä yhdeksi standardiksi. Uusi standardi tullee ilmestymään ISO 12100 -numerolla, ja ISO 14121 jää pois. Siihen asti kunnes yksi yhtenäinen standardi ilmestyy, riskin arviointiin suositellaan tässä yhteydessä toistaiseksi ISO 14121-1 -standardia, koska se on uudempi ja siihen on saatavilla hyvä toteutusohje. SFS-EN ISO 12100-1 -standardi on kuitenkin tarpeellinen niiltä osin kuin SFS-EN ISO 14121-1 -standardi siihen viittaa.

2.4 Koneiden ohjausjärjestelmien turvallisuutta koskevien standardien asettamat vaatimukset

2.4.1 SFS-EN ISO 12100-2

ISO 12100-2 [SFS-EN ISO 12100-2 2004] on yleinen koneiden turvallisuutta koskeva teknisten periaatteiden standardi. Se koostuu joukosta ohjeita ja vaatimuksia koneen turvallisuuden suunnittelua varten. Sen kohta 4.11 liittyy erityisesti ohjausjärjestelmiin; kohta 4.11.1 alkaa seuraavalla vaatimuksella:

> ”Ohjausjärjestelmän suunnittelutoimenpiteet on valittava siten, että niiden turvallisuuteen liittyvä toiminta aikaansaa riittävän suuruisen riskin pienentymisen
> (ks. ISO 13849-1).”

Standardin kohdassa 4.11.7 annetaan ohjeita ja vaatimuksia ohjelmoitaville ohjausjärjestelmille. Vaatimukset ovat yleisellä tasolla, ja niissä viitataan varsinaisiin ohjausjärjestelmästandardeihin IEC 61508, ISO 13849-1 ja IEC 62061. Seuraavassa esimerkki tällaisista vaatimuksista:

> ”Ohjelmoitavan elektronisen ohjausjärjestelmän rakenteen on oltava sellainen, että sellaisten satunnaisten laitevikojen ja systemaattisten vikojen todennäköisyys, jotka voivat haitallisesti vaikuttaa turvallisuuteen liittyvään ohjaustoimintoon (-toimintoihin), on riittävän alhainen. Kun ohjelmoitava elektroninen ohjausjärjestelmä suorittaa valvontatoimintoa (-toimintoja), on järjestelmän käyttäytyminen vian tullessa tunnistetuksi otettava huomioon (ks. lisäopastusta myös IEC 61508-standardisarjasta).
>
> *HUOM. Myös erityisesti koneiden turvallisuuteen liittyvät standardiehdotukset IEC 62061 ja ISO 13849 rev. sisältävät opastusta, joka soveltuu ohjelmoitaville elektronisille ohjausjärjestelmille.*
>
> Ohjelmoitavat elektroniset ohjausjärjestelmät olisi asennettava ja kelpuutettava siten, että voidaan varmistaa, että kullekin turvatoiminnolle määritetty toimintakyky (kuten IEC 61508-standardisarjan tarkoittama turvallisuuden eheyden taso (SIL)) on saavutettu. Kelpuutus koostuu testauksesta ja analyyseistä (esim. staattisia, dynaamisia tai vikaantumisanalyysejä) sen osoittamiseksi, että kaikki osat vaikuttavat toisiinsa oikein turvatoiminnon suorittamiseksi ja että tarkoittamattomia toimintoja ei esiinny.”

Standardin kohdat 4.11.7.3 ja 4.11.7.4 antavat lyhyesti ohjeita ohjelmistojen turvallisuuteen, esimerkiksi kohta 4.11.7.3 kuuluu kokonaisuudessaan näin:

> ”Ohjelmisto (mukaan lukien sisäinen käyttöjärjestelmä (tai varusohjelmisto) ja sovellusohjelmisto) on suunniteltava siten, että se täyttää turvatoimintojen toimintakykymäärittelyt (ks. myös IEC 61508-3).”

Kuten edellä olevista esimerkeistä nähdään, ISO 12100-2 -standardin vaatimukset ovat ohjelmoitavien ohjausjärjestelmien osalta vain yleisellä tasolla. Standardi on kuitenkin tarpeellinen johdanto varsi-

naisten ohjausjärjestelmästandardien käyttöön. Siihen tutustuminen antaa ohjausjärjestelmäsuunnittelijalle laajempaa näkökulmaa koko koneen turvallisuuden suunnitteluun ja muistuttaa esimerkiksi ergonomiavaatimuksista, jotka koskevat osaltaan myös ohjausjärjestelmäsuunnittelijaa, erityisesti käyttäjäliityntöjen suunnittelussa.

2.4.2 SFS-EN ISO 13849-1

ISO 13849-1 [SFS-EN ISO 13849-1 2007] tuo turvallisuuden arviointiin uuden käsitteen ”suoritustaso” (Performance Level, PL), jota käytetään määrittelemään turvallisuuteen liittyvien ohjausjärjestelmän osien kyky suorittaa turvatoiminto ennakoitavissa olevissa olosuhteissa. Standardin mukaan turvallisuuteen liittyville ohjausjärjestelmille luokitellaan suoritustaso (PL) sen mukaan, miten hyvin ne pystyvät suorittamaan toivotun turvatoiminnon. Suoritustaso valitaan kohteen riskin tai, tarkemmin sanottuna, ohjausjärjestelmään kohdistuvan riskin vähennystarpeen mukaisesti. Mitä suurempi vastuu ohjausjärjestelmällä on turvallisuudesta, ja toisaalta mitä suuremmat riskit kohteessa on, sitä korkeamman suoritustason ohjausjärjestelmä on tarpeellinen. Riskin arvioinnissa on aikaisemmin käytetty tarvittavien luokkien määrittelyssä esimerkiksi standardin EN 954-1 [SFS-EN 954-1 1997] liitteen B mukaista riskigraafi-menetelmää. Nykyään luokkien määrittelyyn on myös muitakin keinoja [SFS-EN ISO 13849-1, IEC 61508]. Joissakin C-tyypin konekohtaisissa standardeissa toimintojen luokat on esitetty standardin EN 954-1 mukaan. Tällöin standardin tekijä on jo tehnyt riskianalyysin kyseisen laitteen toiminnolle ja päätynyt tiettyyn tarvittavaan riskin vähennyksen tasoon. Tämä tarkoittaa vaatimusten täsmentymistä ja subjektiivisena koetun riskigraafi-menetelmän käytön vähenemistä. Täsmentyneiden vaatimusten myötä koneiden ohjausjärjestelmien toiminnallinen turvallisuus kehittyy ja tasoittuu. Siten käyttäjä voi luottaa varmistettuihin turvatoimintoihin.

Standardissa ISO 13849-1 suoritustasot ”a…e” (a on matalin taso ja e vaativin taso) vastaavat soveltuvin osin IEC 62061 -standardin SIL-tasoja (vrt. taulukko 1). Tämä helpottaa standardien soveltamista järjestelmään. Ohjausjärjestelmä voidaan jakaa osiin (esim. mittauselektroniikka, ohjauslogiikka ja hydrauliikka). Nämä osat voidaan käsitellä eri standardeilla, sillä SFS-EN 62061 ei käsittele hydrauliikkaa ja toisaalta taas ISO 13849-1 käsittelee suppeammin ohjelmoitavaa elektroniikkaa.

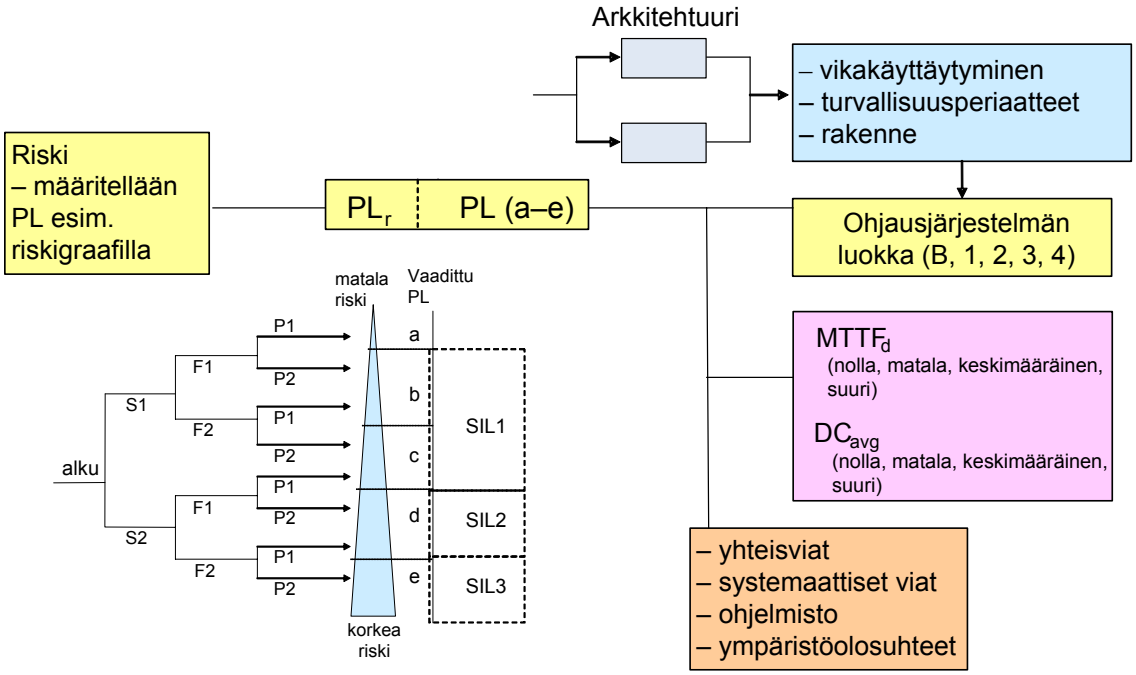
Taulukko 1. Suoritustason PL ja turvallisuuden eheyden tason SIL vastaavuus [13849-1 2007].

Suoritustaso (PL)	Keskimääräinen vikaväli (vuotta)	Keskimääräinen vaarallisen vian todennäköisyys tunnissa (1/h)	Vastaavuus eheystasoihin (SIL)
a	1,14–11,4	$10^{-5} \leq PFH_d < 10^{-4}$	ei
b	11,4–38,1	$3 \cdot 10^{-6} \leq PFH_d < 10^{-5}$	1
c	38,1–114	$10^{-6} \leq PFH_d < 3 \cdot 10^{-6}$	1
d	114–1412	$10^{-7} \leq PFH_d < 10^{-6}$	2
e	1142–11416	$10^{-8} \leq PFH_d < 10^{-7}$	3

Standardin ISO 13849-1 mukaan turvallisuuteen liittyvän ohjausjärjestelmän suoritustaso määritellään arvioimalla seuraavia näkökohtia:

- vaarallinen keskimääräinen vikaantumisaika ($MTTF_d$) jokaiselle yksittäiselle komponentille (ks. standardin liitteet C ja D)
- diagnostiikan kattavuus (DC), (ks. standardin liite E)
- yhteisvikaantuminen (CCF), (ks. standardin liite F)
- rakenne; ohjausjärjestelmän luokat (B, 1, 2, 3 ja 4) (ks. standardin kohta 6)
- turvatoiminnon käyttäytyminen vikatilanteessa (-tilanteissa), (ks. standardin kohta 6)
- turvallisuuteen liittyvä ohjelmisto (ks. standardin kohta 4.6 ja liite J)
- systemaattinen vikaantuminen; systemaattisten vikojen hallinta ja niiden välttäminen (ks. standardin liite G ja ISO 13849-2)
- kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa.

Kuva 5 esittää yhteenvetona, miten ensin määritellään vaatimustaso riskin arvioinnilla tai poimimalla vaatimukset standardista (tai muista lähteistä) ja miten toisaalta vaatimusten toteutuminen tarkastetaan edellä esitetyn listan mukaisesti.

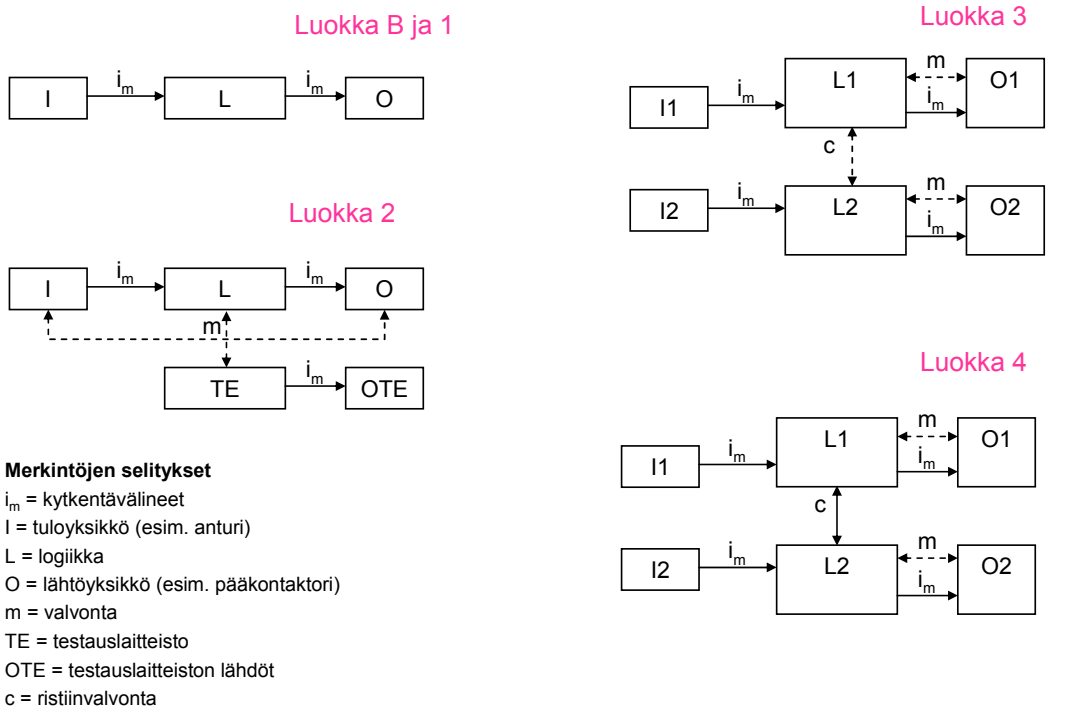


Kuva 5. Suoritustason (PL) määrittäminen. Suorituskyvyn vaatimustaso määritetään esim. riskin arvioinnilla ja ohjausjärjestelmän vaatimusten toteutuminen varmistetaan kuvassa oikealla esitetyillä tarkasteluilla.

Standardissa ISO 13849-1 luokkien käsittelyä on muutettu EN 954-1 standardiin verrattuna siten, että siinä kutakin luokkaa vastaa nimetty rakenne (arkkitehtuuri, ks. kuva 6). $MTTF_d$ ja DC -arvojen laskenta perustuu ISO 13849-1 -standardissa näiden nimettyjen rakenteiden soveltamiseen. Jos käytettäi-

siin muuta rakennetta tai arkkitehtuuria, tässä standardissa esitettyjä taulukoita ja laskelmia ei voisi käyttää. Nimettyjen rakenteiden soveltaminen rajoittaa standardin soveltamista, sillä esimerkiksi kolmikanavaiset järjestelmät eivät vastaa nimettyjä rakenteita. Käytetty rakenne voidaan redusoida vastaamaan nimettyjä rakenteita esimerkiksi siten, että kolmikanavainen järjestelmä redusoidaan kaksikanavaiseksi. Tällöin osa turvatoiminnon suoritustasosta jää laskennallisesti osoittamatta, eli turvatoiminto on käytännössä parempi kuin mitä pystytään osoittamaan.

Luokkien B, 1 ja 2 rakenteet ovat yksikanavaisia, mutta luokassa 2 on lisäksi testaus. Luokkien 3 ja 4 rakenteet ovat kaksikanavaisia (ks. myös liite A).



Kuva 6. Eri luokkien nimetyt rakenteet (arkkitehtuurit).

Usein ohjausjärjestelmien arkkitehtuurit ovat monimutkaisempia kuin nimetyt arkkitehtuurit. Tämän vuoksi ohjausjärjestelmä pitää jakaa alijärjestelmiin. Kunkin alijärjestelmän suoritustaso arvioidaan erikseen. Alijärjestelmiä voidaan tarkastella myös IEC 62061 standardin mukaan. Lopuksi tulokset yhdistetään. Jos alinta suoritustasoa on enemmän kuin 3 kpl (suoritustasoilla b ja c 2 kpl), kokonaisuuden suoritustaso putoaa yhden tason verran.

Standardissa ISO 13849-1 tärkeänä tekijänä on järjestelmän $MTTF_d$-arvo (keskimääräinen vaarallinen vikaantumisaika). Jos vaarallisten vikojen osuutta ei tiedetä tarkasti, yleensä arvioidaan, että puolet vioista on vaarallisia. $MTTF_d$-arvot on luokiteltu seuraavasti:

- matala: $3 \leq MTTF_d < 10$ vuotta
- keskimääräinen: $10 \leq MTTF_d < 30$ vuotta
- korkea: $30 \leq MTTF_d \leq 100$ vuotta.

Kussakin kanavassa $MTTF_d$ -arvot summataan seuraavalla kaavalla (likiarvo):

$$1/MTTF_{dtot} = 1/MTTF_{d1} + 1/MTTF_{d2} + \ldots + 1/MTTF_{dn}$$

Luokan 3 ja 4 järjestelmät ovat kaksikanavaisia, ja niissä pitää laskea lisäksi kanavien symmetroitu arvo, jota käytetään standardin kuvissa ja taulukoissa PL-tason määrittämiseksi. Standardissa ei uskota erittäin hyviin laskennan tuloksiin, ja siksi kunkin kanavan maksimiarvo on 100 vuotta. Komponenttien $MTTF_d$-arvoina käytetään seuraavia lähteitä priorisointijärjestyksessä:

a) käytetään valmistajan antamia tietoja; näitä löytyy nykyään jonkin verran internetistä turvakomponenteillekin
b) käytetään standardin ISO 13849-1 liitteissä C ja D esitettyjä arvoja
c) valitaan 10 vuotta.

Diagnostiikan kattavuuden (DC) arviointia varten standardissa (ISO 13849-1 liite E) esitetään esimerkkejä kuhunkin diagnostiikan tasoon (nolla, matala, keskimääräinen, korkea). Esimerkkien pohjalta käyttäjä arvioi, mitä DC-arvoa ratkaisu muistuttaa. Luokissa 2 ja 3 pitää saavuttaa vähintään arvo ”matala” ja luokassa 4 vähintään arvo ”korkea”.

Standardissa ISO 13849-1 esitetään vaatimuksia myös turvallisuuteen liittyvälle ohjelmistolle. Ohjelmistovaatimuksia on erikseen sovellusohjelmistolle, sulautetulle ohjelmistolle ja parametrointiprosessille. Vaatimukset on esitetty eri suoritustasoille (PL). Vaativien sulautettujen ohjelmistojen tapauksessa viitataan myös standardiin IEC 61508-3. Ohjelmistosuunnitteluprosessi perustuu standardin mukaisesti ns. V-malliin. Prosessin eri vaiheissa suunnittelijan ja ohjelmoijan pitää toteuttaa monenlaisia vaatimuksia. Ohjelmistokoodaajan tulee noudattaa kyseistä kohdetta varten laadittuja ohjelmointisääntöjä (standardin liitteessä J on esimerkki ohjelmointisäännöistä).

Yhteisvikojen tarkastelua varten standardissa on esitetty kysymyslista. Luokkien 2, 3 ja 4 järjestelmien pitää saada tästä listasta vähintään 65 pistettä. Systemaattisten vikojen välttämiseen ja hallintaan standardissa esitetään vaatimuksia. Samantapaisia turvallisuusperiaatteisin liittyviä vaatimuksia esitetään myös standardin 2-osassa. Ohjausjärjestelmän tulee kyetä toimimaan ennakoitavissa olevissa ympäristöolosuhteissa, ja tähän liittyen standardissa on muutamia yleisluonteisia vaatimuksia.

Vaatimusten täsmentyessä vanhojen järjestelmien puutteiden havaitseminen käy aiempaa selkeämmäksi ja helpommaksi, koska tulkinnanvaraisuus vähenee. Toisaalta ohjausjärjestelmien tullessa yhä älykkäämmiksi ja monimutkaisemmiksi myös turvallisuuteen liittyvät haasteet kasvavat. Tähän vaikuttaa erityisesti ohjelmistojen tuomat mahdollisuudet ja toisaalta ohjelmistovirheiden tuomat uhat. Ohjelmiston virheettömyyden ja toisaalta virheiden hallinnan osoittaminen jääkin helposti puutteelliseksi. Ohjelmiston virheettömyyttä kaikenlaisissa käyttöympäristöissä ei yleensä voida osoittaa, vaan vaarallisesti vaikuttavan virheen esiintymisen todennäköisyys voidaan saada pieneksi. Usein järjestelmäsuunnittelijat voivat käyttää turvallisuusluokiteltuja komponentteja, mutta järjestelmän osien yhdistäminen ja ohjelmistot pitää kelpuuttaa tapauskohtaisesti.

2.4.3 SFS-EN ISO 13849-2

SFS-EN ISO 13849-2 [2004] määrittelee vaatimukset ohjausjärjestelmän turvallisuuden kelpuutukselle. Tätä julkaisua kirjoitettaessa ISO 13849-2 -standardia ei ole päivitetty vastaamaan uusinta ISO 13849-1 -standardia, joten se ei tunne esimerkiksi standardin ISO 13849-1 suoritustasoja (PL-tasot).

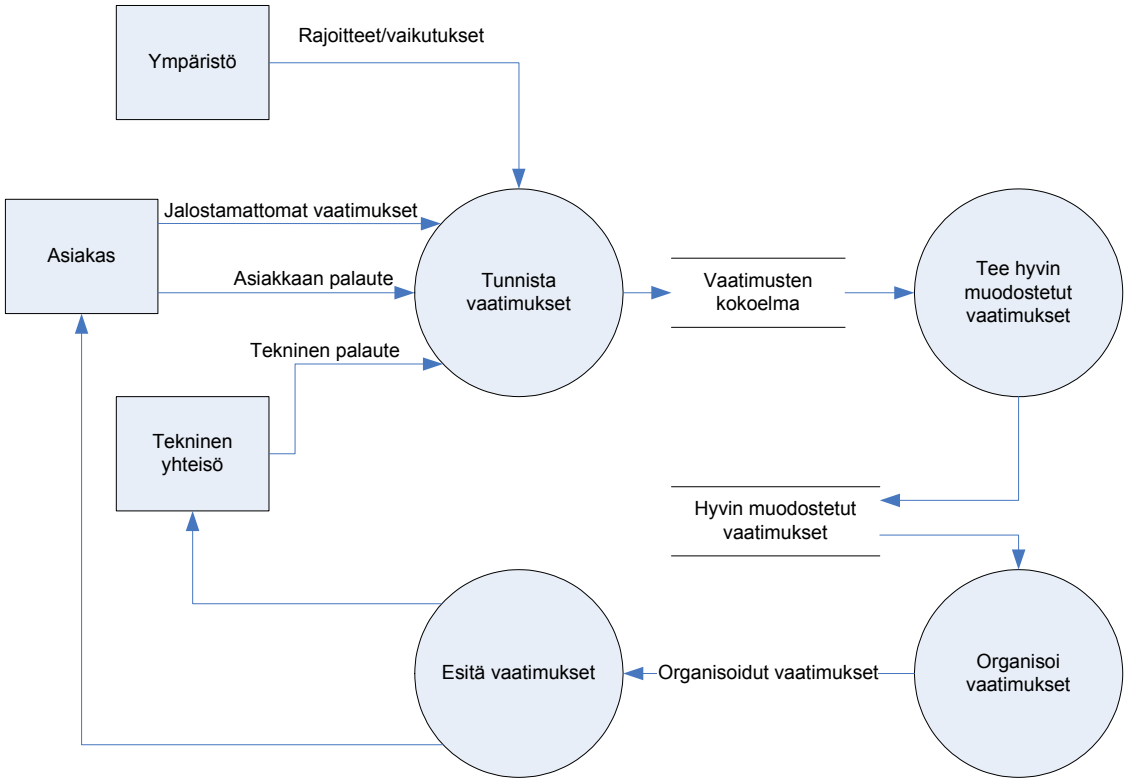
Päivitystyö on kuitenkin käynnissä. Standardissa esitetään turvallisuusperiaatteet ja kattavat komponenttien vikalistat, joita kelpuutusvaiheessa voi käyttää apuna.

2.5 C-tyypin standardien asettamat vaatimukset

Konekohtaisissa standardeissa (C-tyypin standardit) kuvataan yleisiä standardeja (A-tyypin standardit) ja turvallisuusperiaatteita ja -laitteita käsitteleviä standardeja (B-tyypin standardit) tarkemmin koneiden tai koneryhmien erityispiirteitä. Näihin kuuluvat myös ohjausjärjestelmien ominaisuudet. Monissa 90-luvun lopun ja 2000-luvun alun standardeissa viitataan standardin SFS-EN ISO 954-1 luokkiin. Uusimmissa standardeissa ja standardiluonnoksissa viitataan jo PL-tasoihin. PL-tasovaatimuksia on esitetty esimerkiksi robottistandardissa, henkilönostinstandardiluonnoksessa, autonostinstandardiluonnoksessa ja muutamissa paperinkäsittelyyn liittyvissä standardiluonnoksissa.

2.6 IEEE Std 1233

IEEE Std 1233 [1998] on vaatimusmäärittelyjen luontiohje. Se kuvaa vaatimusmäärittelyprosessia kuvan 7 mukaisesti.



Kuva 7. IEEE Std 1233 -standardin näkemys vaatimusmäärittelyprosessista.

Vaatimuslähteitä on IEEE Std 1233 -mallissa kolme: asiakas, ympäristö ja tekninen yhteisö (joka suunnittelee, toteuttaa ja ylläpitää järjestelmää). Tässä mallissa konedirektiivi ja turvallisuusstandardit kuuluvat ympäristö-kategoriaan. Samaan kategoriaan kuuluvat myös poliittiset vaikutukset, markkinatilanteeseen liittyvät vaikutukset, muut standardit ja käytännöt, kulttuurin vaikutukset, organisaation (joka vaatimukset koostaa) vaikutukset sekä ympäristöolosuhteet (lämpötila, kosteus jne.). Tässä mallissa riskianalyysistä tulevat vaatimukset voidaan ajatella kuuluvan kuvan 7 nuoleen ”Tekninen palaute”.

IEEE Std 1233 määrittelee käsitteen *hyvin muodostettu vaatimus*[2]. Tällainen vaatimus on: *sellainen järjestelmän toimintakyvyn ilmaisu, joka voidaan kelpuuttaa, ja joka täytyy voida toteuttaa ao. järjestelmällä asiakkaan ongelman ratkaisemiseksi tai asiakkaan tavoitteiden saavuttamiseksi, ja jolla on mitattavissa olevat määreet ja joka on rajattu rajoitteilla*. Tällainen vaatimus koostuu siis kolmesta osastekijästä:

- toimintakyky
- määre ja
- rajoite.

Hyvä vaatimus on standardin mukaan:

- abstrakti (riippumaton toteutustavasta)
- yksikäsitteinen
- jäljitettävissä oleva
- kelpuutettavissa oleva.

Esimerkki hyvin muodostetusta vaatimuksesta on seuraavanlainen:

> ”Ajoneuvon on kyettävä kuljettamaan ihmisiä Tampereen ja Helsingin välillä 1 h 30 min ajassa enimmäisnopeuden ollessa 220 km/h”

Kyseisessä esimerkissä järjestelmän kykenevyys on ”kuljettaa ihmisiä Tampereen ja Helsingin välillä”, määreenä on ”1 h 30 min ajassa” ja rajoitteena on ”220 km/h:n enimmäisnopeus”.
Vaatimuksiin liitetään yleensä joukko attribuutteja. IEEE Std 1233 ehdottaa seuraavia:

- tunniste (numero tai muu merkkijono)
- prioriteetti
- kriittisyys
- toteutettavuus
- riski
- lähde
- tyyppi (kuten turvallisuusvaatimus).

[2] Engl. ”well-formed requirement”.

Kriittisyys-attribuutti on käytännössä vaikea mieltää erillisenä prioriteetti-attribuutista. Sen sijaan kannattaa harkita seuraavia attribuutteja: tila (luonnos, ehdotettu, hyväksytty, jne.), vastuuhenkilö ja versionumero.

Standardi luettelee joitakin vaatimusmäärittelyn ongelmia:

- vaatimusten seassa on suunnittelu- ja toteutusvalintoja (ne voivat olla hyödyllisiä, mutta ne on kirjattava muualle)
- ylimäärittely
- turhan tiukat rajoitteet
- epämääräisyys (kuten ”oltava halpa” tai ”kohinan oltava vähäinen”)
- oletuksiin perustaminen.

IEEE Std 1233 antaa myös esimerkin järjestelmän vaatimusmäärittelydokumentin sisällöstä (ks. kuva 8).

