

Artikkelisarja turvallisen koneen suunnittelusta

Osa 3: Koneiden järjestelmällinen suunnitteluprosessi

Artikkelisarja turvallisen koneen suunnittelusta

Tämän artikkelisarjan tarkoituksena on selvittää koneautomaation nykyisen nopean kehitysvaiheen vaikutuksia koneen suunnitteluun. Koneiden valmistuksessa tuotantotapa on muuttunut kansainvälisesti verkottuneeksi toiminnaksi ja tällä on ollut merkittäviä vaikutuksia koneiden suunnittelu- ja valmistusprosessiin. Samalla osaamisvaatimukset ovat kasvaneet ja koneiden valmistus on verkottunut kansainväliseksi yhteistoiminnaksi.

Artikkelisarjassa esitetään turvallisen koneen suunnittelun peruseriaatteita ja nykyaikaisen koneautomaation käyttöönottoa. Lähtökohtina ovat koneen suunnittelun ja toteutuksen laadunhallinta ja sen edellyttämä järjestelmällinen suunnitteluprosessi ja sen menettelytavat.

Artikkelisarjassa tarkastellaan tyypillisiä tavaratuotannossa käytettäviä koneita ja konejärjestelmiä, joita valmistetaan toimitettavaksi EU:n talousalueen markkinoille tai siellä käyttöönotettavaksi. Artikkeleissa tulkitaan EU:n konedirektiiviä sen soveltamissuositusten ja siihen liittyvien yhdenmukaistettujen standardien avulla.

Artikkelisarjassa käsitellään usein esiintyviä konedirektiivin soveltamisongelmia ja niiden tulkintoja, joita täydennetään tarvittaessa viittauksilla tietolähteisiin. Siten tässä artikkelisarjassa ei kerrata yksityiskohtaisesti niitä lukuisia turvallisuusteknisiä toimenpiteitä tai muita suojaustoimenpiteitä, joita esitellään koneiden turvallisuusstandardeissa ja laajassa opastavasta kirjallisuudessa.

Monet muutkin uudet vaatimukset vaikuttavat yhä vahvemmin kaikkien koneiden suunnitteluun ja valmistukseen, kuten esimerkiksi koneen energian säästämiseen, päästöjen vähentämiseen, materiaalien kierrättämiseen jne. Näissäkin toiminnoissa automaatio toimii apuna ja helpottaa tavoitteiden saavuttamista. Näitä muita kuin henkilöturvallisuuteen liittyviä vaatimuksia ei käsitellä näissä artikkeleissa.

Artikkelisarjassa tuodaan esille yksi näkökulma konedirektiivin ja koneturvallisuustandardien soveltamiseen. Kirjoittaja tai METSTA eivät vastaa artikkelisarjan perusteella tehdyistä ratkaisuksista. Epäselvissä tapauksissa on nojaututtava alkuperäisiin lähteisiin. Kommentteja ja kehitysehdotuksia voi lähettää osoitteeseen standard@metsta.fi.

Artikkelisarjan osat ovat:

1. Turvallisen koneen suunnittelu – periaatteet, säädökset ja standardit
2. Koneen valmistajan ja muiden osapuolten turvallisuusvastuut ja -velvollisuudet
3. Koneiden järjestelmällinen suunnitteluprosessi
4. Turvallisuuteen liittyvien ohjausjärjestelmien suunnittelu
5. Koneen ohjausjärjestelmän yksinkertaistettu suunnittelumenetelmä Sistema

Johdanto osaan 3

Tämä artikkelisarjan osa 3 koskee koneen turvallisuuden suunnittelumenetelmää, joka määrittää konejärjestelmän suunnittelulle järjestelmällisen etenemistavan. Erityistä huomiota kiinnitetään koneen peruskonseptin määrittämisen jälkeisiin suunnittelun vaiheisiin ja niissä käytettäviin menetelmiin, kuten koneen riskin arvioinnin vaiheet, riskin pienentämisen ensisijaisuusjärjestys, jäännösriskin minimointi ja dokumentointi. Suunnittelun vaiheiden havainnollistamiseksi tarkastellaan turvallisuusvaatimusten ja -ratkaisujen soveltamista robottiyksikköön.

Kirjoittaja

Matti Sundquist, Sundcon Oy

Tekniikan lisensiaatti Matti Sundquist on toiminut valtion työsuojeluhallinnossa yli 30 vuotta. Hänen osaamisalueensa kattaa niin perinteisen koneturvallisuuden kuin myös nykyaikaisen koneautomaation turvallisuuden. Hän toimii nykyisin projektityöntekijänä Sundcon Oy:ssä, jossa hänen toimialueenaan on alan koulutus ja yritysneuvonta.

Sisällys

1 Terminologiaa ja lyhenteitä.....	5
2 Koneen suunnittelun uudet vaatimukset.....	6
2.1 Uudet teknologiat.....	6
2.2 Järjestelmällinen lähestymistapa	7
3 Tehdassuunnittelu	8
3.1 Koneiden sijoittelu ja osastointi	8
3.2 Koneen peruskonseptin suunnittelu	9
4 Koneen riskin arviointi	11
4.1 Koneen riskin arvioinnin ongelmia	11
4.2 Riskin arvioinnin lähtökohdat.....	12
4.3 Konedirektiivin mukainen riskin arviointi	14
5 Vaarojen ja niiden aiheuttamien riskien tunnistaminen ja yksilöinti.....	14
5.1 Koneen raja-arvojen määrittäminen	14
5.2 Riskiskenaario.....	15
5.3 Vaarojen tunnistaminen.....	15
6 Riskin suuruuden ja merkityksen arviointi	16
6.1 Riskin suuruuden arviointi.....	17
6.1.1 METSTAn lomakepohja riskinarviointiin	17
6.1.2 Riskin arviointi riskigraafilla	17
6.2 Riskin suuruuden arviointimenetelmän kalibrointi.....	22
6.3 Riskin merkityksen arviointi	23
7 Riskin arviointi LOPA-menetelmällä	24
8 B- ja C-tyyppin standardeihin perustuva riskin arviointi ja riskin pienentäminen	26
9 Koneen riskin pienentämisen ensisijaisuusjärjestys.....	30
9.1 Vaihe 1: Luontaisesti turvalliset suunnittelutoimenpiteet	31
9.2 Vaihe 2 a: Ohjausjärjestelmästä riippumattomat riskin pienentämisen toimenpiteet	31
9.3 Vaihe 2 b: Turvatoiminnot.....	32
9.4 Jäännösriski	36
9.5 Vaihe 3: Täydentävät suojaustoimenpiteet	36
10 Turvallisuuteen liittyvä dokumentaatio	37
11 Viittauksia ja kirjallisuutta	38

1 Terminologiaa ja lyhenteitä

Tässä artikkelisarjassa käytetään seuraavia lyhenteitä ja termejä:

EU:n talousalue

aikaisemmin EY:n sisämarkkinat, nykyinen Euroopan Unionin talousalue

konedirektiivi, MD

EU:n konedirektiivi ja sitä vastaavaa Suomen kansallinen koneasetus

kone

kone ja/tai koneyhdistelmä

konejärjestelmä

koneiden, koneyhdistelmien ja osittain valmiiden koneiden muodostama valmistuslinja tai -laitos tms.

koneautomaatio

koneiden automaatio- ja ohjausjärjestelmä

puolivalmiste

osittain valmis kone

vaatimustenmukaisuus

konedirektiivin mukainen vaatimustenmukaisuus

standardin mukaisuus

standardin vaatimusten mukaisuus

koneen valmistaja

konedirektiivin tarkoittama koneen valmistaja (juridinen yritys tai henkilö)

työnantaja

(tavallisesti) koneen omistajan edustaja, joka voi olla myös koneen tilaaja

koneen valmistus

koneen suunnittelu ja toteutus

uusi kone

kone, jonka vaatimustenmukaisuus on osoitettu, ja joka on valmis luovutettavaksi EU:n talousalueen markkinoille tai siellä käyttöön otettavaksi

Huom. Viittaukset artikkeleihin, niiden lukuihin ja kohtiin on tehty seuraavasti

- (luku x) = kyseisen artikkelin luku x
- (kohta x.y tai x.y.z) = kyseisen artikkelin luku x kohta x.y tai x.y.z
- (osa n luku x) = artikkelin osa n luku x
- (osa n kohta x.y tai x.y.z) = artikkelin osa n luku x kohta x.y tai x.y.z

Luvussa 11 ”Viittauksia ja kirjallisuutta” standardit luetellaan standardin numerolla ja kirjallisuusviitteet luetellaan [nimilyhenteellä] hakasuluissa.

Suorat lainaukset on kirjoitettu *kursiivilla*.

2 Koneen suunnittelun uudet vaatimukset

2.1 Uudet teknologiat

Kuten kirjoitussarjan osan 1 luvuissa 1 ja 2 on kuvattu, elektroniset ohjausjärjestelmät ovat kasvaneet entistä laajemmiksi ja monimutkaisemmiksi ja niiden sovellusalat laajenevat nopeasti, jolloin koneen tai koneyhdistelmän turvallisuus on aikaisempaa enemmän koneen ohjausjärjestelmän varassa ja tämä tuo mukanaan henkilöturvallisuuden ongelmia (osa 4 kohta 3.2). Näin prosessityyppisen järjestelmän ohjauksen ominaisuudet ovat tulleet myös koneturvallisuuden asiantuntijoiden käsiteltäväksi (osa 2 kohdat 5.3 ja 7.2).

Toisaalta koneautomaation käyttöönotto tekee mahdolliseksi myös entistä tehokkaampien ja turvallisempien koneiden ja konejärjestelmien toteuttamisen. Pitkälle viedyllä automatisoinnilla ja voidaan tuotannon eri työvaiheet sulauttaa yhtenäiseksi prosessiksi ja näin parantaa konejärjestelmän kokonaisuuden ohjattavuutta, luotettavuutta, turvallisuutta ja käytettävyyttä. Koneautomaation avulla työntekijät voidaan erottaa työprosessin vaaroista ja valvoa pääsyä vaaravyöhykkeille. Myös huolto- ja korjaustöiden turvallisuutta voidaan parantaa esim. konelinjojen tai laitosten osastoinnin avulla (kohdat 3.1, 9.2 ja kohta 9.3 kuva 6).

Elektroniset ohjausjärjestelmät yhdessä muiden uusien teknologioiden kanssa tekevät mahdolliseksi myös aivan uudet sovellukset:

Elektroniikan mahdollistamia ratkaisuja

- aikaisempaa monipuolisemmat ohjaus- ja diagnostiikkatoiminnot, joilla saadaan koneeseen uusia toimintoja, esim. aikaisempaa täydellisempi ennakoiva kunnossapito
- uudentyyppiset anturiratkaisut turvatarkoituksiin, esim. yhteistyörobotit
- nopeat verkkoyhteydet, jotka antavat pääsyn suuriin tietovarantoihin, esim. päättelyalgoritmien avulla toteutetaan aikaisempaa monipuolisempaa ohjausta, säätöä, etäohjausta tai koneen autonomian lisäämistä
- turvallisuuden parantaminen ennakoimalla vaaratilanteita ja estämällä niiden kehittymistä tai antamalla varoituksen, hälytyksen tai tekemällä hätäpysäytyksen tai -alasajon
- uudet materiaalit ja valmistusmenetelmät, jotka antavat mahdollisuuksia koneen keventämiseen ja muotoiluun, esim. 3-d tulostus
- uudet akkuratkaisut, jotka antavat mahdollisuudet korvata polttomoottorikäyttöjä sähkökäytöllä, esim. uudentyyppiset mekatroniset laitteet kuten ”dronet”.

Uusista teknologioista huolimatta ihmisiin kohdistuvat tapaturmat ovat kuitenkin samanlaisia kuin ennenkin. Fyysiset vahingot tulevat edelleenkin siitä, että ihminen vahingoittuu kehoon kohdistuvan liian suuren mekaanisen tai muun energian johdosta. Esimerkiksi suurten energiakeskittymien johdosta saattaa konejärjestelmän hallinnan menettäminen johtaa vaaratilanteisiin, kun vikaantumisten johdosta koneen osien hallitsemattomat liikkeet aiheuttavat törmäys-, puristumis- tai iskeytymisvaaroja tai hallitsemattomat energian purkaukset aiheuttavat räjähdyksiä, tulipaloja, koneiden hajoamisia tai rakenteiden sortumisia ym.

Uusien teknologioiden käyttöönoton mukana on tullut myös aivan uusia ongelmia, joista ei vielä ole voitu tehdä riittävän kattavia riskiskenaarioita. Esimerkiksi vielä ei ole tietoja siitä mitä ongelmia tulee pienoishelikopterien yleistyvää käyttöä esim. tavaraliikenteessä. Joka tapauksessa uusienkin järjestelmien yleistyessä tavoitteena tulee olla nolla-toleranssi tapaturmien esiintymiselle (osa 2 luku 2).

Uusittujen ISO:n laatustandardien (osa 1 luku 3) lähtökohtana on riskien hallinta ja tämä on perustana myös koneturvallisuuden perustandardissa ISO 12100, jossa esitettävät riskien hallinnan ja niiden pienentämisen periaatteet ovat edelleen käyttökelpoisia. Nykyisen kattavasti säädellyn ja standardisoidun koneturvallisuuden perusperiaatteet ja menettelytavat eivät ole vanhentuneet, mutta uusien teknologioiden riskien hallinnassa on vielä paljon tutkittavaa ja kehitettävää.

Uusia koneita ja laitteita on suunniteltu ja otettu koekäyttöön tilanteisiin, joissa nykyiset standardisoidut turvallisuuden varmistamisen menetelmät eivät ole riittäviä. Esimerkiksi liikkuvien työkonoiden turvallisuutta ei vielä voida kaikissa ennakoivissa tilanteissa varmistaa nykyisillä anturi- ja liikkeenohjaustekniikoilla. Samoin yhteistoimintarobottien yleistymistä jarruttaa ainakin toistaiseksi turvajärjestelmien rajoittuneisuus, jonka vuoksi niiden käsittelemät työkappaleet ovat yhteistoimintakäytössä toistaiseksi kevyitä ja/tai robotin liikenopeudet on rajoitettu turvanopeudeksi. Toistaiseksi joudutaan joko tinkimään koneen toiminallisuudesta (*functionality*) tai etsimään kokonaan uusia turvallisuusratkaisuja, ja se tapahtuu nykyisin lupaavimmin sensoritekniikan ja turvaelektroniikan kehitysalueilta.

2.2 Järjestelmällinen lähestymistapa

Uusien teknologioiden ja menetelmien hyväksikäyttö edellyttää koneen valmistuksen järjestelmällistä suunnitteluprosessia (kohta 2.2). Kaikki konejärjestelmän turvallisuuteen liittyvät toiminnalliset vaatimukset toteutetaan ohjausjärjestelmällä siten, että eri tekniikoiden alajärjestelmät, kuten mekaaniset, hydrauliset, pneumaattiset, sähköiset ym. järjestelmät yhdistetään toimimaan yhtenä kokonaisuutena. Apuna tarvitaan ajan tasalla olevia eri alojen tietolähteitä kuten säädöksiä, turvallisuusstandardeja ja kirjallisuutta. Erityisesti toiminnallisen turvallisuuden suunnittelussa tietokoneavusteiset työkalut (mm. Sistema) ovat tarpeen turvallisuuteen liittyvän elinkaaren vaiheiden ja dokumentaation hallintaan (osa 4 liite 3).

