Aleksi Jussila

Teollisuusrobotin automaation turvallistamisen todentaminen ja kehittäminen

Insinööri (AMK)

Konetekniikka

Kevät 2018

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä(t): Jussila Aleksi

Työn nimi: Teollisuusrobotin automaation turvallistamisen todentaminen ja kehittäminen

Tutkintonimike: Insinööri (AMK), konetekniikka

Asiasanat: Teollisuusrobotti, turvallistaminen, automaatio, poikkeama-analyysi

Työn toimeksiantaja Prometec Tools Oy on laitevalmistaja, jonka valmistamalla laitteella pyritään ratkaisemaan ongelma biopolttoaineiden näytteenotossa. Prometec Tools on valmistanut robottisolun tähän käyttötarkoitukseen. Suomen lainsäädäntö määrää, että laitevalmistajan tulee valmistaa turvallisia laitteita ja todentaa niiden turvallisuus, sekä antaa määrityksiä, millainen laitteen tulee olla. Standardit tarkentavat lainsäädäntöä ja ohjaavat käyttäjää yleisesti hyväksyttyjen ohjeiden mukaisesti. Standardeja hyödyntämällä voidaan luotettavasti todentaa ja varmistaa laitteen turvallisuus.

Prometec Tools on CE-merkinnyt ja todentanut laitteensa turvallisuuden. Tämän työn tarkoituksena oli selvittää, kuinka kehitetään robotin automaation turvallisuutta ja kehittää toimintasuunnitelma, kuinka korjataan havaittuja puutteita. Lopputuloksena oli poikkeama-analyysipohja, josta tulee löytymään havaitut puutteet, toimintamallit, kuinka puutteet korjataan, testauksen tarpeen selvitys ja raportointitarve. Poikkeama-analyysi jäi yrityksen käyttöön työkaluksi ja yritys alkaa käyttämään sitä toiminnassaan. Työssä myös esiteltiin turvallistamisprosessi, keskeisiä lainsäädäntöjä ja standardeja.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Abstract

Author(s): Jussila Aleksi

Title of the Publication: Verification and Development of Safety in Industrial Robot Automation

Degree Title: Bachelor of Engineering, Mechanical Engineering

Keywords: Industrial robot, safety, automation, differential analysis

Prometec Tools is a machine manufacturer which is trying to solve problems in biofuel sampling. The company has developed and manufactured a fully automated sampling robot. The Finnish law stipulates that every machine should be safe to use. In addition, according to the law the manufacturer should verify the safety of their machines and specify what kind of machine should be used for a particular purpose. The standards specify legislation and guide the user in accordance with the generally accepted instructions. The standards can be used to reliably authenticate and ensure the safety of a device. Prometec Tools has CE- marked their robot and verified the safety of their device.

The purpose of this thesis was to find out how to develop the safety of robot automation and develop a strategy to fix the detected shortages. The final product is a differential analysis which includes the shortages, procedures how to fix them, the need for testing and reporting needs. The company will use the differential analysis as a tool. This thesis report also contains the presentation of the safety process, as well as relevant legislation and useful standards.

Alkusanat

Työn taustalla on Prometec Toolsin tarve selvittää teollisuusrobottinsa automaation turvallisuus ja pyrkiä kehittämään sitä. Tarkoituksena on selvittää, kuinka havaitaan puutteet ja luoda suunnitelmaa, kuinka ne ratkaistaan. Tämä opinnäytetyö on toteutettu Prometec Tools Oy:n toimeksiannosta ja haluan kiittää työn mahdollisuudesta ja aiheesta tuotepäällikkö Sami Karlssonia. Erityiskiitos työn ohjaajalle toimeksiantajan puolelta kehitysinsinööri Olli Kakolle, joka antoi täyden tuen, asiantuntijaosaamisensa ja aikaansa työn edistämiseksi. Kiitos automaatioinsinööreille Jari Kukkoselle ja Jussi Pulkkiselle asiantuntija-avusta.

Sisällys

1 Johdanto 1

2 Asiakasyrityksen nykytila 2

3 Polttoaineen näytteenotto 3

4 Robotin toimintaympäristö ja toiminnankuvaus 4

5 Lainsäädäntö ja standardit 6

6 Huomioitavat lakipykälät ja standardit 8
6.1 Konedirektiivi 2006/42/EY ja koneasetus 400/2008 8
6.2 Asetus työvälineiden turvallisesta käytöstä 403/2008 8
6.3 Työturvallisuuslaki 738/2002 9
6.4 Käytettävät standardit automaation näkökulmasta 9

7 Robottisolun turvallisuus ja käyttö 10
7.1 Robottisolun turvallisuus 10
7.2 Robottisolun käyttö 13

8 Turvallistamisprosessi 14

9 Turvallisuusvaatimusten ja suojaustoimenpiteiden todentaminen ja vahvistaminen tarkistuslistoja käyttäen 16

10 Turvallisuuteen liittyvä ohjausjärjestelmä 19

11 Automaation turvallisuusdokumentointi 21

12 Riskikartoituksen päivittäminen 23

13 Testaussuunnitelmien ja -pöytäkirjojen laadinta 24

14 Turvallisuustestaus 26

15 Yhteenveto 27

Lähteet 28

Liiteluettelo

Liitteet

1 Johdanto

Tämä opinnäytetyö käsittelee teollisuusrobotin automaation turvallistamista, sen todentamista ja kehittämistä. Toimeksiantajana on Prometec Tools Oy.

Tutkimuksen aiheena on Q-Robot-näytteenottorobotti, joka ottaa biopolttoaineista näytteitä suoraan polttoainerekasta. Suomen laki velvoittaa konevalmistajia varmistamaan tuotteen turvallisuus. Jotta tuote voidaan todeta turvalliseksi käyttää, voidaan apuna käyttää kansainvälisiä standardeja toimimaan ohjaavina tekijöinä. Opinnäytetyössä päästandardina toimivat:

- SFS-EN ISO 10218-1: Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 1: Teollisuusrobotit
- SFS-EN ISO 10218-2: Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 2: Robottijärjestelmät ja niiden yhdistelmät.
- SFS-EN ISO 13849-1: Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet.
- SFS-EN ISO 13849-2: Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus.

Työssä käsitellään yleistä teoriaa automaation turvallistamisesta, esitellään asiakasyrityksen nykytila ja turvallistamiskeinot sekä tarkastellaan laitteen turvallistamista verrattuna yleisiin standardeihin ja lainsäädäntöön käyttäen apuna standardeista löytyviä tarkistuslistoja. Työssä esitetään prosessikuvaus, kuinka turvallistamisprosessi etenee. Lopputuloksena on poikkeama-analyysi (Liite 1) ja toimintamalli, kuinka havaitut puutteet korjataan. Työssä keskitytään robottisolun näytteenottorobottiin eli Q-Robottiin. Työn rajauksena on kotimaahan myytävät laitteet.

2 Asiakasyrityksen nykytila

Prometec Tools (jäljempänä Prometec) on kajaanilainen vuonna 2015 perustettu yritys, jonka toimiala on laitevalmistus. Prometecin päätoimena on tuottaa laadunvalvontapalveluita teollisuuslaitoksille, jotka käyttävät biopolttoaineita. Prometecin tavoitteena on tuottaa tietoa polttoaineiden laadusta asiakasyrityksille. Merkittävin osuus laadunvalvonnasta on näytteenottoa ja käsittelyä, jota varten Prometec on kehittänyt robottisolun, jolla voidaan automatisoida näytteenotto ja -käsittely.

Yrityksen tuotteena on robottisolu, joka pitää sisällään Q-Robot näytteenottorobotin, joka ottaa näytteitä biopolttoaineista ja Q-Mixer-näytteenkäsittelyaseman, jossa otetut näytteet käsitellään mitattavaan muotoon. Yritys on tällä hetkellä valmistanut kolme robottisolua.

Prometec on laitetoimittaja, joka vastaa hallinnosta, tuotekehityksestä, markkinoinnista, myynnistä ja automaatiosta. Muut toimet Prometec ostaa alihankkijoilta. Yritys on nuori ja vasta-alkaja laitetoimittajana, joten haasteiksi on koettu laitteiston turvallistaminen. Tiedot yrityksen tilasta perustuvat yrityksen dokumentointiin, sähköpostikeskusteluihin ja haastatteluihin. Haastateltavana ovat kehitysinsinööri Olli Kakko ja automaatioinsinöörit Jari Kukkonen ja Jussi Pulkkinen.

3 Polttoaineen näytteenotto

Biopolttoaineiden laaduntarkkailussa merkittävin ominaisuus on kosteusarvo, joka on merkittävin muuttuja energiasisällössä, joka taas määrää polttoaineen hinnan. Kosteusarvo saadaan selville näytteenoton kautta. Aiemmin näytteenotto on ollut monin paikoin manuaalista, jossa polttoainerekan kuljettaja on lapiolla ottanut kuormasta näytteen, jonka on mitannut polttoainevastaanottaja. Manuaalisessa näytteenotossa on havaittu puutteita, jonka vuoksi on tarvittu uutta ratkaisua. [1]

On arvioitu, että kosteusmäärityksessä virheistä 80 % johtuu näytteenotosta [2]. Lisäksi manuaalisessa näytteenotossa on havaittu runsaasti turvallisuusuhkia, jotka aiheutuvat toimimisesta vaarallisessa ympäristössä. Polttoaineiden purkutaskut ovat usein heikosti suojattuja, joten putoamisvaara on ilmeinen ja suurten rekkojen liikkuminen altistaa rekan törmäämisen ihmiseen. Näytteenotto polttoainetta purettaessa on myös vaarallista, sillä polttoaine yleensä pölyää, joten näkyvyys on heikkoa ja toimiminen pölyävässä ympäristössä on haitalista terveydelle. Polttoainerekkojen purkaessa biopolttoaine saattaa tippua isoina kameina eli yhteen jäätyneinä lohkoina taskuun, joka kokonsa ja painonsa takia tuo vaaroja näytteenottajalle [kuva 1.]. [3].