1. Johdanto
- 1.1 Järjestelmän tarkoitus
- 1.2 Järjestelmän käyttöala
- 1.3 Määritelmät, akronyymit ja lyhenteet
- 1.4 Viitteet
- 1.5 Järjestelmän yleiskatsaus

2. Järjestelmän kuvaus
- 2.1 Järjestelmän konteksti
- 2.2 Järjestelmän moodit ja tilat
- 2.3 Järjestelmän tärkeimmät toiminnot,
- 2.4 Tärkeimmät määreet
- 2.5 Tärkeimmät rajoitteet
- 2.6 Käyttäjien ominaisuudet
- 2.7 Oletukset ja riippuvuudet
- 2.8 Käyttötapaukset

3. Järjestelmän toiminnallisuus, määreet ja rajoitteet
- 3.1 Fyysiset
  - 3.1.1 Rakenne
  - 3.1.2 Kestävyys, kestoikä
  - 3.1.3 Mukautuvuus
  - 3.1.4 Ympäristöolosuhteet
- 3.2 Järjestelmän suorituskyky
- 3.3 Järjestelmän tietoturvallisuus
- 3.4 Tiedonhallinta
- 3.5 Järjestelmän operointi
  - 3.5.1 Inhimilliset tekijät
  - 3.5.2 Kunnossapidettävyys
  - 3.5.3 Käyttövarmuus
- 3.6 Menettelytavat ja säännökset
- 3.7 Järjestelmän ylläpito koko elinkaaren aikana

4. Järjestelmän liityntärajapinnat

Kuva 8. IEEE Std 1233 -standardin esimerkki järjestelmän vaatimusmäärittelydokumentin sisällysluettelosta.

IEEE Std 1233 on varsin käyttökelpoinen ohje laadukkaiden vaatimusmäärittelyjen tekemiseen, mukaan lukien turvallisuusvaatimukset. Laadukkaasti määritelty vaatimusmäärittelyprosessi on perusedellytys turvallisuusvaatimusten hallintaan.

2.7 Muita vaatimusmäärittelyä käsitteleviä standardeja

2.7.1 IEEE-standardit 15288, 12207 ja 1220

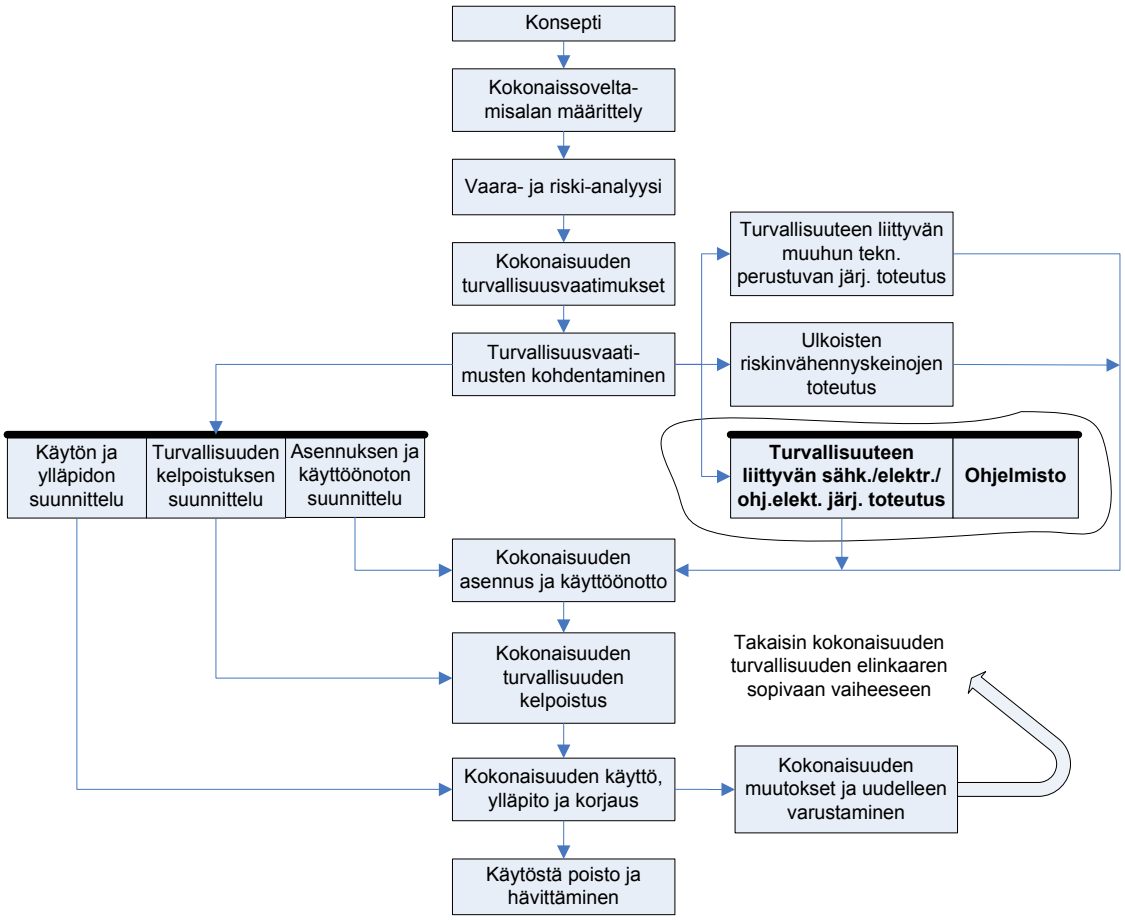
IEEE:n standardisarjassa on muitakin vaatimusmäärittelyä käsitteleviä standardeja kuin IEEE Std 1233. Näistä tässä esitellään lyhyesti IEEE Std 15288 [ISO/IEC/IEEE 15288 2008], IEEE Std 12207 [ISO/IEC/IEEE 12207 2008] sekä IEEE Std 1220 [ISO/IEC 26702 IEEE Std 1220-2005 2007]. Nämä kaikki on julkaistu myös ISO/IEC-standardeina, kaksi ensimmäistä samalla numerolla ja jälkimmäisin numerolla 26702. ISO/IEC/IEEE 15288 ja 12207 ovat alun perin lähtöisin ISO/IEC:stä, mutta IEEE:n tekemät muutokset on otettu mukaan uusimmissa versioissa, ja organisaatioiden versiot standardeista ovat nyt yhtenevät. ISO/IEC 267023 / IEEE 1220 on peräisin IEEE:ltä, ja se on sellaisenaan otettu ISO/IEC-standardiksi vain uusilla kansilla.

Edellä mainitut kolme standardia määrittelevät systeemisuunnittelun kokonaisprosessin. ISO/IEC/IEEE 15288 on yleinen systeemisuunnittelun standardi, kun taas ISO/IEC/IEEE 12207 on pelkästään ohjelmistotekniikkaan keskittyvä standardi, ja on siten periaatteessa 15288-standardin erikoistapaus. Nämä kaksi standardia on pyritty (ja yhä pyritään) harmonisoimaan siten, että ne käyttävät samaa terminologiaa ja samaa prosessimallia. Sen sijaan IEEE Std 1220 määrittelee edellisistä poikkeavan systeemisuunnittelun prosessimallin. Sitä voi toki käyttää ISO/IEC/IEEE 15288 -standardin lisänä; IEEE Std 1220 antaakin tähän ohjeita liitteissään. Joka tapauksessa ISO/IEC/IEEE 15288 on näistä tunnetumpi.

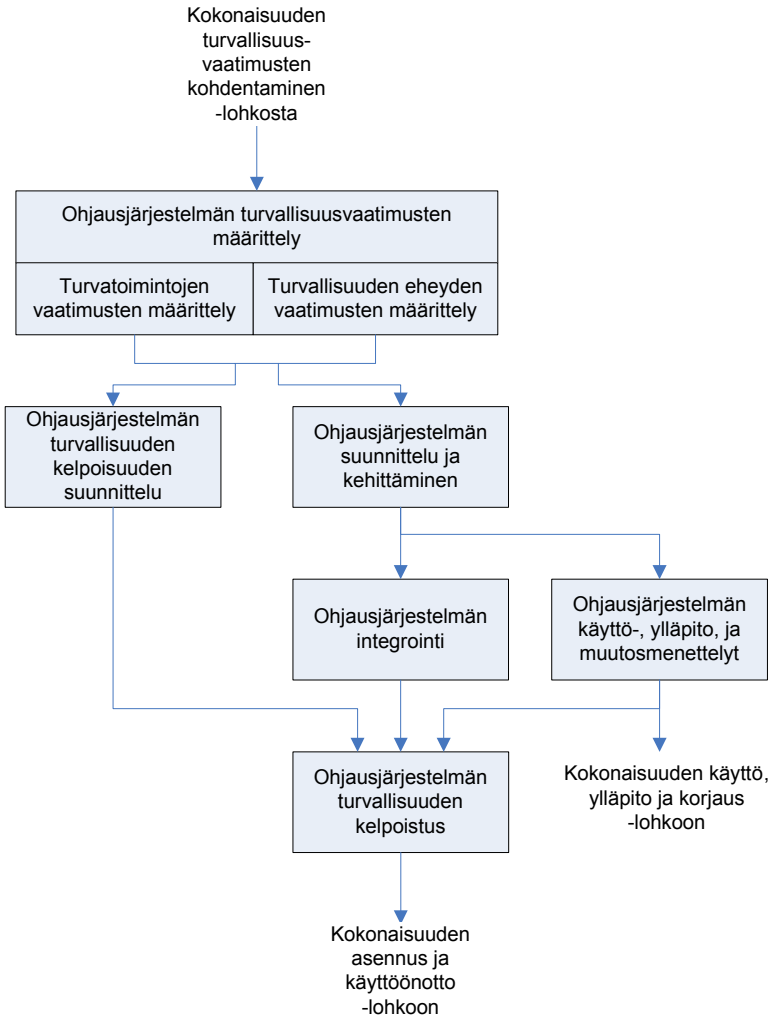
ISO/IEC/IEEE 15288 jakaa vaatimusmäärittelytyön kahteen prosessiin, mitkä ovat asiakasvaatimusten määrittely ja vaatimusten analyysi. Määrittelyvaiheessa asiakkaan tarpeet, odotukset ja toiveet järjestelmän tuottamille palveluille kirjataan asiakkaan ymmärtämässä muodossa. Analyysivaiheen tarkoituksena on kirjoittaa asiakasvaatimukset teknisiksi ja mitattaviksi vaatimuksiksi, jotka kuvaavat palveluja tuottavaa järjestelmää, kuitenkaan ottamatta kantaa toteutustapaan. Näitä prosessimalleja kannattaa käyttää tukena omaa vaatimusmäärittelyprosessia suunniteltaessa. Selkeät ja systemaattiset vaatimusmäärittelyprosessit edesauttavat turvallisuuden parantamista, sillä, kuten luvun 2 johdannossa todettiin, 40–44 % vaaratilanteeseen johtavista virheistä voi johtua virheistä vaatimusmäärittelyissä.

2.7.2 IEC 61508-1

IEC 61508-1 [IEC 61508-1 1998] määrittelee sähköisten, elektronisten ja ohjelmoitavien elektronisten (S/E/OE) turvallisuuteen liittyvien järjestelmien toiminnallisen turvallisuuden yleiset vaatimukset. Sen elinkaarimallissa (ks. kuva 9) turvallisuusvaatimukset kartoitetaan vaara- ja riskianalyysin avulla, ne muunnetaan toiminnallisiksi vaatimuksiksi sekä eheystasovaatimuksiksi ja ne kohdennetaan S/E/OE-osajärjestelmiin, muun teknologian osajärjestelmiin tai ulkoisiin riskinvähennyskeinoihin.



Kuva 9. Järjestelmän turvallisuuden elinkaari IEC 61508-1 -standardin mukaan; ympyröity osuus avattuna kuvassa 10.



Kuva 10. Turvallisuuteen liittyvän ohjausjärjestelmän toteutus; sisältää myös ohjelmiston.

2.7.3 SFS-EN 62061

SFS-EN 62061 [SFS-EN 62061 2005] on IEC 61508 -standardin sovellusstandardi koneiden ohjausjärjestelmiin. IEC 61508-1 ja SFS-EN 62061 antavat ohjeita turvallisuusmäärittelyjen tekemiseen, ei niinkään vaatimusmäärittelyprosessiin, vaan miten turvatoiminnot määritellään (ja IEC 61508-1 -standardissa lisäksi, miten ne kohdennetaan). Ne edellyttävät aina kaksiosaista turvatoiminnon vaatimusten erittelyä: toiminnalliset vaatimukset ja turvallisuuden eheystason määrittely. Toiminnalliset vaatimukset koostuvat itse turvatoiminnon (esim. sanallisesta) kuvauksesta, eli mitä tulotietoja turvatoiminnolla on, mitä tiedolla tehdään (logiikka) ja mitä lähtötietoja turvatoiminto tuottaa. Lisäksi SFS-EN 62061:n mukaan on määriteltävä seuraavat asiat soveltuvin osin (lainaus SFS-EN 62061 -standardista):

- ”koneen olosuhteet (esimerkiksi toimintatapa), jossa turvallisuuteen liittyvän ohjaustoiminnon on oltava aktivoituna tai pois toiminnasta

- niiden toimintojen ensisijaisuus, jotka voivat olla samanaikaisesti aktiivisena ja jotka voivat johtaa ristiriitaiseen toimintatilaan
- jokaisen turvallisuuteen liittyvän ohjaustoiminnon toimintojen taajuus
- vaadittava vasteaika jokaiselle turvallisuuteen liittyvälle ohjaustoiminnolle
- turvallisuuteen liittyvän ohjaustoiminnon ja muiden koneen toimintojen väliset rajapinnat
- vaadittavat vasteajat (esimerkiksi tuloihin ja lähtöihin liittyvät laitteet)
- jokaisen turvallisuuteen liittyvän ohjaustoiminnon kuvaus
- kuvaus vikaan reagoivista toiminnoista ja kaikki niiden rajoitukset, esimerkiksi uudelleen käynnistys tai koneen jatkuva toiminta niissä tapauksissa, joissa alkuperäinen reagointi vikaan on koneen pysäyttäminen
- kuvaus käyttöympäristöstä (esimerkiksi lämpötila, kosteus, pöly, kemikaalit, mekaaninen tärinä ja iskut)
- testaukset ja kaikki niihin liittyvät laitteet (esimerkiksi testauslaitteet ja niiden liitäntäportit)
- toimintajaksojen taajuus, käyttöjakso ja käyttöluokka sähkömekaanisille laitteille, joita on tarkoitus käyttää turvallisuuteen liittyvissä ohjaustoiminnoissa.”

Näiden lisäksi on vielä erikseen määritettävä sähkömagneettisten häiriöiden sietotaso[3].

Turvallisuuden eheyden taso määritellään SFS-EN 62061 -standardissa vain kolmella tasolla, SIL 1, SIL 2 ja SIL 3, kun IEC 61508 -standardissa on lisänä SIL 4 -taso. SIL-taso kuvaa vaarallisen vikaantumisen todennäköisyyttä tunnissa (SIL 1: $< 10^{-5}$; SIL 2: $< 10^{-6}$; SIL 3: $< 10^{-7}$). SIL-tason määritykseen annetaan SFS-EN 62061 -standardin liitteessä A eräs menetelmä, mutta sen käyttö ei ole pakollista.

[3] Ks. erityisesti uudet toiminnalliseen turvallisuuteen liittyvät EMC-standardit IEC 61326-3-1 ja -3-2.

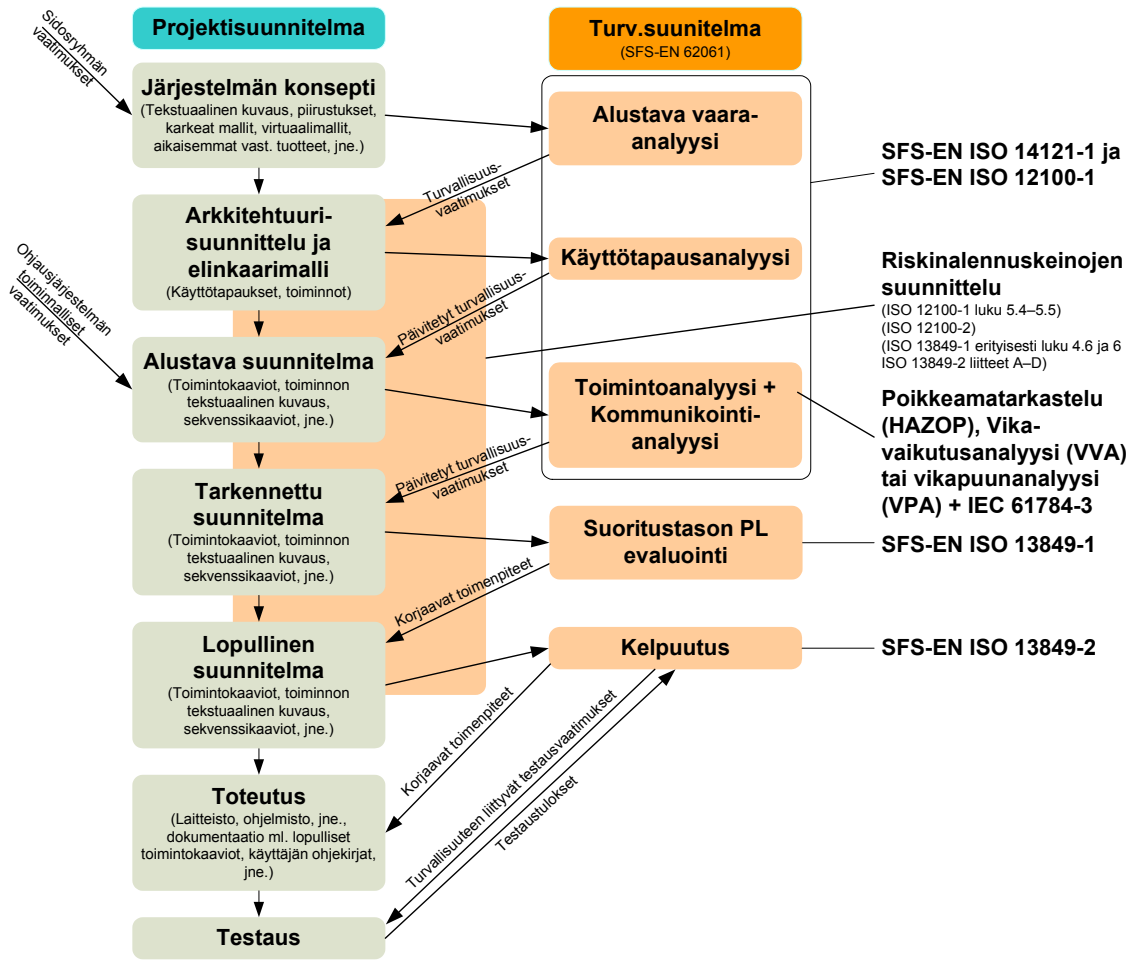
3. Turvallisuusprosessin toimintamalli

3.1 KOTOTU-referenssimalli

KOTOTU-projektissa suunniteltiin kuvan 11 mukainen kolmen iteraatiokierroksen referenssimalli tuotekehitysprosessista ja siihen liittyvästä turvallisuusprosessista, joka noudattaa riskin arvioinnin standardia SFS-EN ISO 14121-1:2007, riskin pienentämisen periaatteiden standardia SFS-EN ISO 12100-2:2003, ohjausjärjestelmien turvallisuusstandardia SFS-EN ISO 13849-1:2007 ja ohjausjärjestelmien kelpuutusstandardia SFS-EN ISO 13849-2:2004. [Tiusanen et al. 2007, Tiusanen et al. 2008]

Turvallisuussuunnitelman malli on lainattu standardista IEC 62061, koska sitä ei ole määritelty edellä mainituissa standardeissa. Turvallisuussuunnitelmassa kuvataan kuvan 11 mukaisen prosessimallin projektikohtainen toteutustapa. Se on suurimmalta osaltaan vakio jokaisessa vastaavassa projektissa, mutta koska tietyt menettelytavat, esim. konfigurointiohjeet, voivat olla projektikohtaisia, projektikohtainen turvallisuussuunnitelma täytyy tehdä. Esitäytetty turvallisuussuunnitelma voidaan tarjota suunnittelijalle yrityksen prosessiohjeissa; turvallisuussuunnitelma on itsessään prosessiohje.

Referenssimalli perustuu siis toiminnallisen turvallisuuden osalta standardiin ISO 13849-1. Vastaavanlainen referenssimalli voitaisiin tehdä käyttäen perustana IEC 62061 -standardia [SFS-EN 62061 2006], mutta tässä yhteydessä on keskitytty ISO 13849-1 -standardiin.



Kuva 11. KOTOTU-projektin turvallisuusprosessin referenssimalli.

Kuvan 11 referenssimallin pääasiallisia riskianalyysikierroksia on kolme: alustava vaara-analyysi, käyttötapausanalyysi[4] sekä toimintoanalyysi. Riskianalyysi etenee siis yleiseltä tasolta signaali- ja komponenttitasolle. Alustavan vaara-analyysin aikana voidaan jo päättää tärkeimmistä turvallisuusratkaisuista, kuten suoja-alueiden käytöstä. Käyttötapausanalyysin aikana etsitään systemaattisesti työn eri vaiheisiin liittyviä ihmisen virheistä aiheutuvia vaaroja. Toimintoanalyysissä, joka voidaan tehdä vika- ja vaikutusanalyysinä, poikkeamatarkasteluna tai vikapuuanalyysinä, tarkastellaan yksityiskohtaisesti ohjausjärjestelmän vikamuotojen aiheuttamia vaaroja. Toimintoanalyysivaiheessa analysoidaan myös kommunikointijärjestelmän turvallisuus [Tiusanen et al. 2001, Tiusanen et al. 2005].

Nämä kolme analyysivaihetta on valittu, koska tyypillisessä koneenohjausjärjestelmässä ne riittävät kattavaan riskianalyysiin ja ne tarkentavat suunnitelmia sopivin portain. Niitä varten tarvittava työaika ei ole kuitenkaan kohtuuton.

[4] VTT:n variaatio yleisemmin tunnetusta toimintovirheanalyysistä.

Kaikissa näissä riskianalyysivaiheissa voidaan tunnistaa turvatoimintoja, mutta pääasiassa ne määritellään alustavan vaara-analyysin ja käyttötapausanalyysin aikana.

Kaksi viimeistä osaprosessia liittyvät suunnitelman todentamiseen ja kelpuuttamiseen. Suoritustason (PL) evaluointi tehdään ISO 13849-1 -standardin mukaisesti ja kelpuuttaminen saman standardin osan 2 mukaan[5].

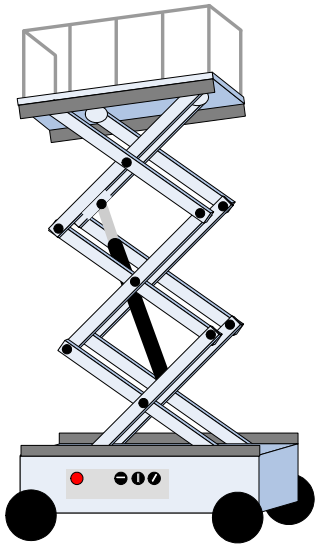
Edellä esitellyt osaprosessit on esitelty tarkemmin liitteessä B.

Näiden riskianalyysi- ja todentamisprosessien lisäksi turvallisuuteen liittyvää työtä tehdään myös suunnittelupuolella. Kuvan 11 referenssimallissa suunnitteluvuon alla oleva ”varjo” kuvaa riskin pienentämiseen liittyvien keinojen suunnittelua. Ohjeita siihen löytyy sekä ISO 12100 -standardeista että ISO 13849 -standardeista kuvassa 11 mainituista luvuista.

3.2 Esimerkkijärjestelmän suunnitteluprosessi referenssimallin mukaisesti

3.2.1 Esimerkkijärjestelmän esittely

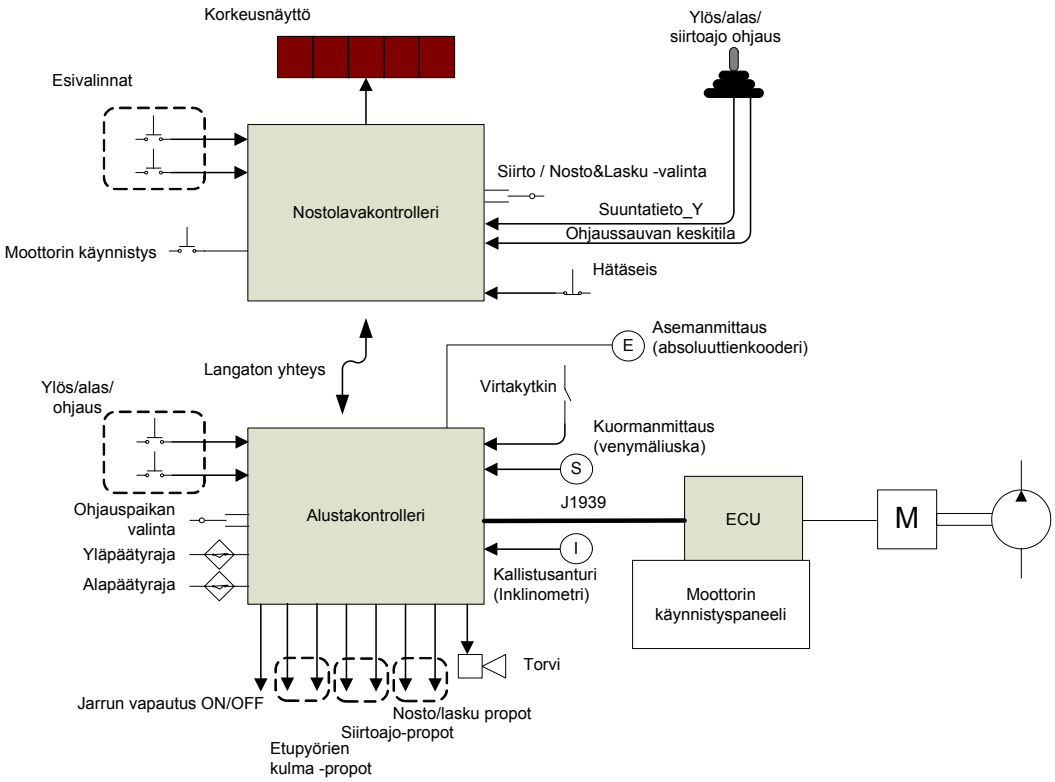
KOTOTU-projektin esimerkkijärjestelmäksi valittiin sähköhydraulisesti ohjattavan saksinosturin (ks. kuva 12) ohjelmoitava ohjausjärjestelmä.



Kuva 12. Kuvitteellinen saksinosturi; esimerkkijärjestelmänä on tämän koneen ohjelmoitava ohjausjärjestelmä.

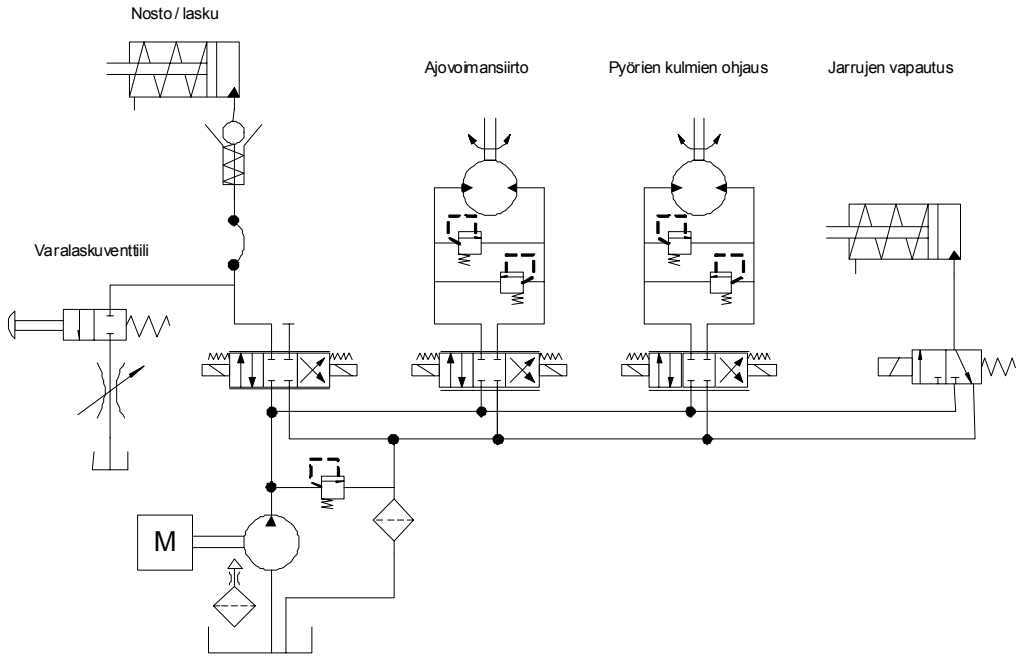
Saksinosturin ohjelmoitavan ohjausjärjestelmän alustava arkkitehtuuri muodostui kuvan 13 mukaiseksi.

[5] Tätä kirjoitettaessa standardin osaa 2 ei ole vielä harmonisoitu osan 1 kanssa.