Konejärjestelmien suunnittelussa ja toteutuksessa on tavallisesti mukana monia toimijoita, kuten suunnittelijoita, laitetoimittajia sekä niitä, jotka yhdistävät sähkö- ja automaatiojärjestelmiä koneisiin (mm. systeemi-integraattorit, osa 2 luku 3). Kaikkiin osaamis- ja vastuualueisiin liittyvät omalta osaltaan luotettavuuden ja turvallisuuden varmistaminen. Lopputulos riippuu pitkälti siitä, kuinka eri alojen toimijoiden ammattitaito ja käytännön toimenpiteet onnistutaan niveltämään yhteen (osa 2 luku 4).

Tarvittavat turvallisuuden varmistamisen toimenpiteet kohdentuvat koneen suunnitteluprosessin elinkaaren eri vaiheisiin ja niihin liittyviin laadunvarmistuksen toimenpiteisiin. Perustana on suunniteltavan koneen koko elinajan pituinen elinkaarimalli (*Product Lifecycle Management, PLM*). Elinkaaren eri vaiheissa tarvitaan turvallisuuden varmistamisessa erilaisia toimenpiteitä, jotka on koordinoitava ja sovitettava yhteen (osa 4 kohta 4.3).

Lisäksi koneen ohjaustoimintoja varten elinkaaren osana on erikseen käytettävissä toiminnallisen turvallisuuden elinkaari (*Functional Safety Lifecycle*, FSLC). Tyypillisiä koneen suunnitteluun liittyviä turvallisuuden elinkaaren vaiheita esitetään seuraavassa yhteenvedossa.

Konejärjestelmien elinkaaren vaiheita

1. Peruskonseptin suunnittelu
2. Riskin arviointi
3. Vaatimusmäärittely
4. Yksityiskohtainen suunnittelu
5. Ohjausjärjestelmän suunnittelu ja toteutus
6. Kelpuutus ja testaukset
7. Käyttöönotto
8. Käyttö
9. Kunnossapito ja muutokset
10. Käytöstä poisto.

Huom. Erityisesti koneen ohjaustoimintojen ja niiden turvallisuuden suunnittelussa ja toteutuksessa käytetään hienojakoisempaa elinkaarimallia. Toiminnallisen turvallisuuden ohjelmaa ja elinkaarimallia käsitellään osassa 4 luku 4.

Teknisen kehityksen mukana projektin hallinnassa yhdistyvät monet tavoitteet kuten käytettävyys, ympäristöturvallisuus, tietoturva jne. Siten myös turvallisuuden suunnittelun dokumenttien hallinta yhdistyy yhä tiiviimmin yrityksen tuotetietojen hallintajärjestelmään (*Product Data Management*, PDM).

3 Tehdassuunnittelu

3.1 Koneiden sijoittelu ja osastointi

Koneyhdistelmien ja -järjestelmien turvallisuuden suunnittelu alkaa jo tehdasjärjestelmän suunnittelusta. Tässä vaiheessa voidaan tehdä koko projektia koskevia ratkaisuja, jotka voivat vaikuttaa monin tavoin riskeihin ja myöhemmin tehtäviin turvallisuusratkaisuihin.

Jos kyseessä on tehdaskokonaisuuden suunnittelu, aluksi on selvitettävä koneen valmistajan määrittämien koneiden käyttötarkoitusten mukaiset ominaisuudet, kuten esimerkiksi fyysiset ja toiminnalliset rajapinnat, jotta koneet voidaan tarvittaessa ryhmitellä valmistusprosessin mukaisesti yhdeksi tai useammaksi koneyhdistelmäksi (osa 2 luku 7). Perustana tässä on toiminnallinen tehdasmalli, josta muodostetaan konkreettinen sijoitus suunnitelma (layout). Yksittäisen koneen peruskonseptin suunnitteluun puolestaan kuuluu koneen teknisten perusratkaisujen laatiminen (eri teknologiat), käyttötapojen määrittäminen ja niihin liittyvien ohjaustoimintojen yksilöinti.

Tehtaan koneiden sijoitussuunnitelma (layout)

- Suunnitellaan koneen tulevaa käyttötarkoitusta vastaavat tuotannolliset toiminnot.
- Määritetään koneen fyysiset mitat ja arvioidaan tarvittavat mitoitus.
- Suunnitellaan osastointi, koneiden ja koneyhdistelmien sijoittelu
- Erotetaan räjähdys- ja palovaaralliset ym. tilat.
- Ennakoidaan alustavasti koneen vaaravyöhykkeitä ja vaaratilanteita sekä niihin liittyviä turvallisuuskriittisiä toimintoja.

Sijoitussuunnitelmassa voi olla esimerkiksi

- laajoja koneyhdistelmiä
- pienempiä koneyhdistelmiä ja konelinja
- yksittäisiä koneita.

Kaikissa näissä tapauksissa jokaisella koneella tai koneyhdistelmällä on oltava valmistaja, joka huolehtii koneen turvallisuudesta ja vaatimustenmukaisuudesta sekä sen osoittamisesta. Jo tässä vaiheessa on edullista kartoittaa vastualueet ja nimetä niistä vastuussa olevat osapuolet (osa 2 kohta 4.1.1).

Koneiden ryhmittelyssä tai osastoinnissa sijoittelun (*lay-out*) vaihtoehtoja:

Esimerkiksi laaja-alaisten konejärjestelmien turvallisuuden hallitsemiseksi konejärjestelmä on useimmiten edullista jakaa paitsi käytettävyyden myös turvallisuuden parantamiseksi fyysisesti ja toiminnallisesti suhteellisen itsenäisiin koneryhmiin tai osastoihin tai jakaa robottijärjestelmät robottiyksiköihin tai -soluihin.

Jakaminen osastoihin (tuotantoyksiköihin) voi mahdollistaa osastojen jonkin asteisen tuotannollisen riippumattomuuden. Esimerkiksi työskennellessä yhdessä osastossa korjaus- tai huoltotöissä kyseistä osastoa voidaan käyttää turvallisesti käsiajon toimintatavalla ja, muissa osastoissa prosessi voi jäädä käyntiin ja.

Tavallisesti erotetaan kaikki koneryhmät tai -linjat muista työtiloista ja järjestetään valvottu pääsy erillisille työalueille (kohta 9.3 kuva 6). Muussa tapauksessa on tehtävä paikallisia suojauksia vaaratekijäkohtaisesti varmistamaan turvallinen työskentely vaara-alueella. Usein käytetään molempien lähestymistapojen yhdistelmiä ja varsinkin käytettyjen koneryhmien tai -linjojen modernisoinnissa (osa 2 kohta 11). Osastoihin jakamisessa on otettava huomioon kunnossapitotyöt koneen vaaravyöhykkeellä, kun koneita tai sen osia käsitellään tehonsyötön ollessa päällä. Tällöin huolimatta osaston tai yksikön automaattisesta pysäytystoiminnosta on otettava huomioon työskentely tehonsyötön ollessa päällä, josta voi seurata pysähtyneen koneen tai sen osan odottamaton käynnistyminen.

3.2 Koneen peruskonseptin suunnittelu

Koneen turvallisuuden suunnittelun elinkaaren ensimmäinen vaihe on koneen peruskonseptin suunnittelu. Koneen peruskonseptilla tarkoitetaan konetta koskevaa suunnitelmaa, jossa koneen käyttötarkoituksen mukaiset perustoiminnot on määritetty ja niiden toteuttamiseen tarvittavat teknologiat on valittu. Heti suunnittelun alussa ja sen edetessä on järjestelmällisesti tunnistettava koneen vaaratekijöitä, -vyöhykkeitä ja -tilanteita ja ne on kirjattava jatkokäsittelyä varten.

Koneen peruskonseptin suunnittelun tehtäviä

- Koneeseen suunnitellut ohjaustoiminnot yksilöidään (esim. eri toimintojen tarkoitus, tyyppi, ominaisuudet yms.).
- Koneen ohjaustoiminnot voivat olla manuaalisia (ihmisen ohjaamia) tai automaattisia (koneen omaan toimintaan kuuluvia) ja usein ne ovat yhdistelmiä molemmista, ks. seuraava yhteenveto.
- Suunnitelmien on oltava riittävän yksityiskohtaisia, jotta voidaan aloittaa riskin arviointi.
- Suunnittelun edetessä palataan usein suunnittelun ja elinkaaren aikaisempiin vaiheisiin aina kun joudutaan täsmentämään tai täydentämään suunnitelmaa (suunnittelun iteratiivinen prosessi (ISO 12100 luku 4 ja kuva 1).
- Koneen suunnittelua voidaan helpottaa koneen tietokonemallin avulla, jolloin voidaan simuloida koneen toimintoja ja toimintojen vuorovaikutuksia.

Peruskonseptissa voi olla myös valmiina koneen käytettävyyttä parantavia ratkaisuja, joita asennetaan ensisijaisesti koneen käytettävyyden parantamiseksi, kuten esimerkiksi systemaattisten virheiden estämistä (osa 4 luku 7 ja osa 5 luku 2 kohta 4.3.2). Käytettävyyden parantamiseksi aikaan saatu parempi luotettavuus vähentää esimerkiksi koneen/prosessin tarpeettomia pysäyttämisiä ja auttaa pysymään tuotannon aikataulussa. Tämä luotettavuuden parantaminen lisää myös toimintojen turvallisuutta ja siten myös näitä toimintoja voidaan käsitellä turvallisuuteen liittyvinä toimintoina. Tässä artikkelisarjassa ei käsitellä tarkemmin ohjaustoimintojen luotettavuutta muutoin kuin turvallisuuden kannalta (osat 4 ja 5).

Koneen peruskonseptissa on tässä vaiheessa erilaisia teknisiä rakenteita ja toimintoja, joiden tarkoituksena on toteuttaa koneen käyttötarkoituksen mukaiset tehtävät. Siten jo peruskonseptissa tunnistetaan alustavasti erilaisia vaarakohtia ja myös vaarallisia toimintoja. Usein toteutetaan myös luonnostaan turvallisia ratkaisuja, kuten esimerkiksi koneen liikkuvien osien turvallisuuden varmistamista rakenteellisin menetelmin (luku 3 ja kohdat 9.1 vaihe 1 ja 9.2 vaihe 2 sekä ISO 12100 luku 4 ja kuva 2).

Monet toiminnot voivat olla turvallisuuteen liittyviä toimintoja paitsi suoraan (esim. käynnistys pysäytys, toimintatavan valinta jne.) myös välillisesti (esim. varolaitteet). Monet toiminnot voivat kuitenkin olla paitsi suoraan (esim. käynnistys pysäytys, toimintatavan valinta jne.) myös välillisesti turvallisuuteen liittyviä toimintoja (esim. varolaitteet). Kaikki toiminnot eivät kuitenkaan ole turvallisuuteen liittyviä, jos virheellinen toiminto ei aiheuta edes välillisesti mitään turvallisuuteen liittyvää vaikutusta suoraan tai muiden toimintojen kautta.

Erityisesti kaikki koneen ja sen laitteiden ohjaustoiminnot, joilla on suora tai epäsuora vaikutus turvallisuuteen muiden toimintojen kautta, yksilöidään tässä vaiheessa tulevia riskin pienentämisen toimenpiteitä varten. Suunnittelun täsmentyessä tarkistetaan näiden ohjaustoimintojen keskinäiset riippuvuudet ja ajoitukset, jotka voivat johtua myös muista toiminnoista tai koneen toimintatiloista tai edellyttää muiden toimintojen määrättyä tilaa. Tarkoituksena on saada kaikki koneen ohjaus- ja turvatoiminnot loogisesti yhteensopiviksi ja niiden ajoitukset kohdalleen. Apuna voidaan käyttää kytkentä-, logiikka-, ajoitus- ym. kaavioita.

Koneen ohjaustoimintoja

- käynnistys ja uudelleen käynnistys
- (tuotanto)pysäytys, turvapysäytys ja hätäpysäytys
- kaksinkäsinhallintalaitteen ohjaustoiminto
- toimintatavan valinta (esim. automaattiajo – käsiajo)
- nopeuden säätö (esim. maksiminopeus)
- nopeuden rajoittaminen (esim. turvanopeus)
- toimintojen lukitukset
- toiminnon kuittaukset
- toimintojen lukitusten vapautukset jne.

Tämä on välttämätöntä mm. sen vuoksi, että myöhemmässä vaiheessa voidaan toisinaan yhdelläkin hyvin suunnitellulla turvatoiminnolla kattaa kerralla useampien toimintojen virheiden ja vikaantumisten aiheuttamia riskejä (esimerkki kohta 9.3).

Samalla voidaan alustavasti selvittää turvallisuuteen liittyvien toimintojen vikaantumisten vaikutuksia. Näitä tietoja voi käyttää tarvittaessa apuna koneeseen lisättävien turvatoimintojen suunnittelussa ja ne on dokumentoitava.

Vaikka tässä vaiheessa koneessa ei ole vielä ole tehty riskin tunnistamista, yksilöintiä eikä arviointia, voidaan kuitenkin ennakoida mahdollisia riskejä ja tehdä niiden pienentämiseen tähtääviä ratkaisuja (riskin pienentämisen vaiheet vaiheet 1 (kohta 9.1) ja 2 b (kohta 9.2). Myöhemmin riskien arvioinnin tulosten perusteella tarkistetaan, onko riskejä pienennetty tarpeeksi. Jäljelle jääneiden riskien pienentämiseksi voi olla tarpeen palata tähän konseptivaiheeseen ja muuttaa koneen rakennetta, sen toimintoja tai varmistaa turvallisuutta erilaisilla teknologioilla ja/tai turvatoiminnoilla riskin pienentämisen menetelmien ensisijaisuusjärjestyksen mukaisesti (luku 9). Lopuksi tarkistetaan, että on saavutettu riittävän pieni jäännösriski (kohta 9.4).

4 Koneen riskin arviointi

4.1 Koneen riskin arvioinnin ongelmia

Nykyiset käytössä olevat dokumentoidut koneiden riskin arviointimenetelmät (esim. ISO/TR 14121-2) soveltuvat sellaisenaan monien erityyppisten koneiden valmistukseen. Kuitenkin joissakin tapauksissa jokin muu menetelmä tai standardin mukaisen menetelmän parametrien tai parametrien arvojen skaalauksen muokkaaminen (kalibrointi) saattaa olla tarpeen.

Erilaisia riskin arviointimenetelmien sovellusalueita

- Käsin ohjattavien koneiden riskin arviointiin, jos turvallisuus riippuu pitkälti koneen käyttäjän jatkuvasta ohjauksesta, olisi otettava mukaan parametri ”ohjattavuus” (*controllability*, esim. liikkuvat työkoneet).
- Prosessityyppisissä järjestelmissä olisi otettava huomioon koneiden osuus prosessiriskien arvioinnissa (esim. lämpövoimalaitos).
- Suurten riskien (*worst-case*) arvioinnissa (esim. koneisiin liittyvät palo- ja räjähdysvaarat) tulisi käyttää riskiparametreihin perustuvan riskin arvioinnin asemesta LOPA-tyyppistä (*layer of protection*) arviointia (kohta 7).
- Fyysisen ja psyykkisen altistumisen aiheuttamia pitkäaikaisen vaikutuksen aiheuttamia riskejä ei voi arvioida koneiden turvallisuutta koskevilla parametreilla.