Kuva 1. Jäätynyt polttoainekami polttoainepurussa

4 Robotin toimintaympäristö ja toiminnankuvaus

Toimintaympäristönä on näytteenottohalli, jossa sijaitsee Q-Robot (kuva 2.) ja Q-Mixer (kuva 3.). Halli on tavallisesti jaettu kahteen osuuteen, näytteenottopuoleen, jossa Q-Robot toimii, ja näytteenkäsittelypuoleen, jossa on Q-Mixer. Toimintaperiaatteena on, että robotti käy hakemassa satunnaisista paikoista polttoainerekan kuormatilasta näytteitä, jotka se pudottaa sekoitinsäiliöihin. Sekoitinsäiliöt sijaitsevat näytteenkäsittelypuolella. Sekoitinsäiliöissä näyte sekoittuu ja näytteet voidaan hakea jatkokäsittelyä varten.

Kuva 2. Q-Robot

Kuva 3. Q-Mixer

Polttoainerekan kulku robotin kautta kulkee siten, että ensimmäisellä kerralla auton tulee saapua tyhjänä halliin tyhjäskannaukseen, jossa konenäkö skannaa auton paikantaen alueet, joista ei voi näytettä kairata, kuten poikkitukien kohdat. Kun tyhjäskannaus on onnistunut, auto voi saapua seuraavalla käyntikerrallaan näytteenottohalliin, jossa kuljettaja voi itsenäisesti käynnistää näytteenoton. Robotilla on järjestelmässään pisteoptiot, joista se valitsee autotyypin mukaisesti näytteenottopisteet. Näistä pisteistä robotti ottaa kairaamalla näytteen, jonka se kerää näytteenkeräimeen. Kun näytteet on kerätty näytteenkeräimeen, robotti käy tyhjentämässä keräimen näyteputkeen, joka ohjaa näytteen yksilölliseen sekoitinsäiliöön. Näyte sekoittuu säiliössä, josta se voidaan noutaa mittaukseen.

5 Lainsäädäntö ja standardit

Lainsäädäntö määrää, että koneiden on täytettävä turvallisuusehdot, jotka ovat vähittäismääritykset. Standardit toimivat ohjenuorina ja yleisesti tunnettuina mittareina asettaen rajaehtoja, millainen koneen tulisi olla. Standardit kertovat tarkentavasti vaatimuksista, jotka laki määrää. Työturvallisuuslaki määrää, että laite on turvallinen käyttää, mutta se ei suoraan ota kantaa koneen turvallisuuteen. Työturvallisuuslain nojalla on asetettu valtioneuvoston asetus koneiden turvallisuudesta 400/2008 ja valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta 403/2008, joilla tarkennetaan vaatimuksia. Vna 400/2008:lla on otettu käyttöön konedirektiivi 2006/42/EY. Konedirektiivi ei koske kaikkia koneita, vaan sen ulkopuolelle on jätetty esimerkiksi kotikäyttöön tarkoitetut kodinkoneet, lentokoneet tai laivat. [4.]

Eurooppalaisessa lainsäädännössä Euroopan unionin (EU) komissio asettaa EU-direktiivejä, jotka liitetään jäsenmaan lakiin. EU-direktiivit ovat osa lakia kaikissa EU:n jäsenmaissa mukaan lukien Euroopan talousalueen (ETA) maat. Tavoitteena lainsäädännöllä on varmistaa tuotteiden vapaa liikkuvuus jäsenvaltioiden välillä, varmistaa koneiden turvallisuusvaatimukset sekä niiden turvallisuuden korkea taso. EU-direktiivien mukaan standardoimisjärjestöt luovat EU-normatiiveja eli standardeja, joista jäsenmaat saavat suosituksia toimintaansa. Koneita, jotka kuuluvat konedirektiivin alaisuuteen, mutta eivät täytä sen vaatimuksia, ei saa välittää eteenpäin. Kaikkiin koneisiin ei sovelleta konedirektiiviä, esimerkiksi lentokoneisiin, sotilaalliseen tai poliisin käyttöön valmistettuihin koneisiin tai kotikäyttöön tarkoitettuihin kodinkoneisiin. [4.]

CE-merkintä on laitevalmistajan vakuutus siitä, että sen valmistamalle koneelle on tehty tarkastus, joka osoittaa sen täyttävän annetut vaateet soveltuvien eurooppalaisten direktiivien ja näissä olevien olennaisten terveys- ja turvallisuusvaatimusten mukaan. Ennen CE-merkin kiinnitystä tulee koneen täyttää 400/2008 koneasetuksen vaatimukset. Jos kone kuuluu konedirektiivin alaisuuteen, niin CE-merkintäprosessi etenee siten, että määritellään, tarvitseeko laitteen täyttää muidenkin direktiivien vaatimuksia. Sitten koneelle tulee tehdä riskin arviointi ja riskien pienentäminen noudattaen konedirektiivien liitettä 1. Riskien pienentämiseen kuuluu turvallisuusohjeiden luonti, jotka tulee luoda tässä vaiheessa prosessia. Tämän jälkeen prosessissa seuraa vaihe, jossa turvallisuus varmistetaan. Valmistajan tulee suorittaa jokin vaatimustenmukaisuuden arviointimenettelyistä todistaakseen koneen direktiivien vaatimustenmukaisuus.

Valmistajan tulee koota tekninen tiedosto, jossa on dokumentaatio koneesta. Konedirektiivin liitteessä IV on annettu vaatimukset, mitä tämän teknisen tiedoston tulee sisältää. Teknisen tiedoston luomisen jälkeen valmistaja voi itse vakuuttaa vaatimustenmukaisuusvakuutuksellaan suunnitelleensa tuotteen vastaamaan direktiivien vaatimuksia. Lopuksi itse CE-merkki tulee kiinnittää laitteeseen konedirektiivin pykälän 9 § mukaisesti. [4.]

Standardit ovat virallisia dokumentteja, joita hyödyntämällä voidaan varmistua tuotteen tai palvelun vähittäisvaatimuksista. Standardien käyttö varmistaa, että tuotteen laatuvaatimukset, turvallisuus, luotettavuus, korvattavuus ja ympäristöystävällisyys ovat vaaditulla tasolla. Standardit ovat suuntaa antavia oppaita, jotka sisältävät kriteerejä, joita noudattamalla voidaan varmistua tuotteen soveltuvuudesta ja laadusta. Standardit ovat asiantuntijaryhmien kokoamia ohjeita, joiden noudattaminen on yleisten käytänteiden mukaan suotavaa. Standardit eivät ole pakotteita, mutta jos niitä ei käytä, on valmistajan velvollisuus osoittaa muilla tavoin tuotteen direktiivien asettamat vähittäismääritysten täyttö. Standardeja käytetään, jotta kansainvälinen kaupankäynti edistyy, käytänteet yhtenäistyvät ja maailmanlaajuinen vuorovaikutus kasvaa. Standardien käytöllä pyritään myös yhdenmukaistamaan tuotteita ja palveluita, mikä mahdollistaa kansainvälisesti tuotteiden yhteensopivuuden ja tietotaidon yhtenäisyyden. [5.]

Standardit jaetaan kolmeen ryhmään, joita ovat tyypit A, B ja C. A-tyypin standardit käsittelevät yleisellä tasolla turvallisuutta. Se antaa perussuunnitteluperiaatteet ja määritelmät, sekä yleiset näkökohdat, joita voidaan soveltaa koneisiin. Tyypin B standardit käsittelevät yhtä turvallisuusnäkökohtaa tai suojausteknistä laitetta, joita voidaan käyttää useissa koneryhmissä. C-tyypin standardit käsittelevät konekohtaisia turvallisuusvaatimuksia. Standardit ovat yksityiskohtaisempia ja tarkempia, ja niitä voidaan suoraan soveltaa tiettyyn koneeseen. [4.]

Standardit jaetaan alueellisesti kolmeen osaan, joissa kyseinen standardi on voimassa. Kansainväliset tasot ovat IEC eli International Electrotechnical Commission ja ISO eli International Organization for Standardization. Eurooppalainen taso on EN, ISO ja IEC. Kolmantena kansallinen taso, joka Suomessa on ISO, EN ja SFS eli Suomen Standardisointiliitto. [6.]

6 Huomioitavat lakipykälät ja standardit

6.1 Konedirektiivi 2006/42/EY ja koneasetus 400/2008

Koneasetuksella 400/2008 pannaan täytäntöön konedirektiivi 2006/42/EY. Koneasetuksesta ja konedirektiivistä löytyvät vähittäisvaatimukset turvalliselle koneelle ja sitä myöten vaatimukset automaatiojärjestelmälle. Laki määrää, että koneiden on täytettävä turvallisen koneen vähittäismääritykset. Koneasetus 400/2008:n tärkeimmät sisällöt automaation näkökulmasta ovat 4. luku 14 § ”Yleiset säännökset”, joihin sisältyy koneen suunnittelua ja rakentamista koskevat olennaiset terveys- ja turvallisuusvaatimukset, sekä erityisesti kohta 1.2 ”Ohjausjärjestelmät”. Robotilla lainsäädäntö näkyy yleisellä tasolla turvallisen koneen rakentamisessa ja korkeimpana auktoriteettina. [7.] Koneasetuksen mukaisesti laite pitää pystyä vakuuttamaan turvalliseksi. Yhdessä työturvallisuuslain 738/2002 ja asetuksen työvälineiden turvallisesta käytöstä 403/2008 mukaisesti laite tulee varmistaa testaamalla turvalliseksi.