Kuva 13. Esimerkkijärjestelmän alustava arkkitehtuuri.

Myös hydrauliikkajärjestelmästä tehtiin alustava suunnitelma, joka on esitetty kuvassa 14.



Kuva 14. Esimerkkijärjestelmän hydrauliikan alustava suunnitelma.

On huomattava, että esimerkkinä suunniteltu ohjausjärjestelmäarkkitehtuuri ei kelpaa todellisen tuotteen esimerkiksi. Tässä on tarkoituksena demonstroida turvallisuusprosessia eikä täydellistä ohjausjärjestelmän suunnitelmaa.

Järjestelmästä voidaan jo tässä vaiheessa tunnistaa osa toiminnoista (ks. taulukko 2).

Taulukko 2. Alustavan suunnittelun aikana tunnistetut toiminnot (osa toiminnoista on jo määritelty, joten niihin on jo liitetty tunniste).

Toiminto	Tunniste
Nostolaitteen virtojen päällekytkentä/sammuttaminen	
Moottorin käynnistys	
Ohjauspaikan valinta	
Työtason manuaalinen nosto/lasku – Kuorman mittaus ja ilmaisu – Kallistuksen mittaus ja ilmaisu – …	FUNC751 FUNC755 FUNC753 …
Työtason pikanosto/-lasku	
Siirtoajo	
Pyörien kääntökulman ohjaaminen	
Jarrujen vapautus	
Hätälasku	
Hätä-seis	
Ohjelmistojen alaslataus	
Parametrointi (konfigurointi)	
…	

Osa toiminnoista on turvatoimintoja. Huomioi turvatoiminnon määritelmä (ISO 13849-1): *"koneen toiminto, jonka vikaantuminen voi aiheuttaa välittömän riskin (riskien) kasvamisen"*. IEC 62061 määrittelee turvatoiminnon samoin, mutta ei käytä sitä varsinaisessa tekstissään, vaan käyttää termiä *"turvallisuuteen liittyvä ohjaustoiminto"*. Se määritellään näin: *"määrätyllä turvallisuuden eheyden tasolla olevan turvallisuuteen liittyvän sähköisen ohjausjärjestelmän toteuttama ohjaustoiminto, jonka tarkoituksena on säilyttää koneen turvallinen tila tai estää riskin (riskien) välitön kasvaminen"*. Näiden määritelmien ero näkyy esimerkiksi Työtason manuaalin nosto/lasku-toiminnon tapauksessa: ISO 13849-1 standardin mukaan ko. toiminto on turvatoiminto (sen vikaantuminen voi aiheuttaa vaaran), mutta se ei ole IEC 62061 -standardin mukainen turvallisuuteen liittyvä ohjaustoiminto (sen tarkoituksena ei ole säilyttää turvallinen tila tai estää riskejä). Tässä yhteydessä pitäydytään ISO 13849-1 -standardin mukaiseen määritelmään, jossa myös normaalit käyttötoiminnot lasketaan turvatoiminnoiksi, jos riskianalyysi niin osoittaa.

3.2.2 Turvallisuussuunnitelma

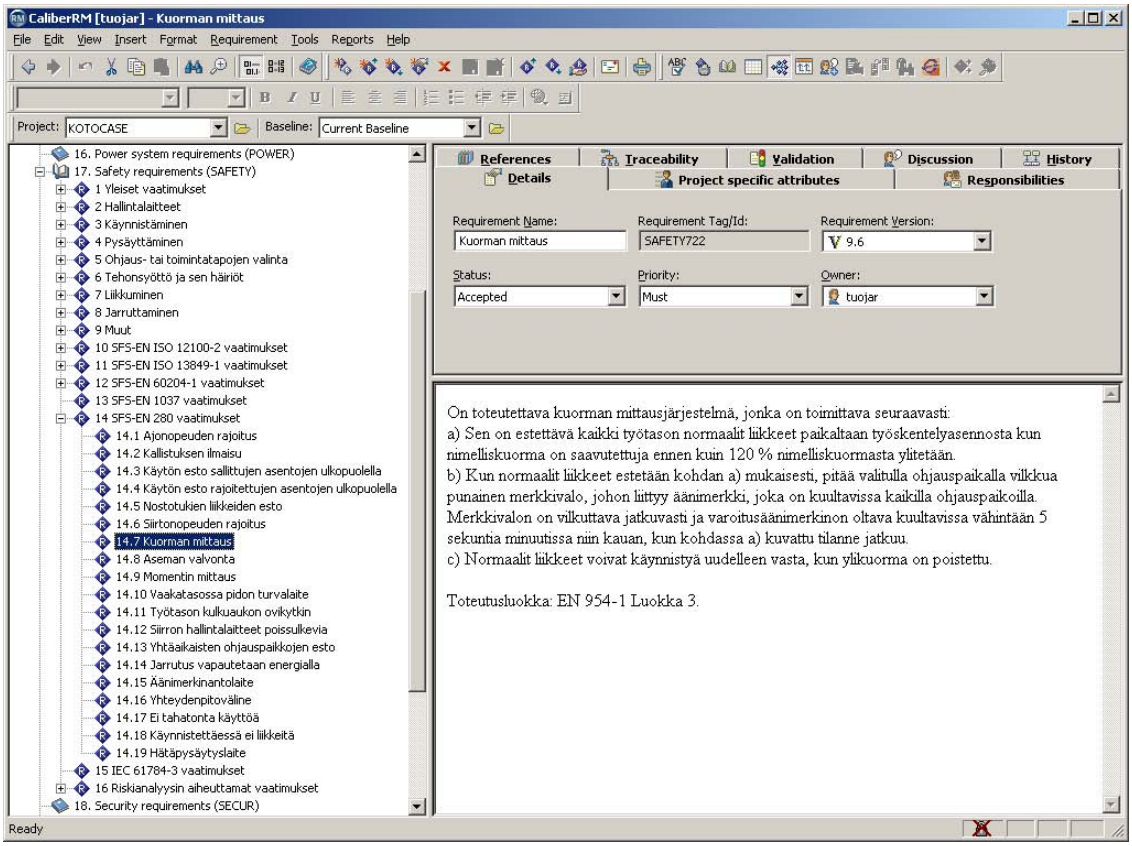
Turvallisuussuunnitelma noudattaa SFS-EN 62061 -standardin vaatimuksia turvallisuussuunnitelmalle. Tässä sisällysluetteloksi muodostuu seuraava luettelo:

1. Dokumentin tarkoitus ja nimeämiskäytännöt
2. Relevantit turvallisuusstandardit, säännökset ja käytännöt
3. Muut soveltuvat dokumentit
4. Relevantit ohjausjärjestelmän turvallisuuteen liittyvät aktiviteetit
5. Politiikka ja strategia, joilla täytetään määritetyt toiminnallisen turvallisuuden vaatimukset
6. Strategia, jolla saavutetaan sovellusohjelmiston toiminnallinen turvallisuus sen kehittämiseen, yhdistämiseen, todentamiseen ja kelpuutukseen
7. Vastuulliset henkilöt, osastot ja muut yksiköt sekä resurssit
8. Menettelytavat ja resurssit turvallisuuden kannalta merkityksellisten tietojen tallentamiseksi ja säilyttämiseksi
9. Muutosten hallinnan strategia
10. Todentamissuunnitelma
11. Kelpuutusssuunnitelma.

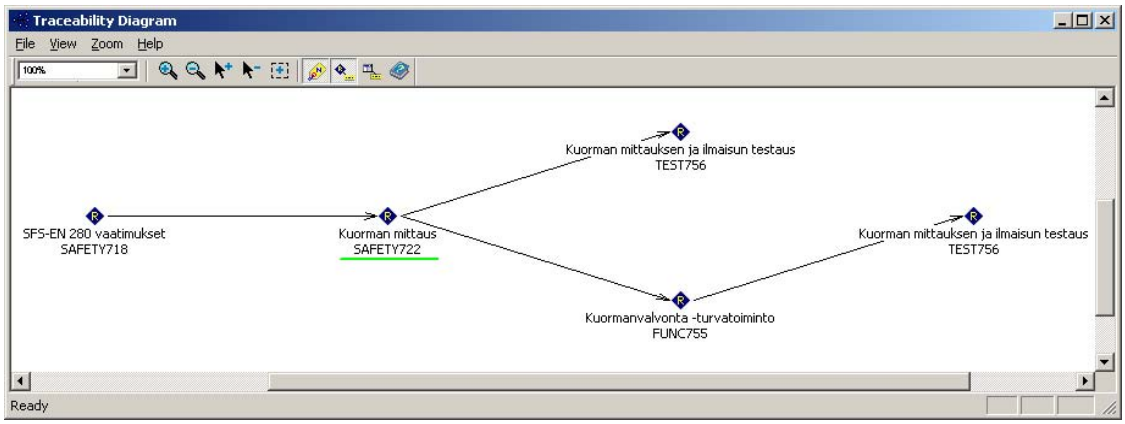
Edellä mainitun turvallisuussuunnitelman luvussa 4 kuvataan kuvan 11 mukaisen turvallisuusprosessin osaprosessit tarkemmin. Ne on esitetty tämän julkaisun liitteessä B.

3.2.3 Esimerkkijärjestelmän turvallisuusvaatimukset

Esimerkkijärjestelmän turvallisuusvaatimukset koottiin uudesta koneasetuksesta (VNa 400/2008), harmonisoidusta turvallisuusstandardeista ja riskianalyysien tuloksista. Koneasetuksen liitteen 1 luvut 1 (yleiset vaatimukset, erityisesti kohta 1.2 on ohjausjärjestelmiä koskeva), luku 3 (liikkuvat koneet), luku 4 (nostolaitteet) ja luku 6 (henkilönostimet) olivat tässä yhteydessä relevantteja. Vaatimukset koottiin vaatimushallintatyökaluun, joka tarjosi myös vaatimusten jäljitettävyyden (ks. kuvat 15 ja 16).



Kuva 15. Ote turvallisuusvaatimusten luettelosta. Kuvan lähde: Borland CaliberRM vaatimustenhallintatyökalu.



Kuva 16. Esimerkki vaatimusten jäljitettävyydestä. Kuvan lähde: Borland CaliberRM vaatimustenhallintatyökalu.

Esimerkkijärjestelmän kaikki vaatimukset, mukaan lukien turvallisuusvaatimukset, koottiin yhteen dokumenttiin *Ohjausjärjestelmän vaatimusmäärittely*. Kyseisen dokumentin alkuluvuissa (luvut 2 ja 3, ks. oheinen tekstilaatikko[6]) annettiin järjestelmän alustava kuvaus. Alustava kuvaus on tehty riskianalyysistandardin ISO 14121-1 lukujen 4.2 ja 5 ohjeiden mukaisesti. Täten vaatimusmäärittelydokumentti käsittää alustavan vaara-analyysin lähtötiedot kokonaan ja suurimman osan käyttötapausanalyysin lähtötiedoista. Vaatimusmäärittelydokumentti sisältää myös käyttötapauskuvaukset, joten ainoastaan arkkitehtuurisuunnitteludokumentti tarvitaan lisänä käyttötapausanalyysiin. Käyttötapauskuvauksesta on esimerkki liitteessä D.

2 JOHDANTO KEHITETTÄVÄÄN JÄRJESTELMÄÄN

2.1 Koneen ja kehitettävän ohjausjärjestelmän alustava kuvaus

2.1.1 Järjestelmän identifiointi ja yleiskuva

2.1.2 Peruselementit

2.1.3 Koneella tehtävä työ

2.1.4 Ohjausjärjestelmän periaatteellinen arkkitehtuuri

2.1.5 Ohjausjärjestelmän alustava suunnitelma

2.2 Säädökset, standardit ja muut sovellettavat dokumentit

2.3 Käyttökokemukset

2.4 Oleelliset ergonomiaperiaatteet

3 KONEEN RAJOJEN MÄÄRITTÄMINEN

3.1 Relevantit elinkaaren vaiheet

3.2 Käytön rajat

3.2.1 Tarkoitettu käyttö

3.2.2 Kohtuudella ennakoitavissa oleva väärinkäyttö

3.3 Tilarajat

3.4 Aikarajat

3.5 Muut rajat

Riskianalyysin tuloksena syntyneet uudet tai päivitetyt turvallisuusvaatimukset päivitettiin vaatimushallintatyökalun kautta vaatimusmäärittelydokumenttiin[7].

[6] Koko vaatimusmäärittelydokumentin sisällysluettelo on liitteessä C.

[7] Vaatimusmäärittelydokumentti on riskianalyysi- ja suunnitteluvaiheessa varsin elävä dokumentti, joten tavallinen tekstinkäsittelytiedosto ei ole paras mahdollinen formaatti tietojen ylläpitoon. Vaatimushallintatyökalu on lähes välttämätön. Muut ko. dokumentin tiedot voidaan tallentaa tietokantaan tai pienempinä osadokumentteina. Varsinainen vaatimusmäärittelydokumentti kootaan sitten automaattisesti näistä omaan tahtiin päivittyvistä osadokumenteista ja tietokannoista (ml. vaatimushallintatietokanta).

3.2.4 Esimerkki alustavasta vaara-analyysistä

Kun koneen ja kehitettävän ohjausjärjestelmän alustava kuvaus on valmiina ja rajat on määritelty, voidaan aloittaa alustava vaara-analyysi. Vaara-analyysin tekemisessä noudatetaan prosessiohjetta, joka on esitelty liitteessä B. Se perustuu standardiin ISO 14121-1 ja sen tekniseen ohjeeseen ISO 14121-2. Taulukossa 3 on analyysilomake, jota käytettiin esimerkkijärjestelmän alustavaan vaara-analyysiin.

Taulukko 3. Alustavan vaara-analyysin lomake (PiD=työtä tekevä henkilö [Person in Duty]; PiV=lähistöllä oleva henkilö [Person in Vicinity]; Se=Vakavuus; Fr=Altistumistaajuus; Pr=Vaarallisen tapahtuman todennäköisyys; Av=Vältettävyys).

Vaara Nro	**Käyttötapaus Nro**	**Tapaturmaskenaario (kuka, mitä, miksi, missä, missä tilanteessa → Seuraukset)**	**Tiedossa olevat suojaustoimenpiteet**	Se	Fr	Pr	Av	PL & SIL	**Ehdotetut uudet suojaustoimenpiteet**
1. Mekaaniset vaarat									
…	…	…							
1.3	Käyttötapauksesta riippumaton	Kone siirtyy tai nousee tai laskee itsestään ja ruhjoo PiD:n tai PiV:n → puristuminen, leikkautuminen, kaatuminen, viskautuminen jne.	Hallintalaitteet palautuvat automaattisesti vapaa-asentoon (ks. turv.vaat.: SAFETY736); Langattomassa ohjauksessa tehdään automaattinen pysäytys, jos oikeita ohjaussignaaleja ei saada tai jos yhteys menetetään (ks. turv. vaat.: SAFETY316)	4	5	2	3	d 2	Liikkeiden sallinta tehdään kaksikanavaisena (yksi vika ei aiheuta tahatonta liikettä) ainakin osittain; Kommunikointikanava rakennetaan SIL 2 tasolle (ks. IEC 61784-3 kohta 5.6.2; analysoi myös muut kuin ”corruption”-virheet)
…	…	…							
2. Sähköstä johtuvat vaarat									
3. Lämpötilasta johtuvat vaarat									
4. Melusta johtuvat vaarat									
5. Tärinästä johtuvat vaarat									
6. Säteilystä johtuvat vaarat									
7. Materiaaleista tai aineista johtuvat vaarat									
8. Ergonomiasta johtuvat vaarat									
9. Koneen käyttöympäristöstä johtuvat vaarat									
10. Vaarojen yhdistelmät									

Riskin suuruuden arviointi tehdään periaatteessa ISO 13849-1 -standardin mukaisen graafin avulla. Taulukon 3 lomakkeessa on kuitenkin räätälöity riskin arviointimenetelmä, joka tehdään IEC 62061 -standardin mukaisesti, mutta samaan riskin arviointimatriisiin sijoitetaan PL-arvot taulukon 4 mukaisesti.

Taulukko 4. Räätälöity riskin arviointimatriisi.

Vakavuus Se	**Luokka Cl**				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2 PL d	SIL 2 PL d	SIL 2 PL d	SIL 3 PL e	SIL 3 PL e
3		PL a	SIL 1 PL b (Cl = 8) PL c (Cl= 9-10)	SIL 2 PL d	SIL 3 PL e
2			PL a	SIL 1 PL b (Cl =11) PL c (Cl= 12-13)	SIL 2 PL d
1				PL a	SIL 1 PL b (Cl =14) PL c (Cl= 15)

On huomattava, että taulukko 4 noudattaa vain osittain ISO 13849-1 -standardia. SIL 2 -tason peilautuminen PL -tasoksi d ja SIL 3 -tason peilautuminen PL -tasoksi e on määritelty standardissa, mutta muilta osin taulukkoa on pidettävä vain ehdotuksena PL -tasojen kohdentamisesta IEC 62061 -standardin SIL -matriisiin. Syynä räätälöityyn riskimatriisiin on mahdollisuus ottaa huomioon vaarallisen tapahtuman todennäköisyys. ISO 13849-1 -standardissa tätä mahdollisuutta ei ole, vaan ainoastaan altistumistaajuus ja vältettävyys voidaan ottaa huomioon riskin todennäköisyyttä arvioitaessa.

Tässä yhteydessä otetaan tarkastelun kohteeksi vaara numero 1.3 eli tahattoman liikkeen vaara, jolle riskin arvioinnissa on PL_r-vaatimustasoksi saatu d. Alustavassa vaara-analyysissä ehdotetaan kaksikanavaista ratkaisua tahattoman liikkeen estoon ja SIL 2 -tasoista kommunikointijärjestelmän toteutusta. Ehdotetut korjaustoimenpiteet analysoidaan seurantavaiheessa suunnittelutiimin toimesta. Seurantavaiheen tulos voi olla esimerkiksi taulukon 5 mukainen.

Taulukko 5. Vaara numero 1.3:n seurantavaihe.

Vaara Nro	Riskin merkityksen arviointi	Riskin pienentämisen toimenpiteet; turvatoiminnon identifiointi ja allokointi	Vastaavien vaatimusten viitenumerot	Jäännösriski
…	…	…	…	…
1.3	Havaittu riski on merkittävä. Toteutetaan ehdotettu toimenpide	1. Toteutetaan liikkeiden sallintakytkin -toiminto. Tehdään ohjaussauvassa olevalla sallintakytkimellä, jota painetaan joko peukalolla tai kämmenellä. Allokointi: Ohjelmoitava ohjausjärjestelmä. Vaatimustaso PL d. 2. Kommunikointikanava rakennetaan SIL 2 -tasolle (ks. IEC 61784-3 luku 5.6.2; analysoi myös muut kuin ”corruption” -virheet). Allokointi: Ohjelmoitava ohjausjärjestelmä (erit. kommunikointijärjestelmä)	1. SAFETY776 2. SAFETY739	Hyväksyttävissä
…	…	…	…	…

Suunnittelutiimi päättää siis toteuttaa ehdotetut toimenpiteet, jotka muunnetaan turvallisuusvaatimuksiksi (vaatimukset SAFETY776 ja SAFETY739). Vaatimus sallintakytkin-toiminnolle, eli vaatimus SAFETY776, kirjattaisiin esimerkiksi taulukon 6 esittämällä tavalla.

Taulukko 6. Vaara numero 1.3:n seurannassa tuotetun vaatimuksen kuvaus.

16.2 Liikkeiden ohjaukseen sallintatoiminto	**Tila:** Hyväksytty **Prioriteetti:** Pakoll.	**Tunniste:** SAFETY776 **Lähde:** Riskianalyysi: PHA vaara nro 1.3
Kelpuutusproseduuri: VVA ja TEST780		**Referenssit:**
Kuvaus: Toteutetaan liikkeiden sallintakytkin -toiminto. Tehdään ohjaussauvassa olevalla sallintakytkimellä, jota painetaan joko peukalolla tai kämmenellä. Liikkeet sallitaan vain, kun sallintakytkin on aktivoitu. Allokointi: Ohjelmoitava ohjausjärjestelmä. Vaatimustaso PL d. Noudatettava myös standardin SFS-EN 60204-1 vaatimusta 9.2.6.3 (ja 10.9) (ks. SAFETY763) sallintakytkimen toteutuksen osalta.		

Kun uusi vaatimus on kirjattu vaatimusmäärittelyihin, on aika aloittaa kyseisen turvatoiminnon suunnittelu. Suunnittelun tuloksena voisi olla esimerkiksi taulukon 7 mukainen määrittely.

Taulukko 7. Tahattoman liikkeen esto -turvatoiminnon määrittely.

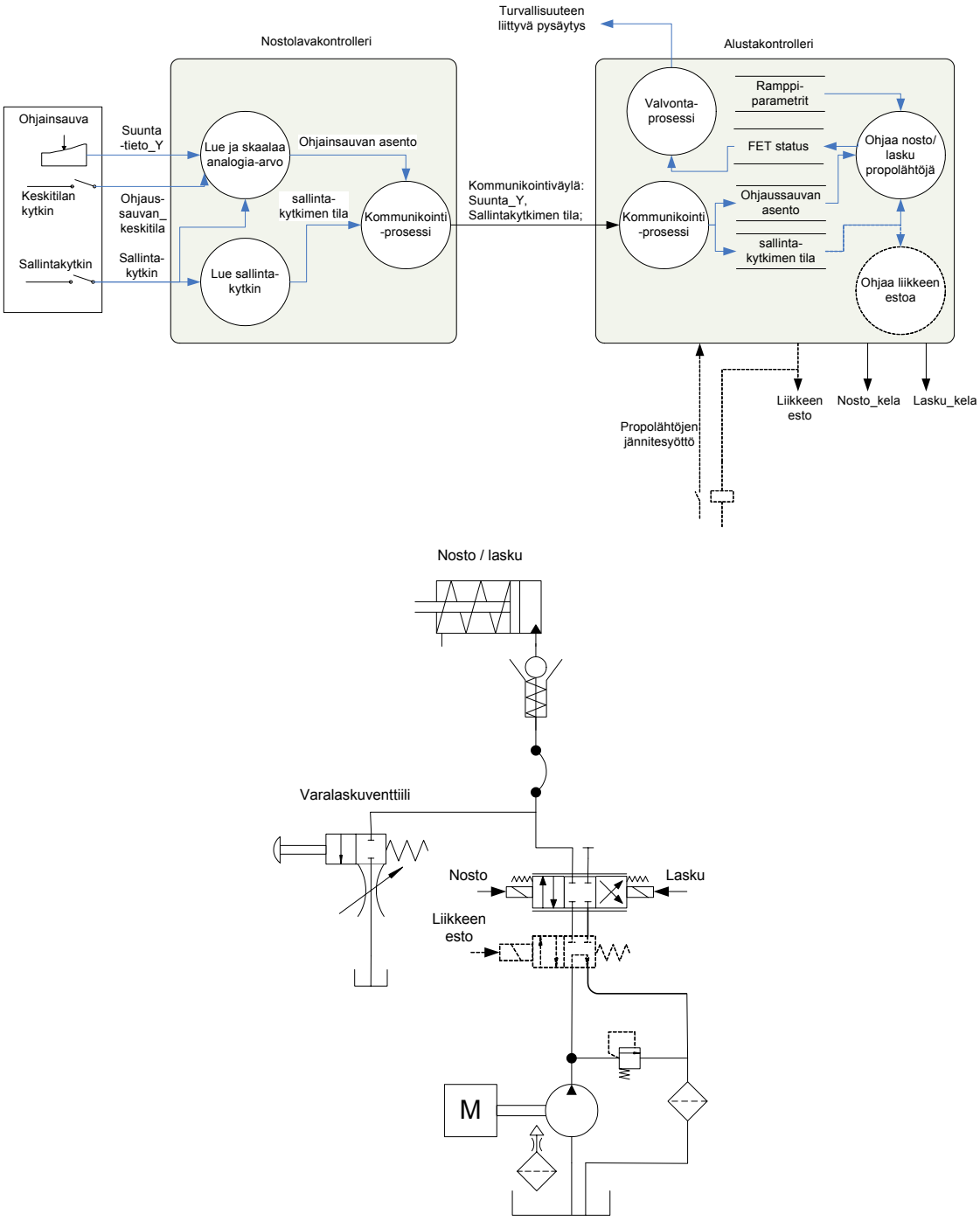
Toiminnon nimi:		**Tahattoman liikkeen esto -turvatoiminto**		
Tunniste:		**FUNC777**		
Versio	**PVM**	**Tila**	**Tekijä(t)**	**Kuvaus**
0.1	10.10.2008	Luonnos	J. Alanen	luotu
Liittyvät käyttötapaukset		USEC759, ...		
Sisääntulot		00003	Sallintakytkin	Oltava aktiivinen eli käyttöjännitteessä, että nosto/lasku voisi tapahtua
		00006	Suuntatieto_Y	Ohjainsauvan Y-akselin jännitesignaali
		00007	Ohjaussauvan_keskitila	Oltava aktiivinen, että liike voidaan aloittaa. Jos liikkeen aikana menee aktiiviseksi, liike pysäytetään
Lähdöt		000001	Nosto_kela	Ylös/Alas propoventtiilin ylös-kelan virta
		000002	Lasku_kela	Ylös/Alas propoventtiilin alas-kelan virta
Väyläsignaalit		10001	Suunta_Y	Y-akselin poikkeamatieto; nolla paikallaan; ...
		10002	Sallintakytkimen tila	Oltava ”1”, että nosto/lasku voisi tapahtua
Parameterit		1000	Ohjaussauvan_skaalaus	Ohjaussauvan skaalauskerroin
		1001	Ohjaussauvan_offset	Ohjaussauvan offset
		...	...	
Osaluettelo		56712	XY-ohjainsauva	Nosto/lasku-liikkeen ohjainsauva
		45123	Nostolavakontrolleri	Moduulityyppi GFD-221
		45124	Alustakontrolleri	Moduulityyppi GFD-221
		...		
Liitynnät muihin toimintoihin (normaali- tai turvatoimintoihin)		...		
Toiminnallinen määrittely		Valitaan sellainen ohjaussauva, jossa on sallintakytkin, jolla NO-kontaktit, eli jos johdin katkeaa tai kytkin likaantuu, liikettä ei sallita, vaikka ohjainsauvan analogiasignaali niin komentaisi. Sallintakytkimen avoimen tilan täytyy myös aiheuttaa se, että kommunikointiväylään lähtevä tieto ohjainsauvan asennosta indikoi keskitilaa, vaikka sauva olisi poikkeutettu. Kytkimen tila lähetetään myös väylälle. (Ks. kuva 17.) Vastaanottava kontrolleri ei ohjaa liikkeen aiheuttavia propoja, jos sallintakytkin-tieto osoittaa ei-sallittua, vaikka ohjainsauvan asento olisi mitä tahansa. Harkitaan, pannaanko vastaanottavan moduulin lähtöön jokin HW-ohjaus, jolla propolähdön virta katkaistaan, jos keskiasentokytkin osoittaa keskiasentotilaa. Voidaan ohjata peräti lisähydrauliventtiiliä, joka katkaisee hydrauliikkatehon, jos halutaan hydrauliikkaosuudesta kaksikanavainen. Voidaan harkita myös ratkaisua, jossa sallintakytkin vaikuttaa ainoastaan ohjainsauvan sisällä eli sallintakytkintä ei johdoteta ulospäin.		