Joskus koneyhdistelmään yhdistettävien koneiden eri valmistajat ovat riskin arvioinnissa käyttäneet erilaisia riskinarvioinnin menetelmiä tai samojen menetelmien erilaisia riskiparametrien asteikkoja tai valintaohjeita, jolloin riskin arvioinnin tuloksia on hankala yhdistää. Ongelmaksi voi tulla koko koneyhdistelmältä vaadittavien ohjaustoimintojen vaatimusten määrittäminen (esim. suoritustasovaatimukset).

4.2 Riskin arvioinnin lähtökohdat

Riskin arvioinnissa tunnistetaan ja yksilöidään mahdollisimman kattavasti

1. kaikki koneen vaarat (vaarakohdat),
2. jokaisen vaaran aiheuttamat riskit ja
3. arvioidaan niiden toteutumisen mahdolliset seuraukset.

Riskin suuruuden arviointi tehdään dokumentoidulla riskin arviointimenetelmällä.

Huom. Riskin arviointi tehdään siinä vaiheessa, kun koneen peruskonsepti on riittävän valmis, mutta koneeseen ei ole vielä lisätty mitään riskin pienentämisen toimenpiteitä.

Riskin arviointi olisi tehtävä asiantuntijatyöryhmässä, jossa on mukana koneen suunnittelijoita, tarpeen mukaan eri teknologioiden ja erityisalojen turvallisuuden asiantuntemusta sekä jos on mahdollista, mukaan tarvittaisiin myös kokeneita koneen käyttäjiä arvioimaan ehdotusten käytettävyyttä. Työryhmään tarvitaan ainakin yksi riskin arviointiin perehtynyt henkilö, joka voi toimia myös työryhmän vetäjänä. Työryhmän tavoitteena on tehdä mahdollisimman kattava, tarkka ja objektiivinen riskin arviointi kaikille vaaroille. Tämän jälkeen päätökset yksilöityjen riskien pienentämisestä tehdään työryhmän kokoonpanossa, jossa on mukana yrityksen vastuullista johtoa.

Alustava riskin arviointi (*preliminary risk assessment*) voidaan tehdä heti, kun koneen peruskonsepti on riittävän yksityiskohtainen vaarallisen tapahtuman kuvaamiseksi (kohta 3.2). Tällöin koneen fyysinen rakenne ja käyttötoiminnot ovat ainakin alustavasti suunniteltu valmiiksi siten, että kone voisi ainakin periaatteessa jo tämän suunnitelman mukaisesti toimia käyttötarkoituksensa mukaisesti, mutta kone ei vielä ole turvallinen, koska siihen ei tässä vaiheessa ole vielä tehty riskin pienentämisen alussa tarvittavia toimenpiteitä (kohdat 9.1 ja 9.2). Kaikkien koneen toimintaan tarvittavien laitteiden ja niiden toimintaa liittyvät rajoitukset,

lukitukset tms. on kuitenkin oltava suunnitelmassa mukana, esimerkiksi koneen käyttöön kuuluvien toimintojen keskinäiset lukitukset.

Jo koneen peruskonseptin suunnittelussa sen rakenteissa voidaan havaita ilmiselviä vaaroja, joiden aiheuttamat riskit dokumentoidaan myöhemmin tehtävää riskin arviointia. Tässä vaiheessa ei vielä suunnitella erikseen mitään turvalaitteita tai -toimintoja. Vasta riskin suuruuden määrittämisen vaiheessa päätetään arvioidun riskin suuruuteen nähden riittävän tehokkaista riskin pienentämisen toimenpiteistä (luku 9):

Riskien pienentämisen suunnitteluvaiheet

- riskinarvioinnin tulosten perusteella tehdään päätökset jokaisen riskin kohdalla siitä, miten vakavia riskit ovat ja miten niitä aiotaan pienentää
- seuraavaksi suunnitellaan tai valitaan riskin suuruuden perusteella riittävän tehokkaat menetelmät kaikkien riskien riittävään pienentämiseen (toimenpiteiden ensisijaisuusjärjestys (kohdat 9.1 ja 9.2 vaiheet 1 ja 2 a))
- sen jälkeen suunnitellaan koneen ohjausjärjestelmän toteuttamat turvatoiminnot huolehtimaan riskien pienentämisestä (kohta 9.3 vaihe 2 b))
- lopuksi selvitetään jäännösriskin suuruus ja tarvittaessa myös sen pienentämisen toimenpiteet (kohdat 9.4 ja 9.5 vaihe 3).

EU:n talousalueen koneturvallisuuden perusstandardissa ISO 12100 ja muissa konetta koskevissa yhdenmukaistetuissa standardeissa esitetään tietoja ja ohjeita siitä, mikä on konedirektiivin vaatimusten täyttämiseen riittävää. Jos kyseiselle koneelle tai koneryhmälle ei ole omaa C-tyyppin standardia, myös muiden koneiden standardeissa voidaan käsitellä samaa tai samanlaista vaaraa/riskiä, ja niitä tietoja on syytä käyttää apuna arvioitaessa riskin pienentämisen riittävyttä. Tavoitteena on riittävän pieni jäännösriski, joka perustuu yrityksen turvallisuussuunnitelmassa esitettäviin riskien hallinnan tavoitteisiin (esim. jäännösriskin suuruus, kohta 9.4 ja osa 1 kohta 3.2).

Koneen peruskonseptiin mahdollisesti jo suunniteltuja toimintoja, joiden vaadittavan suoritustason PLr-arvo ei perustu kyseessä olevan koneen tai täysin vastaava koneen riskien arviointiin, ei voi käyttää sellaisenaan koneen suunnittelussa. Kyseisen toiminnan vaadittava suoritustaso PLr on arvioitava erikseen siinä vaiheessa, kun riskien suuruuden perusteella toteutetut ohjausjärjestelmästä riippumattomat turvallisuustekniset toimenpiteet on suunniteltu (kohta 9.2 vaihe 2 a)).

Jos uusi kone suunnitellaan muunnoksena aikaisemmin toteutetusta konetyypistä, uuden koneen suunnittelijalla pitäisi olla käytettävissä aikaisemman konetyypin tarkat suunnitteludokumentit. Niiden avulla voidaan tarkistaa, ovatko riskin arvioinnissa käytetyt riskiparametrit sovellettavissa sellaisenaan myös uuden koneen vastaavaan riskiin (riskiskenaario kohta 5.2). Jos mitään asiaan kuuluvia eroja ei esiinny, koneen suunnittelija voi soveltaa aikaisemman konetyypin turvallisuusteknisiä toimenpiteitä (kohta 9.2 vaihe 2 a)). Tällöin myös turvatoiminnon suunnittelussa voidaan käyttää samaa vaadittavaa suoritustasoa PLr kuin aikaisemminkin.

Huom. Kaikkien riskin pienentämisen toimenpiteiden jälkeen jäävän ensimmäisen jäännösriskin edelleen pienentäminen on työnantajan velvollisuutena työpaikan työsuojelun toimenpiteillä, kunnes saavutetaan siedettävä toinen jäännösriski (kohta 9.4).

4.3 Konedirektiivin mukainen riskin arviointi

Konedirektiivi velvoittaa koneen valmistajaa tekemään tai teettämään koneen riskin arvioinnin (luvut 5 ja 6) ja sen tulokset on liitettävä koneen tekniseen tiedostoon ja tulosten perusteella on tehtävä tarvittavat riskin pienentämisen toimenpiteet (luku 9).

Konedirektiivin liitteessä I ”*Olennaiset turvallisuus- ja terveysvaatimukset*” kohdassa ”*Yleiset periaatteet 1*” esitetään koneiden riskinarvioinnin vaiheet koneen valmistajalle:

- konedirektiivin liite I ”Yleiset periaatteet”, kohta 1: *Koneen valmistajan tai tämän valtuutetun edustajan on varmistettava, että suoritetaan riskin arviointi, jotta koneeseen sovellettavat terveys- ja turvallisuusvaatimukset voidaan määrittää. Kone on sen jälkeen suunniteltava ja rakennettava ottaen huomioon riskin arvioinnin tulokset.*
- *edellä tarkoitettu riskin arviointi ja riskin pienentäminen on iteratiivinen prosessi, jonka aikana valmistajan tai tämän valtuutetun edustajan on*
- *määritettävä koneen raja -arvot, joihin sisältyvät tarkoitettu käyttö sekä kohtuudella ennakoitavissa oleva väärinkäyttö,*
- *tunnistettava koneen mahdollisesti aiheuttamat vaarat ja niihin liittyvät vaaratilanteet,*
- *arvioitava riskin suuruus ottaen huomioon mahdollisen vamman tai terveyshaitan vakavuus ja todennäköisyys,*
- *arvioitava riskin merkitys sen määrittämiseksi onko riskiä tämän direktiivin tavoitteiden mukaisesti pienennettävä,*
- *poistettava vaarat tai pienennettävä näihin vaaroihin liittyviä riskejä soveltamalla suojaustoimenpiteitä 1.1.2 kohdan b alakohdassa määrättyssä ensisijaisuusjärjestyksessä.”*

Standardissa ISO 12100 esitetään tarkemmin konedirektiivin määritysten mukaiset riskin arvioinnin käsitteet, periaatteet ja vaiheet sekä kuvataan monipuolisesti riskiin vaikuttavia tekijöitä. Teknisessä raportissa ISO/TR 14121-2 esitetään esimerkkejä koneiden riskin suuruuden arvioinnin menetelmistä.

5 Vaarojen ja niiden aiheuttamien riskien tunnistaminen ja yksilöinti

5.1 Koneen raja-arvojen määrittäminen

Aluksi määritetään koneiden ”raja-arvot” tehdassuunnitelman, koneiden sijoittelun (kohta 3.1) sekä peruskonseptin avulla. Määrittämisessä tarkistetaan koko koneen tai koneyhdistelmän fyysiset rajat. Koneyhdistelmien osalta tarkistetaan myös ovatko koneyhdistelmän osina olevat koneet koneyhdistelmän määritelmän mukaisia eli koneet on yhdistetty sekä fyysisesti että toiminnallisesti (osa 2 kuva 5 ja liite 1).

Raja-arvojen määrittämisessä otetaan huomioon myös koneiden toiminnalliset rajoitukset (koneen erilaiset toimintatavat, esim. automaattiajo ja käsiajo) sekä käyttö- ja ympäristöolosuhteiden rajoitukset (esim. ulkona vs. sisällä käytettävät koneet, lämpötilarajat, EMC- ja ATEX-ympäristö ym.). Rajojen tunnistamisessa on otettava huomioon koneen elinkaaren kaikki vaiheet sekä niihin vaiheisiin kuuluvat työtehtävät, koneen toimintatavat ja käyttötilanteet (standardi ISO 12100).

Huom. Ennakoitavissa oleviin vaaratilanteisiin kuuluu myös koneen kohtuudella ennakoitavissa olevat väärinkäytön mahdollisuudet.

5.2 Riskiskenaario

Tunnistetun vaaran aiheuttaman riskin yksilöimiseksi tehdään riskiskenaario, joka on kuvaus siitä, millä todennäköisyydellä kyseisen vaaran aiheuttama riski toteutuu aiheuttaen työtapaturman tai muun vahingollisen tapahtuman. Skenaariossa kuvataan riskin toteutumiseen johtavan tapahtumaketjun erilaisia vaiheita/tapahtumia ja niiden esiintymisen todennäköisyyksiä. Tämän tapahtumaketjun avulla riskin suuruus arvioidaan mahdollisen vahingon vakavuuden ja sen toteutumisen todennäköisyyden perusteella (luku 6).

Robottiesimerkki riskin arvioinnista:

Tässä esimerkissä tarkastellaan robotin vaaravyöhykettä robotin varren liikkeiden muodostamassa tilassa, jossa vaarakohtia ovat robotin varren liikkeiden ja varteen kiinnitetyn työkappaleen kiinnityslaitteen iskut sekä robotin varren ja kiinteiden rakenteiden väliset puristuskohdat. Standardin ISO 12100 mukaisesti riskiskenaario on jaettu seuraaviin vaiheisiin:

- työntekijän työtehtävä: esim. virheellisessä asennossa olevan työkappaleen asemointi käsin oikeaan asentoon
- vaaralle altistuminen riippuu siitä, kuinka usein ja kuinka pitkäksi aikaa kerrallaan työntekijä on vaaravyöhykkeellä
- vaaratilanne syntyy, jos robotti käynnistyy odottamatta
- vaarallinen tapahtuma syntyy, jos työntekijä on altistunut vaaralle (vaaratilanne) ja robotti käynnistyy odottamatta (vaarallinen tapahtuma) eli näiden molempien tapahtumien seurauksena voi tulla henkilövahinko
- henkilövahinko syntyy edellisen vaiheen aikana, jos henkilö ei pysty väistämään vaaraa
- henkilövahingon vakavuudelle valitaan tavallisesti pahin kohtuudella ennakoitavissa oleva vakavuus. Tyypillisen teollisuusrobotin suurista voimista, nopeuksista sekä laajoista liikeradoista johtuen vahinko voi olla tavanomaista korkeampi.

Standardin ISO 12100 taulukoita ja ohjeita on syytä käyttää apuna riskiskenaarion laatimisessa ja riskiparametrien arvojen asettamisessa.

5.3 Vaarojen tunnistaminen

Raja-arvojen selvittämisen jälkeen tunnistetaan mahdollisimman kattavasti kaikki mahdolliset raja-arvojen piiriin kuuluvat vaarat. Jokainen tunnistamaton vaara aiheuttaa piilevän riskin ja tästä johtuvat odottamattomat vaaralliset tapahtumat (esimerkiksi koneen käynnistyminen tai sen ajoitus tapahtuu vastoin koneen käyttäjän odotusta) aiheuttavat koneen käytössä suurimmat riskit.

Kaikki tunnistetut vaarat on luetteloitava ja yksilöitävä (esim. riskigraafit, kohta 6.1).

Tunnistettujen vaarojen analysointi on ensiarvoista turvallisuuden varmistamiselle. Vaarallisen tapahtuman seuraukset ovat pitkälti satunnaisia ja usein väistämällä vaaraa säästytään henkilövahingoilta. Mutta tämä ei aina onnistu, ja siksi yhtään onnistuneesti väistettyä läheltä-piti-tapahtumaa eikä muita harvinaisia tapauksia ei pidä jättää ottamatta huomioon, vaan jokaisesta ei-toivotusta tapahtumasta on otettava opiksi ja pyrittävä estämään vastaavat tapahtumat ennen kuin ne johtavat vahinkoon. Tämä koskee sekä koneen suunnittelijaa, mutta ennen muuta työpaikan työnantajaa, jonka tulee koota tietoja näistä tapahtumista.

Pahimman seurauksen aiheuttava vahinko voi edustaa useita kyseiseen tapaturmatyyppiin kuuluvia seurauksia (*"worst-case studies"*). Esimerkiksi "työntekijän käden puristumisesta konevoimalla liikkuvien osien väliin" voi tulla erisuuruisia seurauksia, jolloin pahimman seurauksen estämisen toimenpiteet voivat samalla estää myös lievemmat seuraukset.