6.2 Asetus työvälineiden turvallisesta käytöstä 403/2008

Valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta 403/2008 pykälät 4 §, 8 §, 9 § ja 10 § ovat automaation kannalta merkittävimmät. 4 § ”Vaaran arviointi ja poistaminen” sisältää vaatimuksen, että vaarat tulee tunnistaa ja pyrkiä poistamaan välittömästi. Jos vaaraa ei pysty poistamaan, tulee jäännösriski minimoida opastuksella, varoituksilla, henkilösuojaimilla ja turvamerkinnöin. 8 § ”Hallintalaitteet ja ohjausjärjestelmät” vaatii, että hallintalaitteet ja ohjausjärjestelmät on suunniteltu turvallisiksi käyttää. 9 § ”Työvälineen käynnistäminen” määrää, että työvälineen käynnistämisen tulee olla turvallista, eikä työvälineen käynnistys saa aiheuttaa vaaraa. Myös 10 §” Työvälineen pysäyttäminen ja hätäpysäytys” vaatii, että työvälineen pysäyttäminen ja hätäpysäytys tulee toteuttaa siten, että siitä ei koidu vaaraa ja työvälineessä tulee olla hallintalaite, jolla se saadaan pysäytettyä täydellisesti ja turvallisesti. [8.]

6.3 Työturvallisuuslaki 738/2002

Työturvallisuuslaki määrittelee työntekijöiden turvallisuuden varmistamiseksi tarvittavat toimenpiteet. Pykälä 19 § ”vikojen ja puutteellisuuksien poistaminen ja niistä ilmoittaminen” vaatii, että työntekijän on viipymättä ilmoitettava havaituista puutteista ja vaaroista. Tämä näkyy automaatiossa siten, että vaaralliseksi havaitut puutteet tulee saattaa myös työnantajan tietoon ja niihin on puututtava välittömästi. [9.] Turvallisuuden todentamisen ja varmistamisen kautta voidaan etukäteen arvioida tulevia riskejä, vaaroja ja turvallisuusuhkia ja puuttua niihin.

6.4 Käytettävät standardit automaation näkökulmasta

- SFS-EN ISO 10218-1 Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 1: teollisuusrobotit
- SFS-EN ISO 10218-2 Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 2: Robottijärjestelmät ja niiden yhdistelmät.
- SFS-EN ISO 13850 Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet
- SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet
- SFS-EN ISO 13849-2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus Teollisuusrobottien turvallisuussuunnittelu
- SFS-EN 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset
- SFS-EN ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen.

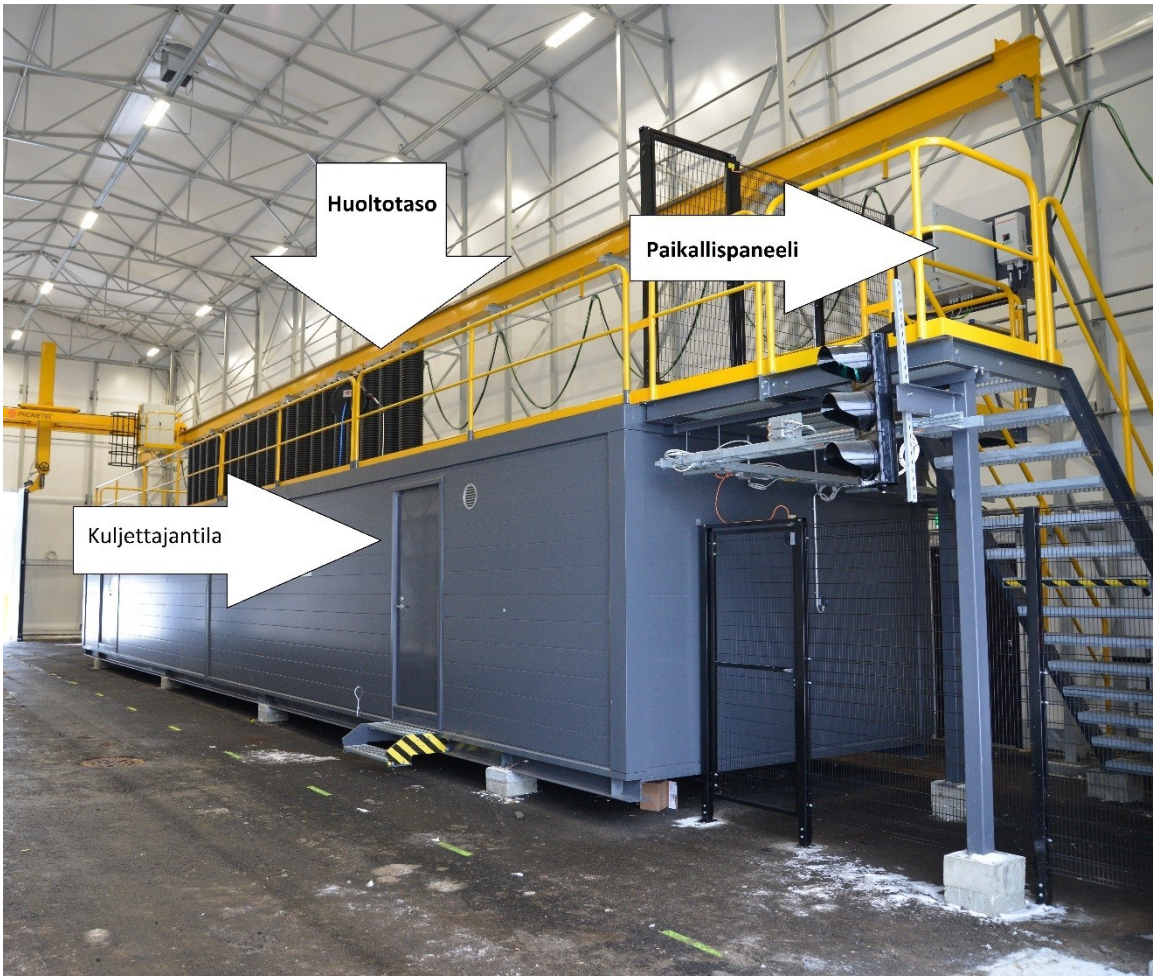
7 Robottisolun turvallisuus ja käyttö

7.1 Robottisolun turvallisuus

Prometec vastaa robotin automaatiosta ja on laitevalmistajana vastuussa laitteen turvallisuudesta. Automaation osalta on vielä kehittämiskohteita turvallisuuden osoittamisessa ja testauksessa. Prometecin tapauksessa on kyseessä konedirektiivi 2006/42/EY, joka on Suomen laissa pantu täytäntöön valtioneuvoston asetuksella 2008/400. Prometec Tools on CE-merkinnyt sekä Q-Robotin että Q-Mixerin. Robottisolu koostuu kahdesta osasta, Q-Robot-näytteenottimesta ja Q-Mixer-näytteenkäsittelyasemasta, joten myös turvallisuusnäkökohdat voidaan näissä jakaa kahteen osuuteen. Työssä käsitellään Q-Robotia.

Robotin liikealueelle pääsy on suurimpana turvallisuusnäkökohtana. Kuljettajan operointialue on rajattu turvaovella, jossa on robotin pysäyttävät turvarajakytkimet. Robotin liikealue on rajattu mekaanisilla esteillä, jotka estävät robotin liikkeet turvaamattomille alueille. Robotin paikallispaneelille kulkua ei ole rajoitettu. Huoltotasolle, joka on robotin liikealuetta, on pääsy estetty turva-aidoilla (kuva 4). Robotti on suojattu mekaanisilta vaaroilta momenttirajoilla, jotka estävät robottia vaurioittamasta itseään. Robotti on pyritty turvallistamaan standardien mukaisesti. Näytteenkäsittelypuolella Q-Mixerin suurimpana turvallisuusnäkökohtana on sekoitinsäiliöiden turvallisuus. Merkittävimpinä laitteessa on puristumisvaarat, joiden minimointi on tärkeintä.

Robotin liikkeiden ohjauksessa käytetään Siemensin S1500- sarjan logiikkaa. Logiikkaohjauksessa on oma SAFETY- puoli, jossa on koodattuna turvallisuustoiminnot. Se on oma osionsa, joka linkittyy muuhun toimintaan, muun muassa, jos turvapiiri aktivoituu, se pysäyttää robotin liikkeet. Logiikan turvallisuusosiot ovat logiikan omia. Turvapiirien in- ja outputit menevät erillisen PROFISAFE-yhteensopivan I/O-kortin kautta.



Kuva 4. Paneelien ja huoltotason sijainnit

Robottia voidaan ohjata kahdelta eri paneelilta. Paikallispaneeli (kuva 5) on koko robottisolun ohjausyksikkö ja kuljettajaterminaalissa kuljettajapaneelilla (kuva 6) käynnistetään näyttöönottosekvenssi. Jälkimmäinen sijaitsee kuljettajan tilassa, jossa käyttäjä voi kuitata turvaoven, valita käsin oman ajoneuvoyhdistelmänsä ja käynnistää näytteenoton. Paneelilta voidaan reaaliajassa seurata näytteenoton kulkua. Huoltotason vieressä on paikallispaneeli, jota laitevalmistajan henkilökunta ja koulutettu voimalaitoksen henkilökunta voivat käyttää. Paikallispaneelilta voidaan käyttää robottia manuaalisesti ja automaattisesti.