	Jos keskiasentokytkimen tila tai ohjainsauvan asento -sanoma lakkaa tulemasta alustakontrollerin kommunikointiprosessille 300 ms:n sisällä, sen on nollattava molemmat tilamuuttujat.
Vikaan reagointi	Jos sallintakytkin ei ole passiivinen virtoja päälle kytkettäessä, annetaan virheilmoitus näyttöön ja estetään ohjelmallisesti reagointi ohjaussauvaan. …
Turvallinen tila	Nosto/laskusylinteri ei aiheuta liikettä
Diagnostiikka	– Monitoroidaan ohjainsauvan keskiasentokytkimen tilaa, ei sallita liikettä, jos keskiasentokytkin osoittaa keskitilaa – Monitoroidaan lähtö-FETien tilaa. Jos FET indikoi oikosulkua käyttöjännitteeseen, ohjataan järjestelmä turvalliseen tilaan turvallisuuteen liittyvän pysäytystoiminnon kautta (FUNC778)
Turvallisuusvaatimukset	SAFETY323: Ohjauslaitteet on suunniteltava tai suojattava siten, että toivottu vaikutus, jos siihen liittyy vaara, voidaan saavuttaa ainoastaan toteuttamalla tarkoituksellinen toiminto.
	SAFETY334: Koneen käynnistäminen saa olla mahdollista vain siten, että vaikutetaan tarkoituksellisesti asianomaiseen ohjauslaitteeseen. Sama vaatimus koskee – uudelleenkäynnistämistä pysähdyksen jälkeen, oli sen syy mikä tahansa – toimintaolosuhteiden huomattavaa muuttamista. Uudelleenkäynnistäminen tai toimintaolosuhteiden muuttaminen voi kuitenkin tapahtua käyttämällä tarkoituksellisesti muuta laitetta kuin tähän tarkoitukseen tarkoitettua ohjauslaitetta, jos tämä ei aiheuta vaaratilannetta. Automaattisessa toimintatilassa olevan koneen käynnistäminen, uudelleenkäynnistäminen pysäytyksen jälkeen tai sen toimintaolosuhteiden muuttaminen voi olla mahdollista ilman toimintaan puuttumista, edellyttäen, että tämä ei aiheuta vaaratilannetta.
	SAFETY360: Koneen tehonsyötön keskeytyminen tai tehonsyötön palauttaminen keskeytyksen jälkeen tai sen millainen tahansa vaihtelu ei saa aiheuttaa koneen odottamatonta käynnistymistä.
	SAFETY725: Koneen käynnistäminen normaalisti tai energiansyötön katkeamisen jälkeen ei saa aiheuttaa muita kuin käyttäjän toimenpiteistä johtuvia liikkeitä.
	SAFETY736: Kone on varustettava hallintalaitteilla, ja kaikki koneen liikkeet tapahtuvat vain vaikuttamalla hallintalaitteisiin. Hallintalaitteiden on vapautettaessa automaattisesti palauduttava vapaa-asentoon. Kaikkien hallintalaitteiden, varsinkin polkimien, tahaton käyttö on oltava estetty.
	SAFETY763: Sallintaohjaus on toteutettava niin, että sen vaikutuksen ohittamismahdollisuus on minimoitu, esimerkiksi edellyttämällä sallintalaitteen vapauttamista ennen koneen käynnistämistä uudelleen. Sallintatoiminnon ohittaminen ei saisi olla helpolla tavalla mahdollista. Kun järjestelmän osana on sallintalaite, toiminnan salliva viesti ohjausjärjestelmälle saa olla mahdollista ainoastaan sallintalaitteen yhdessä asennossa. Muissa asennoissa toiminnan on pysähdyttävä tai oltava estetty. Sallintalaitteet on valittava ja sijoitettava niin, että sen ohittamismahdollisuus minimoidaan. Valitulla sallintalaitteella on oltava seuraavat ominaisuudet: – suunniteltu ergonomisten periaatteiden mukaisesti – kaksiasentoisella tyypillä: - asento 1: kytkimen auki-toiminto (ohjain ei ole vaikutettuna) - asento 2: sallintatoiminto (ohjain on vaikutettuna) – kolmiasentoisella tyypillä: - asento 1: kytkimen auki-toiminto (ohjain ei ole vaikutettuna) - asento 2: sallintatoiminto (ohjain on vaikutettuna keskiasennossaan) - asento 3: auki-toiminto (ohjain on vaikutettuna ohi keskiasennostaan) – kun palataan asennosta 3 asentoon 2, toiminta ei saa tulla sallituksi.

	SAFETY776: Toteutetaan liikkeiden sallintakytkin -toiminto. Tehdään ohjaussauvassa olevalla sallintakytkimellä, jota painetaan joko peukalolla tai kämmenellä. Liikkeet sallitaan vain, kun sallintakytkin on aktivoitu. Vaatimustaso PL d. Allokointi: Ohjelmoitava ohjausjärjestelmä. Noudatettava myös standardin SFS-EN 60204-1 vaatimusta 9.2.6.3 (ja 10.9) (ks. SAFETY763) sallintakytkimen toteutuksen osalta.			
	SAFETY779: Tietojen säilyttämiseen ja käsittelemiseen tarkoitettujen laitteiden (ks. [ISO 14118] kuva 1) turvallisuuteen liittyvät osat on suunniteltava ja niiden rakenneosat on valittava siten, että standardin ISO 14121 mukaisesti suoritetussa riskin arvioinnissa huomioon otettuun odottamattomaan käynnistämiseen johtavien käynnistyskäskyjen syntymisen todennäköisyyttä voidaan pitää riittävän pienenä näissä laitteissa. HUOM. 1 Lisätietoja löytyy lähteestä: – ISO/TR 12100-2:1992, 3.7; – IEC 60204-1:1997, erityisesti sen kohdista 9 and 11. Ks. myös ISO 13849-1. HUOM. 2 Tämän hetkisen tietämyksen perusteella on vaikea varmuudella määrittää, kuinka paljon voidaan luottaa koneen ohjaukseen käytettävän yksikanavaisen ohjelmoitavan elektronisen järjestelmän toimimiseen oikealla tavalla. Siihen asti kunnes tällaisten järjestelmien oikein toimimisesta voidaan olla riittävän varmoja, on harkitsematonta luottaa pelkästään yksikanavaiseen järjestelmään, jos ohjausjärjestelmän virheellisestä toiminnasta voi aiheutua merkittävää vaaraa (ks. IEC 60204-1:1997, kohdan 11.3.4 huomautus).			
Identifioidut turva-alitoiminnot	Ei (kyseinen toiminto on itsessään turva-alitoiminto)			
Linkki toimintokaavioon	../../Diagrams/FUNC777_Tahattoman_liikkeen_esto.vsd			
Linkki malliin	…			
Onko itsessään turvatoiminto?	**X**	**Vaadittu PL**	d	
Linkki riskianalyysiin	Alustava vaara-analyysi vaara numero 1.3			
Koneen tilat, joissa sallittu	Kaikissa	**Koneen tilat, joissa estetty**	Ei missään	
Käyttötaajuus	Jatkuva, aina kun virrat on päällä ja ei ohjata nosto/lasku-liikettä			
Sähkömekaanisten komp. toimintajaksot	Ohjainsauva (sekä potentiometri että sallintakytkin): – 250 päivää vuodessa – 10 tuntia päivässä – 360 sekunnin välein keskimäärin			
Prioriteetti	Ei saa estää hätälaskua			
Vasteaikavaatimus	200 ms koko ketjulle, siitä kun sallintakytkin vapautetaan, siihen kun hydraulisylinterin männän liike pysähtyy.			
Toimintaympäristön kuvaus	Sivuilta avoin, mutta katettu ja asvaltoitu varastotila, jonka lämpötila on -30 ºC … 40 ºC. Kostea tila, mutta ei roiskevettä. Ihmisiä liikkuu jatkuvasti läheisyydessä, kun tätä toimintoa käytetään. Nostettavat kappaleet painoltaan korkeintaan 100 kg. Hydrauliikkakoneikkoa pyörittävä polttomoottori tuottaa pakokaasuja, jotka voivat tyynellä säällä haitata. Ks. tarkemmat ympäristöolosuhdemäärittelyt …			
Testausmenetelmä tai viittaus testitapaukseen	– Poikkeutetaan ohjainsauvaa painamatta sallintakytkintä. Liikettä ei saisi tapahtua. – Painetaan sallintakytkintä, mutta ei poikkeuteta ohjainsauvaa. Liikettä ei saisi tapahtua. –…			
Turvallisuuden perusperiaatteet	– Energiattomaksi tekemisen periaatteen soveltaminen – Elektroniikka valitaan tai suunnitellaan ja testataan kestämään ympäristöolosuhteet, myös EMC, käyttöjännitteet sekä niiden vaihtelut ja häiriöt			

	– Odottamattomalta käynnistykseltä suojautuminen – …
Koetellut turvallisuus-periaatteet	- Koskettimet ovat mekaanisesti pakkotoimisia - Kaapelivikojen välttäminen - Ylimitoittaminen - …
Koetellut komponentit	Ei SFS-EN ISO 13849-2 mukaisia. Käytössä olevat hydrauliventtiilit on käytännössä koeteltu hyvin
Vikaolettamat ja vikojen poissulkemiset	- Ohjainsauvan ja kytkimien johtimien katkokset ja oikosulut maapotentiaaliin (ei oikosulkua käyttöjännitteeseen, koska sellaista ei kaapeloinnissa ole lähellä) - Kommunikointiväylällä kaikki IEC 61784-3 -standardin mukaiset viat - FET-lähtöjen katkokset ja oikosulut maapotentiaaliin ja käyttöjännitteeseen - …
Muita kommentteja	

Edellä määriteltyyn turvatoimintoon liittyy toimintokaavio, joka on esitetty kuvassa 17.



Kuva 17. Tahattoman liikkeen eston toimintokaavio (sisältää ohjelmoitavan järjestelmän ja hydrauliikan).

Kun turvatoiminto on näin määritelty, sille tehdään poikkeamatarkastelu (HAZOP) tai vika- ja vaikutusanalyysi (VVA). Lopulta tehdään ISO 13149-1 -standardin mukainen suoritustason (PL) evaluointi. Kuten toiminnon määrittelystä nähdään, tavoitetaso PL_r on d. Tavoitetaso on peräisin alustavasta vaara-analyysistä. Esimerkki suoritustason evaluoinnista annetaan kohdassa 3.2.7.

3.2.5 Esimerkki käyttötapausanalyysistä

Riskianalyysiä jatketaan tekemällä käyttötapausanalyysi, joka pureutuu koneen kanssa operoivien henkilöiden virheisiin. Käyttötapausanalyysivaihe tehdään liitteessä B esitetyn prosessiohjeen mukaan. Käyttötapausanalyysi perustuu toimintovirheanalyysin menetelmään. Toimintovirheanalyysistä on saatavissa lisätietoa ja valmiita lomakepohjia osoitteesta riskianalyysit.vtt.fi [viitattu 13.10.2008]. Taulukko 8 kuvaa analyysilomaketta, jota käytettiin esimerkkijärjestelmän käyttötapausanalyysiin.

Taulukko 8. Käyttötapausanalyysin lomake (PiD=työtä tekevä henkilö [Person in Duty]; PiV=lähistöllä oleva henkilö [Person in Vicinity]; Se=Vakavuus; Fr=Altistumistaajuus; Pr=Vaarallisen tapahtuma todennäköisyys; Av=Vältettävyys).

Vaara Nro	**Työvaihe**	**Toimintovirhe: tapaturmaskenaario (kuka, mitä, miksi, missä, missä tilanteessa → Seuraukset)**	**Tiedossa olevat suojaustoimenpiteet**	Se	Fr	Pr	Av	PL & SIL	**Ehdotetut uudet suojaustoimenpiteet**
Käyttötapaus USEC766: Työtason nostaminen etäpaneelilta ohjattuna korkeudelta A korkeudelle B									
…									
USEC766.3.1	3.	Ylimääräinen (nosto/laskuliike): PiD pudottaa huolimattomuuttaan ohjauspaneelin käyttäessään sitä etäkäyttöpaneelina, jolloin aiheutuu tahattomia liikkeitä, esim. kone ajaa päälle, jos PiD tai PiV on koneen reitillä → puristuminen, leikkautuminen, kaatuminen, viskautuminen jne.	Hallintalaitteet palautuvat automaattisesti vapaa-asentoon (ks. turv.vaat.: SAFETY736)	4	4	2	3	d 2	Lisätään sallintakytkin, joka sijoitetaan niin, että se ei vahingossa aktivoidu yhtä aikaa ohjausvivun kanssa.
…									

Tässä yhteydessä otetaan tarkastelun kohteeksi vaara numero USEC766.3.1 eli etäpaneelin pudottamisen ja siitä seuraavan tahattoman liikkeen vaara. Käyttötapausanalyysissä ehdotetaan sallintakytkintä, joka ei aktivoidu mekaanisesta kosketuksesta ohjainsauvaan. Ehdotetut korjaustoimenpiteet analysoidaan seurantavaiheessa suunnittelutiimin toimesta. Seurantavaiheen tulos voi olla esimerkiksi taulukon 9 mukainen.

Taulukko 9. Vaara numero USEC766.3.1:n seurantavaihe.

Vaara Nro	**Riskin merkityksen arviointi**	**Riskin pienentämisen toimenpiteet; turvatoiminnon identifiointi ja allokointi**	**Vastaavien vaatimusten viitenumerot**	**Jäännösriski**
…	…	…		
USEC766.3.1	Havaittu riski on merkittävä. Toteutetaan ehdotettu toimenpide.	Toteutetaan ehdotettu sallintakytkin, joka estää käsipaneelin putoamisesta aiheutuvan liikkeen. Allokointi: Ohjelmoitava ohjausjärjestelmä. Vaatimustaso PL d.	SAFETY762	Hyväksyttävissä
…	…	…		

Suunnittelutiimi päättää siis toteuttaa ehdotetun toimenpiteen, joka muunnetaan turvallisuusvaatimukseksi. Vaatimus sallintakytkin-toiminnolle, eli vaatimus SAFETY762, kirjattaisiin esimerkiksi taulukossa 10 esitetyllä tavalla.

Taulukko 10. Vaara numero USEC766.3.1:n seurannassa tuotetun vaatimuksen kuvaus.

16.2 Sallintakytkin ohjauspaneeliin	**Tila:** Hyväksytty **Prioriteetti:** Pakoll.	**Tunniste:** SAFETY762 **Lähde:** Riskianalyysi: OHA vaara nro USEC762.3.1
Kelpuutusproseduuri: VVA ja TEST765		**Referenssit:**
Kuvaus: Kannettavaan ohjauspaneeliin toteutetaan putoamisesta aiheutuvan liikkeen esto -turvatoiminto, joka sallii nosto/lasku-liikkeen vain, kun kyseiseen sallintalaitteeseen vaikutetaan samanaikaisesti, kun ohjaussauvaan vaikutetaan. Sallintalaite on toteutettava siten, että se ei aktivoidu vahingossa yhtäaikaa ohjaussauvan kanssa, jos ohjauspaneeli putoaa tai ohjaussauvaan nojataan. Noudatettava myös standardin SFS-EN 60204-1 vaatimusta 9.2.6.3 (ja 10.9) (ks. SAFETY763) sallintakytkimen toteutuksen osalta.		

Kun uusi vaatimus on viety vaatimustenhallintaan, on aika aloittaa kyseisen turvatoiminnon suunnittelu. Turvatoiminto on tässä tapauksessa nimeltään *putoamisesta aiheutuvan liikkeen esto*. Se määritellään samalla tavalla kuin kohdan 3.2.4 esimerkki. Kun turvatoiminto on näin määritelty, sille tehdään poikkeamatarkastelu (HAZOP) tai vika- ja vaikutusanalyysi (VVA). Lopulta tehdään ISO 13149-1 -standardin mukainen suoritustason (PL) evaluointi. Tässä julkaisussa näitä vaiheita ei esitellä tarkemmin.

3.2.6 Esimerkki toimintojen analyysistä

Toimintojen analyysi tehdään liitteen B prosessiohjeen mukaan. Tässä yhteydessä tehdään signaalipohjainen poikkeamatarkastelu (HAZOP). Analyysin kohteena on nosto- ja laskutoiminto. Taulukossa 11 on esitelty vastaava analyysilomake ja esimerkkipoikkeamana on kuormanmittaussignaalin poikkeama.

Esimerkkitapauksessa syntyy uusi vaatimus: *kuormanmittausanturi on kahdennettava*. Tässä tapauksessa ei kuitenkaan tunnisteta tarvetta uudelle turvatoiminnolle; kuormanvalvonta on jo sinänsä turvatoiminto. Sille on siis tehtävä ISO 13849-1 -standardin mukainen PL-tason evaluointi. Tässä yhteydessä kyseistä evaluointia ei esitetä, sillä se olisi hyvin samankaltainen kohdassa 3.2.7 esitetyn PL-tason esimerkkievaluoinnin kanssa.

Tämä esimerkkitapaus on siinä mielessä huono, että standardi [SFS-EN 280] vaatii, että esimerkin kaltaisessa nostolaitteessa kuormanvalvontatoiminnon on noudatettava EN 954-1 -standardin luokkaa 3, mikä käytännössä merkitsee mm. kahdennettua kuormanmittausanturia. Täten suunnittelijan olisi pitänyt tehdä kuormanmittaus lähtötilanteessa tiedetyn vaatimuksen mukaiseksi jo ennen toimintojen analyysiä. Joka tapauksessa käytännössäkin voi käydä niin, että riskianalyysit paljastavat riskejä, jotka on jo C-tyypin standardeissa huomioitu, eli niihin on standardissa turvatoiminnot ja muut turvallisuusvaatimukset jo määritelty. Tällainen päällekkäinen riskianalyysi on turvallisuuden kannalta myönteinen asia.

Taulukko 11. Poikkeamatarkastelun lomake (PiD=työtä tekevä henkilö [Person in Duty]; PiV=lähistöllä oleva henkilö [Person in Vicinity]; Se=Vakavuus; Fr=Altistumistaajuus; Pr=Vaarallisen tapahtuman todennäköisyys; Av=Vältettävyys).

Poikkeama Nro	**Avainsana**	**Tulkinta**	**Syyt**	**Seuraukset**	**Tiedossa olevat havaitsemis- ja suojaustoimenpiteet**	Se	Fr	Pr	Av	PL & SIL	**Ehdotetut uudet suojaustoimenpiteet**
FUNC751: Työtason manuaalinen nosto/lasku työtason ohjaimelta											
Signaali: 7. Nostolavaan kohdistuva paino (kuormanmittausanturilta)											
…											
FUNC751.7.2	Vähemmän	Kuorman paino näyttää vähemmän kuin paino on oikeasti	1. Kuormanmittausanturi vioittunut; 2. Anturin johdin oikosulussa maapotentiaaliin	Nostolaite voi kaatua tai lava voi laskeutua alas vauhdilla rakenteiden pettäessä → PiD:n kaatuminen, putoaminen, PiD:n ja PiV:n iskuvaara, ruhjoutuminen	2. Oikosulku maahan havaitaan diagnostiikalla, josta annetaan varoitus näyttöön ja kuorma tulkitaan ylipainoiseksi	4	5	1	3	d 2	1. Kahdennetaan kuormanmittausanturi
…											

3.2.7 Esimerkki suoritustason evaluoinnista

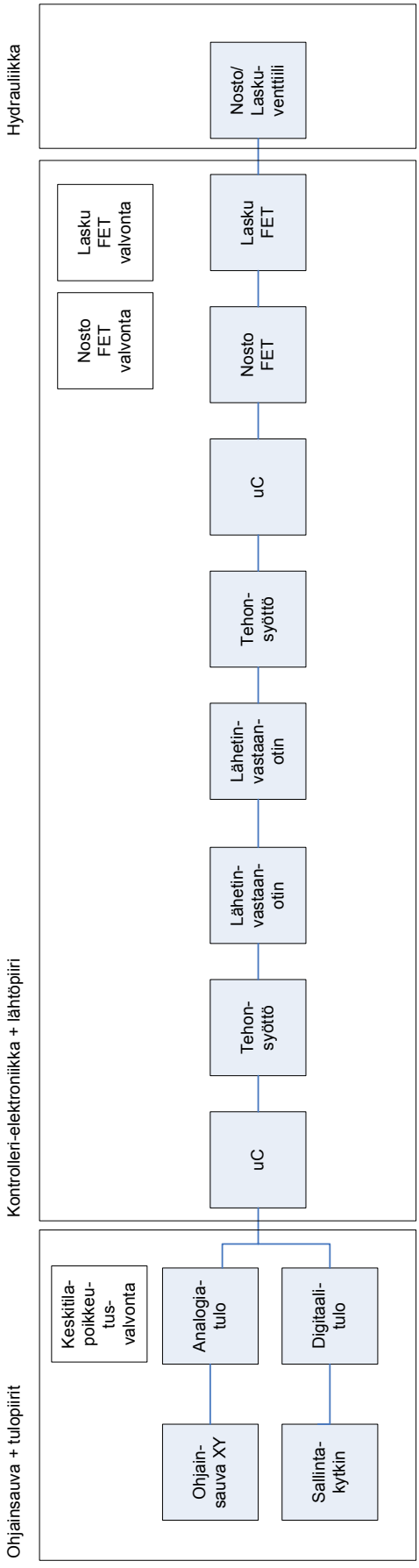
Tässä otetaan tarkasteltavaksi kohdassa 3.2.4 määritelty turvatoiminto: tahattoman liikkeen esto. Työ aloitetaan tekemällä turvallisuuteen liittyvä lohkokaavio toimintokaavion (ks. kuva 17) perusteella (esimerkkejä on lähteessä [Hauke et al. 2008]). Kuvassa 18 on esimerkkitapauksen lohkokaavio. Järjestelmä jaetaan tässä kolmeen osajärjestelmään, tulot, logiikka ja hydrauliikkajärjestelmä. Jotta suoritustaso PL voitaisiin laskea, jokaiselle lohkolle on määriteltävä $MTTF_d$-arvo. Tässä tapauksessa MTTF-arvot saatiin MIL HDBK 217F -käsikirjasta ja ISO 13849-1 -standardista. MTTF-arvoja voidaan etsiä eri lähteistä (ks. esimerkkejä kohdasta 4.2.2) tai yritys voi itse tehdä tilastollista seurantaa komponenteille MTTF-arvoista. $MTTF_d$-arvoksi arvioidaan tässä olevan 2 x MTTF standardin ISO 13849-1 nyrkkisäännön mukaisesti.

Tässä tapauksessa saadaan taulukon 12 mukaiset $MTTF_d$-arvot.

Taulukko 12. Esimerkkitapauksen lohkojen $MTTF_d$ -arvot.

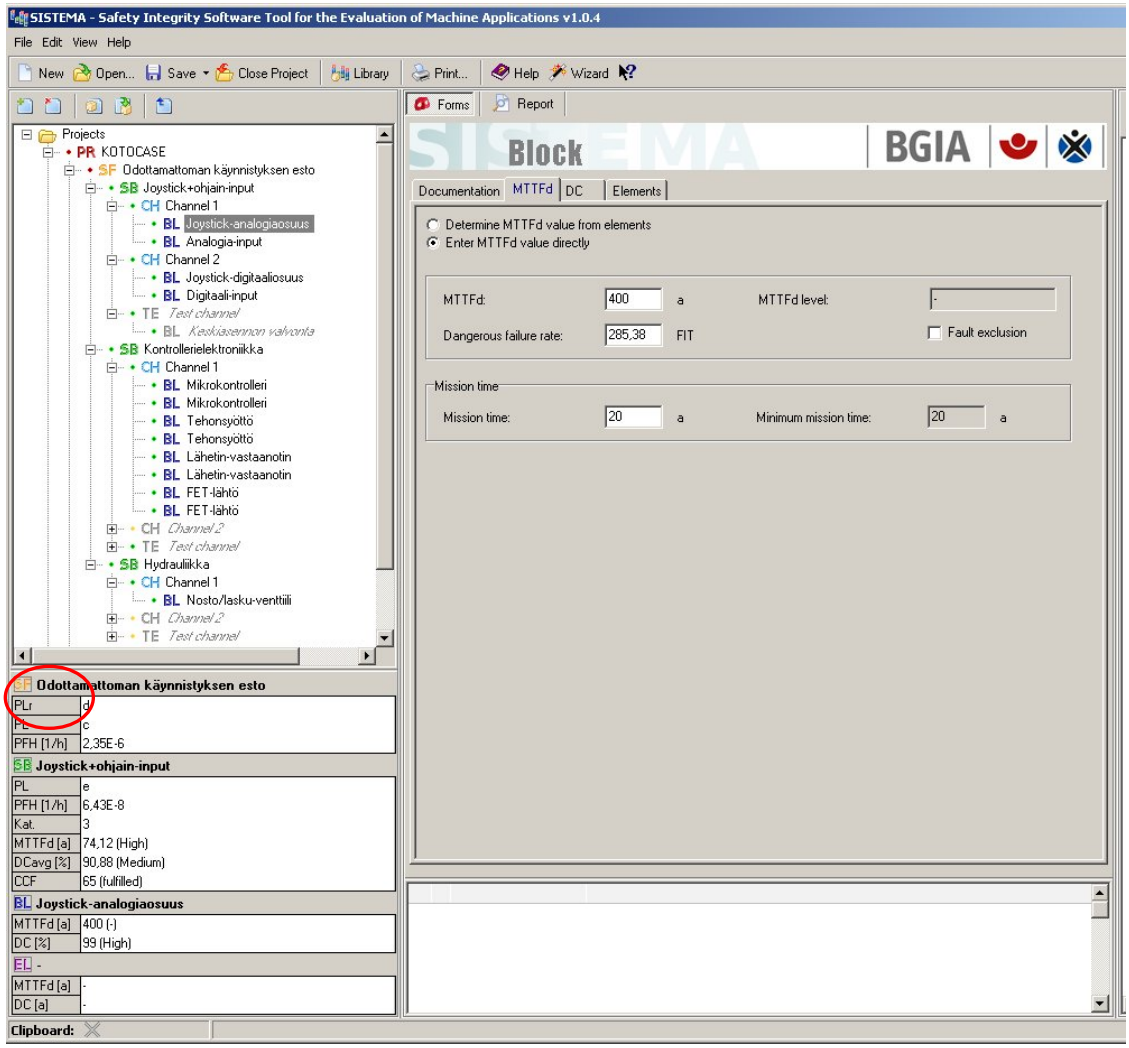
Lohko	**$MTTF_d$ (vuotta)**	**MTTF-lähde**
Ohjainsauva XY	400	ISO 13849-1 laskentakaava (B10d) ja valmistajan ilmoitus keskimääräisestä eliniästä
Analogiatulo	4035	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
Sallintakytkin	40	ISO 13849-1 laskentakaava (B10d) ja valmistajan ilmoitus keskimääräisestä eliniästä
Digitaalitulo	3184	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
uC (mikrokontr.)	1494	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
Tehonsyöttö	3789	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
Lähetinvastaanotin	795	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
Nosto/lasku FET	5977	MIL Hdbk 217F, kun kytkennän komponentit ovat tiedossa
Nosto/lasku -venttiili	300	ISO 13849-1

Järjestelmän lohkokaaviorakenne ja $MTTF_d$-arvot syötetään SISTEMA-työkaluun, joka esitellään kohdassa 4.1.1. Tätä ennen elektroniikkalohkojen, kuten analogiatulo-lohko ja digitaalitulo-lohko, $MTTF_d$-arvot on laskettu yksittäisistä elektroniikkakomponenteista käyttäen hyväksi KOTOTU-projektissa kehitettyä työkalua, joka esitellään kohdassa 4.4. Periaatteessa yksittäiset elektroniikkakomponentit olisi voinut syöttää SISTEMA-työkaluun elementteinä, mutta jos esimerkiksi kytkennässä on useita samoja komponentteja, kuten vastuksia, ne joudutaan jokainen syöttämään omana rivinään SISTEMA-työkaluun. KOTOTU-työkalulla lohkon $MTTF_d$-arvot voidaan laskea valmiiksi käyttäen hyväksi komponenttimääriä.



Kuva 18. Tahattoman käynnistyksen esto -turvatoiminnon turvallisuuteen liittyvä lohkokaavio.

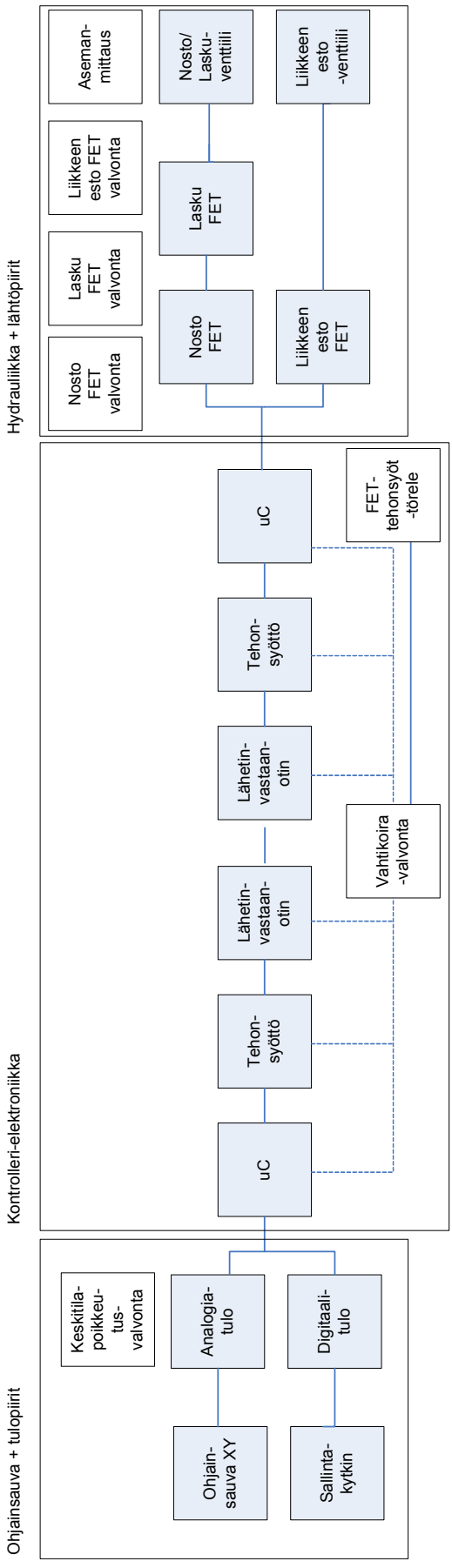
Kuvassa 19 on esitelty, miten kuvan 18 turvallisuuteen liittyvä lohkokaavio $MTTF_d$-tietoineen on syötetty SISTEMA-työkaluun. MTTF-arvo voidaan laskea SISTEMA-työkaluun syötetyistä elementeistä (lohkon ”BL” alla oleva seuraava hierarkiataso, joka ei ole kuvassa näkyvissä) tai se voidaan antaa suoraan, jos se on tiedossa tai jos se on laskettu muulla työkalulla, kuten tässä tapauksessa. $MTTF_d$-arvojen lisäksi SISTEMA-työkaluun syötetään rakenteen luokka sekä arviot diagnostiikan kattavuudesta ja yhteismuotoisten vikojen hallinnasta.