Samasta syystä johtuvia tapaturmia, jotka ovat vakavuudeltaan erilaisia, voidaan käsitellä riskin arvioinnissa myös erikseen. Tällöin mahdollisiin erilaisiin tilanteisiin (esim. automaattiajo, käsiajo jne.) voidaan valita erityyppisiä turvallisuusteknisiä ratkaisuja (esim. liikenopeuksien hidastaminen, turvalaitteet, varoituslaitteet ym.), joilla voi olla erilaiset PL-tasot.

Robottiesimerkki robotin liikkeiden nopeuksista: Joskus robotin yhteistoimintarobotin määrätyt työvaiheet joudutaan tekemään suurella nopeudella ja tällöin työvaihe on merkittävästi vaarallisempi kuin robotin tavanomaiset työvaiheet hitaalla nopeudella. Tällöin robottiyksikkö voidaan varustaa esimerkiksi kahdella erillisellä turvatoiminnolla, jossa suuremman nopeuden tilannetta ohjataan kauempaa suojatulta paikalta ja hitaalla nopeudella voidaan toimia yhteistyörobotin kanssa lähietäisyydellä. Näistä ratkaisuista esitetään tarkat ohjeet robottiyksikköjen turvallisuusstandardissa ISO 10218-2.

6 Riskin suuruuden ja merkityksen arviointi

Koneiden riskin suuruuden arviointiin on lukuisia erilaisia menetelmiä, mutta valtaosa niistä perustuu riskiparametreihin. Erilaisille vaarallisimmille koneryhmille on kehitetty (kalibroitu) tyypillisiä riskiparametreja, riskiparametrien asteikkoja ja parametrien arvojen valintaohjeita. Eräillä koneryhmillä on myös niille tyypillisiä "omia" riskiparametreja, esim. autoalan teknisen turvallisuuden standardissa on konepuolen riskiparametrien lisäksi tärkeä parametri "ohjattavuus".

Standardissa ISO 12100 esitetään riskin arvioinnin periaatteet ja ohjeita. Tämän lisäksi teknisessä raportissa ISO/TR 14121-2 esitetään erilaisia riskin arvioinnin menetelmiä ja käytännön esimerkkejä koneiden riskien arvioinnista. Riskin arvioinnin dokumentit ja tulokset ovat perustana riskien pienentämisen turvallisuusteknisille toimenpiteille ja sen jälkeen myöhemmin vaadittavien suoritustasojen PLr määrittämiseen.

Tyypillisesti vaarallisen tapahtuman ilmaantuessa turvalaite pysäyttää koneen ja pitää sen turvallisessa tilassa. Jos kyseessä on erilliset yksittäiset koneet, joiden vaaravyöhyke rajoittuu koneen välittömään läheisyyteen, koneen pysäyttäminen vaaratilanteessa on tavallisesti riittävä ratkaisu.

Sen sijaan automaattisten valmistusjärjestelmien kehittyessä valmistetaan laajoja konejärjestelmiä, joiden vaaravyöhykkeet voivat olla myöskin laaja-alaisia. Näissä tapauksissa, varsinkin kun kyseessä ovat hyvin vakavat tai kuolemaan johtavat vaarat, on syytä käyttää yksityiskohtaisempia riskin arvioinnin menetelmiä, jotka perustuvat tapaturmaskenaarioihin (vaaran etenemisen malleihin, esim. IEC 61508-5). Nämä mallit alkavat olla yhä ajankohtaisempia automaattisille valmistusjärjestelmille (osa 2 kohdat 5.3 ja 7.2).

Siten turvallisuusvaatimuksiin on tullut mukaan myös vaatimuksia toiminnan käytettävyyden parantamiseen (luotettavuuden ja jatkuvuuden vaatimukset), kuten vaatimuksia esimerkiksi

- hälytysten hallintaan
- häiriöiden sattuessa hyvin lyhyisiin toipumisaikoihin
- operaattorin toimintaan osana prosessia.

Esimerkiksi ohjausjärjestelmien turvallisuuteen liittyvät komponentit ovat usein samoja sekä konejärjestelmien että prosessien ohjauksessa eikä komponenttien SIL- ja PL-tasojen määrittelyssäkään ole suuria eroja. Molempia käytetään yhä enemmän puolin ja toisin ja ne ovat alajärjestelmien tasolla vaihtokelpoisia (osa 4 kohta 5.2.3). Siten myös konejärjestelmien ohjauksessa otetaan huomioon aikaisempaa monipuolisemmin paitsi tekniset näkökohdat myös käyttäjän/operaattorin toiminta [Valvomo, Suunnitteluperiaatteet...: Kirjallisuutta].

6.1 Riskin suuruuden arviointi

6.1.1 METSTAn lomakepohja riskinarviointiin

Metalliteollisuuden standardisointiyhdistys METSTA on laatinut riskin arviointia varten lomakealustan, jonka avulla voidaan valita ja tallentaa johdonmukaisesti riskin arviointiin tarvittavat tiedot. Seuraavassa lomakepohjan esittely:

”METSTA on julkaissut excel-muotoisen riskin arviointiin soveltuvan lomakepohjan, joka perustuu standardiin SFS-EN ISO 12100:2010 ja tekniseen raporttiin SFS-ISO/TR 14121–2:2013. Lomakepohja on laadittu helpottamaan riskin arvioinnin aloittamista ja tarjoamaan vinkkejä ja hyviä menettelytapoja.

Lomakepohja on tarkoitettu erityisesti PK-sektorille. Avoimena ja excel-muotoisena sitä on helppo jatkojalostaa yrityksen omiin tarpeisiin.

Tässä lomakepohjassa käytettävä menetelmä soveltuu koneasetuksen (400/2008) tarkoittamille uusille koneille ja koneyhdistelmille. Taulukkoa voi soveltaa myös käytössä olevien koneiden riskien arviointiin ja modernisointitöihin. Lomake sopii muistilistaksi kartoitettaessa koneen riskejä.

On huomattava, että tämä mallipohja on vain yksi lähestymistapa ja riskin arviointi voidaan yhtä hyvin tehdä myös muunlaisia tekniikoita käyttäen.

Mallipohjaan on sisällytetty riskinarvioinnin esimerkkinä pituusleikkurin muutamia vaaroja.

Lue tarkemmat ohjeet lomakkeen saatesanoista.”

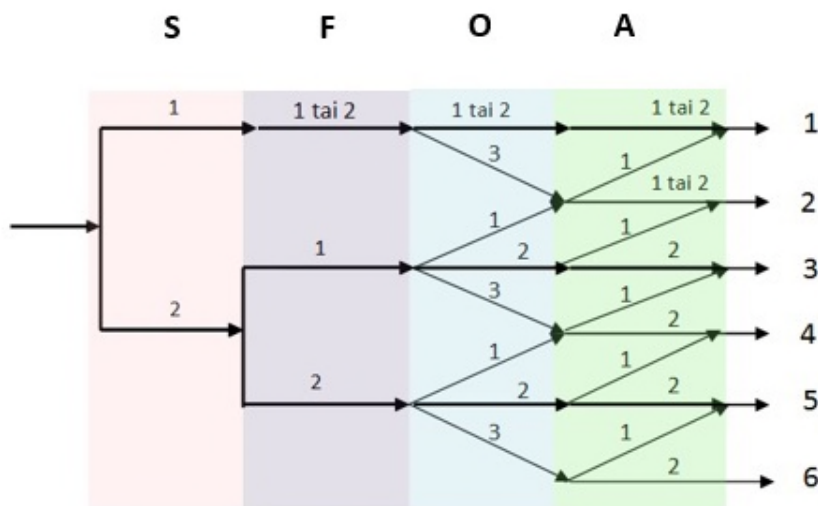
6.1.2 Riskin arviointi riskigraafilla

Seuraavassa taulukossa esitetään koneturvallisuuden perusstandardissa ISO 12100 esitettävät riskiparametrit, jotka sopivat tavanomaisten valmistustekniikan koneiden riskien suuruuden arviointiin.

Riskin suuruuden arviointi: riskiparametrit (ISO 12100)

- Riski on vaarallisen tapahtuman seurausten ja riskin esiintymistodennäköisyyden yhdistelmä (funktio).
- Riskitekijät (riskiparametrit) ovat:
 - a) seuraus S (Severity), joka luokitellaan sen vakavuuden mukaan,
 - b) seurausten esiintymistodennäköisyys P (Probability), joka määritetään seuraavien riskitekijöiden avulla:
 1. vaaralle altistumisen taajuus ja/tai kesto, F (Frequency)
 2. vaarallisen tapahtuman esiintymistodennäköisyys, O (Occurrence)
 3. mahdollisuus välttää vaaraa, A (Avoidance of danger).

Robottiesimerkki riskin suuruuden arvioinnista: Tässä esimerkissä riskin suuruuden arviointi tehdään yhdistämällä riskiparametrien arvot teknisessä raportissa ISO/TR 14121-2 esitetävän taulukon B.1 riskigraafin avulla (kuva 1). Esitystapa on havainnollinen, koska siitä näkyy miten eri riskiparametrit suhtautuvat toisiinsa ja vaikuttavat lopputulokseen.



Kuva 1 Tapaturmaskenaarion mukainen riskigraafi (ISO/TR 14121-2 taulukko B.1)

Riskigraafin muuttujien valintaohjeet (ISO/TR 14121-2, kohta 6.2.2)**Vahingon vakavuus S (severity):**

S1: Lievä vamma: (tavallisesti palautuva, esimerkiksi naarmut, viillot, mustelmat tai ensiapua vaativat pienet haavat jne.) ja kyvyttömyys suorittaa samaa tehtävää ei kestä pitempää kuin kaksi päivää.

S2: Vakava vamma: (tavallisesti palautumaton, mukaan luettuna kuolema: esimerkiksi murtuneet, irtirevenneet tai puristuneet raajat, luunmurtumat, tikkejä vaativat vakavat haavat, huomattavat tuki- ja liikuntaelimistön ongelmat jne.), kyvyttömyys suorittaa samaa tehtävää kestää pitempään kuin kaksi päivää.

Vaaralle altistumisen taajuus ja/tai kesto F (frequency):

F1: Harvoin tapahtuvasta usein tapahtuvaan ja/tai lyhyt altistumisaikaa

Altistuminen vaaralle enintään kahdesti työvuoron aikana tai alle 15 minuutin kerääntyvä altistuminen työvuoron aikana.

F2: toistuvasta jatkuvaan altistumiseen ja/tai pitkä altistumisaika

Altistuminen vaaralle useammin kuin kahdesti työvuoron aikana tai yli 15 minuutin kerääntyvä altistuminen työvuoron aikana.

Vaarallisen tapahtuman esiintymistodennäköisyys O (occurrence):

O1: pieni (niin epätodennäköinen, että tapahtuma ei ehkä toteudu)

Kehittynyt teknologia, koeteltu ja arvostettu turvallisuussovelluksissa, jämäkkyys.

O2: keskimääräinen: (todennäköisesti tapahtuu joskus)

Tekninen vikaantuminen havaittu viimeksi kuluneen kahden vuoden aikana. Hyvin koulutetun riskiestä tietoisien ja enemmän kuin kuusi kuukautta työpisteessä työskennelleen henkilön virheellinen toiminta.*

O3: suuri: (tapahtuu todennäköisesti usein)

Toistuvasti havaittu tekninen vikaantuminen (joka kuudes kuukausi tai useammin).

*Kouluttamattoman alle kuusi kuukautta työpisteessä työskennelleen henkilön virheellinen toiminta.**

Vahingon välttämisen tai rajoittamisen mahdollisuus A (avoidability):

A1: mahdollista jossain tilanteissa:

- *Jos osat liikkuvat alle 0,25 m/s nopeudella ja vaaralle altistuva henkilö tuntee hyvin riskin sekä vaaratilanteen tai tulossa olevan vaarallisen tapahtuman ennusmerkit. Työntekijän on myös pystyttävä havaitsemaan vaaratilanne ja kyettävä reagoimaan siihen*
- *riippuen kyseisen tilanteen olosuhteista (lämpötila, melu, ergonomia jne.).*

A2: ei mahdollista.

***Huomautus riskimuuttujaan O/MS:** Jos käyttäjän on tehnyt useita virheitä huolimatta puolen vuoden koulutuksesta ja harjaantumisesta viimeisten kahden vuoden aikana, tämä tarkoittanee kuitenkin sitä, että koneen käyttöliittymässä on puutteita eikä kyse välttämättä ole ns. ”keskimääräisen” ammattitaitoisen käyttäjän osaamispuutteista. Koulutusvaatimukset koskevat työnantajaa eikä koneen valmistajaa (lukuun ottamatta mahdollista koneen luovutuksen yhteydessä annettavaa käyttäjäkoulutusta).

Robottiesimerkki robottiyksikön riskin suuruuden arvioinnista (esimerkkiä robottiyksikön turvallisuusstandardi ISO 10218-2).

Tämän kohdan tarkoituksena on havainnollistaa riskin suuruuden ja merkityksen arviointia robottiesimerkin avulla.

Riskin arviointi tehdään standardin ISO 12100 vaiheiden mukaisesti ja teknisen raportin ISO/TR 14121-2 esitettävän riskigraafin avulla (vahingon vakavuuden ja sen todennäköisyyden arviointi). Arvioinnin tulosten perusteella päätetään riskin merkityksestä ja tarvittavista riskin pienentämisen toimenpiteistä (luku 9).

Uusi robottiyksikkö on koottu käytetystä NC-työstökoneesta ja siihen yhdistetystä tavallisesta käytetystä teollisuusrobotista. Robotti on ohjelmoitu syöttämään työkappale työstökoneeseen ja poistamaan valmis työkappale työstökoneesta (kuva 2).



Kuva 2 Robottiyksikössä vanha sorvi on varustettu työkappaleen syöttölaitteena toimivalla teollisuusrobotilla.

Robottiyksikön kuvaus ja sen työkierto: Tarkoituksena on yhdistää käytettyyn NC-sorviin teollisuusrobotti työkappaleen syöttölaitteeksi. Kyseessä on uuden koneyhdistelmän (robottiyksikkö) valmistus, koska työstökoneen käyttötapa muuttuu merkittävästi (osa 2 kohta 11.2). Konedirektiivin mukaisesti yhdistelmän valmistaja vastaa siitä, että valmis koneyhdistelmä täyttää kaikki konedirektiivin vaatimukset ennen koneyhdistelmän käyttöön luovutusta ja sen vaatimustenmukaisuus on osoitettu (osa 2 luku 7).

Tässä vaiheessa robottiyksikön peruskonsepti on selvillä, mutta koneyhdistelmään ei vielä ole suunniteltu tarvittavia turvallisuusteknisiä toimenpiteitä. Sitä varten seuraavassa tehdään ensin selvitys robottiyksikön toiminnasta ja sen jälkeen riskin arviointi.

Työkierron alussa istukassa ei ole työkappaletta, työstötilan suojus on auki ja koneen kaikki liikkeet ovat pysähtyneenä. Robotti on liikkumatta koneen edessä kotiasemassaan. Työkierto käynnistetään käsin käynnistyspainikkeella.