Kuva 5. Paikallispaneeli

Kuva 6. Kuljettajapaneeli kuljettajan tilassa

Koneasetus määrää ohjaustavan valinnan siten, että saa olla yksi ohjauspaikka kerrallaan käynnissä:

> *Jos ohjauspaikkoja on enemmän kuin yksi, ohjausjärjestelmä on suunniteltava sellaiseksi, että yhden ohjauspaikan käyttäminen estää muiden käytön, pysäytys- ja*

hätäpysäytyslaitteita lukuun ottamatta. Jos koneessa on kaksi tai useampia käyttöpaikkoja, jokainen paikka on varustettava kaikilla vaadituilla ohjauslaitteilla ilman, että käyttäjät voivat häiritä toisiaan tai saattaa toisiaan vaaratilanteeseen. [10.]

7.2 Robottisolun käyttö

Robottisolun turvallistamisessa pyritään jakamaan robottisolun käyttö kolmeen osioon, jonka mukaan turvallisuus tarkastetaan. Nämä kolme ovat koneen normaali käyttö, huolto ja testaus. Koneen käyttöön lasketaan koneen normaali ja määritelty käyttö tarkoituksenmukaisella tavalla. Huoltoon liittyy koneen huoltotoimenpiteisiin liittyvät toiminnot, kuten vuosihuolto. Testaukseen kuuluu toiminta, jossa laitevalmistaja suorittaa testaustoimintoja laitteella.

Polttoainerekan kuljettaja on käyttäjä, joka käynnistää näytteenottorobotin. Kuljettaja toimii kuljettajaterminaalissa, joka on aidattu alue ja jonka ovi on varustettu turvarajakytkimellä. Kuljettajalla ei ole mahdollisuutta poistua terminaalista pysäyttämättä robotin liikettä. Kuljettajapaneeli ilmaisee näytteenoton vaiheet ja sen, milloin alueelta on turvallista poistua.

Koneturvallisuus voidaan jakaa kahteen osioon, henkilö- ja laiteturvallisuuteen. Henkilöturvallisuudella pyritään minimoimaan henkilöihin kohdistuvat riskit ja vaarat. Laiteturvallisuudella pyritään minimoimaan laitteisiin kohdistuvat vauriot ja riskit.

8 Turvallistamisprosessi

Automaation turvallistamisessa menettelytavat ovat prosessin kaltaisia ja iteratiivisia eli toistuvia. Kohdat tulee käydä järjestyksessä läpi, mikä helpottaa prosessin läpikäyntiä, työ on systemaattista ja kaikki kohdat tulee käydä läpi. Lähtiessä turvallistamaan laitetta tulee luoda toimintasuunnitelma, jonka mukaan edetään. Seuraavassa on vaihe vaiheelta käytynä läpi, kuinka turvallistamisprosessi etenee. Sama menettelytapa tuodaan myös Prometec Toolsille aputyökaluksi.

1. Tunnistetaan C-luokan standardit, jotka vaikuttavat suoraan laitteeseen tai joita voidaan käyttää ohjeistavina standardeina. Poikkeama-analyysiin kirjataan noudatettavat standardit ja niitä verrataan vaatimustenmukaisuusvakuutuksessa ilmoitettuihin standardeihin.

2. Listataan kyseisten C-luokan standardien vaatimukset, jotka koskevat automaation turvallistamista ja kehittämiskohdetta. Prometecin tapauksessa automaation ulkopuolelle jäävät asiat rajataan pois.

3. Listataan sovellettavien valtioneuvoston asetusten määrittämät vaatimukset automaatioon liittyen.

4. Selvitetään, mitä vaatimuksia on ja millaisella dokumentaatiolla niiden olemassaolo voidaan todentaa.

5. Tutustutaan yrityksen olemassa oleviin dokumentteihin. Standardeissa velvoitettuja dokumentteja verrataan olemassa oleviin dokumentteihin. Jos havaitaan puutteita, niin ne lisätään yrityksen työlistalle. Työlistan yhteenvedosta muodostuu poikkeama-analyysi, josta löytyy puutteet.

6. Listataan, mistä olemassa olevista dokumenteista löytyy mitkäkin vaateet ja millaisista dokumenteista löytyy kyseinen tieto.

7. Havaitut puutteet ja sen hetkinen tekniikan taso käsitellään yrityksen automaatioosaston kanssa.

8. Tehdään oma työlista, mitä dokumentteja on tuotettava missäkin vaiheessa.

    a. Sähkökomponenttien vaatimukset selvitetään ja etsitään käytettyjen komponenttien tekniset tiedot ja vaatimustenmukaisuusvakuutukset. Pyritään

korvaamaan ilman dokumentteja olevat komponentit sellaisiin, joista löytyy dokumentit. Läpikäydään komponentit, jotta havaitaan, mitkä eivät täytä niille asetettuja vaatimuksia, esimerkiksi toiminta-alueen tai lämmönkeston vaatimuksia. Tämän jälkeen selvitetään pitääkö komponentti vaihtaa vai riittääkö, jos suojaa komponentin oikein.

b. Jotkut todentamiset vaativat testaamista. Listataan vaadittavat testit ja missä vaiheessa ne tulisi tehdä. Testauspöytäkirjat hahmotellaan valmiiksi, jotta testien dokumentointi tapahtuisi alusta alkaen.

c. Käyttöä koskevat tiedot tulee löytyä käyttöohjeista. Havaitut puutteet käyttöohjeissa korjataan ja päivitetään käyttöohjeet.

9. Poikkeama-analyysia käytetään puutteiden listauksessa, jonka jälkeen olemassa olevat puutteet kirjataan automaatio-osastolle heidän työlistalle.

10. Automaatio-osaston tehtyä korjaukset päivitetään käyttöohjeet, testausohjeet ja tekninen dokumentaatio. Päivitetään yrityksen johtamisjärjestelmän ohjeistukset ja toimitusprojektien aikataulut.

Liitteessä 2 on esitetty lohkokaavion muodossa turvallistamisprosessi ja mikä vaihe kuuluu mille osastolle ja tapahtuuko vaihe toimistossa vai kentällä robotin luona.

9 Turvallisuusvaatimusten ja suojaustoimenpiteiden todentaminen ja vahvistaminen tarkistuslistoja käyttäen

Standardi SFS-EN ISO 10218-1 kohta 6 ”Turvallisuusvaatimusten ja suojaustoimenpiteiden todentaminen ja vahvistaminen” toteaa että:

> *Robotin valmistajan on huolehdittava robottien suunnittelun ja rakentamisen todentamisesta ja vahvistamisesta, mukaan lukien sopivat turvalaitteet kohtien 4 ja 5 periaatteiden mukaisesti. Riskien arviointi olisi tarkastettava, jotta voidaan arvioida, onko kaikki kohtuullisesti ennakoitavissa olevat vaarat tunnistettu ja korjaavat toimenpiteet tehty.*
>
> *HUOM. Koska kaikki liitteessä A tunnistettavat vaarat eivät koske jokaista robottia, tiettyyn vaaralliseen tilanteeseen liittyvä riskitaso ei ole sama kaikille roboteille. Riskien arviointia tarvitaan määrittämään sopivat suojatoimenpiteet tietylle robotille.*
>
> Näin ollen Prometecin robotille tulee tehdä turvallisuuden todentaminen ja vahvistaminen. Standardi jatkuu:
>
> *6.2 Todentamisen ja vahvistamisen menetelmät*
>
> *Todentaminen ja vahvistaminen voidaan tehdä mm. seuraavilla menetelmillä:*
>
> *— A silmämääräinen tarkastus*
>
> *— B toimintakokeet*
>
> *— C mittaukset*
>
> *— D toiminnan tarkkailu*
>
> *— E sovelluskohtaisten kaavioiden, piirikaavioiden ja suunnitteluun liittyvän aineiston tarkastelu*
>
> *— F tehtäväperusteisen riskin arvioinnin tarkastelu*
>
> *— G spesifikaatioiden ja käyttöä koskevien ohjeiden tarkastelu.*
>
> *Ks. taulukko F.1.*

6.3 Vaadittu todentaminen ja vahvistaminen

Liitteessä F on lueteltu erityisiä suorituskyvyn vaatimuksia, jotka on tunnistettu oleellisiksi sellaisen robotin turvallisuuden kannalta, joka todennetaan tai vahvistetaan, tai molempia. Vaatimukset on arvioitava käyttäen sopivia menetelmiä, jotta voidaan määrittää täyttävätkö robotin suunnittelu ja rakentaminen ne riittävän hyvin.

HUOM. 1 Taulukossa F.1 listatut kohdat eivät välttämättä kaikki koske jokaista robottia. Voi olla tapauksia, jolloin on mahdotonta todentaa ja/tai vahvistaa tiettyjä kohtia.

HUOM. 2 Taulukko F.1 ei ole kaikenkattava eikä rajoittava. Siinä saattaa olla ylimääräisiä todentamisvaatimuksia riippuen kunkin robotin suunnittelusta.

HUOM. 3 Valmistajan vastuulla on varmistaa, että kaikki soveltuvat kohdat on todennettu tai vahvistettu, tai molempia.

HUOM. 4 Jos taulukkoa F.1 käytetään tarkistuslistana, sisällys on tarkistettava ja rajoitettava edustamaan todellista robotin kokoonpanoa ja sopivaa menetelmää tälle arvioinnille. [11]

Standardin liitteenä olevaa F.1- taulukkoa käytetään apuna turvallisuuden todentamisessa ja vahvistamisessa. Taulukkoa F.1 käytetään tarkastuslistana, mutta HUOM.4 mukaisesti sisällys tarkistetaan ja rajoitetaan soveltumaan todelliselle robotin kokoonpanolle. Tarkistuslistassa edetään siten, että tarkistuslistasta yliviivataan osiot, jotka eivät kuulu automaatioon. Yliviivaamattomat kohdat tarkistetaan, onko ne jo tarkastettu ja dokumentoitu. Jos on, niin yliviivataan nämäkin kohdat. Tämän jälkeen yliviivaamattomille suunnitellaan toimenpiteet. Puutteet lisätään poikkeama-analyysiin.