Kuva 19. Esimerkkiturvatoiminnon syöttäminen SISTEMA-työkaluun (PR=projekti, SF=turvatoiminto; SB=alijärjestelmä; CH=kanava; BL=lohko; TE=testikanava).

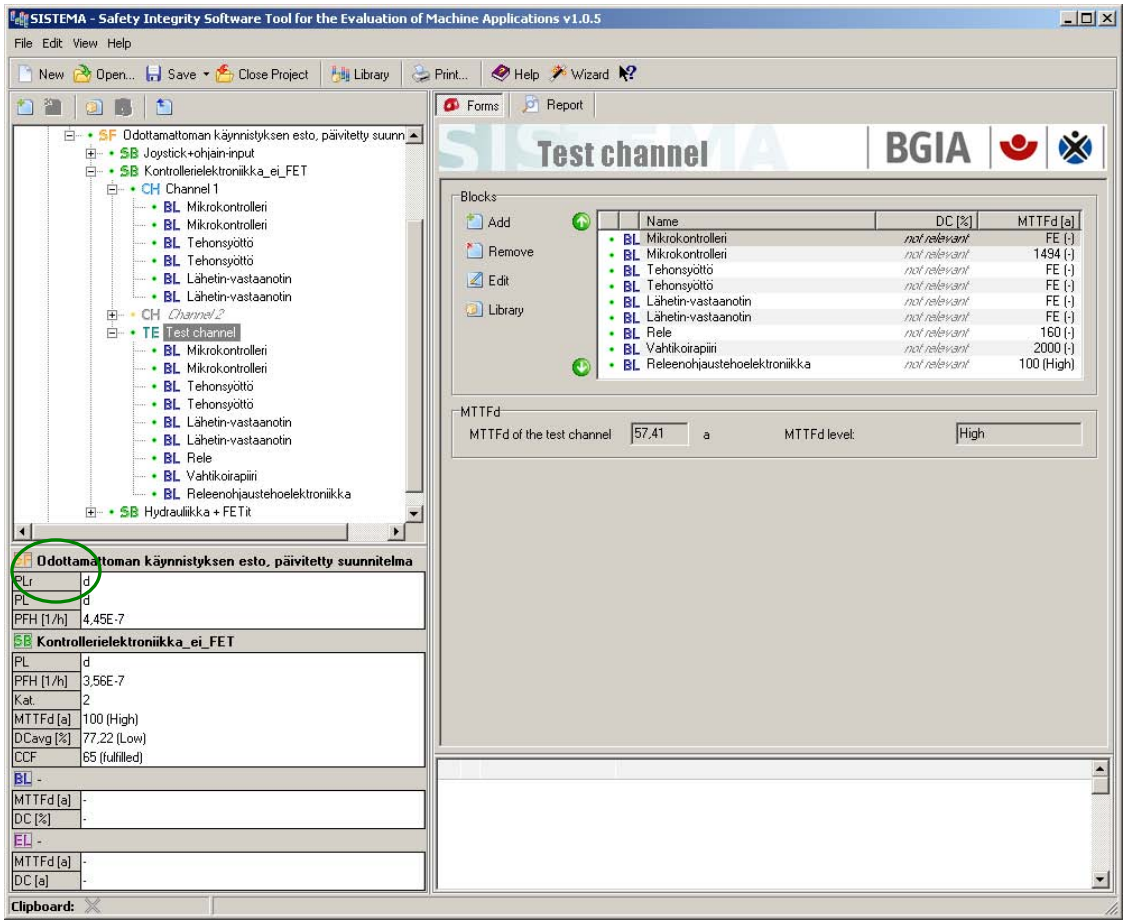
Kuvasta 19 nähdään, että turvatoiminnolle vaadittua suoritustasoa PL_r = d ei saavuteta, vaan sen suhteen jäädään tasolle c. Syynä tässä tapauksessa on kontrollerielektroniikan ja hydrauliikan jääminen c-tasolle, mikä taas johtuu siitä, että molemmat alijärjestelmät ovat luokan 1 järjestelmiä (eli yksikanavaisia ja ilman automaattista toiminnon tarkistusta käytön aikana). Luokan 1 osajärjestelmällä ei ole mahdollista päästä PL-tasolle d.

Koska vaadittavaa suoritustasoa ei saavutettu, suunnitelmaa päivitetään siten, että hydrauliikkaan lisätään liikkeen esto -venttiili, jota ohjataan omalla FET-lähdöllä sallintakytkimen tilan perusteella, ja kontrollerielektroniikkaan järjestetään vahtikoiravalvonta. Vahtikoiravalvonta toteutetaan siten, että ensimmäiseen kontrollerimoduuliin lisätään kanttiaaltogeneraattori ja toiselle kontrollerimoduulille lisätään vahtikoirapiiri, joka ohjaa FET- tai relelähtöä. Ensimmäisen kontrollerimoduulin mikrokontrolleri lukee kanttiaaltoa ja lähettää sen toiselle kontrollerimoduulille, jossa mikrokontrolleri herättää vahtikoiran nousevilla ja laskevilla kanttiaallon reunoilla. Jos kontrollerimoduuleista koostuva kanava vikaantuu, kanttiaalto jää tulematta, jolloin vahtikoiran lähtö passivoituu ja liike estetään. Elektroniikan ja ohjelmiston toteutustavasta riippuu, saadaanko tästä valvontatoiminnosta riittävän hyvä yhteismuotoisten vikojen kannalta. Tässä oletetaan, että onnistunut ratkaisu löydetään. Tällöin turvallisuuteen liittyvästä lohkokaaviosta tulee kuvan 20 mukainen.



Kuva 20. Tahattoman käynnistyksen esto -turvatoiminnon turvallisuuteen liittyvä lohkokaavio, päivitetty suunnitelma.

Kuvan 20 ratkaisulla hydrauliikkaosajärjestelmästä tulee luokan 3 järjestelmä ja kontrollerielektroniikasta tulee luokan 2 järjestelmä. Näillä ratkaisuilla koko järjestelmän PL-tasoksi saadaan taso d (ks. kuva 21)[8], joka riskianalyysin perusteella oli vaatimuksena ao. turvatoiminnolle.



Kuva 21. Päivitetyn suunnitelman PL-tason laskenta SISTEMA-työkalulla (PR=projekti, SF=turvatoiminto; SB=alijärjestelmä; CH=kanava; BL=lohko; TE=testikanava).

[8] Huom! Tässä esitettyä vahtikoiralla toteutettua valvontakytkentää ei voi pitää esimerkkiratkaisuna, jota voisi sellaisenaan käyttää todellisissa järjestelmissä. Sen tarkoituksena on tässä ainoastaan osoittaa se, että PL-tasolle d on mahdollisuus päästä myös luokan 2 ratkaisuja käyttäen, jos MTTF-arvot ovat riittävän korkeat. On huomattavaa myös, että tässäkin esimerkkitapauksessa vaatimusmäärittelyyn on kirjattu (ks. taulukko 6), että ao. turvallisuustoiminto analysoidaan kelpuutusvaiheessa vika- ja vaikutusanalyysillä. Näin ollen viimeistään siinä vaiheessa todetaan, onko vahtikoiraratkaisu pätevä.

Systemaattinen vikaantuminen, ohjelmiston turvallisuusvaatimukset ja muut lisävaatimukset

Kuten kuvasta 5 havaitaan, ISO 13849-1 -standardi vaatii (sen kohdassa 4.5.1), että PL-tason todentamista varten täytyy vielä arvioida systemaattinen vikaantuminen ja todentaa ohjelmiston turvallisuusvaatimukset sekä arvioida järjestelmän kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa. Näitä ei voida arvioida SISTEMA-työkalun avulla. Systemaattisen vikaantumisen hallinta ja estäminen sekä ohjelmiston turvallisuusvaatimukset voidaan todentaa KOTOTU-työkalun avulla, jossa yksinkertaisten tarkistuslistojen avulla käydään läpi ISO 13849-1 -standardin vaatimuslistat taulukoiden 13 ja 14 mukaisesti.

Taulukko 13. Systemaattisen vikaantumisen hallinnan suojauskeinojen todentaminen (sisältää vain osan ISO 13849-1 vaatimuksista; vastaava taulukko on tarjolla myös systemaattisen vikaantumisen estämiselle).

Vaaditut toimenpiteet systemaattisen vikaantumisen hallintaan	**Kuvaus, miten toteutettu**	**Korjaavat toimenpiteet; vastuuhenkilö**
— Käytetään energiattomaksi tekemisen periaatetta (ks. standardi ISO 13849-2)	Järjestelmä on suunniteltu niin, että nostolava jää paikalleen tehonsyötön katketessa; kone ei ole myöskään siirrettävissä hallintalaitteiden kautta	Ei korjaavia toimenpiteitä
— Toimenpiteet jännitteen katkeamisen, jännitteen vaihteluiden, ylijännitteen ja alijännitteen vaikutusten hallitsemiseksi.	Ohjausjärjestelmän lähdöt menevät turvalliseen tilaan käyttöjännitteiden katketessa; jännitevaihteluita, yli- ja alijännitteitä vastaan on suojauduttu SAE J1455- ja ISO 7637 -standardien mukaisesti	Ei korjaavia toimenpiteitä
— Toimenpiteet fyysisen ympäristön hallintaan tai sen vaikutusten estämiseen (esim. lämpötila, kosteus, vesi, tärinä, pöly, korroosiota aiheuttavat aineet, sähkömagneettinen häiriö ja sen vaikutukset).	Järjestelmän ympäristöolosuhdespesifikaatiot (ml. EMC) on määritelty dokumentissa XXXXXX.XXX. Järjestelmä testataan testausspesifikaation YYYYYY.YYY mukaisesti.	Ei korjaavia toimenpiteitä
…	…	…

Taulukko 14. Sulautetun ohjelmiston vaatimusten todentaminen (sisältää vain osan ISO 13849-1 vaatimuksista; vastaava taulukko on tarjolla myös sovellusohjelmistolle ja parametrointiprosessille).

Vaatimukset	**Kuvaus, miten toteutettu**	**Korjaavat toimenpiteet; vastuuhenkilö**
— Elinkaarimallin mukainen ohjelmistonkehitys, johon kuuluu todentamista ja kelpuutusta	Ohjelmisto on toteutettu perinteiseen V-malliin perustuvalla W-mallilla, jota on käytetty ohjelmiston suunnittelevassa yrityksessä neljän vuoden ajan	Ei korjaavia toimenpiteitä
— Erittelyn ja suunnittelun dokumentaatio	Järjestelmän vaatimukset on määritelty dokumentissa XXXXXX.XXX, joista on johdettu ohjelmiston vaatimusmäärittelydokumentti YYYYYY.YYY. Ohjelmiston suunnitteludokumentit ovat seuraavat: ….	Ei korjaavia toimenpiteitä
— Modulaarinen ja rakenteinen ohjelmisto	Järjestelmä on ohjelmoitu IEC 61131-3 -standardin mukaisella toimilohkokaaviolla, mikä tekee ohjelmiston rakenteesta modulaarisen ja rakenteellisen	Ei korjaavia toimenpiteitä
…	…	…

Edellä todettiin, että arvio järjestelmän kyvystä toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa on myös tehtävä. Taulukossa 13 ja vastaavassa listassa systemaattisten vikojen estämiselle on mukana ympäristöolosuhdevaatimuksiin liittyvät vaatimukset, joten myös siltä osin todennusprosessi tulee täydelliseksi.

ISO 13849-1 antaa lisäksi lyhyesti vaatimuksia ergonomisille näkökohdille ja kunnossapidolle. Vaatimukset ovat lähinnä viittauksia muihin tarkempiin standardeihin. Liitteen B prosessimallissa ergonomia- ja kunnossapitovaatimusten täyttymisen arviointi on siirretty kelpuutusprosessin puolelle, joten niitä ei tässäkään sisällytetä PL-tason evaluointiin, joka on tämän luvun aiheena. Kelpuutusprosessi sisältää myös ympäristöolosuhdevaatimuksiin liittyvän kelpuutuksen, joten viimeistään siinä yhteydessä järjestelmän kyky toimia oikein vaadituissa ympäristöolosuhteissa tulee yksityiskohtaisesti arvioitua ja testattua.

Tässä yhteydessä ei käydä läpi kommunikointijärjestelmän analyysiä. Liitteen B prosessimallissa kommunikointianalyysi tehdäänkin jo PL-tason evaluointia edeltävässä prosessivaiheessa. Periaate joka tapauksessa on, että kommunikointijärjestelmää ei evaluoida PL-tasolle, vaan SIL-tasolle standardin IEC 61784-3 [2007] mukaisesti. SIL-tasosta (tai sitä vastaavasta PFH_D-arvosta) päätellään sitten PL-taso. Kommunikointijärjestelmien turvallisuuteen ja niiden analyysiin löytyy ohjeita julkaisusta [Alanen et al. 2004]. Kyseisen tiedotteen kirjoittamisen aikaan IEC 61784-3 -standardia ei ollut olemassa, mutta tiedotteessa esitetty BIA:n ohjeisiin ja EN 50159 -standardiin perustuva malli kommunikointijärjestelmien turvallisuuden analyysiin on lähes täsmälleen sama kuin IEC 61784-3 -standardissa.

4. Turvallisuussuunnittelun työkalut

4.1 Kaupallisia PL- ja SIL-tasojen laskennan työkaluja

Tässä esitellään lyhyesti projektin aikana käytettävissä olleita PL- ja SIL-tasojen laskennan työkaluja.

4.1.1 SISTEMA

SISTEMA[9] (**S**afety **I**ntegrity **S**oftware **T**ool for the **E**valuation of **M**achine **A**pplications) on BGIA:n kehittämä työkalu, joka on tarkoitettu standardin SFS-EN ISO 13849-1 soveltamisen apuvälineeksi. SISTEMA-työkalulla on mahdollista arvioida kvantitatiivisesti järjestelmän kanavien suoritustaso (PL) lähtien liikkeelle järjestelmän yhden kanavan komponenttien $MTTF_d$-arvoista. Arvioitavan järjestelmän tiedot on mahdollista dokumentoida SISTEMAssa, ja sen sisältämien kirjastotoimintojen käyttö mm. komponenttitietojen tallennukseen myöhempää käyttöä varten on mahdollista.

SISTEMAn käyttöliittymä koostuu varsinaisesta työtilasta (jossa eri osakomponenttien parametriarvot syötetään), puumaisesta navigointi-ikkunasta (johon lohkokaaviorakenne syötetään), työkalupalkista, help-ikkunasta ja PL-esikatselusta (ks. kuva 19). SISTEMAan on mahdollista tallentaa useita projekteja, joita voidaan myös kopioida ja muokata myöhempää käyttöä varten.

SISTEMA ei sisällä ohjelmiston eikä systemaattisten vikojen arviointia. Sen sijaan yhteismuotoiset viat ja niiden standardinmukainen pisteytys on mahdollista SISTEMAssa käsitellä.

SISTEMAssa päätasona on projekti eli koneenohjausjärjestelmä. Tämän alla on järjestelmän turvatoiminnot eli SF:t (safety function). Turvatoiminto voi koostua yhdestä tai useammasta alijärjestelmästä eli SB:stä (subsystem), ja nämä puolestaan koostuvat kanavista (CH). Kanavat koostuvat lohkoista (BL) ja lohkot elementeistä (EL).

Turvatoimintotasolle annetaan toimintokuvaukseen liittyviä tietoja, kuten vaadittava suoritustaso eli PL_r joko riskigraafin perusteella tai suoraan (ks. taulukko 15). SB-tasolle annetaan $MTTF_d$ (joko suoraan tai laskien kanava-, lohko- tai elementtitasolta), DC_{avg} ja CCF (tulos yhteismuotoisten vikojen pisteytystaulukosta). Kanavatasolle annetaan lohkot. Lohkotasolle annetaan $MTTF_d$ ja DC_{avg} (kumpi-

[9] Tämä teksti perustuu SISTEMAn versioon 1.0.5.

kin joko suoraan tai elementtitasolta laskien). Elementtitasolla voi olla esim. releitä tai asemantunto-kytkimiä. Tietoja voi myös dokumentoida usealla eri tasolla.

Taulukko 15. SISTEMAan annettavat tiedot eri tasoilla.

Tasot	$MTTF_d$	DC / DC_{avg}	Luokka	PL / PL_r	CCF
SF				PL_r annetaan suoraan tai riskigraafin avulla	
SB	Voi antaa tässä tai lasketaan lohkoista	Voi antaa tässä tai lasketaan lohkoista	Annetaan tässä	Voi antaa tässä tai lasketaan kanavista	Annetaan tässä suoraan tai lasketaan. Vain luokissa 2, 3 ja 4
CH	Annetaan ainoastaan kanavaan liittyvät lohkot				
BL	Voi antaa tässä tai lasketaan elementeistä	Voi antaa tässä tai lasketaan elementeistä			
EL	Annetaan tässä	Annetaan tässä			

SISTEMA ilmoittaa saavutetun PL-tason vasemmassa alakulmassa olevassa ikkunassa. Siellä näkyvät myös lasketut $MTTF_d$-, DC_{avg}- ja CCF-arvot. SISTEMA ilmoittaa työtilan ylälaidassa, jos jokin parametri ei vaikuta laskentaan lainkaan.

SISTEMA laskee osajärjestelmien yhdistämisen PFH_D arvojen avulla (PFH_D = vaaraa aiheuttavan vian todennäköisyys tuntia kohden), mutta standardissa SFS-EN ISO 13849-1 lasketaan kunkin osajärjestelmän PL-taso erikseen ja osajärjestelmät yhdistetään standardissa esitetyn taulukon avulla. PFH_D -laskennalla tulos on hieman tarkempi, vaikka sitä ei standardissa esitetäkään. Lisäksi SISTEMAssa PFH_D lasketaan hieman eri tavalla kuin standardissa IEC 61508, koska yhteisvikojen beta-tekijää (yhteisvikojen osuus) ei osista tiedetä, mutta tällä erolla ei ole paljon merkitystä.

SISTEMAsta on olemassa englanninkielinen ja saksankielinen versio. Suomenkielinen versio SISTEMAsta on tekeillä.

4.1.2 PAScal

PAScal on Pilz-yhtiön kehittämä laskentaohjelma, jolla voidaan tarkistaa koneiden turvatoiminnoilla saavutettava suoritustaso PL ja turvallisuuden eheystaso SIL laskemalla nämä käytettyjen komponenttien perusteella. Laskennan tulosta verrataan standardin SFS-EN ISO 13849-1 mukaisiin PL-vaatimuksiin tai standardin SFS-EN 62061 mukaisiin SIL-vaatimuksiin. Käyttäjä voi nähdä graafisena esityksenä ne kohteet ja komponentit, joissa mahdollista turvaparannusta tarvitaan.

Järjestelmän tietojen syöttäminen tapahtuu loogisesti kuudessa vaiheessa. Demonstraatioversiossa ensimmäiset viisi vaihetta ovat käytettävissä, mutta raportin luominen vaatii lisensoidun version ohjelmasta. Ohjelmassa on myös ISO 13849 standardin mukainen yhteisvikaantumista (CCF) estävien

toimenpiteiden arviointi- ja pisteytystaulukko. Toisaalta standardia SFS-EN 62061 käytettäessä ohjelma laskee CCF-tekijän arvon järjestelmälle käyttäjän lomakkeelle täyttämien pisteiden perusteella.

PAScal määrittää sekä PL-tasot että SIL-tasot PFH_D-arvojen perusteella. Standardin SFS-EN 62061 mukaisesti tehtäessä voidaan PFH_D-arvon määrittymistä tarkastella myös graafisesti. PL-tavoitetaso voidaan laskea käyttämällä myös standardissa esitettyä riskigraafia, jolloin PAScal määrittää PL-tason ja sitä ohjelmassa vastaavan PFH_D-välin, eli tilanne palautuu käytännössä samaksi kuin PL-tason määrittäminen suoraan PFH_D-arvojen perusteella.

Ohjelman avulla on helppo rakentaa omia järjestelmiä valmiina olevien Pilzin ja Danfossin komponenttikirjastojen avulla. Järjestelmissä voidaan käyttää antureita, sisäänmenoja, ulostuloja, toimilaitteita ja väyläliityntöjä. Omien komponenttien ja komponenttikirjastojen luominen on myös mahdollista. Omaa komponenttia syötettäessä voidaan syöttää seuraavia ominaisuuksia: komponentin nimi, onko kyseessä kuluva osa, sisäisen diagnostiikka, komponentin kuvaus, sisäinen arkkitehtuuri (yksi- tai kaksikanavainen), onko kyseessä mekaaninen kytkin, diagnostiikan kattavuuden ominaisuus, MTTF-arvo tai vikatyyppisuhde. Mikäli komponentissa on sisäistä diagnostiikkaa, ohjelmaan syötetään MTTF-arvon ja vikatyyppisuhteen sijasta PFH_D-, SIL, CL- ja PL-arvot sekä yhdelle että kahdelle kanavalle, ja tämän lisäksi toiminta-aika (mission time). Samat komponenttiominaisuudet löytyvät myös valmiiksi tehdyistä komponenteista.

PAScal-ohjelmaa kannattaa käyttää laskennassa silloin kun halutaan nopeasti saada selville etupäässä Pilzin komponenteista koostuvan turvatoiminnon PL-tason toteutuminen. Jos taas järjestelmä sisältää paljon eri valmistajien komponentteja, joista ainakin osalle löytyy tarvittavat MTTF-arvot, SISTEMA on parempi, sillä PAScal-ohjelmaa käytettäessä muut kuin Pilzin komponentit on aluksi määriteltävä ohjelmalle kaikkine parametreineen, mikä voi olla työlästä.

4.1.3 RiskCat

RiskCAT on ulkoasultaan hyvin pelkistetty työkalu, jota voidaan käyttää apuvälineenä standardin IEC 61508 soveltamisessa. Sen valmistaja on saksalainen Hitex Development Tools.

RiskCAT on tarkistuslistatyyppinen työkalu, jossa IEC 61508 -standardin vaatimukset esitetään SIL-tasovaatimuksesta riippuvana listana. Tähän merkitään käytetyt menetelmät ja perustellaan, miten vaatimukset on käytännössä toteutettu. RiskCAT on siis kelpuutustyökalu. SIL-taso voidaan määrittää joko riskigraafiin pohjaten muuttamalla riskiä kuvaavat parametrit vastaamaan käsiteltävää kohdetta tai määrittämällä hyväksytty vikaantuvuus (failure rates). Toisaalta haluttu SIL-taso voidaan määrätä suoraan ja tämän jälkeen säätää muuttujia sopiviksi siten, että määrätty taso saavutetaan. SIL-tasojen määritys on työkalussa yksinkertaista ja loogista.

RiskCAT ohjelmalla saadaan selville, mitkä menetelmät ja toimenpiteet ovat IEC 61508 -standardin mukaisesti kussakin tilanteessa pakollisia, erittäin suositeltavia, suositeltavia, mahdollisia tai sellaisia, joiden käyttöä ei suositella. Lisäksi RiskCAT lajittelee toistensa suhteen vaihtoehtoiset menetelmät ja merkitsee ne harmaalla taustavärillä. Tämän jälkeen käyttäjä pääsee itse valitsemaan käytettävät menetelmät. RiskCAT antaa toisaalta mahdollisuuden valita myös esimerkiksi kaikki pakolliset menetelmät suoraan, jolloin jokaista käytettävää menetelmää ei tarvitse erikseen etsiä ja valita. Mahdollisia syötettäviä asioita tässä työkalussa on erittäin vähän, ja esimerkiksi tietoja kohteena olevasta järjestelmästä ei pysty ohjelmaan syöttämään.

RiskCAT ohjelmaa voidaan käyttää KOTOTU-referenssimallin kelpuutusprosessissa ohjelmiston kelpuutuksen yhteydessä, jos päädytään IEC 61508 -3 -standardin ohjelmistovaatimuksiin.

4.2 Kaupallisia luotettavuusanalyysin työkaluja

Luotettavuusanalyyseihin (FMEA, FTA, ETA, HAZOP, LCC jne.) ja riskien arviointiin on saatavana useita kaupallisia työkaluja. Tässä esitellään niistä lyhyesti muutama.

4.2.1 Relex-työkalut

Relex on Relex Software Corporationin tuottama, luotettavuustekniikan tarpeisiin kehitetty ohjelmistotyökalujen paketti, joka koostuu seuraavista luotettavuusanalyysin menetelmistä:

- Tapahtumapuuanalyysi (Event Tree Analysis, ETA)
- Vikapuu (Fault Tree Analysis, FTA)
- Vika- ja vaikutusanalyysi (Failure Modes and Effects Analysis, FMEA, myös FMECA)
- Vikojen raportointi-, analysointi- ja korjaustoimenpidejärjestelmä (Failure Reporting, Analysis, and Corrective Action Systems, FRACAS)
- Inhimillisiin tekijöihin liittyvä riskianalyysi (Human Factors Risk Analysis)
- Elinkaarikustannukset (Life Cycle Cost, LCC)
- Kunnossapidettävyyden ennustus (Maintainability Prediction)
- Markovin analyysitekniikat
- Luotettavuuden ennustaminen (Reliability prediction)
- Luotettavuuslohkokaaviot (Reliability Block Diagram, RBD)
- Weibullin tekniikat.

Relex-ohjelmistotyökalupaketti ei sisällä suoritustasojen (PL) laskentaan liittyvää työkalua. Sen sijaan esim. kvantitatiivista MTBF-laskentaa työkalupaketin osilla voidaan tehdä, ja esimerkiksi vikapuita mallintaa myös kvantitatiivisesti. Lisäksi työkalupaketin osilla voidaan tehdä KOTOTU-referenssimallin mukaista toimintojen analyysiä (esim. FMECA).

4.2.2 Item Software -työkalut

Item Software toimittaa ohjelmistotyökaluja järjestelmien luotettavuuden ja turvallisuuden analysointiin ja riskien arviointiin. Item Softwaren Toolkit muodostaa sarjan analyyttisiä ja ennustavia rakenneosia elektronisten ja mekaanisten komponenttien ja järjestelmien luotettavuuden, käyttövarmuuden, huollettavuuden ja turvallisuuden (RAMS) analysointiin. Tämä Toolkit-ohjelmistopaketti sisältää seuraavat osat:

- Luotettavuuden ennustaminen (perustuu seuraaviin standardeihin: MIL-HDBK-217, IEC 62380, Telcordia, NSWC, China 299b)
- FMECA
- RBD-analyysi
- FTA

- ETA
- Markov
- Main Train
- Spare cost.

Lisäksi Item Software tarjoaa ohjelmistoa kvantitatiiviseen riskien arviointiin (Quantitative Risk Assessment System Software).

Item Softwaren Toolkit-ohjelmistopaketin osilla ei voida laskea PL-suoritustasoja. Sen sijaan KOTOTU-referenssimallin mukaista toimintojen analyysiä (esim. FTA ja FMECA) voidaan ohjelmistopaketin osilla tehdä.

4.2.3 Isograph-työkalut

Isograph on vuonna 1986 perustettu luotettavuuteen, käyttövarmuuteen, huollettavuuteen ja turvallisuuteen (RAMS) liittyvien ohjelmistotyökalujen valmistaja. Näitä työkaluja käytetään useilla eri teollisuuden aloilla (ilmailu, rautatiet, elektroniikka, auto, puolustusväline, kaivos, valmistus, kemia, prosessi, energia, jne.). Analyysityövälineistöön kuuluu mm. käytettävyystyökaluja (esim. LCC, Weibull-analyysi), luotettavuusanalyysin työkaluja (esim. FMECA, FTA, ETA, RBD, Markovin mallit), HAZOP- ja FRACAS-työkalut sekä komponenttikirjastot (mm. elektroniset ja mekaaniset komponentit).

Isograph-työkalujen joukossa ei ole PL-tasojen laskentaan tarkoitettua työkalua, mutta sen sijaan KOTOTU-referenssimallin mukaista toimintojen analyysiä eri työkalujen avulla (esim. FTA, FMECA, HAZOP) voidaan kuitenkin Isograph-analyysityövälineillä tehdä.

4.2.4 Sydvestin työkalut

Norjalainen Sydvest toimittaa luotettavuuden ja turvallisuuden analysointiin ja hallintaan tarkoitettuja työkaluja. Sydvest on tehnyt ohjelmien kehittämisessä yhteistyötä mm. SINTEFin kanssa. Vikapuiden laatimiseen Sydvestiltä löytyy CARA-ohjelmisto ja FMEA/FMECA -analyysejä varten on kehitetty Sabaton-ohjelmisto. Lisäksi Sydvestin kautta on saatavana SINTEFin julkaisemia SIS-järjestelmien (Safety instrumented Systems) analysoinnin apuna käytettäviä luotettavuustiedon käsikirjoja.