Vaihe 1: Työntekijä käynnistää työstökoneen ja robotin valmiustilaan.

Vaihe 2: Jos anturitieto ilmoittaa, että rullakuljettimella odottaa työkappale, robotti poimii sen ja vie sen työstökoneen tyhjään kiinnitysstukkaan. Työkappale kiinnittyy automaattisesti istukaan, robotti vetäytyy takaisin kotiasemaan.

Vaihe 3: Työstökoneen lastunsuojus sulkeutuu, työstöohjelma käynnistyy automaattisesti ja työstö alkaa. Rullakuljetin tuo uuden työkappaleen odottamaan työstöä.

Vaihe 4: Kun työkappaleen työstöohjelma on ajettu loppuun, työstö pysähtyy, työstötilan suojus avautuu ja robotti ottaa työkappaleen pois istukasta, joka avautuu automaattisesti, ja robotti asettaa työkappaleen kuormalavalle.

Vaihe 5: Viides vaihe sisältää kaksi vaihtoehtoa:

5 a) Jos rullakuljettimelle on tullut uusi työkappale, työkierto alkaa edellä kuvatulla tavalla jälleen automaattisesti vaiheesta 3.

5 b) Jos rullakuljettimella ei ole valmiina poimittavia työkappaleita, robotti jää kotiasemaan odottamaan sitä. Kun työkappale saapuu työkappaleen poiminta-asemaan, käynnistyy työkierto vaiheesta 2.

Vaihe 6: Näin jatkuu, kunnes koneyhdistelmän työkierto pysäytetään.

Robottiesimerkki: Riskiskenaario ja riskin tunnistaminen. Robotin työkiertoon kuuluvien toimintojen oikeellisuus ja keskinäiset riippuvuudet on tässä vaiheessa tarkistettava ja tarvittaessa peruskonseptia korjattava (kohta 3.2). Jos edellä mainitut toiminnot todetaan riskin arvioinnin perusteella turvallisuuteen liittyviksi toiminnoiksi, näitä toimintoja käsitellään samalla tavalla kuin myöhemmässä vaiheessa lisättäviä turvatoimintoja (kohta 9.3 vaihe 2 b).

Koneelle tehdään riskin arviointi, kun koneen peruskonsepti (kohta 3.2) on teknisesti valmis, mutta kone on vielä ilman turvallisuuden parantamiseksi asennettuja suojuksia tai turvatoimintoja. Jos koneyhdistelmässä on jo edellä mainittuja turvallisuuteen liittyviä toimintoja tai erikseen turvallisuuden varmistamiseksi lisättyjä turvatoimintoja, tässä vaiheessa niitä ei oteta huomioon (tai riskejä arvioidaan ikään kuin niitä ei vielä olisi), jos ei käytetä yhdenmukaistettujen standardien soveltamista luvussa 8 kuvatulla tavalla.

Tässä esimerkissä tarkastellaan vain seuraavaa vaaratilannetta ”Robotin varren (tarttujan) työliikkeen odottamattoman käynnistyminen työntekijän ollessa vaaravyöhykkeellä”.

Odottamaton käynnistyminen

Odottamaton käynnistyminen voi johtua useista eri syistä, kuten

- sähkömekaanisten osien vikaantumisesta (liittimen irtoaminen, koskettimien juuttuminen tms.)
- ohjausjärjestelmän vikaantumisesta tai virheestä (esim. komponentin vikaantuminen, ohjelmistovirhe tms.)
- ulkoisten häiriöiden johdosta (esim. EMC-häiriö, ohjauskaapin korkea lämpötila, kosteus tms.)
- uudelleenkäynnistymisestä työkierron tavanomaisen pysähdysvaiheen jälkeen, kun työntekijän ei ole sitä odottanut tai on arvioinut ajoituksen väärin
- toisen työntekijän tekemästä vahinkokäynnistyksestä jne.

Taulukossa 1 esitetään tapaturmaskenaarioon perustuva yksinkertaistettu lomake riskien yksilöimiseksi. Esimerkissä käsiteltävän odottamattoman liikkeen eteneminen vaaralliseksi tapahtumaksi.

Taulukko 1 Tapaturmaskenaarion alkutilanne ja etenemisvaiheet. Esimerkki riskin pienentämisen toimenpiteistä (tekninen raportti ISO/TR 14121-2 taulukko A.3)

Vaaran tunnistaminen

Kone (tunnistetiedot)				Menetelmä (työkalu)	
Lähdeaineistot (tekniset ja rakennetiedostot, suunnitteludokumentit)				Analyyisin tekijä	
				Versio	
Laajuus (esim. elinkaaren vaihe, koneen (osa)toiminnot)				Päiväys	
Viite nro.	Vaaravyöhyke	Tehtävä/käyttötoiminto	Vaara	Vaaratilanne	Vaarallinen tapahtuma
1.1	Robotin liikkeiden alue	Virheiden korjaus- ja säätötoiminnot	Robotin osien liike	Työntekijä on robotin toiminta-alueella korjaus- ja säätötehtävien aikana	Robotin liikkeen odottamaton käynnistyminen
1.2					
jne.					

6.2 Riskin suuruuden arviointimenetelmän kalibrointi

Jos riskin arviointimenetelmien käyttäjillä on erilaisista käsityksistä riskiskenaariosta ja riskiparametrien arvojen asettamisesta, jolloin riskin suuruuden arviointiin tulee suurta hajontaa. Siten parametrien lukumäärän tai parametristeikkojen tihentäminen ei välttämättä lisää arvioinnin luotettavuutta. Sen sijaan riskiparametrien arvojen valintaan käytettävien ohjeiden parantamisella ja kohdentamisella tyypillisin koneryhmiin voidaan vähentää hajontaa. Jos havaitaan poikkeamia riskin arvioinnin tulosten ja yhdenmukaistetuissa standardeissa esitettävien vaatimustasojen välillä, on syytä tarkistaa riskiparametrien asteikot ja riskiparametrien arvojen valintaohjeet (IEC 61511-3).

Riskin arviointimenetelmät (asteikkojen skaalaus ja parametrien valintaohjeet) olisi kalibroitava tutkimalla riskin suuruuden arviointeja riskitekijöiden erilaisilla yhdistelmillä esimerkiksi toimiala-, yritys- tai koneryhmäkohtaisesti tutkimalla riskin suuruuden arvioinnin tuloksia useilla riskitekijöiden erilaisilla yhdistelmillä. Tämä voidaan tehdä kohdistamalla tarkasteltavan yksittäisen koneen riskin arvioinnissa saatuja erilaisia riskin suuruuden tasoja vastaaviin C-tyyppin standardissa esitettyihin tasoihin ja tarkistamalla, että eri parametrien arvojen yhdistelmät antavat riittävän tasaisen logaritmisien tapaisen jatkumon ja parametrien valintaohjeet ovat tämän mukaisia.

Uusien koneturvallisuusstandardien valmistelutyöryhmissä on riskin arvioinnin helpottamiseksi seuraavia lisätietoja:

- koneen C-tyyppin standardin alussa esitetään standardin kattamien merkittävien riskien luettelo
- riskeihin liittyvät turvallisuusvaatimukset ja vaatimuksiin liittyvät riskin pienentämiseen sopivat toimenpiteet esitetään loogisessa tai muuten sopivassa järjestyksessä

- lopuksi esitetään tarkistuslista turvallisuusvaatimuksista, jossa jokaiselle vaatimukselle osoitetaan tarvittavat tarkistusmenetelmät.

6.3 Riskin merkityksen arviointi

Riskinarviointityöryhmän asiantuntemuksen ja kokemuksen perusteella arvioidaan kaikkien riskien merkitys. Tässä vaiheessa, toisin kuin edellä riskin suuruuden arvioinnissa (luku 6), työryhmän kokoonpanossa olisi asiantuntijoiden lisäksi mukana oltava myös päätöksistä ja ainakin yksi henkilö, jolla on valtuudet päättää resurssien käytöstä. Riskin arvioinnin tulosten perusteella tehdään asiantuntijoiden ehdotusten mukaiset päätökset riskin pienentämisen toimenpiteistä.

Koneen riskin arvioinnin tulosten perusteella voidaan, muiden kuin ohjausjärjestelmästä riippuvien turvallisuustoimenpiteiden jälkeen, suunnitella alustavasti myös ohjausjärjestelmän toteuttamia turvatoimintoja. Koneen riskin arvioinnin menetelmällä ei voida suoraan määrittää esimerkiksi turvallisuuteen liittyvien ohjaustoimintojen vaatimustasoja. Tähän tarvitaan ohjausjärjestelmien suunnittelun arviointimenetelmiä, joita kuvataan osan 4 kohdassa 7. Näissä menetelmissä tarvitaan koneen riskin arvioinnissa saatuja tietoja.

Robottiesimerkki riskin merkityksen arvioinnista: Kohdan 6.1.2 esimerkissä esitetyn robottiyksikön riskin suuruuden arvioinnin tulokset ja riskin merkityksen arviointi:

Huomattava, että riskin suuruuden arvioinnissa koneeseen ei ole vielä lisätty mitään turvallisuustoimenpiteitä (kuva 2). Siten tässä esimerkissä robotin varren odottamattoman liikkeen riskiparametrit (kohta 6.1.2) valitaan seuraavasti:

F 3: Robotin vaaravyöhykkeellä käydään useasti korjaamassa virheitä ja säätämässä järjestelmää (kaksi hyvin erilaista käytettyä konetta uutena yhdistelmänä, jossa voi olla ”lastentauteja”)

O 3: Vaarallisen tapahtuman todennäköisyys on melko suuri, koska edellisenkin kohdan mukaisesti koneessa on paljon säädettävää ja korjattavaa

A 2: Vaaran väistämisen mahdollisuus on pieni, koska

- riskin havaitseminen: käyttäjä on selin robottiin, jolloin ei käyttäjä ehdi nähdä robotin liikkeellelähtöä
- paikka: käyttäjä on säätö- ja korjaustöiden vuoksi usein robotin ja koneen välisessä ahtaassa paikassa, josta voi olla vaikea päästä nopeasti vaaravyöhykkeen ulkopuolelle
- aika: robotin liikenopeuden ja pitkän pysähtymismatkan vuoksi käyttäjä ei ehdi reagoida ennen kuin robotin varsi (työkappale tai sen kiinnitystyökalu) osuu käyttäjään

S 2: Robotin odottamaton liike työntää käyttäjän päin koneen työstötilan teräviä kohtia, jolloin seuraukset ovat hyvin vakavat ja myös kuolemantapaus on mahdollinen esim. selkärankaan kohistuvan iskun johdosta.

S = 2, F = 2, O = 3 ja A = 2, jolloin seuraavan taulukon mukaisesti riskin merkitys on 6

Jos riskin suuruuden perusteella riski on merkityksellinen, on ryhdyttävä riskin pienentämisen toimenpiteisiin.

Riskin merkitys

1. Merkitys 1...2 (pieni riski):

ei tarvita korjaavia toimenpiteitä, mutta seurataan ja valvotaan tilannetta ja tarvittaessa tehdään riskin uudelleen arviointi

2. Merkitys 3...4 (keskimääräinen riski):

ryhdytään toimenpiteisiin riskin pienentämiseksi, ja laaditaan aikataulu korjaaville toimenpiteille

3. Merkitys 5...6 (suuri riski):

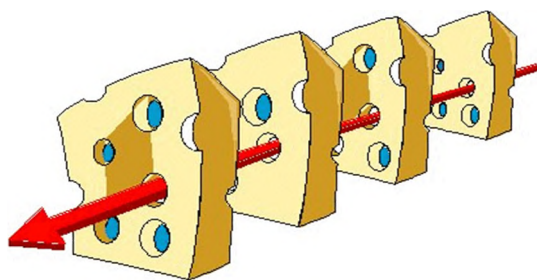
koneen uudelleen suunnittelu tai modernisointi on välttämätöntä, sen toteutuksen jälkeen tehdään uusi riskin arviointi ja toimitaan sen tulosten edellyttämällä tavalla.

Tässä esimerkissä riskin merkitys saa suurimman arvon 6 ja siten koko robottisolun on suunniteltava uudelleen siten, että työntekijän altistuminen robotin varren liikkeen aiheuttamalle vaaralle poistetaan tai sitä pienennetään riittävästi. Samalla on tarkistettava uudelleen kaikki muutkin turvallisuuteen liittyvät riskit ja toteutettava tarvittavat turvallisuustoimenpiteet (ISO 10218-2).

7 Riskin arviointi LOPA-menetelmällä

Vaaratekijöiden ja niiden aiheuttamien riskien tunnistamiseksi on laadittu riskin etenemisen malleja eli skenaarioita (kuva 3 ja taulukko 1). Riskin etenemisen mallissa seurataan määrätyn vaaran aiheuttaman riskin etenemistä ja arvioidaan jokaisen etenemisvaiheen todennäköisyys. Jokaiseen vaiheeseen suunnitellaan riskin pienentämisen toimenpiteitä. Tavoitteena on, että näiden toimenpiteiden samanaikaisen työstämisen tuloksena jäljelle jäävä lopullinen riski on pienempi kuin tavoitteena oleva riskitaso.

Esimerkki: Suojauskerrokset tulisi olla toisistaan riippumattomia, jolloin riskin aiheuttaman vahingon sattumisen todennäköisyys voidaan arvioida seuraavan havainnollistavan mallin mukaisesti.



Kuva 3 Riskin etenemisen malli (Reason)

Kuva 3 mukaisen tilanteen riskin laadullinen arviointi (*qualitative assessment*):

1. Vaara (*hazard*) on jatkuvasti olemassa (punainen nuoli)
2. Vaarallinen tilanne (*hazardous situation*) esiintyy jatkuvasti, kun työntekijä on vaaravyöhykkeellä (vaaran mahdollisella vaikutusalueella)

3. Vaarallinen tapahtuma (*hazardous event*) esiintyy satunnaisesti, jolloin syntyy vahingon mahdollisuus (kuvassa 3 punainen nuoli) lähtee etenemään kohti henkilöä,
4. Riski toteutuu ja syntyy vahinko (tapaturma) (*harm, accident*), jos vaaran (nuoli) edetessä se läpäisee kaikki neljä kuvan 3 suojauskerrosta ja aiheuttaa vahingon työntekijälle.

Kuva 3 mukaisen tilanteen riskin määrällisen arviointiin (*quantitative assessment*) tarvitaan lisää oletuksia malliin syötettävistä tiedosta:

1. Oletetaan, että vaarallinen tapahtuma eli tapaturman mahdollisuutta kuvaava nuoli lähtee kohti työntekijää keskimäärin 10 kertaa vuodessa (eli todennäköisyys on 10/vuosi).
2. Oletetaan, että kunkin suojauskerroksen ”reikien” yhteenlaskettu pinta-ala on yksi kymmenesosa suojauskerroksen kokonaispinta-alasta, jolloin nuoli pääsee satunnaisesti yhden suojauskerroksen läpi keskimäärin kerran kymmenestä vaarallisesta tapahtumasta eli tapaturman todennäköisyys pienenee jokaisen suojauskerroksen kohdalla yhteen kymmenesosaan.
3. Oletetaan, että kaikki neljä suojauskerrosta ovat toisistaan riippumattomia, jolloin nuolen läpäisymahdollisuus pienenee jokaisen suojauskerroksen kohdalla kymmenteen osaan eli kertoimella 0,1 ja kaikkien neljän suojauskerroksen toisistaan riippumattomasta yhteisestä vaikutuksesta nuolen läpäisyn todennäköisyys pienenee neljä kertaa kymmenenteen osaan eli tapaturman keskimääräinen esiintyminen pienenee arvoon $10 \times 0,1 \times 0,1 \times 0,1 \times 0,1 = 0,001/\text{vuosi}$.
Lopputulos: tapaturma sattuu todennäköisesti keskimäärin kerran tuhannessa vuodessa (tai jos tuhat työntekijää on vastaavassa vaaratilanteessa, yksi työntekijä joutuu tapaturma uhriksi keskimäärin kerran vuodessa). Riippuu mahdollisen vahingon suuruudesta, onko tämä sallittua!