Standardi SFS-EN ISO 10218-2:2011 toteaa, että:

Robottijärjestelmän valmistajan tai integraattorin on tehtävä robottijärjestelmien suunnitelman ja toteutuksen todentaminen ja kelpuutus, mukaan lukien niihin kuuluvat sopivat turvalaitteet, kohdissa 4 ja 5 kuvattujen periaatteiden mukaisesti. Läpikäymällä riskin arviointi on arvioitava, ovatko kaikki kohtuudella ennakoitavissa olevat vaarat yksilöity ja ryhdytty oikeisiin korjaaviin toimenpiteisiin.

HUOM. Koska kaikki liitteessä A yksilöidyt vaarat eivät koske jokaista robottijärjestelmää, määrättyyn vaaralliseen tilanteeseen liittyvän riskin taso ei ole sama

> *robottijärjestelmästä toiseen, ja määrättyjen robottijärjestelmien sovelluksiin kuuluu vaaroja, joita ei ole tunnistettu liitteessä A. Riskin arviointi on tarpeen tehdä määrittämään, millaiset menetelmät sopisivat kyseiselle robottijärjestelmälle.* [12.]

Turvallisuusvaatimusten ja -toimenpiteiden todentamisen menetelmät kohdassa liite G, taulukko G.1 käytetään tarkistuslistana. Standardin mukaisesti taulukkoa tarkastellaan siltä osin, kuinka se soveltuu robottijärjestelmään. Tarkistelu tapahtuu ensin rajaamalla listasta pois automaation ulkopuolelle jäävät osiot. Jäljelle jäävistä kohdista erotellaan jo varmistetut tapaukset. Lopulliset kohdat, jotka kuuluvat automaatioon, muttei ole vielä todennettu ja/tai varmistettu, luodaan toimenpiteet.

10 Turvallisuuteen liittyvä ohjausjärjestelmä

Turvallisuuteen liittyvän ohjausjärjestelmän tehtävänä on valvoa ja ylläpitää tilaa, jossa kone on turvallinen, eivätkä koneen käyttäjät joudu vaaraan. Ohjausjärjestelmä tulee suunnitella ja toteuttaa seuraavien standardien mukaisesti:

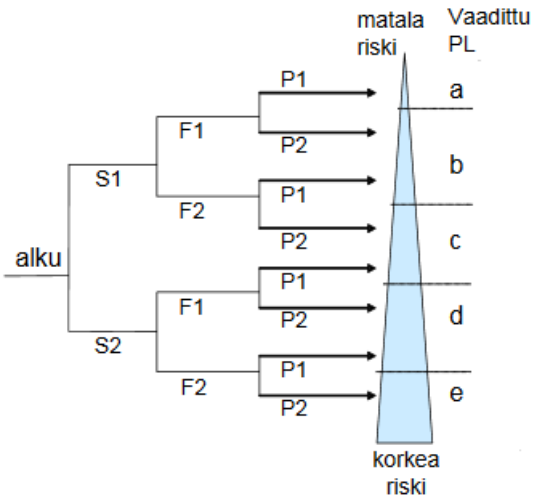
- ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet
- ISO 13849-2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus

Ohjausjärjestelmälle on tärkeää, että se soveltuu käytettävään sovellukseen ja on tarpeeksi kestävä käyttöolosuhteisiin nähden. Logiikkayksikössä tapahtuvat viat tai komponentti- tai ohjelmistoviat eivät saa aiheuttaa vaarallisia tilanteita. Myöskään inhimilliset virheet eivät saa aiheuttaa vaaroja. Ohjausjärjestelmää luodessa ensimmäisessä vaiheessa on riskien arviointi, mikä pitää sisällään koneen raja-arvojen määrityksen, vaarojen tunnistuksen ja riskien suuruuden ja merkityksen arvioinnin. Suunnitteluvaiheessa ohjausjärjestelmää tärkein vaihe on ensimmäiseksi määrittää vaadittava suoritustaso PLr eli required Performance Level. PLr tason määrittäminen esitetty jäljempänä. Tämän tason tulee ohjausjärjestelmän vähintään täyttää, jotta saavutetaan tarpeeksi korkea luotettavuus ja turvallisuuden taso. Riskien pienentämisen jälkeen suunnitellaan tarkemmin järjestelmä komponenttitasolla ja arkkitehtuurin valinnalla. Suoritustaso tulee arvioida ja todentaa. Järjestelmän käyttöönotossa asennetaan ohjausjärjestelmä ja lopuksi suoritetaan järjestelmän kelpuutus. Ohjausjärjestelmän turvallisen käyttöönoton vaiheet ovat kuvattuna liitteessä 3.

Turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelun prosessi on iteratiivinen ja se etenee siten, että ensin tunnistetaan turvatoiminnot, jotka ohjausjärjestelmän tulisi toteuttaa. Sen jälkeen määritellään jokaiselta toiminnolta vaadittavat ominaisuudet erikseen ja määritetään myös vaadittava suoritustaso PLr. Tämän jälkeen toteutetaan kyseinen turvatoiminto. Sitten arvioidaan suoritustaso PL, joka on todellinen saavutettu suoritustaso. Tästä päästään havaitsemaan onko PL suurempi tai suurempi kuin PLr. Jos kyllä, niin jatketaan tutkimaan, onko kaikki vaatimukset täytetty eli kelpuutettu ja kaikki turvatoiminnot analysoitu. Lohkokaavio järjestyksestä esitetty liitteessä 4. [13.] PLr koostuu vamman vakavuudesta, vaaralla altistumisen ajasta ja mahdollisuudesta välttää vaara. PL taas koostuu arkkitehtuurista, virheiden paljastumismekanismista, yhteisvikaantumisesta,

komponenttien luotettavuudesta, turvallisuuteen liittyvästä ohjelmistosta, systemaattisesta vikaantumisesta ja ympäristö- ja käyttöolosuhteista. PLr tason pystyy määrittelemään kuvassa 7 löytyvällä laskentamallilla. Alku on aloituspiste, josta lähdetään etenemään.

- S vamman vakavuus
    - S1 Lievä, tavallisesti palautuva vamma
    - S2 Vakava, palautumaton vamma tai kuolema
- F Vaaralle altistumisen taajuus
    - F1 Harvoin, toisinaan tai lyhyt altistumisaika
    - F2 Toistuvasti, jatkuvasti tai pitkä altistumisaika
- P Mahdollisuus välttää vaara tai vaarallisen tilanteen esiintyminen
    - P1 Mahdollista
    - P2 Tuskin mahdollista



Kuva 7 PLr tason määritys

11 Automaation turvallisuusdokumentointi

Automaation turvallisuusdokumentointiin tarvitsee tehdä testaussuunnitelmat, automaation toiminnan kuvaukset ja standardin SFS-EN ISO 13849-1 kohdan 8 mukaisesti:

> *Turvallisuuteen liittyvien ohjausjärjestelmän osien toteutus on kelpuutettava. Kelpuutuksella on osoitettava, että kunkin turvatoiminnon toteuttava turvallisuuteen liittyvien ohjausjärjestelmän osien yhdistelmä täyttää standardin ISO 13849 tämän osan kaikki asiaan kuuluvat vaatimukset.*

Standardin SFS-EN ISO 13849-1 kohta 10 ”Tekniset asiakirjat” toteaa, että:

> *Suunniteltaessa turvallisuuteen liittyvää ohjausjärjestelmän osaa suunnittelijan on dokumentoitava vähintäänkin seuraavat turvallisuuteen liittyviin osiin kuuluvat asiaankuuluvat tiedot:*
>
> — *turvallisuuteen liittyvien ohjausjärjestelmän osien toteuttamat turvatoiminnot*
>
> — *kunkin turvatoiminnon ominaisuudet*
>
> — *turvallisuuteen liittyvien ohjausjärjestelmän osien tarkat alku- ja loppukohdat*
>
> — *ympäristöolosuhteet*
>
> — *suoritustaso (PL)*
>
> — *valitut luokat*
>
> — *luotettavuuden kannalta merkitykselliset muuttujat (MTTFD, DC, CCF ja toiminta-aika)*
>
> — *toimenpiteet systemaattisen vikaantumisen estämiseksi*
>
> — *käytetyt teknologiat*
>
> — *kaikki tarkastelussa mukana olleet turvallisuuteen liittyvät viat*
>
> — *vikojen poissulkemisen perustelut (ks. ISO 13849-2)*
>
> — *suunnittelun loogiset perustelut (esim. huomioon otetut viat, poissuljetut viat)*
>
> — *ohjelmistoa koskeva dokumentaatio*

— *toimenpiteet kohtuudella ennakoitavissa olevan väärinkäytön estämiseksi.* [14.]

Prometec Tools vastaa laitteensa turvallisuudesta ja turvallisuuteen liittyvät toiminnot tulisi olla dokumentoituina. Prometecilla ei ole käytössä johtamisjärjestelmää, mutta tiedonhallinta on järjestelty tiedostonhallintapalveluun, josta löytyy dokumentit laitteesta. Liitteessä 5 on esitetty, mitä Prometecin tulee dokumentoida.