Sydvest ei toistaiseksi tarjoa PL-tasojen laskentaan tarkoitettua työkalua, mutta KOTOTU-referenssimallin mukaisessa toimintojen analyysissä Sydvestin työkaluja (mm. FMEA, FTA) voidaan käyttää.

4.2.5 CIRSMA

CIRSMA™ (Corporate Industrial Risk and Safety Management Application) on riskien arviointiin ja hallintaan tarkoitettu työkalu. Sen on kehittänyt kanadalainen Industrial Safety Integration. Työkalu pohjautuu riskien pienentämisen kolmen askeleen periaatteeseen, joka on esitetty standardissa SFS-EN 292. CIRSMA on tietokantapohjainen työkalu, joka auttaa vaarojen ja riskien systemaattisessa käsittelyssä ja dokumentoinnissa. Ohjelman avulla määritetään kohteen vaaratekijät ja arvioidaan niistä aiheutuvien riskien suuruutta. Tietokantaan voidaan tallentaa myös kuvia esim. riskien arvioinnin koh-

teista. Työkalua voidaan käyttää myös verkossa usean käyttäjän sovelluksena. CIRSMA-ohjelmaa markkinoidaan siten, että siitä on saatavilla perusohjelma, johon voidaan tarpeen mukaan ostaa erilaisia lisämoduuleja.

CIRSMA ei ole PL-tasojen tai muun kvantitatiiviseen tiedon laskentaan tarkoitettu työkalu. Sen sijaan KOTOTU-referenssimallin alkuvaiheen alustavassa vaara-analyysissä sitä voitaisiin käyttää työkaluna.

4.3 Vikataajuustietokantoja ja työkaluja

4.3.1 SPIDR

SPIDR™ (System and Part Integrated Data Resource) on Alion System Reliability Centerin (SRC) tuottama sähköisesti toimiva luotettavuustietokanta. Sen demoversion voi ladata SRC:n sivujen kautta. SPIDR korvaa seuraavat vanhentuneet tietokannat tiedoilla, joita päivitetään vuosittain:

- Nonelectronic Part Reliability Data (NPRD-95)
- Electronic Part Reliability Data (EPRD-97)
- Failure Mode and Mechanism Distributions (FMD-97)
- Electrostatic Discharge Susceptibility Data 1995 (VZAP).

SRC ylläpitää sekä määrällisiä että laadullisia komponentti- ja järjestelmätietokantoja useilta eri teollisuuden aloilta. SPIDR:stä on saatavana sekä PC:llä toimiva että palvelinpohjainen versio.

4.3.2 SN 29500

SN 29500 on Siemensin ja tämän yhteistyökumppaneiden käyttöön kehitetty komponenttien vikataajuustietokanta [SN 29500]. Se pitää sisällään säännöllisesti päivitettäviä tietoja vikataajuuksista huomioiden vertailuolosuhteet ja rasitusmallit, jotka ovat tarpeen osien laskennan ja osien rasituksen ennustamisessa.

Tämä Siemensin standardi sisältää kokemukseen ja sovelluksiin perustuvaa tietoa, huomioiden ulkopuoliset lähteet, mm. MIL-HDBK-217. Komponentit on luokiteltu moneen ryhmään, joissa jokaisessa on hieman erilainen luotettavuusmalli. Mallissa käytettävät piikertoimet ottavat huomioon vaihtelut laitteen toimintalämpötilassa ja sähköisessä rasituksessa. Standardi on saatavissa Siemensin kautta.

4.3.3 OREDA

OREDA on kahdeksan öljy- ja kaasualan yhtiön muodostama projektiorganisaatio, jonka päätarkoituksena on kerätä ja vaihtaa luotettavuustietoa yhteistyöhön osallistuvien yritysten kesken. OREDA on perustanut luotettavuustiedosta kattavan tietokannan, ja samanniminen ohjelmisto on kehitetty tiedon keräämistä, hakua ja analysointia varten. Tietokanta sisältää tietoja 260 asennetusta järjestelmästä ja 16 000 laitteistoyksiköstä vika- ja ylläpitotietoineen (36 000 vikatallennetta ja 64 000 ylläpitotallennetta). OREDA-tietokannassa on tietoja mm. pyörivistä koneista (sähkögeneraattorit ja -moottorit,

kompressorit, kaasuturbiinit, polttomoottorit jne.), mekaanisista laitteistoista (nosturit, lämmönvaihtimet, höyrykattilat, vinssit, jne), ohjaukseen ja turvallisuuteen liittyvistä laitteistoista (ohjauslogiikkayksiköt, tehomuuntajat, venttiilit jne.) ja merenalaiset (subsea) laitteistot (ohjausjärjestelmät, putkistot, voimavirran jakelu jne.).

OREDAn luotettavuustietoja voidaan käyttää mm. tuotannon käytettävyyden ja suorituskyvyn arviointiin, redundanssitarpeen määrittämiseen, kriittisten vikojen todennäköisyyksien määrittämiseen sekä muihin turvallisuus- ja luotettavuusanalyyseihin.

4.3.4 MIL-HDBK-217F

MIL-HDBK-217F -käsikirjan tarkoituksena on laatia ja ylläpitää yhtenäisiä menetelmiä alun perin sotilaskäyttöön tarkoitettujen elektronisten laitteiden ja järjestelmien luotettavuuden arvioimiseen [MIL-HDBK-217F 1991]. Käsikirja on tarkoitettu käytettäväksi suunniteltavan laitteen luotettavuuden kasvattamiseksi. Se tarjoaa yleisen perustan mm. kilpailevien suunnitteluratkaisujen luotettavuuden vertaamiseen ja arviointiin. Käsikirjassa on esitetty kaksi menetelmää luotettavuuden ennustamiseen: ns. ”Parts stress analysis” ja ”Parts count”. Näistä edellinen vaatii runsaasti yksityiskohtaista tietoa järjestelmästä, ja se voidaan tehdä vasta suunnittelun myöhäisemmässä vaiheessa. Jälkimmäinen taas voidaan tehdä suunnittelun varhaisessa vaiheessa, ja se vaatii vähemmän lähtötietoa.

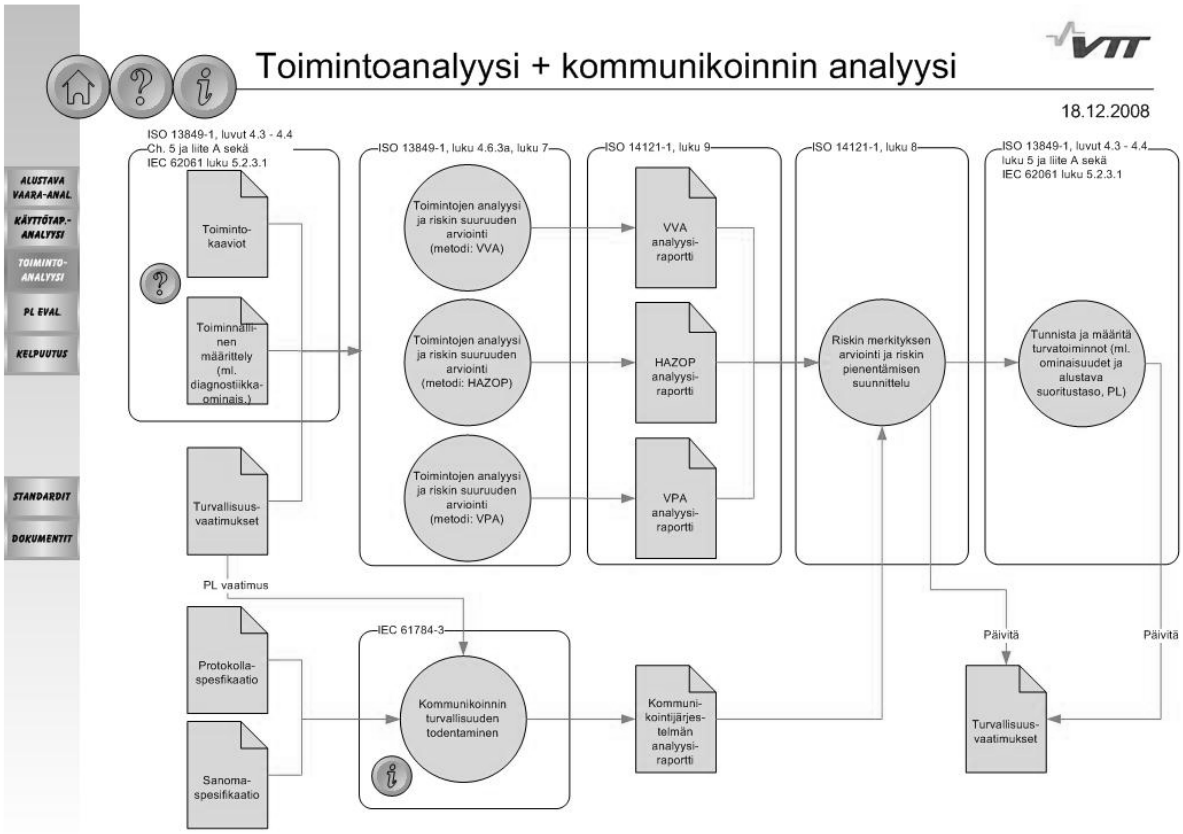
4.4 KOTOTU-prosessityökalu

KOTOTU-prosessityökalu koostuu liitteen B prosessimallin mukaisesta web-sovelluksesta ja Excelillä toteutetusta KOTOTU-laskentatyökalusta (KOTOTU_tool).

Web-sovelluksen käyttöliittymä näyttää samalta kuin kuva 11. Kuvan turvallisuusprosessin eri vaiheita napsauttamalla päästään niitä vastaaviin osaprosesseihin, jotka näyttävät jälleen samanlaisilta kuin niitä vastaavat prosessikuvat (ks. liite B). Kuvien yhteydessä olevia standardiviittauksia napsauttamalla kyseinen standardi avautuu viittauksen mukaiselta sivulta. Dokumenttikuvakkeesta valitsemalla avautuu kyseinen dokumentti, dokumentin osa tai dokumenttipohja. Kaavion prosessi-kohdan kuvakkeesta valitsemalla avautuu prosessiin liittyvä työkalu, jos sellainen on olemassa. Esimerkiksi kuvan 22 prosessikuvakkeesta ”Vaaditun suoritustason (PL) saavuttamisen todentaminen ja dokumentointi” avautuu KOTOTU-projektissa kehitetty Excel-työkalu, jolla PL-taso voidaan laskea. Vaihtoehtoisesti voidaan käyttää BGIA:n (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung) ilmaiseksi tarjoamaa SISTEMA-työkalua.

Jokaisella sivulla on myös painikkeet kyseisen prosessivaiheen prosessiohjetta varten sekä painike lisäinformaatiota varten (ks. kuva 22). Myös itse prosessikaavion sisällä voi olla prosessiohjeita tai lisäinformaatiota eri tehtäviä varten. Kotipainikkeesta päästään kuvan 11 mukaiselle prosessipääsivulle.

Web-sovelluksessa on lisäksi omat sivut standardikokoelman sekä turvallisuuteen liittyvien dokumenttien selailuun.



Kuva 22. Esimerkki web-sovelluksen käyttöliittymäsivusta.

Työkalu voidaan toteuttaa tiedostopohjaisena sovelluksena, jolloin se voidaan siirtää esim. CD-levylle tai jopa koneen ohjaustietokoneen kiintolevylle. Täten koko turvallisuuteen liittyvä prosessi dokumentteineen on helposti esiteltävissä esimerkiksi viranomaisille tai tarkastuslaitoksille, eli se toimii myös teknisenä rakennetiedostona edellyttäen, että kaikki konedirektiivin liitteen VII vaatimat dokumentit on mukana.

4.4.1 KOTOTU-laskentatyökalu

KOTOTU-laskentatyökalu tukee standardin SFS-EN ISO 13849-1 käyttöä. Laskentatyökalu on tarkoitettu ammattilaisille, jotka tuntevat standardia ja soveltavat ainakin jotakin työkalun osa-aluetta. Laskentatyökalun tehtävänä on toimia opetustyökaluna, dokumentointityökaluna ja projektityökaluna ja auttaa turvallisuuden suorituskyvyn (PL) arvioinnissa. Menetelmä on puoliautomaattinen, ja siinä voidaan makroilla siirtää tuloksia vaiheesta seuraavaan. Osajärjestelmien tunnuslukuja voidaan antaa myös suoraan ilman yksityiskohtaista laskentaa tai määrittelyä.

KOTOTU-laskentatyökalu soveltaa standardin SFS-EN ISO 13849-1 vaatimuksia, kaavoja ja graafeja standardissa esitetyillä menetelmillä. SISTEMA-ohjelmaan verrattuna KOTOTU-laskentatyökalu ei laske yhtä tarkasti, koska se ei käytä todennäköisyyspohjaista PFH_D-laskentaa. Toisaalta $MTTF_d$-arvojen laskennassa tietojen syöttö laskentatyökalussa on helpompaa kuin nykyisessä SISTEMAssa, koska arvot saadaan usein taulukosta, josta ne voidaan kopioida Exceliin. Tämän vuoksi Excel-

työkalulla kannattaa usein laskea kanavakohtaiset $MTTF_d$ -arvot ja tarvittaessa syöttää ne SISTEMAan jatkolaskentaa varten.

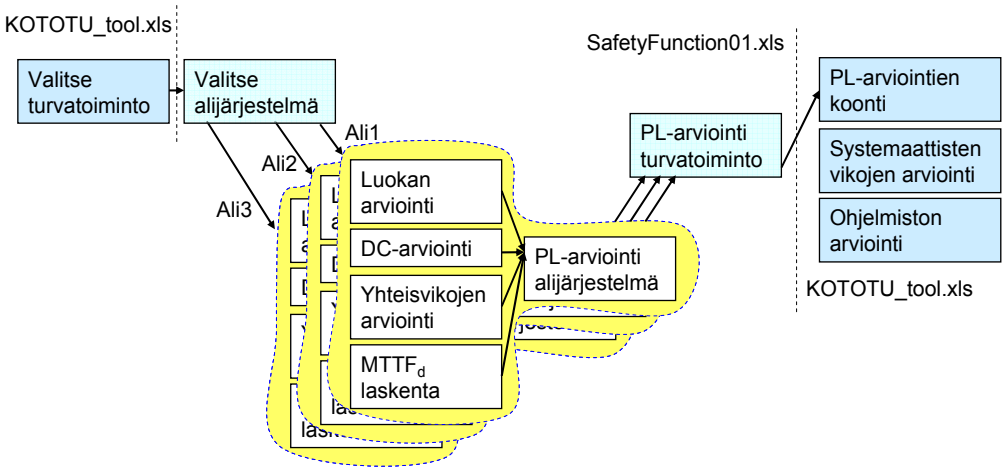
Riskin arviointi on erotettu työkalussa omaksi tiedostokseen ja siihen päästään KOTOTU-prosessityökalulla tai avaamalla suoraan tiedosto. Riskin arvioinnissa esille tulleet vaatimukset pitää kirjoittaa manuaalisesti KOTOTU-laskentatyökaluun.

Lähtökohdat PL-laskentaan

Kuhunkin PL-tasoon liittyy joukko kvalitatiivisia vaatimuksia ja lisäksi kvantitatiivisia vaatimuksia, joilla saavutettu PL-taso lasketaan. Kvalitatiivisia vaatimuksia ovat mm. turvallisuusperiaatteisiin, systemaattisiin vikoihin ja yhteisvikoihin liittyvät vaatimukset sekä ohjelmistovaatimukset. Turvallisuusperiaatteisiin liittyviä vaatimuksia esitetään myös standardissa SFS-EN ISO 13849-2. Laskentaa varten tarvitaan tiedot komponenttien keskimääräisestä vaarallisten vikojen vikataajuudesta ($MTTF_d$), diagnostiikan kattavuudesta (DC) ja ohjausjärjestelmän (turvallisuus)luokasta. Luokat liittyvät ohjausjärjestelmien arkkitehtuureihin. Ohjausjärjestelmästä laadittu turvallisuuslohkokaavio tulee sovittaa standardissa SFS-EN ISO 13849-1 esitettyihin nimettyihin rakenteisiin, jotta standardissa esitettyjä kaavoja ja graafeja voidaan soveltaa. Standardin tekijät ovat laskeneet Markovin mallien avulla nimettyjä rakenteita vastaavat PFH_d-arvot ja piirtäneet niistä vastaavat graafit. Laskennan tuloksena saadaan PL-taso, joka vastaa tiettyä SIL-tasoa. Osia tai kokonaisuuksia voidaan laskea myös standardin SFS EN 62061 mukaan tai esim. Markovin malleilla.

KOTOTU-laskentaprosessi

KOTOTU-laskentaprosessi aloitetaan piirtämällä arvioitavasta ohjausjärjestelmästä turvallisuuslohkokaavio. Excel-työkalussa lähtökohtana on kolme alijärjestelmää (esim. tuloyksikkö, logiikka ja lähtöyksikkö) sisältävä kokonaisuus. Tämä mahdollistaa melko monipuolisen arkkitehtuurivalikoiman. Suurempi alijärjestelmien lukumäärä lisää standardin kaavoissa vian todennäköisyyttä ja sen vuoksi joku muu menetelmä (tarkempaa laskentaa) saattaisikin olla käytännöllisempi. Pääohjelmassa toteutetaan vaiheet, jotka pätevät yleensä koko ohjausjärjestelmälle. Aliohjelmissa (esim. SafetyFunction01.xls) toteutetaan funktiokohtaisia arviointeja. Kukin aliohjelma on jaettu kolmeen alijärjestelmään, joissa tarkastellaan kutakin alijärjestelmää itsenäisesti.



Kuva 23. KOTOTU-laskentaprosessin jako alijärjestelmiin.

Standardissa SFS-EN ISO 13849-1 esitetään MTTF-arvoja muutamille tavallisille peruskomponenteille. Näitä voidaan käyttää, jos valmistaja ei ilmoita MTTF-arvoja. Yhä useammin löytyy esim. internetistä valmistajien ilmoittamia MTTF-arvoja, mutta edelleen suurimmalle osalle komponenteista arvot pitää jotenkin arvioida tai laskea. Tälläisessa tilanteessa pitää varmistaa, että käytetyt arvot eivät ole liian optimistisia. Erilaiset oletukset pitää tehdä pessimistiseen suuntaan sellaisen tuloksen saamiseksi, josta voidaan taata, että todellisuus on parempi kuin oletus. Jos MTTF-arvoa ei löydetä, standardi sallii, että MTTF-arvona käytetään lukua 10 vuotta, mikä on yleensä hieman pessimistinen arvaus. MTTF-arvojen määrittämisessä on hyvä huomioida, mitkä komponentit vaikuttavat merkittävästi lopputulokseen ja panostaa juuri niihin. Myös diagnostiikan kattavuuden arvot on yleensä vaikea selvittää. Yksinkertaisissa relekytkennöissä tämä arvo on mahdollista laskea, mutta monimutkaisia järjestelmiä joudutaan vertailemaan esimerkkeihin ja päättelemään DC.

Alijärjestelmän kunkin kanavan keskimääräinen vaarallisen vian väli ($MTTF_d$) lasketaan taulukolla omalla sivulla. Taulukkoon lisätään puuttuvat komponentit, merkitään komponenttien lukumäärä, MTTF ja vaarallisten vikojen osuus. Laskenta voidaan toteuttaa tavallisilla arvoilla tai pahimman tapauksen arvoilla, jolloin lopputulos on dekadin pessimistisempi. Osakokonaisuuksien tai laitteiden $MTTF_d$-arvoja voidaan antaa kanaville myös suoraan ilman komponenttikohtaista laskentaa. Lopuksi kanavan vikataajuudet summataan ja tulokseksi saadaan kanavan keskimääräinen vikaväli vaarallisten vikojen osalta. Kaksikanavaisissa järjestelmissä tehdään vielä kanavien $MTTF_d$-arvojen symmetrointi, jonka lopputulosta käytetään myöhemmissä laskelmissa. Ennen tulosten käyttöä seuraavassa vaiheessa tarkastetaan, että kanavakohtainen $MTTF_d$ ei ole yli 100 vuotta, ja että luokassa 2 testikanavan $MTTF_d$ on vähintään puolet pääkanavan $MTTF_d$ arvosta. Näillä standardin esittämillä rajoituksilla estetään se, että yksistään erittäin hyvä laskennallinen MTTF-arvo takaisi korkean PL-tason. Kuva 3 esittää osaa yhden kanavan laskentataulukosta.

Diagnostiikan kattavuuden (DC) arviointi on työkalussa toteutettu siten, että käyttäjä voi kertoa suoraan järjestelmän osien DC-arvot, joista laskentatyökalu laskee $MTTF_d$ -arvolla painotetun keskiarvon. Vaihtoehtoisesti käyttäjä voi vertailla omaa järjestelmää standardissa esitettyihin kunkin DC-tason tyypillisiin ratkaisuihin ja valita DC-arvon esimerkkien pohjalta. Yhteisvikojen arvioinnissa standardin mukaan varmistetun järjestelmän pitää saavuttaa kysymyslistassa esitetyistä kysymyksistä vähintään

65 pistettä. Laskentatyökalu laskee pisteet, ja työkalun käyttäjä kirjaa taulukkoon kunkin kohdan perustelut.

Kun kaikki alijärjestelmät on käyty läpi ja todettu kunkin alijärjestelmän täyttävän yhteisvikoihin liittyvät minimivaatimukset, tarkastellaan kokonaisuutta. Alijärjestelmien tulokset siirtyvät automaattisesti aloitus/lopetussivulle (Kuva 24). Sivulta nähdään, täyttyvätkö turvatoiminnolle asetetut vaatimukset tarkasteltujen vaatimusten osalta.

PL-tason arviointi

TURVATOIMINTO: Manuaalinen nosto/lasku

		$MTTF_d$	DC	CCF	Cat	PL
Osajärjestelmä 1: Arvioi PL		74,1	medium	OK	2	PL=d
	Kanava 1	100,0				
	Kanava 2	5,0				
Osajärjestelmä 2: Arvioi PL		100,0	low	OK	2	PL=d
	Kanava 1	100,0				
	Testikanava	36,5				
Osajärjestelmä 3: Arvioi PL		67,4	medium	OK	2	PL=d
	Kanava 1	100,0				
	Testikanava	11,4				
Koko järjestelmä				N_{low}=	3	**PL=d**
				PI_{low}=	d	

Vaatimustaso PL_r = c

CCF vaatimukset täyttyvät

Vaatimukset täyttyvät tässä tiedostossa käsiteltyjen tekijöiden osalta

Kuva 24. KOTOTU-laskentaprosessin turvatoiminnon aloitus/lopetussivu.

Ohjelmistovaatimuksiin ja systemaattisiin vikoihin liittyy sanallisia vaatimuksia, jotka on ryhmitelty aihepiireittäin. Ohjelmiston osalta vaatimusten luokittelu on tehty ohjelmistotyypin ja luokan mukaisesti. Käyttäjä näkee ainoastaan valittuun tyyppiin ja luokkaan liittyvät vaatimukset. Kunkin vaatimuksen kohdalle on varattu tilaa perusteluille siitä, miten kyseinen vaatimus tulee täyttää. Ohjelmistovaatimukset ja systemaattisiin vikoihin liittyvät vaatimukset tarkistetaan KOTOTU_TOOL pääohjelmassa. Niitä ei siis arvioida kullekin turvatoiminnolle erikseen, koska ne pätevät usein koko järjestelmälle. Jos eri turvatoimintojen toteutuksessa on eroja ohjelmistojen tai systemaattisten vikojen välttämisen periaatteissa, pitää tarkastelu tehdä erillisessä tiedostossa. Sama pätee myös kokonaisuuteen, jossa alijärjestelmiä on enemmän kuin kolme. Tällöin tulosten yhteenveto pitää toteuttaa manuaalisesti.

5. Pohdintaa

Nykyaikaiset laatujärjestelmät perustuvat prosessikuvauksiin, joiden käyttöliittymänä toimii web-selain. Tässä julkaisussa esitelty koneenohjausjärjestelmien turvallisuusprosessin referenssimalli antaa esimerkin, miten vastaavaa laatuprosessia voidaan soveltaa myös koneiden ohjausjärjestelmien turvallisuussuunnittelussa. Referenssimalli on tässä yhteydessä tehty noudattamaan SFS-EN ISO 13849-1 -standardia, mutta se voidaan muuttaa noudattamaan myös SFS EN 62061 -standardia. Prosessikäyttöliittymän luonti on tehty niin helpoksi, että turvallisuusprosessi voidaan räätälöidä jopa projektikohtaisesti. Referenssimallin ja sen web-toteutuksen tavoitteena on ollut luoda toimintamalli systemaattisen ja sujuvan turvallisuusprosessin luomiseen. Tarkoitus ei ole, että referenssimallia ja sen toteutusta käytettäisiin sellaisenaan koneyritysten tuotekehitysprosesseissa, vaan että referenssimallin perusteella yrityksiin luotaisiin heidän tuotekehitysprosessimalleihinsa sopiva muunnelma referenssimallista.

Uudet ohjausjärjestelmien turvallisuusstandardit edellyttävät kvantitatiivista turvallisuuden analyysiä. Tietokonepohjaiset laskentatyökalut nopeuttavat merkittävästi ohjausjärjestelmien turvatoimintojen PL- ja SIL-arvojen laskemista. Toisaalta standardeissa on paljon myös sanallisia kvalitatiivisia vaatimuksia, joiden ryhmittely nopeuttaa ja tehostaa arviointia. KOTOTU-laskentatyökalu auttaa suunnittelijoita esimerkiksi siten, että he voivat kokeilla työkalun avulla erilaisten ratkaisujen vaikutuksia ja tehdä siltä pohjalta turvallisuusteknisiä päätöksiä. Työkalusta on hyötyä erityisesti silloin, kun tilanne toistuu, eli suunniteltavia kohteita on enemmän kuin yksi. Laskentatyökalu sopii myös koulutukseen ja dokumentointiin.

Lähtötietojen saaminen toiminnallisen turvallisuuden tunnuslukujen laskemiseksi on vaikeaa. Tällä hetkellä läheskään kaikille komponenteille ja (turva)laitteille ei ole vielä saatavissa vikataajuuksia ja muita tunnuslukuja, mutta tilanne on muuttumassa. Toisaalta ne tiedot, mitä eri valmistajilta on saatavissa, eivät välttämättä ole yhteismitallisia eli niissä saattaa olla huomattavia eroja.

Standardin SFS-EN ISO 13849-1 kaavat ja rajoitukset ovat hieman pessimistisiä ja siksi erityisesti PL-tasolle ”e” voi olla vaikeata päästä. Tämä liittyy järjestelmiin, joiden laskettu vikaväli on erityisen pitkä (kanavakohtainen rajoitus 100 vuotta) ja joissa käytetään paljon redundanssia (moninkertaisille järjestelmille ei ole nimettyä rakennetta; esim. 1oo3 järjestelmät) ja paljon peräkkäisiä alijärjestelmiä (peräkkäisten alijärjestelmien lukumäärä voi pudottaa PL-tasoa). Koneiden osalta tämä tilanne tulee vastaan melko harvoin, mutta tämä osaltaan ohjaa käyttämään standardia SFS EN 62061, jossa ei ole vastaavia rajoituksia. Ohjelmoitavissa sulautetuissa järjestelmissä voidaan lisäksi tarvita standardia SFS EN 61508-3. Toisaalta monissa konejärjestelmissä on hydrauliikkaa tai pneumatiikkaa, jolloin tarvitaan standardia SFS-EN ISO 13849-1. Käytännössä tämä tarkoittaa sitä, että koneen ohjausjärjes-

telmän turvallisuuden toteuttamisessa standardien yhteiskäyttö on tarpeen siten, että alijärjestelmiä voidaan käsitellä eri standardilla kuin kokonaisuutta.

Kaksi erillistä, toisistaan merkittävästi poikkeavaa standardia muodostavat ongelman standardien soveltajille (esimerkiksi kumpaa standardia lähdetään missäkin tilanteessa soveltamaan). Turvallisuusstandardeja kuitenkin kehitetään koko ajan, ja tulevaisuudessa standardit SFS-EN 13849-1 ja SFS-EN 62061 tullaan todennäköisesti yhdistämään yhdeksi standardiksi. Uudet tai uudistetut eurooppalaiset C-tyypin standardit viittaavat useimmiten PL-tasoihin, joten ne johdattelevat jossakin määrin suunnittelijoita suosimaan SFS-EN 13849-1 -standardia.

Turvallisuuskriittisten ohjelmistojen suunnitteluun tarvitaan hankkeessa kehitetyn työkalukokonaisuuden lisäksi muita työkaluja. Vuonna 1998 voimaan tulleessa IEC 61508-3:ssa esitetään turvallisuusvaatimukset ohjelmistoille sekä tekniikoita, menetelmiä ja toimenpiteitä turvallisuuden toteuttamiseksi ohjelmistoissa. Ohjelmointitekniikat ja -tavat kuitenkin kehittyvät, ja tässä standardissa esitettyjä vaatimuksia ja menetelmiä ohjelmistojen turvallisuuden toteuttamiseksi päivitetään parhaillaan. Ohjelmistojen vastuu turvallisuuden toteuttamisessa kasvaa. Siksi on ajankohtaista tutkia tarkemmin ohjelmistojen turvallisuuden kehittämismenetelmiä ja -tapoja.