Edellä kuvatun suojauskerroksen menetelmän periaatteita käytetään useimmiten prosessiteollisuudessa (IEC 61511-3). Sitä voidaan soveltaa myös konejärjestelmien riskin arvioinnissa ja turvallistamisessa, kun riskit ovat suuria tai kyseessä on prosessimainen riskin etenemisen malli, varsinkin

- jos riskiskenaariossa on useampia suojauskerroksia (vaatimus riskin pienentämiseen vähintään 0,1) tai
- jos riski etenee suhteellisen hitaasti ja siihen ehditään reagoida (esim. poistumalla nopeasti vaaravyöhykkeeltä) tai
- jos riskin etenemiseen voidaan vaikuttaa erilaisilla riskiä pienentävillä menetelmillä kuten esimerkiksi hälytyksillä tai prosessiohjauksella tms.
- tai edellisten yhdistelmiä.

Suurilla riskin tasoilla pahimman tapauksen (*worst-case*) analyysi olisi tehtävä erikseen ja yksityiskohtaisesti, esim. vikapuun (*Fault Tree Analysis*, FTA) tapahtumapuun (*Event Tree*), LOPA tms. menetelmän avulla siten, että samalla suunnitellaan kuhunkin vaiheeseen sopivia muutoksia tai suojauskerroksia pienentämään riskiä ennen seuraava vaihetta, esim. altistuksen pienentäminen, automaation lisääminen (esim. materiaalin syöttölaite), turvalaitteiden, ohjausjärjestelmän kahdennusten ja diagnostiikkatoimintojen lisääminen tms.

Koneturvallisuudessa riskit ovat useimmiten nopeasti eteneviä ja vaaravyöhykkeellä oleva työntekijä ei useinkaan voi estää riskin toteutumista vetäytymällä nopeasti pois vaarakohdasta, käyttämällä hätäpysäytystä tms. Varsinaisia suojauskerroksia on usein vain yksi automaattiajolle (esim. valoverho koko vaaravyöhykkeen turvalaitteena) ja toinen käsiajolle (esim. pakkotoiminen käyttöohjain, turvanopeus ja varalla oleva hätäpysäytyslaite). Ohjattavissa koneissa kuten esim.

nostolaitteet, liikkuvat työkoneet ja kulkuvälineet, ohjattavuus voidaan määrittäillä edellytyksillä katsoa riippumattomaksi suojauskerrokseksi (esim. näkyvyyden parantaminen kaikille suunnille näyttölaitteiden avulla tai lähellä olevien henkilöiden tunnistaminen lisänä olevilla turvajärjestelmillä).

8 B- ja C-tyyppin standardeihin perustuva riskin arviointi ja riskin pienentäminen

Riskin arvioinnin jälkeen riskin arvioinnin tulosten perusteella voidaan suunnitella riskin pienentämisen turvallisuustekniset toimenpiteet. Tässä on syytä käyttää apuna B- ja C-tyyppin standardeja (osa 1 luku 6), mikä auttaa varmistumaan siitä, että kone täyttää konedirektiivin vaatimukset. Koneryhmäkohtaisissa C-tyyppin standardeissa yksilöidään erilaisten koneiden merkittäviä/olennaisia vaaroja (*remarkable hazards/constituent hazard*) ja esitetään niiden pienentämiseen soveltuvia turvallisuusteknisiä toimenpiteitä. B-tyyppin standardeissa puolestaan käsitellään kattavasti erilaisia vaaratekijöitä ja niiden pienentämiseen soveltuvia turvallisuusteknisiä ratkaisuja ja menetelmiä.

B- ja C-tyyppin standardien käyttö suoraan riskin pienentämiseen ei vapauta koneen valmistajaa velvollisuudesta tehdä riskin arviointia (vaarojen tunnistaminen ja yksilöinti), mutta riskin suuruuden arviointia voidaan helpottaa kyseistä konetta koskevien B- ja C-tyyppin standardien avulla. Parhaassa tapauksessa voidaan nojautua B- ja C-tyyppin standardeihin koko koneen osalta, jolloin riskin suuruuden arviointia ei tarvitse erikseen tehdä.

Siten C-tyyppin standardiin nojautuminen edellyttää, että

- 1) kyseinen kone kuuluu kyseisiltä osin C-tyyppin standardin soveltamisalaan ja
- 2) standardissa yksilöidyt riskit kattavat koneen merkittävät vaarat (kuva 4).

Jos edellä mainitut kriteerit täytetään, koneen valmistajan ei tarvitse tehdä riskin suuruuden arviointia (esim. riskigraafi), koska B- ja C-tyyppin standardien asiantuntijaryhmä on jo laajalla tunnistanut, yksilöinyt ja arvioinut kyseisen koneen merkittävät vaarat. C-tyyppin standardissa on tämän jälkeen riskin suuruuden arvioinnin perusteella määritetty riskien pienentämiseen tarvittavia turvallisuusteknisiä toimenpiteitä ja siinä nojaututtu myös B-tyyppin standardeissa esitettyihin turvallisuusvaatimuksiin ja ratkaisuihin (C-tyyppin standardeissa voi olla useita kymmeniä viittauksia B-tyyppin standardeihin).

Huom. Jos B-tyyppin standardien ja C-tyyppin standardien vaatimukset ovat erilaisia, C-tyyppin standardien vaatimukset ovat ensisijaisia.

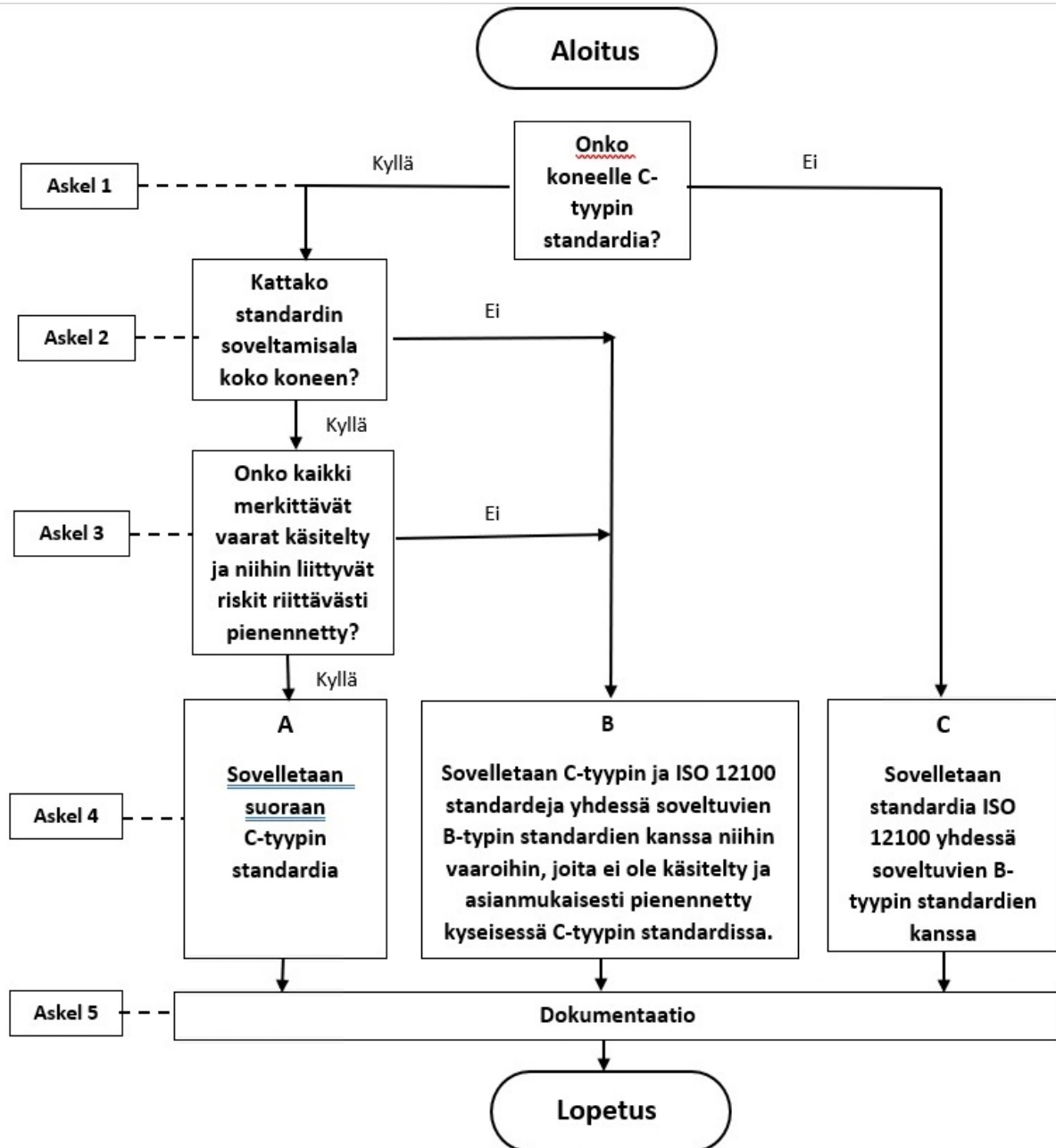
Siten aluksi toimitaan kuin aikaisemminkin riskin arvioinnin perusmenetelmän mukaisesti (ISO 12100) eli tunnistetaan kaikki koneen vaarat ja yksilöidään niiden aiheuttamat riskit. Tästä eteenpäin koneen valmistaja voi alustavasti suunnitella turvallisuusteknisiä toimenpiteitä nojautumalla edellä mainittuihin C-tyyppin standardeihin, jos standardin soveltamisen kriteerit täytetään (kuva 4). B-tyyppin standardeja voidaan kaikissa tapauksissa käyttää suunnittelun apuna. Riskit ja niihin liittyvät suojaustekniset ratkaisut toimenpiteet dokumentoidaan ja näin saadaan helposti aikaan yhdenmukaisuus konedirektiivin vaatimusten kanssa, esim. voimansiirtolaitteet suojataan B-tyyppin standardin ISO 14120 mukaisesti. Valitun turvallisuusratkaisun kuvausta

koneen dokumentoinnissa helpotetaan tekemällä viittaukset em. standardin asiaan kuuluviin kohtiin. Kun harmonisoituja standardeja sovelletaan edellä kuvatulla tavalla, voidaan saada aikaan oletus siitä, että konedirektiivin olennaiset turvallisuusvaatimukset tulevat täytetyksi.

Jos kone täyttää vain osittain kriteerin 2, niin C-typin standardin merkittävien riskien tai niiden luettelon ulkopuolella oleviin riskeihin sovelletaan kaikkia riskin arvioinnin perusmenetelmän vaiheita ja siten myös arvioidaan riskin suuruus ja sen perusteella riskin pienentämisen vaatimusten mukaisesti suunnitellaan riittävän tehokkaat turvallisuustekniset menetelmät.

Huom. Jos riskin suuruuden arviointi antaa tulokseksi pienemmän riskin kuin mitä samasta asiasta esitetään konetta koskevassa C-typin standardissa, kyseinen ratkaisu ei täytä olettamusta konedirektiivin vaatimusten täyttämisestä. Tällöin ratkaisun vaatimustenmukaisuus olisi osoitettava erikseen, mikä voi olla vaikeata.

Edellinen huomautus johtaa myös siihen, että jokaisella koneen valmistajalla on oltava käytössään valmistamaansa konetta koskeva C-typin standardi ja siihen liittyvät tärkeimmät B-typin standardit. Ainoastaan niiden avulla valmistaja voi tarkistaa valmistamansa koneen vaatimustenmukaisuuden ennen kuin laatii vaatimustenmukaisuusvakuutuksen ja toimittaa koneen EU:n talousalueen markkinoille tai siellä käyttöönotettavaksi.



Kuva 4 Standardeihin perustuva riskin arviointi ja riskin pienentäminen koneen suunnittelussa (tekninen raportti ISO/TR 22100-2).

Taulukko 2 A-, B- ja C-tyyppin koneturvallisuusstandardeja**Robottiyksikköä koskevia standardeja****Suunnitteluperiaatteet**

SFS-EN ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen, 2010

SFS-ISO/TR 14121-2 Koneturvallisuus. Riskin arviointi. Osa 2: Käytännön opastusta ja esimerkkejä menetelmistä, 2012

SFS-EN 1037 + A1 Koneturvallisuus. Odottamattoman käynnistymisen estäminen, 2008

SFS-EN ISO 11161 + A1 Koneturvallisuus. Valmistusjärjestelmien koneyhdistelmät. Perusvaatimukset, 2010

SFS-EN ISO 14120 Koneturvallisuus. Suojukset. Kiinteiden ja avattavien suojusten suunnittelun ja rakenteen yleiset periaatteet, 2015

Mitoitus

SFS-EN ISO 13857 Koneturvallisuus. Turvaetäisyydet yläraajojen ja alaraajojen ulottumisen estämiseksi vaaravyöhykkeille, 2008

Koneturvallisuus SFS-EN 349 + A1 Koneturvallisuus. Vähimmäisetäisyydet kehon osien puristumisvaaran välttämiseksi, 2008

SFS-EN ISO 13855 Koneturvallisuus. Suojausteknisten laitteiden sijoitus ottaen huomioon kehon osien lähestymisnopeudet, 2010

Ohjaustoiminnot

SFS-EN 574 + A1 Koneturvallisuus. Kaksinkäsinhallintalaitteet. Toiminnalliset näkökohdat. Suunnitteluperiaatteet, 2008

SFS-EN ISO 13849-1 ja -2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet, 2015, osa 2: Kelpuutus, 2012

SFS-EN 62061 Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus, 2005

SFS-EN ISO 13850 Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet, 2015

SFS-EN ISO 14119 Koneturvallisuus. Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta, 2013

Tehon siirto

SFS-EN ISO 4413 Hydraulinen tehon siirto. Järjestelmiä sekä niiden komponentteja koskevat yleiset periaatteet ja turvallisuusvaatimukset, 2011

SFS-EN ISO 4414 Pneumaattinen tehon siirto. Järjestelmiä sekä niiden komponentteja koskevat yleiset periaatteet ja turvallisuusvaatimukset, 2011

SFS-EN 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset, 2006

Lisäksi teollisuusrobottia koskee C-tyyppin ISO standardi ISO 10218-1 ja robottiyksikköä koskee C-tyyppin standardi ISO 10218-2.