Prometecin automaation turvallistamisen dokumentaatiossa on kehitettävää. Laite on turvallistettu ja CE-merkitty eli vakuutettu turvalliseksi ja säädöstenmukaiseksi. Dokumentaatiota tulisi kehittää, sillä turvallisuusominaisuuksien todentaminen on hankalaa ja tiedon hakeminen työlästä. Jos tieto on yrityksen henkilökunnalla, mutta ei dokumentoituna, se lisää merkittävästi riskiä tiedon katoamiseen.

Dokumentit tulee luoda siinä järjestyksessä, kun se on luontevaa. Käytetyt teknologiat tulee dokumentoida ensin, jotta selviää, miltä teknologiaa ja komponentteja on käytössä ja mitkä niiden turvaominaisuudet ovat. Valittu turvallisuuden taso ja luokat dokumentoidaan sitten, jotta nähdään mikä tavoitetila on. Lopuksi vertaillaan olemassa olevat teknologiat tavoitteisiin, jotta nähdään, millä tasolla ollaan menossa. Komponenttitasolla dokumentaatiot tulee tarkistaa valmistajien vaatimustenmukaisuusvakuutuksista, minkä suojaustason ja turvatoiminnon ne täyttävät.

Testaus tarvitaan, jotta voidaan todentaa, että konkreettiset turvallistamisominaisuudet vastaavat dokumenteissa esitettyjä ominaisuuksia. Testaus tulee suorittaa, kun osa-alue on dokumentoitu. Vaadittavat tiedot asiakirjoja varten löytyy käytettyjen teknologioiden ja komponenttien valmistajien tiedoista ja asiantuntijoilta. Dokumenttien täyttö vaatii asiantuntijan joko tekemään tai avustamaan dokumentin teossa, tarpeeksi kattavat tiedot dokumentoitavasta kohteesta, sekä helppokäyttöisen ja käytännöllisen dokumenttipohjan.

12 Riskikartoituksen päivittäminen

Riskikartoitukset robottisolulle on tehty jokaiselle robottisolulle erikseen, sillä ne ovat yksilöllisiä, joten riskitkin voivat vaihdella. Riskikartoitus tulisi päivittää, sillä laitteessa on voinut tapahtua muutoksia tai kehitystä, jolloin riskikartoitus ei ole enää pätevä. Riskikartoituksessa käytetään standardia SFS-EN ISO 12100 ”Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen”. Automaatiota koskee erityisesti:

- 6.2.11 ”Luontaisesti turvallisten suunnittelutoimenpiteiden soveltaminen ohjausjärjestelmiin”. Se pitää sisällään ohjausjärjestelmiin liittyvän riskien arviointiin ja pienentämiseen. Riskikartoitusta tehdessä ja päivittäessä tulee tutustua ensin standardiin, jonka jälkeen tutustutaan olemassa oleviin riskianalyyseihin, havaitaan mahdolliset puutteet ja korjataan puutteet.

- 6.2.12 ”Turvatoimintojen vikaantumistodennäköisyyden minimointi”, joka pitää sisällään komponenttien käyttöön ja ominaisuuksiin liittyviä huomioita.

13 Testaussuunnitelmien ja -pöytäkirjojen laadinta

Turvallisuuden todentamisen prosessin mukaisesti tulee hahmotella ja luoda testaussuunnitelmat niille prosessin osille, jotka tarkasteluissa ovat osoittautuneet testausta vaativiksi. Ennen varsinaista testausta suunnitelmat tulee tehdä, jotta testit ovat toistettavia ja kaikki kohdat tulee läpikäytyä. Dokumentointi on tärkeää myös, jos tarvitsee palata testaukseen myöhemmin. Testaussuunnitelmien teko auttaa myös jatkossa testien tekoa, sillä suunnitelmapohjat on jo luotu. SFS-EN ISO 10218-1 kohta 6.2 ”todentamisen ja vahvistamisen menetelmät” [15.] antavat yhdeksi todentamisen ja vahvistamisen vaihtoehdoksi toimintakokeet. SFS-EN ISO 10218-2 kohta 6.2 ”Todentamisen ja kelpuutuksen menetelmät” antaa myös yhdeksi menetelmäksi käytännön testaukset [16.]. SFS-EN ISO 13849-2 kohta 6 ”Kelpuutus testauksen avulla” antaa ohjeita testauksen suorittamiseen. Testaus on tehtävä kelpuutuksen loppuun saamiseksi, jos analyysin avulla kelpuutus ei ole lopullinen. Kelpuutustestit ovat suunniteltava ja toteutettava loogisesti. Testaussuunnitelma on suunniteltava ennen testausta ja siihen kuuluu testauksen erittelyt, vaadittavat tulokset, jotka osoittavat vaatimustenmukaisuuden ja testauksen aikajärjestyksen. Suunnitelmasta tulee löytyä testaajan nimi, ympäristöolosuhteet, testiproseduurit ja käytetyt välineet, päivämäärä ja tulokset. Testauksen tallenteita on verrattava testisuunnitelmaan, jotta määritetyt toiminnallisuudet ja suorituskykytavoitteet on tavoitettu. [17.]

Testaussuunnitelman rakenteen esimerkki [18.]:

1. Muutoshistoria
    a. Sisältää testaajan nimen, päiväyksen, version ja kommentin muutoksesta
2. Johdanto
    a. Esitellään dokumentin tarkoitus ja sisältö
3. Määritelmät ja termien selitykset
    a. Selitetään lyhyesti termit määritelmät
4. Testauksen kohde ja tavoitteet
    a. Kuvataan testattavana olevaa järjestelmää
    b. Kuvataan testin tavoitteet

5. Testausympäristö
    a. Kuvataan testausympäristö ja laitteet
6. Testattavat toiminnot
    a. Listataan ja kuvataan testattavat toiminnot
7. Erikoistilanteet
    a. Listataan mahdolliset erikoistilanteet, joita voisi tapahtua, jos käyttäjä tekee jotakin arvaamatonta. Selvitetään, kuinka testattava käyttäytyy tällaiseen tilanteeseen
8. Ominaisuudet, joita ei testata
    a. Kaikkea ei välttämättä pysty testaamaan, joten ne tulee selvittää myös. Näin ollen tuodaan ilmi, että kyseiset huomiot on otettu huomioon ja havaittu.
9. Testauksen organisointi ja raportointi
    a. Testausryhmän kokoonpano, johon kirjataan nimet ja roolit
    b. Raportoinnin vaiheet, kelle ja milloin raportointi.

Testauspöytäkirjoihin merkitään testauksen aikana tulokset ja havainnot. Pöytäkirja luodaan ennen testausta ja siihen pyritään keräämään kaikki tarvittavat tiedot raportointia varten. Pöytäkirjan huolellisella etukäteissuunnittelulla saadaan luotua dokumentti, joka pitää sisällään tarvittavan informaation, on selkeä, sitä ei tarvitse testin aikana muokata ja joka on tarpeeksi kattava.

Prometecilla löytyy testauspöytäkirjoja, joita pystyy hyödyntämään. Testaussuunnitelmaa luodessa tulee tarkistaa, onko yrityksellä olemassa jo hahmotelmia, joita voi käyttää.

14 Turvallisuustestaus

Turvallisuustestaus tulee suorittaa laitteelle ennen laitteen luovutusta, sillä laitteen tulee olla turvallinen käyttäjälle. Turvallisuustestaus on iteratiivista ja sitä tulee tehdä ennen laitteen käyttöönottoa ja aina, kun turvallisuuskomponentteihin- tai ohjelmistoon tulee muutos. Robotin käyttöönottovaiheessa turvallisuustestaus tulee tehdä aina, kun siihen on mahdollisuus, eikä testauksen aloitusta tule viivyttää. Esimerkiksi muuttaessa robotin turvarajoja, ne tulee testata, ennen kuin robottia ajetaan. Käyttöönottovaiheessa luodaan oma osuutensa, jossa käydään turvallisuuspuoli läpi noudattaen turvallisuusprosessia. Turvallisuustestaukset tulisi tehdä FAT- testin (Factory Acceptance Test) aikana, jolloin laitteiston toiminta testataan ja tarkastetaan laitetoimittajan tarjoamassa paikassa. Robotin tapauksessa FAT-testi suoritetaan ennen laitteen viemistä asiakkaan kohteeseen kokoonpanotilassa. Hyväksymistestauksen, eli SAT- testin (Site Acceptance Test) aikana tehdään lopullinen testaus turvallisuusautomaatiolle ja laitteistoille. Tämä testi suoritetaan silloin, kun koko laitteisto on valmis otettavaksi käyttöön.

Automaation logiikkaan kuuluvat turvallisuustoiminnot testataan varmistamalla sen toimintakyky ja luomalla ongelmatilanteita kattavasti ja testaamalla, pystyykö ohjelma suoriutumaan turvallisesti ongelmatilanteissa. Testaus raportoidaan aiemmin työssä kohdassa 13 ”Testaussuunnitelmien ja -pöytäkirjojen laadinta” mukaisella tavalla.

15 Yhteenveto

Prometec Tools on laitetoimittaja, jonka valmistama laite on automaattinen näytteenotto-robotti. Lainsäädäntö määrää, että laitteiden tulee olla turvallisia käyttää ja säädösten mukaisia. Prometec on CE – merkinnyt ja todennut laitteensa turvalliseksi käyttää. Automaation turvallisuuden todentamisessa on kehitettävää. Turvallisuuden todentamisessa pyritään noudattamaan turvallistamisprosessia, jotta kaikki oleellinen tulee havaittua, toiminta olisi jäsenneltyä ja työ helpottuu, kun on selkeät toimintamallit, jonka mukaan edetä. Turvallisuuden todentamisessa selvitetään täytettävä lainsäädäntö ja standardit, joita voidaan käyttää toimintaa ohjaavina. Laitteen turvallisuus tulee selvittää muun muassa riskianalyyseilla, tarkistuslistojen avulla ja tutustumalla laitteen turvallistamiskeinoihin. Turvallistamiskeinoja peilataan lainsäädäntöön ja standardeihin. Havaitut puutteet kirjataan ylös, esimerkiksi poikkeama-analyysiin, johon kirjataan havaitut puutteet, toimintatavat puutteen poistamiseksi, dokumentointitarve, testaustarve ja aikataulu työn suorittamiseksi. Raportti käydään läpi automaatio-osaston kanssa, joka ottaa tehtävät työlistalleen. Turvallistaminen tulee dokumentoida, jotta tieto säilyy paremmin, on toistettavissa myöhemmin ja pystytään todentamaan turvallisuuden tila.