Tässä julkaisussa esitetty KOTOTU-prosessityökalu ja KOTOTU-laskentatyökalu toteutettiin suomenkielisinä. Tarvetta on ilmennyt myös englanninkielisille työkaluille. On keskusteltu myös tietokantapohjaisesta työkalusta, jolloin suunnittelutiedon ja turvallisuuteen liittyvän tiedon, mukaan lukien riskianalyysit, tallennuspaikkana olisi tietokanta eikä esimerkiksi Word-dokumentit. ”Paperidokumentit” toimisivat ainoastaan yhtenä tiedon esitysmuotona, esimerkiksi tarkastavaa viranomaista varten, mutta suunnittelijat näkisivät tiedot suoraan suunnittelutyökaluissa.

Lähdeluettelo

Alanen, J., Hietikko, M. & Malm, T. 2004. Safety of digital communications in machines. VTT, Espoo. VTT Tiedotteita 2265 93 s. + liitt. 1 s. http://www.vtt.fi/inf/pdf/tiedotteet/2004/T2265.pdf

Chambers, C., Croll, P.R. & Bowell, M. 1999. A study of incidents involving programmable electronic safety-related systems. Interacting with Computers, 07, Vol. 11, No. 6, s. 597–609. ISSN 0953-5438. http://dx.doi.org/10.1016/S0953-5438(98)00045-9.

FAET; FAEM III, BIA, Prüfung und Zertifierung von "Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten", Stand 28.05.2000 (English version available: Proposal of a Guideline for the Test and Certification of "Bus Systems for the Transmission of Safety Relevant Messages"; Fachausschuss Elektrotechnik, Gustav-Heinemann-Ufer 130, 50698 Köln).

Hauke, M., Schaefer, M., Apfeld, R., Bömer, T., Huelke, M., Borowski, T., Büllesbach, K.-H., Dorra, M., Foermer-Schaefer, H.-G., Grigulewitsch, W., Heimann, K.-D., Köhler, B., Krauß, M., Kühlem, W., Lohmaier, O., Meffert, K., Pilger, J., Reuß, G., Schuster, U. & Zilligen, H. Funktionale Sicherheit von Machinensteuerungen – Anvendung der DIN EN ISO 13849. BGIA Report 2/2008. 260 s.

HSE 2003. Out of control – Why control systems go wrong and how to prevent failure. Vol. HSG238. 2nd. ed. HSE Books. 85. ISBN 0717621928.

IEC 61508-1 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. 1998-12-15 ed. Geneva: International Electrotechnical Commission. 115 s.

IEC 61508-3 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Requirements for software. 1998-12-15 ed. Geneva: International Electrotechnical Commission. 95 s.

IEC 61784-3, 2007. Industrial Communications – Fieldbus Profile – Part 3: Profiles for functional safety communications in industrial networks. 2007-12 edn. Geneva: International Electrotechnical Commission.

IEEE Std 1233 1998. IEEE guide for developing system requirements specifications. 1998th ed. New York: Institute of Electrical and Electronics Engineers. 36 s.

ISO/IEC 26702 IEEE Std 1220-2005 2007. Systems engineering – Application and management of the systems engineering process. First edition 2007-07-15 ed. International Organization for Standardization, International Electrotechnical & Institute of Electrical and Electronics Engineers. c1–88 s.

ISO/IEC/IEEE 12207 2008. Systems and Software Engineering – Software Life Cycle Processes. 2008-02-01 ed. International Organization for Standardization, International Electrotechnical &Institute of Electrical and Electronics Engineers. c1–138 s.

ISO/IEC/IEEE 15288 2008. Systems and Software Engineering – System Life Cycle Processes. 2008-02-01 ed. International Organization for Standardization, International Electrotechnical &Institute of Electrical and Electronics Engineers. c1–84 s.

ISO/TR 14121-2 2007. Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods. 2007-12-03 ed. Geneva: International Organisation for Standardization. 71 s.

Koneasetus VNa 400/2008. Valtioneuvoston asetus koneiden turvallisuudesta. 56 s.

Konedirektiivi. 2006/42/EY. Valtioneuvoston päätös koneiden turvallisuudesta. 63 s.

MIL-HDBK-217F. 1991. Military handbook. Reliability prediction of electronic equipment. Department of Defence, Washington DC. 205 s.

Parviainen, P., Hulkko, H., Kaariainen, J., Takalo, J. & Tihinen, M. 2003. Requirements engineering. Inventory of technologies. Technical Research Centre of Finland, Espoo. VTT Publications 508. 106 s. http://www.vtt.fi/inf/pdf/publications/2003/P508.pdf

SFS-EN 280 2001. Siirrettävät henkilönostimet. Suunnittelulaskelmat. Vakavuus. Rakenne. Turvallisuus. Tarkastukset ja testit. Helsinki: Suomen Standardisoimisliitto SFS ry. 138 s. + Muutos A1, 2006, 22 s.

SFS-EN 954-1 1997. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki: Suomen Standardisoimisliitto SFS ry. 65 s.

SFS-EN 62061 2006. Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. 2006-03-27 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 198 s.

SFS-EN ISO 12100-1 2004. Koneturvallisuus. Perusteet ja yleiset suunnitteluperiaatteet. Osa 1: Peruskäsitteet ja menetelmät. 2004-04-16 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 98 s.

SFS-EN ISO 12100-2 2004. Koneturvallisuus. Perusteet ja yleiset suunnitteluperiaatteet. Osa 2: Tekniset periaatteet. 2004-04-16 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 76 s.

SFS-EN ISO 13849-1 2007. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 2007-06-01 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 177 s.

SFS-EN ISO 13849-2 2004. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. 2004-03-08 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 96 s.

SFS-EN ISO 14121-1 2007. Koneturvallisuus. Riskin arviointi. Osa 1: Periaatteet. 2007-10-15 ed. Helsinki: Suomen Standardisoimisliitto SFS ry. 64 s.

SN 29500. Failure Rates of Components. Saatavana osoitteesta: Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739 München.

Tiusanen, R., Hietikko, M., Alanen, J., Pátkai, N. & Venho, O. 2008. System Safety Concept for Machinery Systems. VTT, Espoo. VTT Tiedotteita 2437. 53 s. http://www.vtt.fi/inf/pdf/tiedotteet/2008/T2437.pdf

Tiusanen, R., Hietikko, M. & Alanen, J. System safety concept for remotely controlled mobile machine systems. 5th International Conference Safety Of Industrial Automated Systems (SIAS 2007). Tokyo, Japan, 12–13 Nov. 2007. Proceedings. JNIOSH; AIST; JMF; JEMA; JARA; NECA (2007), s. 52–57.

Tiusanen, R., Helin, K. & Karjalainen, J. 2005. Operating Hazard Analysis for automated mining machine systems. VTT Publications 582. Human practice in the life cycle of complex systems. Challenges and methods. Nuutinen, M. & Luoma, J. (eds.). VTT, Espoo, 26–32. http://www.vtt.fi/inf/pdf/publications/2005/P582.pdf

Tiusanen, R. & Alanen, J. 2001. HAZOP analysis of a wireless communication system in large scale machine automation applications. 2nd International Conference Safety of Industrial Automated Systems. Bonn, DE, 13–15 Dec. 2001. Berufsgenossenschaftliches Institut für Arbeitssicherheit BIA. San Augustin 2001, s. 89–95.

Liite A: Yhteenveto luokkien vaatimuksista

Luokka	Yhteenveto vaatimuksista	Järjestelmän käyttäytyminen	Turvallisuuden saavuttamiseksi käytettävä periaate	Kunkin kanavan $MTTF_d$	Keskimääräinen diagnostiikan kattavuus DC_{avg}
B	Turvallisuuteen liittyvät ohjausjärjestelmien osat ja/tai niihin liittyvät turvalaitteet sekä niiden komponentit on suunniteltava, rakennettava, valittava, kokoonpantava ja yhdistettävä asiaankuuluvien standardien mukaisesti siten, että ne voivat kestää odotettavissa olevat vaikutukset. Turvallisuuden perusperiaatteita on noudatettava.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen.	Pääasiassa luonnehdittavissa komponenttien valinnalla.	Matala … Keskimääräinen	Nolla
1	Luokan B vaatimuksia on sovellettava. Hyvin koeteltuja komponentteja ja periaatteita on sovellettava.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen, mutta vian esiintymisen todennäköisyys on pienempi kuin luokassa B.	Pääasiassa luonnehdittavissa komponenttien valinnalla.	Korkea	Nolla
2	Luokan B vaatimuksia ja hyvin koeteltuja periaatteita on sovellettava. Koneen ohjausjärjestelmän on tarkistettava turvatoiminnot sopivin väliajoin.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen tarkistusten välisenä aikana. Turvatoiminnon menetys paljastetaan tarkistuksella.	Pääasiassa luonnehdittavissa rakenteella.	Matala … Korkea	Matala … Keskimääräinen
3	Luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita on sovellettava. Turvallisuuteen liittyvät osat on suunniteltava siten, että: – yksittäinen vika missä tahansa näissä osissa ei johda turvatoiminnon menettämiseen, – jos on kohtuudella mahdollista, yksittäinen vika paljastuu.	Yksittäisen vian esiintyessä turvatoiminto suoritetaan aina. Muutamat viat paljastuvat, mutta eivät kaikki. Paljastumattomien vikojen kerääntyminen voi johtaa turvatoiminnon menettämiseen.	Pääasiassa luonnehdittavissa rakenteella.	Matala … Korkea	Matala … Keskimääräinen

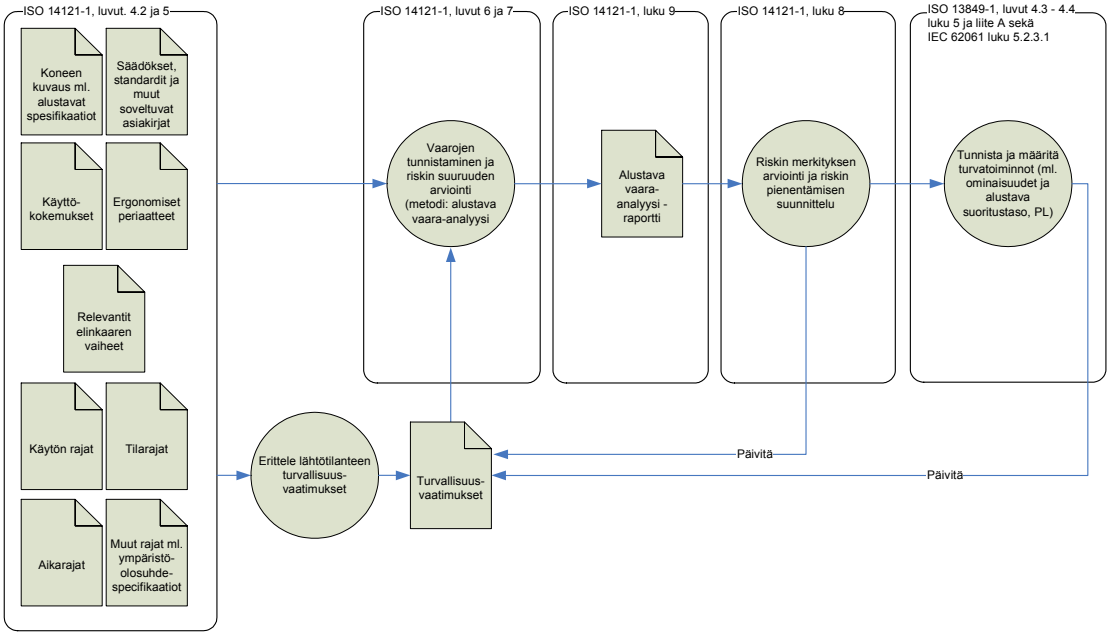
Luokka	Yhteenveto vaatimuksista	Järjestelmän käyttäytyminen	Turvallisuuden saavuttamiseksi käytettävä periaate	Kunkin kanavan $MTTF_d$	Keskimääräinen diagnostiikan kattavuus DC_{avg}
4	Luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita on sovellettava. Turvallisuuteen liittyvät osat on suunniteltava siten, että: – yksittäinen vika missä tahansa näissä osissa ei johda turvatoiminnon menettämiseen, – yksittäinen vika paljastuu turvatoiminnon seuraavan vaateen yhteydessä tai ennen sitä, mutta jos tällainen vikojen paljastuminen ei ole mahdollista, vikojen kerääntyminen ei saa johtaa turvatoiminnon menettämiseen.	Yksittäisen vian esiintyessä turvatoiminto suoritetaan aina. Vikojen kerääntymisen paljastuminen vähentää turvatoiminnon menettämisen todennäköisyyttä (DC on korkea). Viat paljastuvat ajoissa turvatoiminnon menettämisen estämiseksi.	Pääasiassa luonnehdittavissa rakenteella.	Korkea	Korkea, vikojen kerääntyminen otetaan huomioon

Lähde: SFS-EN ISO 13849-1. 2007. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki, Suomen Standardisoimisliitto SFS. 177 s.

Liite B: Relevantit ohjausjärjestelmän turvallisuuteen liittyvät osaprosessit

Alustava vaara-analyysi

Riskianalyysiprosessi aloitetaan alustavalla vaara-analyysillä. Se toteutetaan ISO 14121-1:2007 -standardin mukaisesti. Se kattaa kaikki mahdolliset vaarat, mekaaniset, sähköstä johtuvat, lämpötilasta johtuvat, melusta johtuvat jne. Se ei siis keskity ohjausjärjestelmään. Alustava vaara-analyysi ei ole kaiken kattava tai lopullinen riskianalyysi, vaan sitä seuraa muut riskianalyysivaiheet, kuten käyttötapausanalyysi ja vika- ja vaikutusanalyysi (tai poikkeamatarkastelu, HAZOP). Alustavan vaara-analyysin prosessi on kuvattu kuvassa B1.



Kuva B1. Alustavan vaara-analyysin prosessikuvaus.

Lähtötiedot koostuvat kaikesta taustatiedosta, joka on tarpeellista vaara-analyysin tekemiseen. Lähtötietojen on katettava ne tiedot, jotka vaaditaan standardin ISO 14121:2007 kohdissa 4.2 ja 5.

Ennen vaarojen tunnistamista eritellään lähtötilanteessa tiedetyt turvallisuusvaatimukset. Ne kerätään konedirektiivistä, relevanteista standardeista ja ohjeista, aikaisemmista kokemuksista sekä asiakkaan vaatimuksista. Turvallisuusvaatimuksiin kirjatut suojaustoimenpiteet ovat lähtötietoina itse vaara-analyysiin; ne otetaan huomioon riskiä pienentävinä tekijöinä. Siksi on tärkeää, että turvallisuusvaatimukset toteutetaan systemaattisesti ja jäljitettävästi ohjausjärjestelmän suunnitelmissa.

Vaarojen tunnistaminen ja riskin suuruuden arviointi tehdään standardin ISO 14121-1 lukujen 6 ja 7 ohjeiden mukaisesti alustavan vaara-analyysin-metodia (engl. PHA) käyttäen (lisäohjeita: ISO/TR 14121-2).

Alustavan vaara-analyysin raportti sisältää osittain asiat, joita vaaditaan standardin ISO 14121-1 luvussa 9, mutta varsinainen riskianalyysiraportti, joka sisältää täysin ISO 14121-1 -standardin luvun 9 vaatiman sisällön, tehdään kelpuutusvaiheessa. (Riskianalyysiraportti on yhteenveto kaikista riskianalyysivaiheista sisältäen kaikkien analyysiraporttien tiedot sekä seurantavaiheessa analyysiraporttien perusteella tehtyjen suojaustoimenpiteiden kuvauksen ja lopullisen jäännösriskin arvion.)

Alustavan vaara-analyysin seurantavaiheessa tehdään riskin merkityksen arviointi ISO 14121-1 -standardin luvun 8 ohjeiden mukaisesti. Arvioinnin perusteella määritellään riskin pienentämisen keinot (suojaustoimenpiteet). Ne kirjataan turvallisuusvaatimuksiin.

Seurantavaiheessa voidaan tunnistaa tarve turvatoiminnoille. Turvatoiminnot määritellään ISO 13849-1 -standardin luvun 5 ja kohtien 4.3–4.4 mukaisesti sekä sen liitteen A mukaisesti. Katso myös standardin IEC 62061 kohta 5.2.3.1, missä on yksityiskohtainen lista asioista, jotka tarvitaan turvallisuuteen liittyvien ohjaustoimintojen toiminnallisten vaatimusten erittelyyn. Turvatoimintojen määrittelystä on erillinen ohje[10]. Turvatoimintojen spesifikaatiot kirjataan turvallisuusvaatimuksiin tai niihin tehdään ainakin viittaus turvallisuusvaatimuksista.

Seurantavaihe dokumentoidaan omalla lomakkeella, joka on analyysilomakkeen jatkeena lisäsarakkeina tai itsenäisenä lomakkeena linkitettynä analyysilomakkeen riveihin (vaaroihin). Täytetty analyysilomake ja sen seurantalomake ovat analyysiraportin liitteinä. Analyysiraportin liitteenä olevaa seurantalomaketta siis päivitetään seurantavaiheessa.

HUOM! Alustava vaara-analyysi tehdään koko koneelle, ei ainoastaan ohjausjärjestelmälle. Vaara-analyysiä ei tarvitse tehdä puhtaalta pöydältä, jos ko. konetyypille on jo tehty vaara-analyysi ja se on saatavilla (esim. C-tyypin standardi). Siinä tapauksessa vaara-analyysin tulokset tai C-tyypin standardin vaatimukset on siirrettävä turvallisuusvaatimuksiksi.

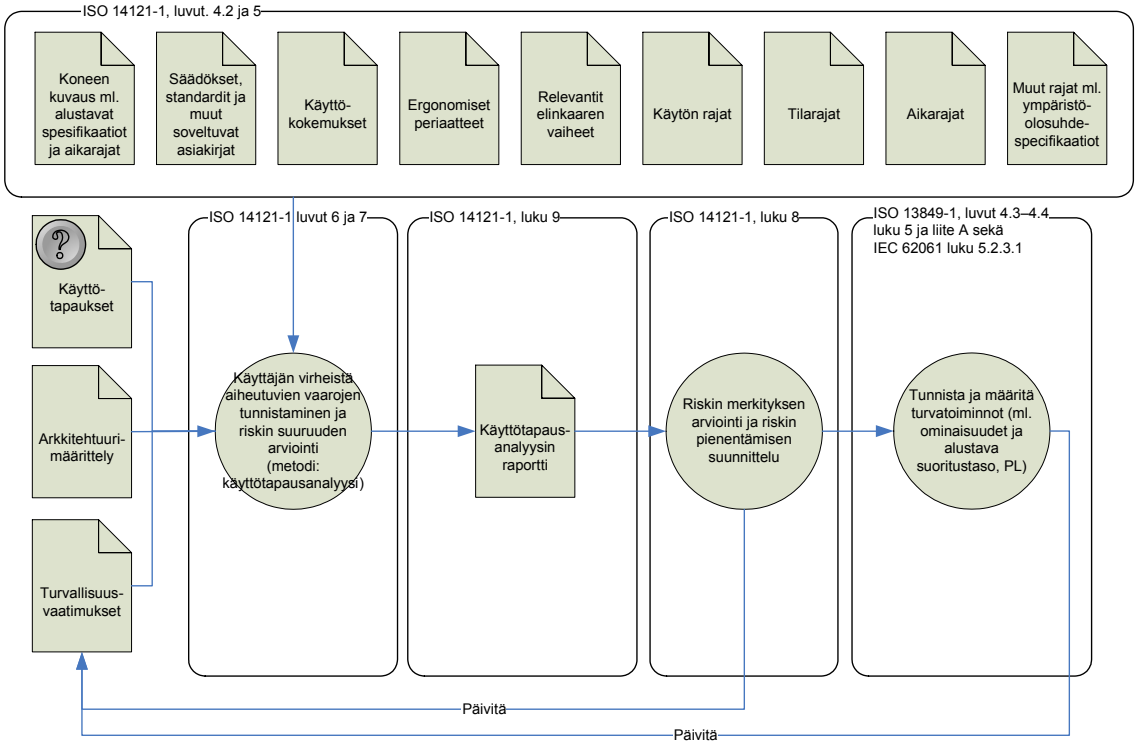
Riskien pienentämiskeinojen suunnittelu alustavan vaara-analyysin jälkeen

Vaara-analyysin perusteella tarpeelliseksi havaitut tarvittavat riskin pienentämiskeinot suunnitellaan noudattaen ISO 12100-1 -standardin kohtia 5.4 ja 5.5 sekä koko ISO 12100-2 -standardia. Lisäksi noudatetaan ISO 13849-1 -standardia (erityisesti lukua 6) sekä ISO 13849-2 -standardin liitteitä A–D turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa.

Käyttötapausanalyysi

Käyttötapausanalyysi kohdentaa riskianalyysin ihminen–kone-vuorovaikutukseen koko elinkaaren aikana. Käyttötapausanalyysin prosessi on kuvattu kuvassa B2.

[10] Ei sisälly tähän julkaisuun. Esimerkki turvatoiminnon määrittelystä löytyy kohdasta 3.2.4 (taulukko 7).



Kuva B2. Käyttötapausanalyysin prosessikuvaus.

Käyttötapausanalyysiin käytetään samoja lähtötietoja kuin alustavaan vaara-analyysiinkin, paitsi että tässä vaiheessa käyttötapauskuvausten ja arkkitehtuurimäärittelyn oletetaan olevan valmiina. Turvallisuusvaatimuksiin kirjatut suojaustoimenpiteet ovat lähtötietoina itse käyttötapausanalyysia varten; ne otetaan huomioon riskiä pienentävinä tekijöinä. Siksi on tärkeää, että turvallisuusvaatimukset toteutetaan systemaattisesti ja jäljitettävästi ohjausjärjestelmän suunnitelmissa. Tässä vaiheessa relevantteja turvallisuusvaatimuksia ovat esimerkiksi vaatimukset käyttää suojuksia; tällaiset vaatimukset vaikuttavat käyttötapauksiin ja siten myös käyttötapausanalyysiin.

Analyysi tehdään ISO 14121-1 -standardin lukujen 6 ja 7 ohjeiden mukaisesti yleisemmin tunnettua toimintovirheanalyysimetodia noudattaen; erona tässä on ainoastaan tapa kuvata analysoitavat vaiheet käyttötapauskuvauksina. Analyysissä tarvittavat käyttötapauskuvaukset tehdään erillisen ohjeen mukaisesti. Käyttötapauskuvaukset sisältävät suuren osan ISO 14121-1 -standardin vaatimasta tiedosta. Käyttötapauskuvauksesta on erillinen ohje[11].

Käyttötapausanalyysin raportti sisältää osittain asiat, joita vaaditaan standardin ISO 14121-1 luvussa 9, mutta varsinainen riskianalyysiraportti, joka sisältää täysin ISO 14121-1 -standardin luvun 9 vaatiman sisällön, tehdään kelpuutusvaiheessa. (Riskianalyysiraportti on yhteenveto kaikista riskianalyysivaiheista sisältäen kaikkien analyysiraporttien tiedot sekä seurantavaihees-

[11] Ei sisälly tähän julkaisuun. Esimerkki käyttötapauskuvauksesta löytyy liitteestä D.

sa analyysiraporttien perusteella tehtyjen suojaustoimenpiteiden kuvauksen ja lopullisen jäännösriskin arvion.)

Käyttötapausanalyysin seurantavaiheessa tehdään riskin merkityksen arviointi ISO 14121-1 -standardin luvun 8 ohjeiden mukaisesti. Arvioinnin perusteella määritellään riskin pienentämisen keinot (suojaustoimenpiteet). Ne kirjataan turvallisuusvaatimuksiin.

Koska käyttötapauskuvaukset ja arkkitehtuurimäärittely ovat valmiina, on aika tunnistaa toiminnot, jotka tarvitaan käyttötapausten toteuttamiseen. Sekä käyttötapausanalyysin että vaaraanalyysin tuloksien perusteella on mahdollista tunnistaa ja määrittää turvatoiminnot[12] kaikkien toimintojen joukosta tai niiden lisäksi. Jos toimintoa ei voi selkeästi osoittaa ei-turvallisuuskriittiseksi, se merkitään alustavasti turvatoiminnoksi, että se tulisi analysoitua VVA/HAZOP/VPA-analyyseissä (ks. luku ”Toimintojen analyysi”). Turvatoiminnot määritellään ISO 13849-1 -standardin kohtien 5 ja 4.3–4.4 mukaisesti sekä sen liitteen A mukaisesti. Katso myös standardin IEC 62061 luku 5.2.3.1, jossa on yksityiskohtainen lista asioista, jotka tarvitaan turvallisuuteen liittyvien ohjaustoimintojen toiminnallisten vaatimusten erittelyyn. Turvatoimintojen määrittelystä on erillinen ohje[13]. Turvatoimintojen spesifikaatiot kirjataan turvallisuusvaatimuksiin tai niihin tehdään ainakin viittaus turvallisuusvaatimuksista.

Seurantavaihe dokumentoidaan omalla lomakkeella, joka on analyysilomakkeen jatkeena lisäsarakkeina tai itsenäisenä lomakkeena linkitettynä analyysilomakkeen riveihin (vaaroihin). Täytetty analyysilomake ja sen seurantalomake ovat analyysiraportin liitteinä. Analyysiraportin liitteenä olevaa seurantalomaketta siis päivitetään seurantavaiheessa.

HUOM.! Käyttötapausanalyysi tehdään koko koneelle, ei ainoastaan ohjausjärjestelmän osuudelle. Käyttötapausanalyysiä ei tarvitse tehdä, jos ko. konetyypille on jo tehty käyttötapausanalyysi ja se on saatavilla. Siinä tapauksessa käyttötapausanalyysin tulokset on siirrettävä vaatimusmäärittelyihin.

Riskien pienentämiskeinojen suunnittelu käyttötapausanalyysin jälkeen

Käyttötapausanalyysin perusteella tarpeelliseksi havaitut tarvittavat riskin pienentämiskeinot suunnitellaan noudattaen ISO 12100-1 -standardin kohtia 5.4 ja 5.5 sekä koko ISO 12100-2 -standardia. Lisäksi noudatetaan ISO 13849-1 -standardia (erityisesti lukua 6) ja ISO 13849-2 -standardin liitteitä A–D turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa.

---

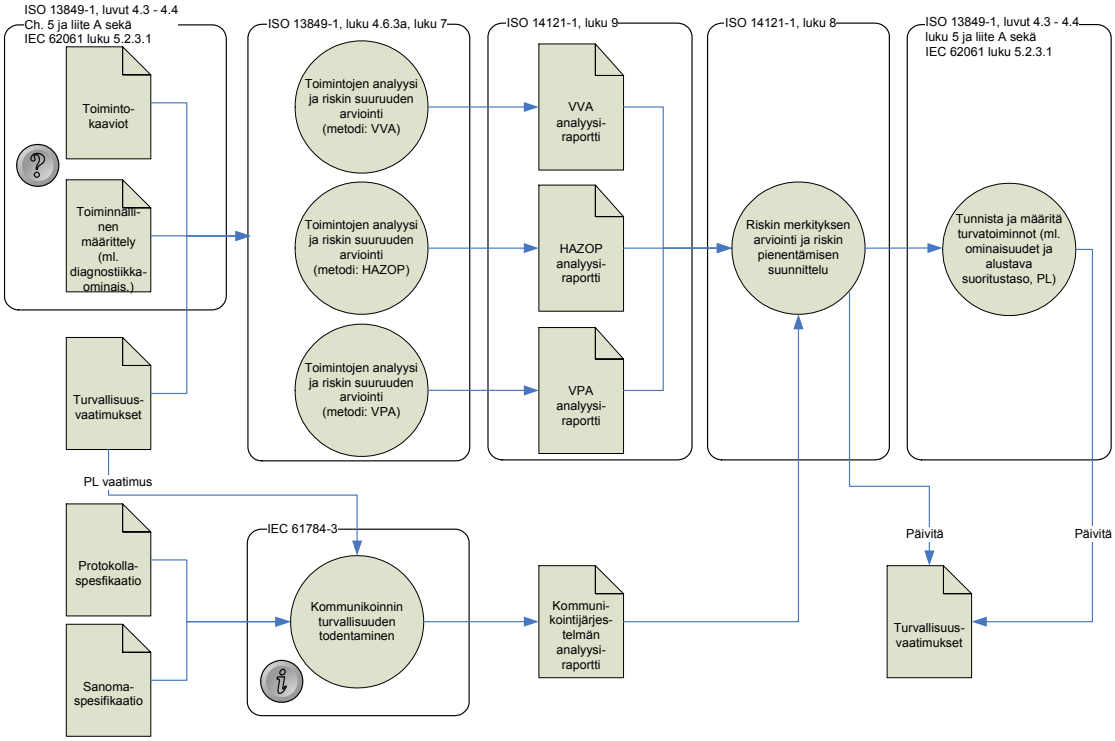
[12] Huomioi turvatoiminnon määritelmä: “koneen toiminto, jonka vikaantuminen voi aiheuttaa välittömän riskin (riskien) kasvamisen” (ISO 13849-1). IEC 62061 määrittelee turvatoiminnon samoin, mutta ei käytä sitä varsinaisessa tekstissään, vaan käyttää termiä ”turvallisuuteen liittyvä ohjaustoiminto”; mikä määritellään näin: ”määrätyllä turvallisuuden eheyden tasolla olevan turvallisuuteen liittyvän sähköisen ohjausjärjestelmän toteuttama ohjaustoiminto, minkä tarkoituksena on säilyttää koneen turvallinen tila tai estää riskin (riskien) välitön kasvaminen”.