Huom. Muita koneturvallisuuteen liittyviä standardeja ovat esim. koneen kulkuteitä, ergonomiaa ja tässä yhteydessä erityisesti hallintalaitteita koskevat ISO-standardit [Standardit].

9 Koneen riskin pienentämisen ensisijaisuusjärjestys

Riskin pienentämisen käsitteet, periaatteet ja menetelmät esitetään koneturvallisuuden perusstandardissa ISO 12100 ja myös standardin ISO 13849-1 kohdassa 4.2.1 ja kohdan 6.1.1 kuvassa 1.

Riskin arvioinnin tarkoituksena on saada selville jokaisen yksilöidyn vaaratekijän aiheuttamat merkittävät riskit, jotta niitä voidaan pienentää poistamalla kokonaan vaaratekijä tai pienentämällä riittävästi vaaratekijän aiheuttamaa riskiä. Riskiä voidaan pienentää joko pienentämällä

1. riskin aikaansaaman mahdollisen vahingon vakavuutta tai
2. riskin toteutumisen mahdollisuutta (vahingon esiintymistodennäköisyyttä) tai molempia.

Ennen koneen riskin pienentämisen menetelmien suunnittelua on syytä tarkastella mahdollisia tehdastason toimenpiteitä. Riskien poistaminen tässä vaiheessa on edullisinta, jos luodaan kestävät ja turvalliset perusratkaisut:

Laaja-alaisten konejärjestelmien turvallisuusnäkökohtia

- koneiden ja koneryhmien osastointi (kohta 9.3 kuva 6)
- järjestetään turvallinen pääsy työskentelypaikkoihin ja huoltokohteisiin
- liikkuvien työkonoiden toiminta-alueet ja ihmisten kulkuväylät erotetaan selkeästi toisistaan
- määritetään sijoituskaavion (*lay-out*) mukaisesti toimintojen vaikutusalueet ja vyöhykkeet:
 - turvalaitteiden vaikutusalueet (*span of control*, esim. tuotantosolukohtaisesti)
 - käynnistysvyöhykkeet (esim. useampi käyttöpaikka ja tarvittaessa kone voidaan käynnistää vain yhdestä kerrallaan)
 - pysäytysvyöhykkeet (esim. useampi käyttöpaikka, joista kone saadaan pysäytettyä)
 - hätäpysäytysvyöhykkeet (yksi vyöhyke tai useampia erillisiä tai päällekkäisiä vyöhykkeitä)
 - tietoturvavyöhykkeet ("automaatiosaarekkeit")

Standardien mukaisesti riskejä on pienennettävä seuraavassa ensisijaisuusjärjestyksessä (ns. kolmen askeleen menetelmä):

Riskin pienentämisen ensisijaisuusjärjestys (vaiheet)

1. Luontaisesti turvalliset suunnittelutoimenpiteet
2. Suojaustekniset toimenpiteet
 - a) Ulkoiset riskin pienentämisen toimenpiteet (ohjausjärjestelmistä riippumattomat toimenpiteet, esim. aitaukset, suojukset, turvalaitteet)
 - b) Turvatoiminnot (ohjausjärjestelmästä riippuvat toimenpiteet, esim. turvallisuuden liittyvät ohjaustoiminnot ja turvatoiminnot)
 - c) Täydentävät suojaustekniset toimenpiteet (varotoimenpiteet)
3. Käyttöä koskevat tiedot (esim. asennus-, käyttö- ja kunnossapito-ohjeet).

9.1 Vaihe 1: Luontaisesti turvalliset suunnittelutoimenpiteet

Toimenpiteiden ensisijaisuuden vaiheessa 1 turvallisuus varmistetaan suunnittelemalla kone tai konejärjestelmä alun perin mahdollisimman turvallisesti. Jo peruskonseptin suunnittelussa pyritään suunnittelemaan sellaisia koneita, jotka aiheuttavat mahdollisimman vähän henkilövahinkoja, täyttävät mm. ympäristövaatimukset ja jotka kuluttavat mahdollisimman vähän energiaa ym.

Suurempien konejärjestelmien osalta luontaisesti turvallisten koneiden suunnittelu tarkoittaa yhä kattavampaa automaation käyttöönottoa. Automaation avulla työntekijä saadaan ohjaamaan prosessia turvallisesti vaaravyöhykkeiden ulkopuolelta.

Mekaanisten vaaratekijöiden osalta pyritään rakentamaan koneen liikkuvat osat siten, että ei synny vaarallisia puristus- tai leikkauskohtia. Ajan kuluessa on kehitetty monia koneita ja komponentteja, jotka ovat mekaanisilta ominaisuuksiltaan hyvin turvallisia, esimerkiksi monet pumput, konetoimiset venttiilit jne.

Robottiesimerkki riskin pienentämisestä: Koneen riskin arvioinnissa määritetyt merkittävät riskit on pienennettävä riittävästi, jotta saavutetaan siedettävä jäännösriski. Tässä esimerkissä riskigraafin avulla (kohdat 6.1 ja 6.3) saadun arvioinnin tuloksena riskin merkitys on tasoilla 5...6, jolloin esimerkkinä olevaa robottiyksikköä ei saa turvallisesti ilman perusteellista modernisointia (osa 2 kohta 11.5). Vanhan työstökoneen turvallistaminen vastaamaan robottiyksikön tuotannollisia ja turvallisuuteen liittyviä vaatimuksia voi osoittautua vaikeaksi.

Vaatuksena on robottiyksikön riskien pienentäminen perusteellisella uudelleensuunnittelulla. Tehokkain menetelmä kuuluu toimenpiteiden ensisijaisuuden vaiheeseen 1 eli koneen suunnittelu kokonaan uudelleen siten, että vaaratekijöitä saadaan kokonaan poistettua suunnittelun avulla (esim. ryhmitellään koneet uudelleen, muutetaan koneen toimintaperiaatetta, koteloidaan liikkuvat koneenosat rungon sisälle jne.).

9.2 Vaihe 2 a: Ohjausjärjestelmästä riippumattomat riskin pienentämisen toimenpiteet

Tavoitteena on kaikkien merkittävien riskien riittävä pienentäminen siten, että jäännösriskit ovat mahdollisimman pieniä ("ensimmäinen jäännösriski" kohta 9.4).

Tässä vaiheessa koneen toimintaan tarvittavat rakenteet ja tuotannolliset toiminnot on suunniteltu (sijoituskaavio, palvelut, esim. tehonsyöttöpisteet yms.), koneiden asennukset, aitaukset, portit, kuljettimen suojaus jne.). Edellisen kohdan luontaiset turvalliset tekniset ym. ratkaisut on suunniteltu.

Tässä toimenpiteiden ensisijaisuusjärjestyksen vaiheessa 2 a suunnitellaan ohjausjärjestelmästä riippumattomat (ns. ulkoiset riskin pienentämisen) toimenpiteet käyttämällä mekaanista, tekniikkaa esimerkiksi lisäämällä koneeseen tarvittavia aitauksia, suojuksia sekä mekaanisia turvalaitteita ja -välineitä. Useimmiten kuitenkin vaarakohtia joudutaan erikseen suojaamaan esimerkiksi erikseen muotoiluilla suojuksilla, esimerkiksi kuvassa 5 esitettävän robottiyksikön kuljettimen hihnapyörien ja nielujen suojukset suojattava (voimansiirtoelimet on aina suojattava).

Robottiyksiköissä ulkoisena perusratkaisuna on tavallisesti koko robottisolun ympäröiminen pääsyn estävillä suojuksilla ja aitauksilla (esim. standardi ISO 10218-2 ja ISO 16111). Useimmiten kuitenkin vaarakohtia joudutaan erikseen suojaamaan esimerkiksi kohteen mukaisesti muotoiluilla suojuksilla. Näiden turvallisuusteknisten toimenpiteiden suunnitteluun on käytettävissä kattavasti yhdenmukaistettuja standardeja [Standardit].

Koneen ohjausjärjestelmästä riippumattomia turvallisuustoimenpiteitä

- Mekaaniset turvallisuustekniset toimenpiteet kuten aitaukset, suojuukset, lukitukset jne.
- Eri teknologioilla (pneumaattiset, hydrauliset, sähköiset ym.) toteutetut koneen ohjaustoiminnoista erilliset turvallisuustoimenpiteet, kuten mekaaniset pitoventtiilit, liikealueiden mekaaniset rajoittimet jne.
- Paikallaan pysymisen varmistukset, esim. säppilaitteet, jarrut, tarraimet
- Loukkuun jääneen henkilön vapauttamisen menetelmät energian syötön ollessa pois päältä.

Koneen peruskonseptissa on jo suunniteltu koneen toiminallisuus eli koneen erilaisia toimintoja, mutta tässä vaiheessa koneeseen suunnitellaan ne sähköiset, mekaaniset, hydrauliset, pneumaattiset ym. järjestelmät, jotka toteuttavat näitä toimintoja, mutta varsinaisia koneen ohjausjärjestelmän toteuttamia turvallisuuteen liittyviä toimintoja suunnitellaan vasta seuraavassa vaiheessa kun riskin arvioinnin tulokset ovat käytettävissä. Tässä vaiheessa suunnitelluista koneen käyttötoiminnoista monien voidaan myöhemmin todeta turvallisuuteen liittyviksi ja silloin niitä käsitellään samalla tavalla kuin muitakin turvallisuuteen liittyviä toimintoja (osa 4 kohta 6.2).

Jos myöhemmin seuraavassa vaiheessa 2 b todetaan jonkin käyttötoiminnon olevan hyvin turvallisuuskriittinen, sitä käsitellään kuten muitakin turvatoimintoja ja voi olla, että sitä toteuttavien komponenttien pitääkin olla turvakomponentteja. Siten koneen käyttötoiminnoilta vaadittavan turvallisuustason arviointia ei kannata siirtää kovin pitkälle koneen suunnittelussa, koska korkeammat turvallisuusvaatimukset vaikuttavat kyseisten toimintojen suunnitteluun ja sen seurauksena voi tulla vaatimuksia esimerkiksi turvakomponenttien käytöstä ja muista varmennuksista (osa 5 kohta 4.3.6).

9.3 Vaihe 2 b: Turvatoiminnot

Kun esimerkiksi säätö-, korjaus- ja kunnossapitotöissä on mentävä vaaravyöhykkeille, näiden työtehtävien turvallistamiseksi järjestelmään on lisättävä turvatoimintoja, ja ne useimmiten toteutetaan tavallisesti ohjausjärjestelmän avulla (riskin pienentämisen vaihe 2 b). Tällöin koneen ohjaustoiminnot ovat aikaisempaa monipuolisempia, mutta sen vuoksi myös monimutkaisempia ja siten ohjaustoimintojen oikeellisuus ja luotettavuus ovat keskeisiä suunnittelukohteita (osa 4 kohdat 6.1 ja 7.1).

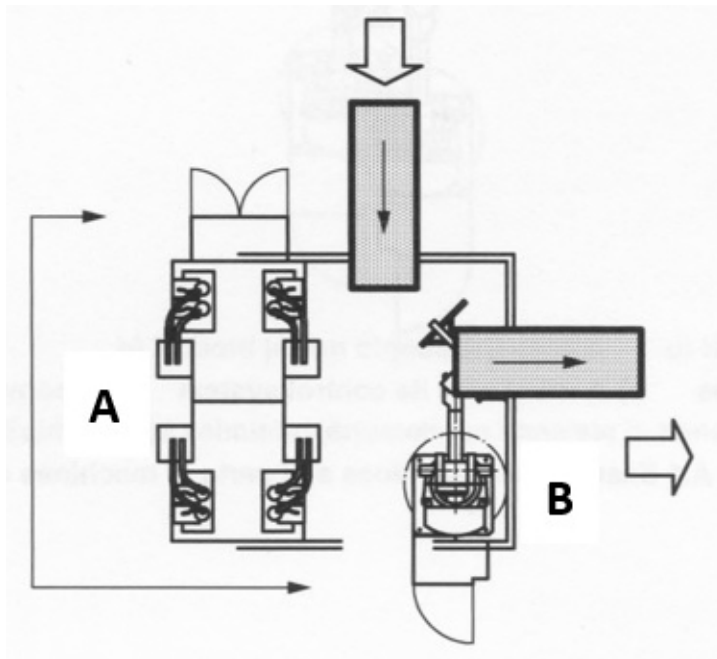
Koneen turvallisuuteen liittyviä toimintoja (ISO 13849-1)**Turvatoimintoja**

- turvalaitteen käynnistämä turvallisuuteen liittyvä pysäytystoimintoa pakkokäyttöinen ohjaustoiminto
- passivointitoiminto
- sallintalaitteen toteuttama toiminto
- odottamattoman käynnistuksen estäminen
- loukkuun henkilön vapauttaminen ja pelastaminen

Muita turvallisuuteen liittyviä toimintoja

- käsikäyttöinen kuittaustoiminto
- käynnistys tai uudelleenkäynnistystoiminto
- paikallisohjaustoiminto
- toimintatavat ja niiden valinta
- erottamis- ja energian purkamistoiminto
- hätäpysäytystoiminto (täydentävä suojaustoimenpide).

Robottiesimerkki turvatoiminnoista: Luvuissa 6 esitetyn robottiesimerkin riskin arvioinnin tulokseksi saatiin, että koko robottijärjestelmä on suunniteltava uudelleen ja sitä on käsiteltävä uutena koneena. Kuvassa 5 esitetään uuden robottisolun periaate (ISO 11161, kuva A.2), jossa robotti B palvelee työstökoneetta A.



Kuva 5 Esimerkki robottiyksikön uudelleenjärjestämisestä. Robotti A toimii työkappaleen vaihtajana työstökoneeseen B. Robottiyksikön sivuun käännettävät ovet on kytketty koneen toimintaan (ISO 11161).

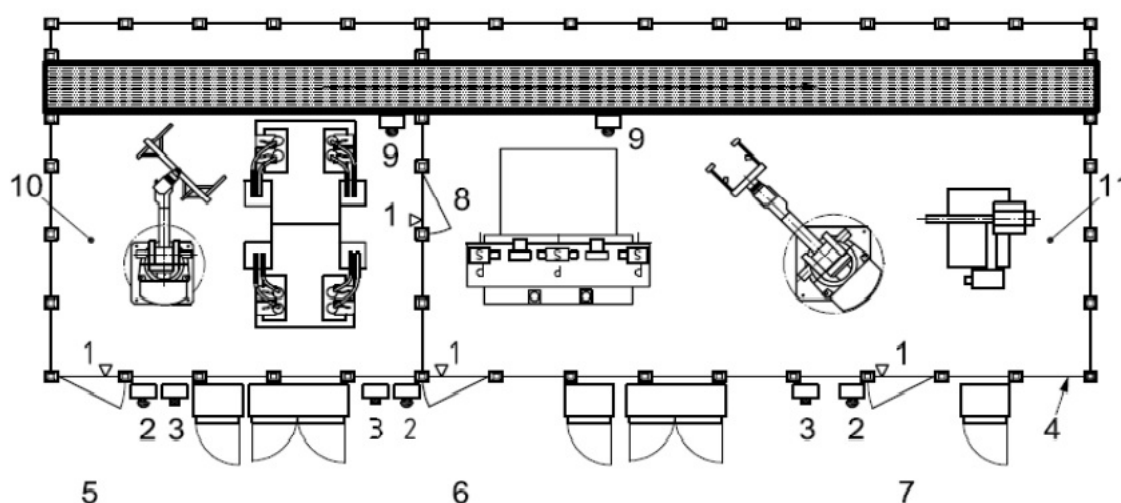
Kun portti avataan, robotin kaikki liikkeet pysähtyvät ja ne pidetään paikoillaan. Kun robotti käynnistetään, ovet suljetaan ja kuittauksella varmistetaan, että ketään ei ole vaaravyöhykkeellä ja

kaikki tarvittavat turvatoimenpiteet on tehty. Työstökoneessa on robotin toiminnasta riippumaton työstötilan suojus, joka voidaan avata vain työstökoneen ollessa pysähtyneenä. Sekä robottia että työstökoneita voidaan ohjata suojusten ollessa auki hidastetuilla käsiohjauksella.