Työn tuloksena on kaksi valmista poikkeama-analyysipohjaa, joita Prometec pystyy hyödyntämään ja selvitys, kuinka turvallisuusprosessi etenee. Työssä selvitettiin käytettäviä standardeja, dokumentointilista, mistä selviää dokumentoitavat asiat ja luotiin turvallistamisprosessi, jonka mukaan turvallisuuspuutteita lähdetään korjaamaan. Poikkeama-analyysiin tehdään suunnitelma, kuinka tarkistetaan, onko puutteita. Havaitut puutteet kirjataan ylös analyysiin ja luodaan toimenpiteet tapauskohtaisesti. Listataan, mistä löytyy asianmukaiset standardit ja lait. Samalla luodaan järjestys, miten luetaan standardeja, mistä kappaleesta ne löytyvät ja mihin standardiin lukija ohjataan esimerkiksi velvoittavilla viitteillä. Standardit tarkastellaan yksityiskohtaisesti verraten niitä omaan laitteeseen.

Automaation turvallistaminen on iteratiivinen prosessi, joka pitää käydä läpi väliajoin. Erityisesti tähän tulee kiinnittää huomiota, kun työskennellään uudessa projektissa tai automaatioon tulee muutoksia.

Lähteet

1 Mustonen M. Automaattisen biomassanäytteenottimen laadullinen tutkimus. Opinnäytetyö; Kajaanin Ammattikorkeakoulu; 2017

2 Alakangas E, Hurskainen M, Laatikainen-Luntama J, Korhonen J. Suomessa käytettävien polttoaineiden ominaisuuksia. VTT Technology 258 2016: 41 s.

3 Rissanen T. Turvallisuus ennen kaikkea. Haettu osoitteesta https://prometec.fi/fi/11942-tyoturvallisuus-ennen-kaikkea/

4 Pilz. Koneturvallisuuden asiantuntija. CE-merkintä ja konedirektiivi. Koulutusmateriaali. 2018: Diat 11-92.

5 Suomen Standardisoimisliitto SFS ry. Usein Kysyttyä. Haettu osoitteesta: https://www.sfs.fi/julkaisut_ja_palvelut/usein_kysyttya

6 Suomen Standardisoimisliitto SFS ry. SFS, EN, ISO? Haettu osoitteesta: https://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/sfs_en_iso

7 Finlex Valtioneuvoston asetus koneiden turvallisuudesta 400/2008. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2008/20080400

8 Valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta. Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2008/20080403#Pidp451137360

9 Työturvallisuuslaki 738/2002. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2002/20020738#L4P19

10 Finlex Valtioneuvoston asetus koneiden turvallisuudesta 400/2008 14§. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2008/20080400

11 SFS-EN ISO 10218-1 Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 1: teollisuusrobotit. 3.p. Helsinki: Suomen Standardisoimisliitto SFS

12 SFS-EN ISO 10218-2:2011. Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 2: Robottijärjestelmät ja niiden yhdistelmät. 1.p. Helsinki: Suomen Standardisoimisliitto SFS

13 Pilz. Koneturvallisuuden asiantuntija. Turvallisuuteen liittyvien ohjausjärjestelmien suunnittelu perustuen standardiin ISO 13849-1. Koulutusmateriaali. 2018: Diat 24-73.

14 SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 3.p. Helsinki Suomen Standardisoimisliitto SFS

15 SFS-EN ISO 10218-1. Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 1: Teollisuusrobotit. Kappale 6.2. Helsinki: Suomen Standardisoimisliitto SFS

16 SFS-EN ISO 10218-2. Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 2: Robottijärjestelmät ja niiden yhdistelmät. Kappale 6.2. Helsinki: Suomen Standardisoimisliitto SFS

17 SFS-EN ISO 13849-2. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. Kappale 6. 3.p. Helsinki: Suomen Standardisoimisliitto SFS

18 Testauksen organisointi ja raportointi dokumentti. Kajaanin ammattikorkeakoulu. haettu osoitteesta https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwifxrqrutfaAhVBGZoKHfOL-CUkQFghFMAQ&url=https%3A%2F%2Fwww.kamk.fi%2Floader.aspx%3Fid%3Dd473c83c-6ebb-4505-a36e-4923df081d89&usg=AOvVaw3co1vvklnxM7lfnxs-i3wW

Kuvat: Prometec Tools Oy. Kuva-arkisto. 2017.

Liiteluettelo

Liite 1. Poikkeama-analyysi versiot

Liite 2. Lohkokaavio turvallistamisprosessista

Liite 3. Lohkokaavio ohjausjärjestelmän turvallistamisesta

Liite 4. Lohkokaavio ohjausjärjestelmän osien suunnittelusta

Liite 5. Automaation turvallistamisen dokumentointi

Poikkeama-analyysi

Havaittu puute	Toimenpiteet	Raportointitarve	Hyödynnettävä standardi	Dokumentointi	Testaustarve	Tekijän nimi	PRIORITEETTI	TILA	ALOITUSPÄIVÄ	MÄÄRÄPÄIVÄ	HUOMAUTUKSIA
Esimerkki puute							Normaali	Ei aloitettu	7.5.2018	14.5.2018	
							Pieni	Ei aloitettu	7.4.2018	12.5.2018	
							Pieni	Ei aloitettu	14.4.2018	24.4.2018	
							Normaali	Ei aloitettu	22.4.2018	28.5.2018	
							Suuri	Ei aloitettu	2.5.2018	16.5.2018	

Liite 1. Poikkeama-analyysi vaihtoehto 1

PROMETEC

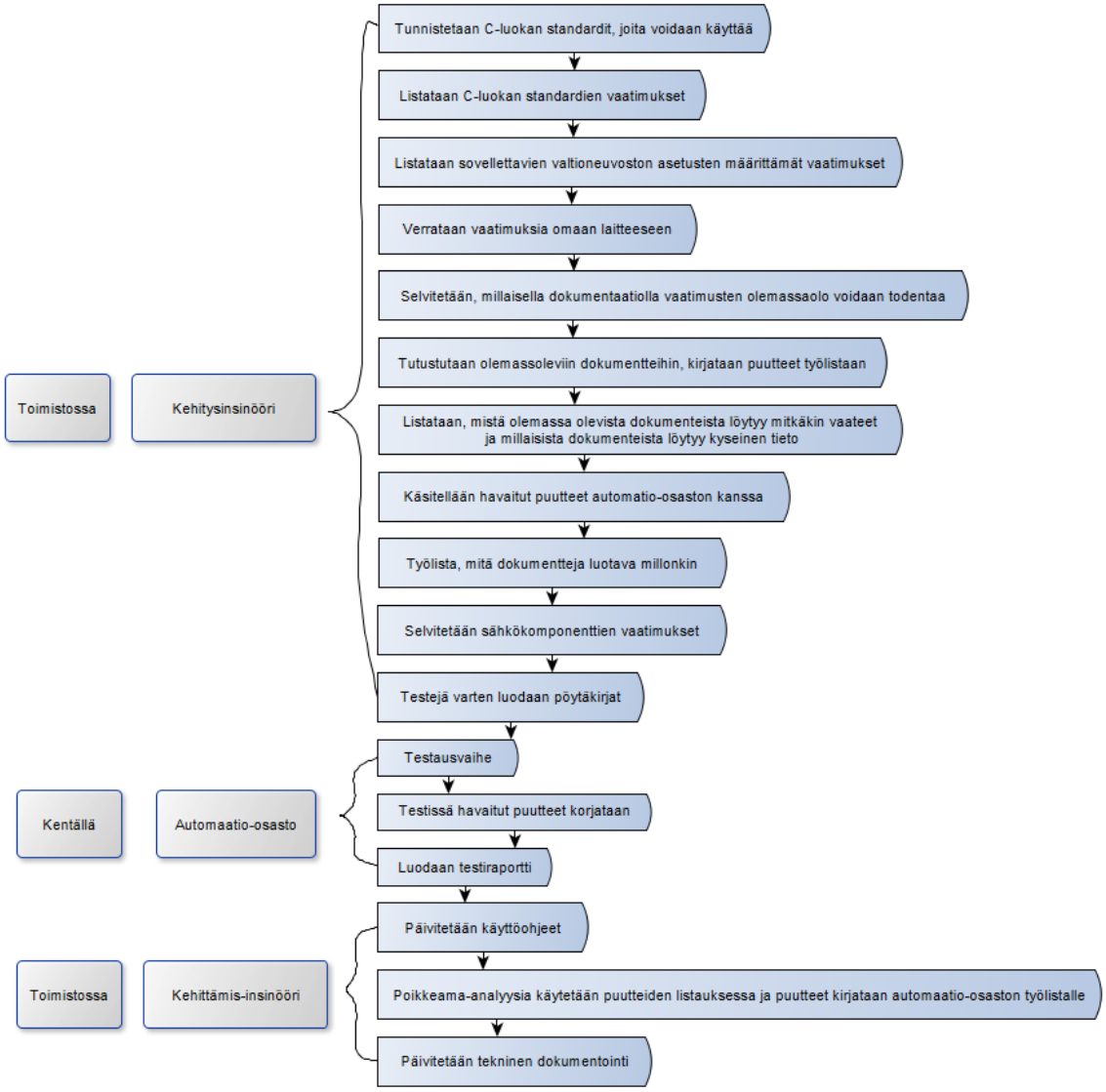
Poikkeama-analyysi v01

Havaittu puute	Toimintaohje	Dokumentoitu (kyllä/ei)	Vastuuhenkilö	Standardi	Testaustarve	PVM	Kuittaus