[13] Ei sisälly tähän julkaisuun. Esimerkki turvatoiminnon määrittelystä löytyy luvusta 3.2.4 (taulukko 7).

Toimintojen analyysi

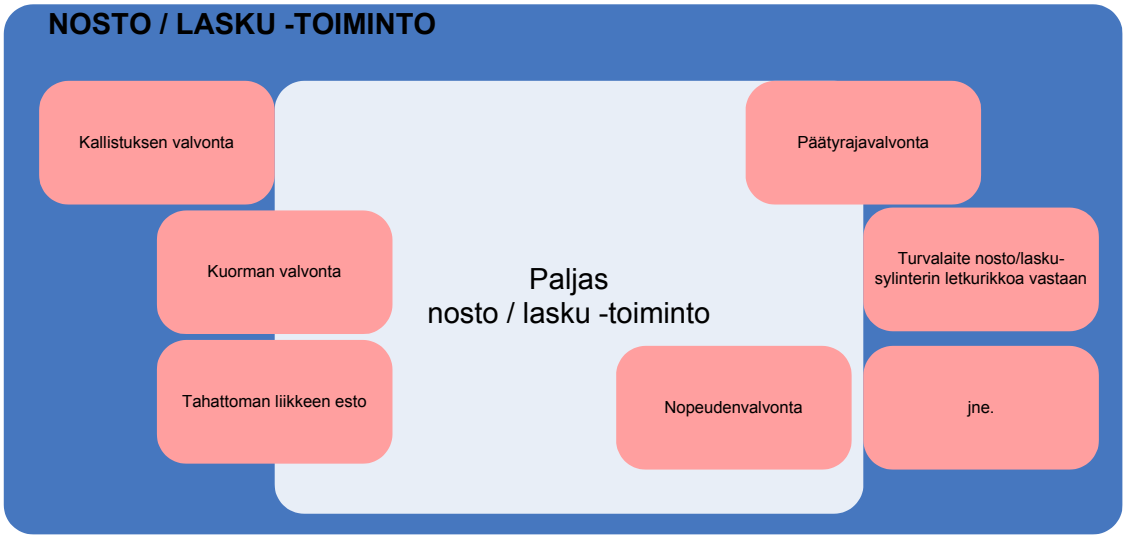
Riskianalyysien kolmas ja viimeinen vaihe kohdistuu toimintoihin. Se koostuu vika- ja vaikutus -analyysistä (VVA) tai HAZOP-analyysistä tai niiden yhdistelmistä. Myös vikapuuanalyysejä (VPA) voidaan tehdä tässä vaiheessa. HAZOP voidaan tehdä joko signaalitasolla tai toimintotasolla. Signaalitasolla analyysitapauksena on signaalin poikkeama, esimerkiksi jonkin mittauksen tai kytkintiedon poikkeama; toimintotasolla tarkastellaan toiminnon poikkeamaa, esim. puomi liikkuu liian nopeasti. Tapaturmaskenaario voisi olla esimerkiksi seuraava: nopeusanturi rikkoutuu, nopeusmittaus näyttää liian pientä arvoa, puomia ajetaan liian nopeasti, koneen stabiliteetti pettää, kone kaatuu ja näiden seurauksena kuljettaja loukkaantuu. Tässä VVA lähtee liikkeelle nopeusanturin rikkoutumisesta, signaalipohjainen HAZOP nopeusmittauksen poikkeamasta, toimintopohjainen HAZOP puomin ohjaustoiminnan poikkeamasta, ja VPA taas lähtee liikkeelle koneen kaatumisesta.

Vaiheen kuvaus on esitetty kuvassa B3.



Kuva B3. VVA- / VPA- / HAZOP -analyysien prosessikuvaus.

Tämä analyysivaihe keskittyy toimintoihin. Järjestelmä sisältää sekä normaaleja käyttötoimintoja että turvatoimintoja. Käyttötoiminnolla tarkoitetaan tässä esimerkiksi nostolavan laskuja nostotoimintoa. Siihen liittyy joukko turvatoimintoja, joilla käyttötoiminta tehdään turvalliseksi (ks. kuva B4).



Kuva B4. Varsinainen käyttötoiminto ja siihen liittyviä turvatoimintoja.

Analyysi voidaan tehdä, ja kannattaakin tehdä, aluksi poikkeamatarkasteluna varsinaiselle käyttötoiminnolle; myöhemmin, ehkä vasta kelpuutusvaiheessa voidaan tehdä tarvittaessa VVA- tai signaalitason HAZOP-turvatoiminnoille. Joka tapauksessa kelpuutusvaiheessa analyysiä päivitetään sen mukaan, mitä korjaustoimenpiteitä on tehty suunnitteluvaiheen HAZOP- tai VVA- tai VPA-analyysin seurannan perusteella.

Toiminnot on ennen tätä vaihetta määritelty ja turvatoiminnot on ainakin alustavasti tunnistettu. Täten toimintokuvaukset toimintokaavioineen ovat olemassa, joten VVA, VPA tai HAZOP voidaan suorittaa. VVA tehdään standardin IEC 60812 ohjeiden perusteella ja HAZOP standardin IEC 61882 perusteella.

VVA-, VPA- ja HAZOP-analyysit saattavat paljastaa uusia vaaroja. Samoin analysoinnin kohteena olevien turvatoimintojen suoritustason vaatimukseen (PL_r) voi tulla muutoksia, joko alaspäin tai ylöspäin.

Tässä yhteydessä analysoidaan myös kommunikointijärjestelmän turvallisuus IEC 61784-3 -standardin mukaisesti.

HAZOP-, VVA- tai VPA-analyysiraportti sekä kommunikointijärjestelmän analyysiraportti sisältää osittain asiat, joita vaaditaan ISO 14121-1 -standardin luvussa 9, mutta varsinainen riskianalyysiraportti, joka sisältää täysin ISO 14121-1 -standardin luvun 9 vaatiman sisällön, tehdään kelpuutusvaiheessa. (Riskianalyysiraportti on yhteenveto kaikista riskianalyysivaiheista sisältäen kaikkien analyysiraporttien tiedot sekä seurantavaiheessa analyysiraporttien perusteella tehtyjen suojaustoimenpiteiden kuvauksen ja lopullisen jäännösriskin arvion.)

Toimintoanalyysin seurantavaiheessa tehdään riskin merkityksen arviointi ISO 14121-1 -standardin luvun 8 ohjeiden mukaisesti. Arvioinnin perusteella määritellään riskin pienentämisen keinot (suojaustoimenpiteet). Ne kirjataan turvallisuusvaatimuksiin.

Toimintoanalyysinkin aikana voidaan tunnistaa tarve uusille turvatoiminnoille. Turvatoiminnot määritellään ISO 13849-1 -standardin kohtien 5 ja 4.3–4.4 mukaisesti sekä sen liitteen A mukaisesti. Katso myös standardin IEC 62061 kohta 5.2.3.1, jossa on yksityiskohtainen lista asioista, jotka tarvitaan turvallisuuteen liittyvien ohjaustoimintojen toiminnallisten vaatimusten

erittelyyn. Turvatoimintojen määrittelystä on erillinen ohje[14]. Turvatoimintojen spesifikaatiot kirjataan turvallisuusvaatimuksiin tai niihin tehdään ainakin viittaus turvallisuusvaatimuksista.

Seurantavaihe dokumentoidaan omalla lomakkeella, joka on analyysilomakkeen jatkeena lisäsarakkeina tai itsenäisenä lomakkeena linkitettynä analyysilomakkeen riveihin (vaaroihin). Täytetty analyysilomake ja sen seurantalomake ovat analyysiraportin liitteinä. Analyysiraportin liitteenä olevaa seurantalomaketta siis päivitetään seurantavaiheessa.

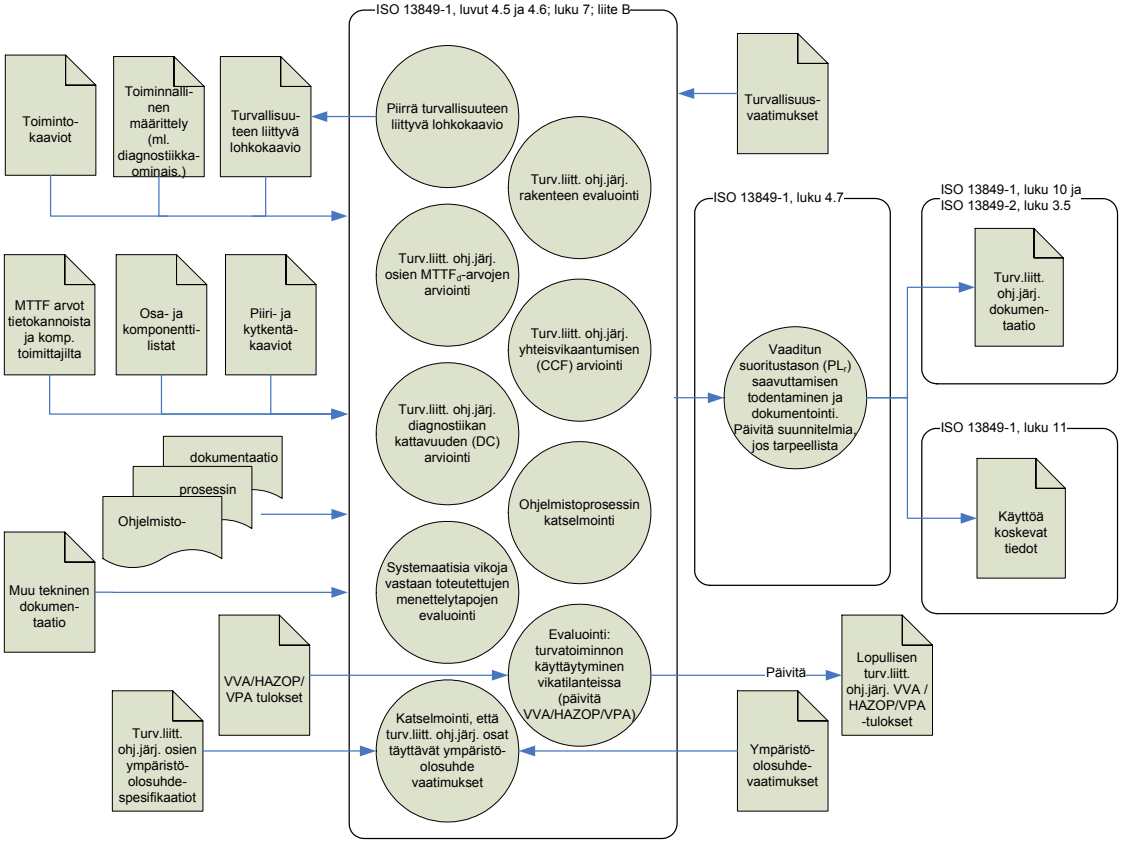
Riskien pienentämiskeinojen suunnittelu VVA-, VPA- JA HAZOP-analyysien jälkeen

VVA-, VPA- ja HAZOP-analyysien perusteella tarpeelliseksi havaitut tarvittavat riskin pienentämiskeinot suunnitellaan noudattaen ISO 12100-1 -standardin kohtia 5.4 ja 5.5 sekä koko ISO 12100-2 -standardia. Lisäksi noudatetaan ISO 13849-1 -standardia (erityisesti kohtia 4.6 ja 6) ja ISO 13849-2 -standardin liitteitä A–D turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa. Kommunikointianalyysin perusteella havaitut tarvittavat riskin pienentämiskeinot valitaan IEC 61784-3 -standardin kohdassa 5.4 ja 5.5 esitellyistä puolustuskeinoista. Puolustuskeinot toteutetaan standardissa olevien ohjeiden mukaisesti.

Suoritustason (PL) evaluointi

Turvallisuuteen liittyvän ohjausjärjestelmän suunnitelma on nyt viimeisessä luonnosvaiheessa, joten on aika tehdä sen suoritustason (PL) evaluointi. Tässä vaiheessa tarvittavat lähtötiedot ovat nähtävissä kuvassa B5.

[14] Ei sisälly tähän julkaisuun. Esimerkki turvatoiminnon määrittelystä löytyy luvusta 3.2.4 (taulukko 7).



Kuva B5. Suoritustason (PL) evaluoinnin prosessikuvaus.

Suoritustason evaluointi (jota voitaisiin kutsua todentamiseksi) koostuu tehtävistä, jotka on lueteltu ISO 13849-1 -standardin kohdassa 4.5.1 käyttäen hyväksi standardin ISO 13849-1 kohtien 4.5 ja 4.6 sekä luvun 7 ohjeita. Ensimmäinen tehtävä on piirtää turvatoiminnoista turvallisuuteen liittyvä lohkokaavio. Ohje siihen löytyy standardin ISO 13849-1 liitteestä B.

Todentaminen, että suunniteltu turvallisuuteen liittyvän ohjausjärjestelmän osan suoritustaso (PL) saavuttaa vaaditun suoritustason (PL_r), tehdään ISO 13849-1 -standardin luvun 4.7 mukaisesti.

Tässä yhteydessä turvallisuuteen liittyvä ohjausjärjestelmän osa dokumentoidaan ISO 13849-1 -standardin luvun 10 ja ISO 13849-2 -standardin kohdan 3.5 mukaisesti. Dokumentin sisältö näkyy tarkemmin kelpuutusprosessin yhteydessä (ks. kuva).

Suunnitelmia päivitetään, jos vaadittua suoritustasoa ei saavuteta. Korjaavat toimenpiteet viedään suunnitteluun vaatimusmäärittelyjen kautta (ei näy kuvassa B5).

Turvatoimintojen käyttäytyminen vikatilanteessa on jo pääosin tehty aikaisemmin VVA-/HAZOP-vaiheessa, joten tässä vaiheessa VVA-/HAZOP-analyysejä ainoastaan päivitetään.

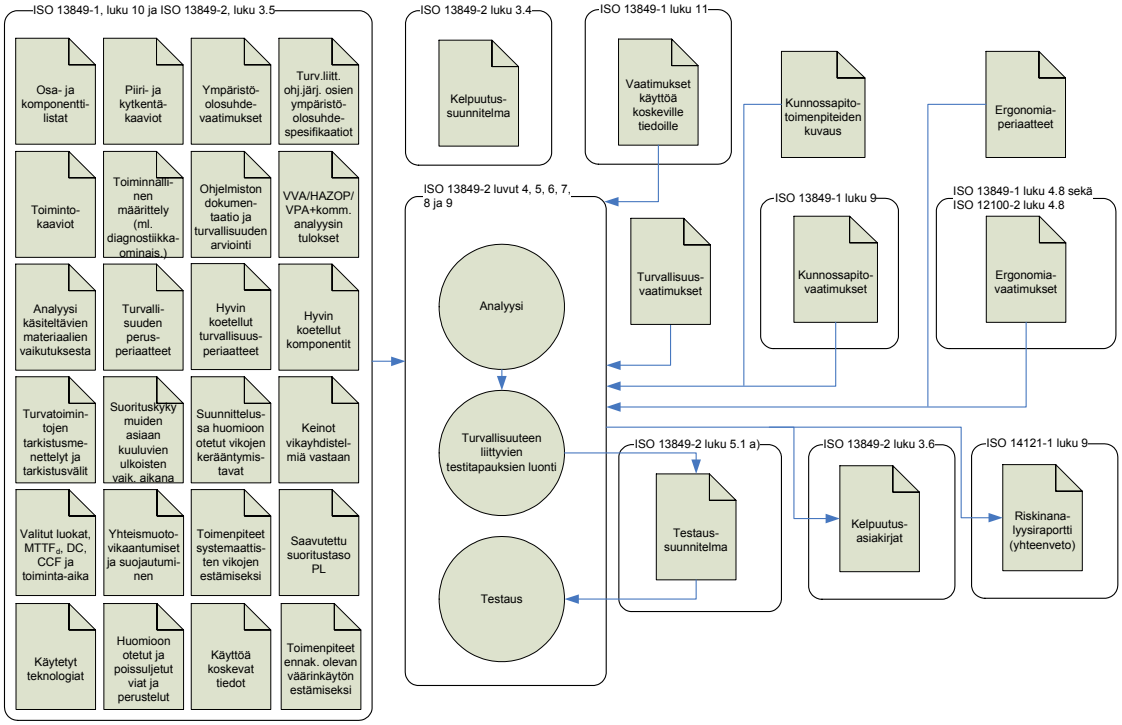
Turvallisuuteen liittyvät ohjausjärjestelmän osat dokumentoidaan, kuten standardissa ISO 13849-1 esitetään. Suuri osa tästä informaatiosta on valmiina kuvan B5 lähtötietodokumenteissa.

Riskien pienentämiskeinojen suunnittelu suoritustason evaluoinnin jälkeen

Jos saavutettu suoritustaso (PL) ei yllä tavoitetasolle PL_r, suunnitelmia päivitetään noudattaen ISO 12100-1 -standardin kohtia 5.4 ja 5.5 sekä koko ISO 12100-2 -standardia. Lisäksi noudatetaan ISO 13849-1 -standardia (erityisesti kohtia 4.6 ja 6) sekä ISO 13849-2 -standardin liitteitä A–D turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa.

Kelpuutus

Viimeisenä prosessivaiheen on kelpuutus. Se on kuvattu kuvassa B6.



Kuva B6. Kelpuutusvaiheen prosessikaavio.

Kelpuutus aloitetaan tekemällä kelpuutussuunnitelma noudattaen standardin ISO 13849-2 kohtaa 3.4. Kelpuutussuunnitelma on osa turvallisuussuunnitelmaa, mutta se voi olla kuitenkin myös itsenäinen dokumentti.

Kelpuutuksen tekevien henkilöiden olisi oltava riippumattomia järjestelmän suunnittelusta, mutta heidän ei välttämättä tarvitse olla muusta organisaatiosta.

Kuvan B6 mukaiset lähtötiedot kattavat ISO 13849-1 -standardin luvun 10 ja ISO 13849-2 -standardin kohdan 3.5 vaatimukset, mutta myös asiat, jotka vaaditaan ISO 13849-1 -standardin luvussa 9 (kunnossapitovaatimukset) ja ISO 13849-1 – ja ISO 12100-2 -standardien kohdassa 4.8 (ergonomiset periaatteet). Tässä yhteydessä katselmoidaan myös käyttöä koskevat tiedot, jotka on tehty aikaisemmissa prosessivaiheissa ISO 13849-1 -standardin mukaisesti.

Kelpuutus suoritetaan ISO 13849-2 -standardin lukujen 4, 5, 8 ja 9 mukaisesti. On huomioitava, että kelpuutuksessa vaadittava analyysityö on jo suurelta osin tehty VVA- ja HAZOP-

analyyseissä, joten niitä tarvitsee vain päivittää. Jos jokin turvatoiminnoista täytyy analyysien lisäksi testata (esim. VVA/HAZOP-analyysien perusteella), kirjoitetaan testaussuunnitelma. Testauksen voi suorittaa turvallisuusprosessista vastuussa olevat henkilöt tai testit voidaan sisällyttää muiden testien joukkoon, jolloin ne suoritetaan testaushenkilöstön toimesta.

Kelpuutusasiakirjat tehdään ISO 13849-2 -standardin kohdan 3.6 mukaisesti.

Tässä vaiheessa tehdään myös yhteenveto riskianalyyseistä; dokumentin sisältö tehdään ISO 14121-1 -standardin luvun 9 mukaisesti. Riskianalyysiraportti on yhteenveto kaikista riskianalyysivaiheista sisältäen kaikkien analyysiraporttien tiedot sekä seurantavaiheessa analyysiraporttien perusteella tehtyjen suojaustoimenpiteiden kuvauksen ja lopullisen jäännösriskin arvion.

Riskien pienentämiskeinojen suunnittelu kelpuutuksen jälkeen

Jos kelpuutus antaa negatiivisen tuloksen, suunnitelmia päivitetään noudattaen ISO 12100-1 -standardin kohtia 5.4 ja 5.5 sekä koko ISO 12100-2 -standardia. Lisäksi noudatetaan ISO 13849-1 -standardia (erityisesti lukuja 4.6 ja 6) ja ISO 13849-2 standardin liitteitä A–D turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa.

Liite C: Vaatimusmäärittelydokumentin sisällysluettelo

Liite D: Käyttötapauskuvauksen esimerkki

Käyttötapauksen nimi:		**Työtason nostaminen työtasolta ohjattuna korkeudelta A korkeudelle B**		
Tunniste:		**USEC759**		
Versio	**PVM**	**Status**	**Tekijä(t)**	**Kuvaus**
0.1	24.04.2008	Luonnos	J. Alanen	Luotu
Tilanteen kuvaus		Testaus, Käyttöönotto, Koulutus, Normaali operointi, Asetusten teko, Vianhaku, Puhdistus		
Toimijat		Koneen käyttäjä, Asentaja, Huoltomies, Kouluttaja		
Muut henkilöt vaara-alueella		Rakennus- tai varastotyömiehet		
Toimijan esiehdot		Perehtyminen käyttöohjeisiin, ei koulutusvaatimusta		
Käyttötapauksen esiehdot		Hätä-seis on vapautettu. Nostolaite on käynnistetty ja ohjauspaikka (työtaso) on valittu (ks. käyttötapaus USEC757). Toimija on työtasolla (ks. käyttötapaus USEC758)		

Tapauksen kulku		1. Jos moottori ei ole vielä käynnissä, se voidaan käynnistää ohjauspaneelissa olevasta start-painikkeesta
		2. Valitaan toimintojen valintakytkimestä pöydän nosto- ja laskutoiminta
		{
		3. Ohjaussauvasta työnnetään eteenpäin, jos halutaan ylöspäin, tai vedetään itseen päin, jos halutaan alaspäin
		4. Kun haluttu korkeus on saavutettu, vapautetaan ohjaussauva
		5. Vallitseva korkeus voidaan panna muistiin painamalla pitkään jompaa kumpaa pikavalintanappia A tai B
		} TAI
		{
		6. Valitaan pikavalinnalla haluttu korkeus, johon pöytä ajaa automaattisesti
		}
		7. Kuljettaja voi seurata nostokorkeutta ohjauspaneelin numeronäytöstä
		Molemmissa tapauksissa nosto/lasku tapahtuu kaksin käsin tai kuolleenmiehen kytkimen periaatteella: taso ei lähde liikkeelle, jos kuolleenmiehenkytkintä ei paineta
		[Poikkeus: Nosto/lasku toimintoa ei sallita]		

Poikkeukset		Nosto/lasku -toimintoa ei sallita: Nosto/lasku -toiminta on estetty, jos kuorma on liian suuri tai työtaso on jommassa kummassa päädyssä		
Lopputulema		Nostopöydän korkeus on halutulla tasolla		
Suoritustaajuus		Päivittäin (8 h) tehdään noin 100 siirtoa (nostoa tai laskua)		
Ohjeet		Nosto/lasku -toiminto on kuvattu käyttöohjeessa Doc1234.PDF kappaleessa 2.4.5		
Kommentit		Pitäisi vielä miettiä, olisiko ohjaussauvan sijasta painonappiratkaisu ergonomisesti ja turvallisuusmielessäkin parempi.		
Alustava riskiskenaario		Litistymisen vaara ilmeinen, esim. pikavalinta ajaa odottamattomaan korkeuteen tai liike jatkuu tahattomasti. Laitevaurio (palovaara?) myös mahdollinen, jos ohjainsauvaa pidetään käännettynä, vaikka päätetaso on jo saavutettu. Liikkeitä ei saisi tapahtua, kun moottori käynnistetään tai kun valitaan nosto/lasku-toiminto.		**Analysoidaan X**

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2485
VTT–TIED–2485

Tekijä(t)
Marita Hietikko, Timo Malm & Jarmo Alanen

Nimeke

Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen

Tiivistelmä

Koneiden ja niiden ohjausjärjestelmien turvallisuusvaatimusten määrittelyvaiheessa tehdään ratkaisuja, joilla on vaikutusta koneen koko myöhempien elinkaaren vaiheiden turvallisuuteen. Turvallisuusvaatimusten määrittelyssä tehtyjen virheiden on havaittu olevan syynä suureen osaan tapaturmista.

Tähän julkaisuun on kerätty KOTOTU-hankkeen (Koneiden ohjausjärjestelmien toiminnallinen turvallisuus) tulokset. Hankkeessa kehitettiin turvallisuussuunnittelun toimintamalli eli KOTOTU-prosessityökalu, jonka avulla koneiden ohjausjärjestelmien turvallisuuteen liittyvät riskit voidaan arvioida ja turvallisuusvaatimusten määrittely toteuttaa koneen ja sen ohjausjärjestelmän elinkaaren varhaisessa vaiheessa. Hankkeessa kehitettiin myös suunnittelijan työtä helpottava KOTOTU-laskentatyökalu, jonka avulla saavutettu turvallisuustaso (suoritustaso = PL) voidaan laskea ja arvioida standardin SFS-EN ISO 13849-1 mukaan. Työkalut soveltuvat ohjausjärjestelmien turvallisuuden suunnitteluun, arviointiin ja koulutukseen. Julkaisussa on kuvattu näiden työkalujen käyttö ja soveltaminen sovellusesimerkin avulla. Julkaisu antaa ohjeita myös muiden uusimpien koneiden ohjausjärjestelmien turvallisuutta käsittelevien standardien soveltamiseen.

ISBN
978-951-38-7298-4 (URL: http://www.vtt.fi/publications/index.jsp)

Avainnimeke ja ISSN	Projektinumero
VTT Tiedotteita – Research Notes 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	

Julkaisuaika	Kieli	Sivuja
Toukokuu 2009	suomi	75 s. + liitt. 14 s.

Projektin nimi	Toimeksiantaja(t)
KOTOTU	Työsuojelurahasto

Avainsanat	Julkaisija
machines, functional safety, control systems	VTT PL 1000, 02044 VTT Puh. 020 722 4520 Faksi 020 722 4374

Series title, number and
report code of publication

VTT Research Notes 2485
VTT–TIED–2485

Author(s)
Marita Hietikko, Timo Malm & Jarmo Alanen

Title

Functional safety of machine control systems. Instructions and tools for the creation of standard safety process

Abstract

In the specification phase of a machine and its control system such decisions are frequently made that affect the safety of all the later life cycle phases of the machine. Errors made in the definition of safety requirements are found out to be a reason for large amount of accidents.

This report includes results of the project “Functional safety of machine control systems” (KOTOTU). In this project a functional model for the safety design, i.e. KOTOTU process tool, was developed, which helps safety designers to assess safety risks and define safety requirements of a machine control system in the early phase of system life cycle. In addition, in this project a KOTOTU calculation tool was developed, which helps the designer for assessing and calculating the attained performance level (PL) according to ISO 13849-1 standard. These tools can be applied to control system safety design, evaluation and education. The use and application of these tools are described in this report with the aid of an example system. This report gives instructions also for the application of the newest control system safety related standards.

ISBN
978-951-38-7298-4 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN
VTT Tiedotteita – Research Notes
1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

Project number
16458

Date	Language	Pages
May 2009	Finnish, eng. abstr.	75 p. + app. 14 p.

Name of project
KOTOTU

Commissioned by
Työsuojelurahasto

Keywords
machines, functional safety, control systems

Publisher
VTT Technical Research Centre of Finland
P.O.Box 1000, FI-02044 VTT, Finland
Phone internat. +358 20 722 4520
Fax +358 20 722 4374

VTT LUO TEKNOLOGIASTA LIIKETOIMINTAA
Teknologia- ja liiketoimintaennakointi • Strateginen tutkimus • Tuote- ja palvelukehitys • IPR ja lisensointi
• Asiantuntijaselvitykset, testaus, sertifiointi • Innovaatio- ja teknologiajohtaminen • Teknologiakumppanuus

Julkaisussa kuvataan koneiden ohjausjärjestelmien turvallisuussuunnittelun toimintamalli ja laskentatyökalu, joilla voidaan suunnitella, laskea ja arvioida ohjausjärjestelmiä standardin SFS-EN ISO 13849-1 mukaisesti. Aihetta tarkastellaan sovellusesimerkin avulla. Ohjeita esitetään myös muiden uusimpien koneiden ohjausjärjestelmien turvallisuutta käsittelevien standardien soveltamiseen.

ISBN 978-951-38-7298-4 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)