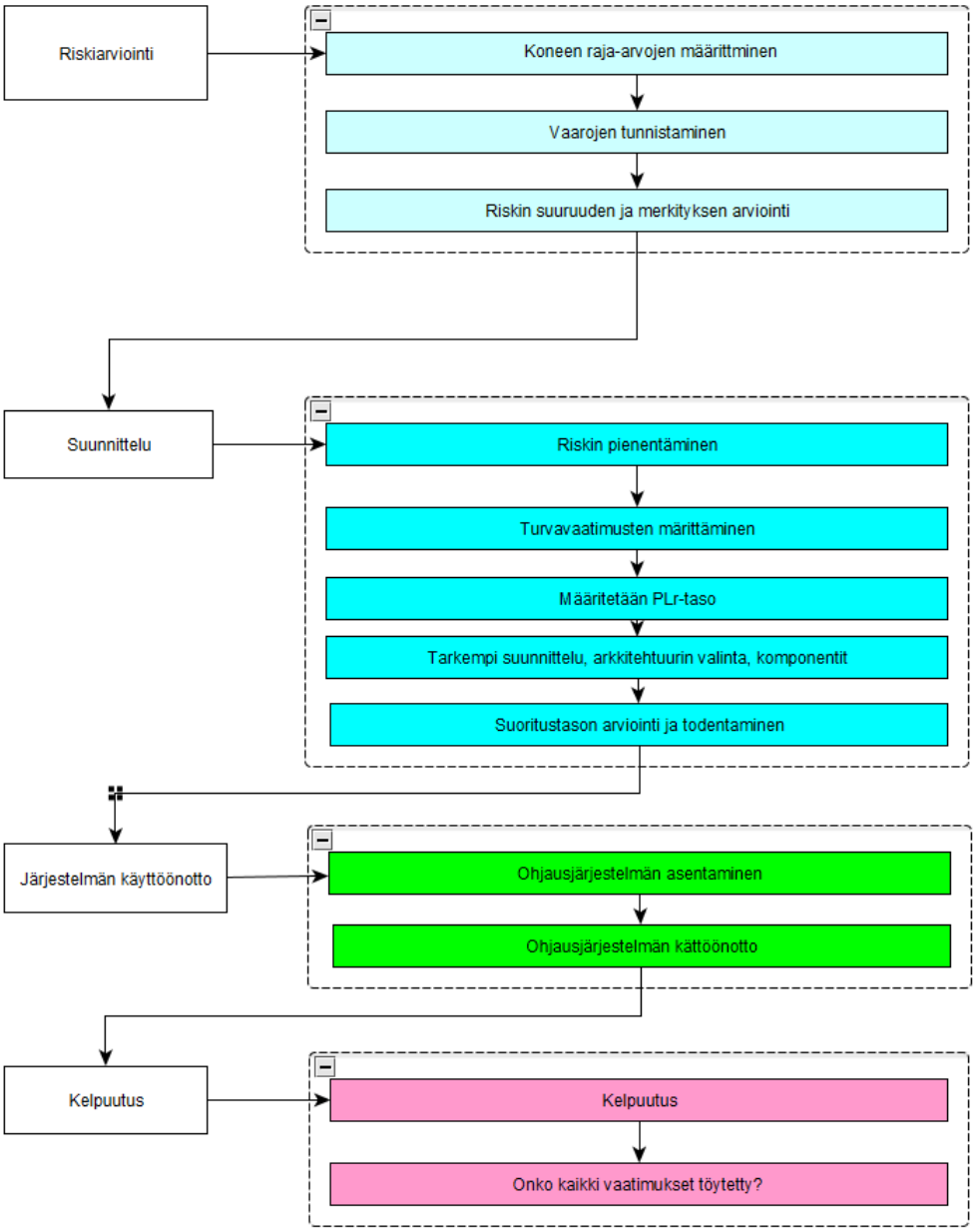
14.5.2018

1/66

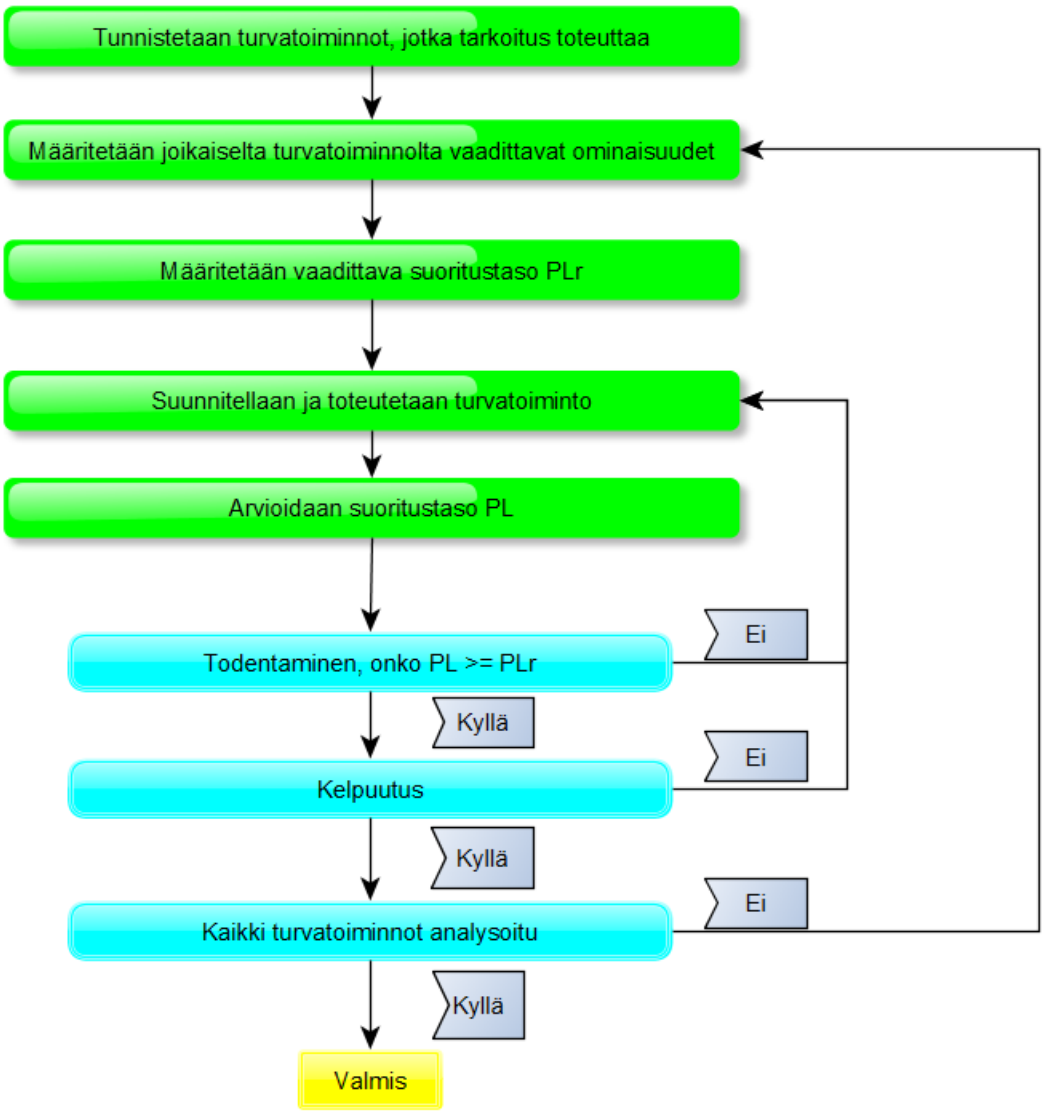
Liite 1. Poikkeama-analyysi vaihtoehto 2



Liite 2. Lohkokaavio turvallistamisprosessista



Liite 3. Lohkokaavio ohjausjärjestelmän turvallisuudesta



Liite 4. Lohkokaavio ohjausjärjestelmän osien suunnittelusta

Dokumentit	Lisätieto	Onko dokumentoitu	Dokumentoidaanko	Huomiot
turvallisuuteen liittyvien ohjausjärjestelmän osien toteuttamat turvatoiminnot				
kunkin turvatoiminnon ominaisuudet				
turvallisuuteen liittyvien ohjausjärjestelmän osien tarkat alku- ja loppukohdat				
ympäristöolosuhteet				
suoritustaso (PL)				
valitut luokat				
luotettavuuden kannalta merkitykselliset muuttujat (MTTFD, DC, CCF ja toiminta-aika)				
toimenpiteet systemaattisen vikaantumisen estämiseksi				
käytetyt teknologiat				
kaikki tarkastelussa mukana olleet turvallisuuteen liittyvät viat				
vikojen poissulkemisen perustelut (ks. ISO 13849-2)				
suunnittelun loogiset perustelut (esim. huomioon otetut viat, poissuljetut viat)				
ohjelmistoa koskeva dokumentaatio				
toimenpiteet kohtuudella ennakoitavissa olevan väärinkäytön estämiseksi				

Liite 5. Automaation turvallistamisen dokumentointi