Työkappaleiden syöttö tapahtuu kuljettimella kuvassa 5 ylhäältä alaspäin ja josta robotti käy poimimassa työkappaleet. Koneessa on erilliset, yhteen sovitettavat ohjausjärjestelmät CNC-koneelle ja teollisuusrobotille. Valmiit työkappaleet poistuvat kuljettimella oikealle.

Robottiyksikkö on valmistettu konedirektiivin vaatimusten mukaisesti ja apuna on käytetty yhdenmukaistettuja turvallisuusstandardeja.

Kuvan 6 robottiyksikkö on jaettu kahteen itsenäisesti toimivaan robottisoluun. Koko työalue on aidattu ja pääsy vaaravyöhykkeelle tapahtuu koneen toimintaan kytkettyjen porttien kautta. Kun riskin pienentämiseen käytetään ohjausjärjestelmän toteuttamia turvatoimintoja, yhdellä turvatoiminnolla voidaan useimmiten pienentää useiden erilaisten vaarojen aiheuttamia riskejä. (turvalaitteiden vaikutusalueet, esimerkiksi standardi ISO 11161). Kuitenkin tässäkin tapauksessa on otettava huomioon riskit vaaravyöhykkeellä työskenteleminen tai erityisvaatimukset tilapäiseen pääsyyn koneen vaaravyöhykkeelle koneen käydessä, jolloin voidaan tarvita toinenkin käyttötapa ja sen turvatoiminto, esim. sallintalaite ja hidastetut liikkeet.



1 = toimintaankytkentä

3 = Kuittauslaitteet

2 ja 9 = Hätäpysäytyslaitteet

4 = Ympäröivä aitaus

5...8 = Portit

Kuva 6 Koneyhdistelmä (robottiyksikkö) koostuu robotin lisäksi lukuisista koneista, osittain valmiista koneista sekä muista laitteista ("ympäryskoneet/-laitteet"). Lopullisen koneyhdistelmän valmistajan (kokoonpanija) on osoitettava koko koneyhdistelmän vaatimustenmukaisuus (ISO 11161).

Kun kuvan 6 mukaisessa osastoidussa robottiyksikössä tulee tarve mennä yhteen osastoon korjaus-, säätö- tai muuta toimenpidettä varten, kaikkien tässä osastossa olevien koneiden tulee pysähtyä turvalliseen tilaan ja siten myös työkappaleiden syöttö ja poisto kuljettimen tulee pysähtyä. Jotta

viereinen osasto voisi pysyä tuottavassa toiminnassa, osaston läpi menevän kuljettimen pitäisi päinvastoin pysyä käynnissä.

Tämä ristiriita voidaan ratkaista siten, ensin kaikki kuljettimen ja siinä olevien työkappaleiden mahdolliset aiheuttamat riskit arvioidaan ja sen perustella täydennetään kuljettimen suojausta. Lisäsuojuksilla voidaan varmistaa, että mihinkään liikkuvaan osaan ei pääse kosketukseen lukuun ottamatta kuljettimen hihnaa ja siinä vapaana olevia työkappaleita. Tämän vuoksi on mahdollisesti asetettava rajoitukset työkappaleiden koolle, kuljettimen nopeudelle (pienentää esimerkiksi puoleen, koska vain toinen osastoista on käytössä) jne. Koneen käynnistyksessä, pysäyttämässä ja uudelleen käynnistyksessä sekä kuittauksessa on noudatettava seuraavassa esitettäviä koneen toimintoja koskevia ohjeita.

Automaattisen koneen ohjaustoimintojen keskinäisiä riippuvuuksia

- koneen käynnistäminen saa olla mahdollista vain käsikäyttöisesti
- jos vaaravyöhykkeelle on pääsy, koneen käynnistystoiminto edellyttää, että
 - ensin tarkistetaan, että vaaravyöhykkeellä ei ole ketään (ei myöskään koneiden takana), suljetaan kaikki suojukset ja aktivoidaan turvatoiminnot
 - kun tarkistus on tehty, kuittauspaikalta tehdään käsikäyttöinen kuittautustoiminto (laajassa konejärjestelmässä voidaan tarvita useampia kuittauspaikkoja, ja kaikissa on erikseen tehtävä kuittaus)
 - suurissa koneissa voidaan tarvita käynnistyshälytys
 - jos koneessa on automaattiajon ja käsiajon toiminnot, tarvitaan koneen toimintatavan valintakytkin
 - tarvittaessa automaattiajon toimintatavan valinta on aktivoituna vain määrätyn lyhyen ajan, jossa kone on mahdollista käynnistää automaattiajolle
- koneen käynnistäminen saa olla mahdollista vain käsikäyttöisesti
- pysäytystoiminnon tulee estää, niin kauan kun sen on oltava voimassa, mistä tahansa ohjaimesta, anturista, logiikasta ym. tuleva toiminnan uudelleen käynnistämisen signaalin vaikutus
- etäaseman lukitustoiminnon on estettävä kaikkien työasemien päällekkäisten toimintojen yhdistelmät niiltä osin kuin ne voivat aiheuttaa riskiä
- laitteiden hetkelliset toiminnot, kuten esimerkiksi koskettimien tai venttiilien avautuminen tai sulkeutumien voi riippua koneen tilasta tai tilamuutosten ajoituksista, ja tämä edellyttää oikeaa ajoitusta

Koneeseen lisättyjen turvatoimintojen lisäksi koneessa voi olla lukuisia ohjausjärjestelmän toteuttamia käyttö- ja ohjaustoimintoja, joiden vikaantuminen voi aiheuttaa vaaraa (kohdat 4.2 ja 9.2). Näitä turvallisuuteen liittyviä toimintoja käsitellään samalla tavalla kuin edellä mainittuja turvatoimintoja. Lisäksi on otettava huomioon ohjaustoimintojen ennakoitavissa oleva tahallinen tai tahaton väärinkäyttö. Koneen turvallisuuteen liittyvien toimintojen luotettavuutta käsitellään tämän osissa 4 ja 5.

9.4 Jäännösriski

Jäännösriskin pienentämisen vaatimukset eritellään standardin ISO 12100 kohdassa 3.13 seuraavasti:

1. suunnittelijan toteuttamien suojausteknisten toimenpiteiden jäljelle jäävä ”ensimmäinen jäännösriski”,
2. jonka jälkeen riskiä on vielä edelleen pienennettävä varotoimenpiteillä (pääasiassa työnantajan työsuojelun toimenpiteillä), jolloin jäljelle jää ”toinen jäännösriski”, ja
3. jonka on oltava ”siedettävä jäännösriski”.
(kohta 9.4).

Koneen jäännösriskin pienentäminen

- Riskeihin voi kuulua mekaanisten riskien lisäksi esimerkiksi sähköisiä, hydraulisia ja pneumaattisia riskejä sekä energian varastoitumisesta, kemikaaleista, lämpötiloista, melusta ja säteilystä johtuvia riskejä.
- Tarkistetaan toiminnallisilla testauksilla, onko turvallisuusteknisistä toimenpiteistä huolimatta koneessa jäännösriskejä, ja jos on, onko niistä varoitettu ja onko niiden pienentämisestä ilmoitettu käyttöohjeessa.
- Tarkistetaan, onko koneen mukana toimitettu ohjeet siitä, miten näistä vaaroista aiheutuvat riskit voidaan asianmukaisesti poistaa tai pienentää riittävästi.
- Otetaan selville, mitä varotoimenpiteitä tarvitaan hätätilanteiden varalle ja huolehditaan niitä koskevien ohjeiden laatimisesta ja henkilöstön toiminnan opastamisesta.

9.5 Vaihe 3: Täydentävät suojaustoimenpiteet

Täydentäviä suojausteknisiä toimenpiteitä

- odottamattoman käynnistymisen estäminen toiminnanestokytkimellä tai siirtoavaimella
- varotoimenpiteitä kuten mekaaninen hätäpysäytys, palonsammutuslaitteet, räjähdysvaarallisten tilojen tuuletus koneen ohjausjärjestelmästä erillisellä järjestelmällä jne.

Ohjausjärjestelmän riskien pienentämisen toimenpiteitä

- asetetaan turvallisuuteen liittyvien parametrien rajoitukset, esim. vasteaika, nopeus, liike tai paine
- tehon syötön vaihteluiden, menetyksen ja palautumisen hallinta
- erilaisten turvallisuuteen liittyvien fyysisten ja toiminnallisten osien yhteensopivuus
- loukkuun jääneen henkilön vapauttamisen menetelmät energian syötön ollessa päällä tai pois päältä.

10 Turvallisuuteen liittyvä dokumentaatio

HUOM. Dokumentoinnin merkityksestä sanotaan nykyisin ”Mitä ei ole dokumentoitu, sitä ei ole!”.

Esimerkiksi jos valmistettaessa uutta koneversiota tarkkaa dokumentaatiota ei ole käytettävissä, ei voi nojautua edellisiin koneversioihin ja suuri osa aikaisemmintehdystä työstä jää hyödyntämättä.

Koneen turvalliseen käyttöön ja turvallisuuden ylläpitämiseen kuuluu koneen kattava dokumentaatio, josta käy ilmi koneen turvallisuuteen liittyvät yksityiskohdat ominaisuudet ja toiminnot. Siten konedirektiivissä lueteltujen konedirektiivissä esitettävien dokumenttien lisäksi konedirektiivissä on vaatimukset muistakin koneen teknisen rakenteen ja toimintojen dokumenteista niiltä osin kuin ne koskevat koneen turvallisuutta ja sen ylläpitoa.

Myös koneiden hankkijat vaativat koneen luovutus-vastaanottotarkastuksissa yhä useammin koneen turvallisuuteen liittyvien dokumenttien katselmuksia voidakseen ylläpitää koneen turvallisuutta. Koneen suunnittelun, toteutuksen ja testausten aikana syntyy paljon tuotetietoja, jotka koneen valmistajan on tallennettava. Koneiden muuttuessa yhä monipuolisemmiksi järjestelmiksi, myös koneiden eri versioiden turvallisuuteen liittyvien dokumenttien ja niiden monikielisten käännösten hallinta tulevat tärkeiksi osiksi koneen valmistuksen tuotetietojen hallintajärjestelmää (*Product Document Management*, PDM).

Koneen dokumentteihin kuuluu selvitykset siitä, miten yhdenmukaistettuja standardeja on käytetty koneen suunnittelussa ja vaatimustenmukaisuuden osoittamisessa. Mitä enemmän koneen valmistaja on nojautunut standardien mukaisiin ratkaisuihin, sitä helpompaa on tehdä koneen dokumentaatio (luku 10). Koska aina ei viitata koko standardiin, viittaukset on yksilöitävä. Useimmissa yhdenmukaistetuissa standardeissa on lueteltu kyseiseen standardiin liittyvät dokumentit. Tällöin voi olla riittävää, kun turvallisuuteen liittyvien sovellusten ratkaisujen kuvauksia tehdään itse vain niiltä osin, joissa yhdenmukaisiin standardeihin ei ole suoraan ja täysimääräisesti nojauduttu.

Dokumentteja tarvitaan mm. käyttäjän huolto- ja kunnossapitotehtäviin sekä koneen kunnossapitoon, muutostöihin ja modernisointiin (osa 2 luku 11). Dokumenttien toimittamisesta on hyvä sopia etukäteen. Valmistajan omia tietoja ei tarvitse toimittaa koneen tilaajalle, mutta tilaajan tarvitsemia osia tiedostosta voidaan antaa pyynnöstä tilaajan käyttöön.

Myöhemmin koneen valmistaja voi käyttää dokumentteja uusien koneversioiden tai -tyyppien suunnitteluun. Dokumentteja on toimitettava myös viranomaiselle sen pyytäessä. Näin ollen turvallisuuteen liittyvät tiedot on syytä luokitella erikseen tai varustaa dokumentit tunnuksilla (esim. PDM-järjestelmässä) siten, että ne on helppo koota toimitusta varten.

Huom. Osan 1 liitteessä 1 esitetään luettelo EU:n talousalueella koneen vaatimustenmukaisuuden osoittamiseen vaadittavista dokumenteista.

Erityisesti turva-automaatioon liittyvää teknistä dokumentaatiota esitetään osan 4 kohdassa 14 ja yhteenveto ohjausjärjestelmän turvallisuuteen liittyvistä dokumenteista esitetään osan 4 liitteessä 3.

11 Viittauksia ja kirjallisuutta

Direktiivien, säädösten ja soveltamisohjeiden haku tapahtuu helpoiten Metstan koneturvallisuuden teemasivuilta ”Linkit ja oppaat”:

http://www.metsta.fi/www/koneturvallisuuden_teemasivut/linkit.php www.metsta.fi

Direktiivit (Metsta)

- Konedirektiivi: (*Machinery Directive*, MD) 2006/42/EY
- Pienjännitedirektiivi (*Low Voltage Directive*, LVD) 2006/95/EY
- Konedirektiivin soveltamisohje (suomeksi)
- Pienjännitedirektiivin ja painelaitedirektiivin soveltamissuosituksia, Kemikaali- ja turvallisuusvirasto Tukes

Säädökset (Metsta ja Finlex: www.finlex.fi)

- ”Konelaki”: Laki eräiden teknisten laitteiden vaatimustenmukaisuudesta (L 1016/2004)
- ”Koneasetus”: Valtioneuvoston asetus koneiden turvallisuudesta (VNa 400/2008)
- ”Työturvallisuuslaki”: L 738/2002 (muutoksia)
- ”Käyttöasetus”: Valtioneuvoston asetus työssä käytettävien työvälineiden turvallisesta käytöstä ja tarkastamisesta (VNa 403/200).

Standardeja

Koneturvallisuuden ISO-standardeja

- ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen, 2010
- ISO 13849-1 ja -2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet, 2015, osa 2: Kelpuutus, 2012
- ISO/TR 14121-2 Koneturvallisuus. Riskin arviointi. Osa 2: Käytännön opastusta ja esimerkkejä menetelmistä, 2012
- ISO 10218-2 Teollisuusrobotit – Osa 2: Robottijärjestelmät ja niiden yhdistäminen.
- ISO/TR 22100-2:2015 Koneturvallisuus. Suhteet standardiin ISO 12100. Osa 1: Miten B-tyypin ja C-tyypin standardit liittyvät standardiin ISO 12100
- ISO 14120 Koneturvallisuus. Suojukset. Kiinteiden ja avattavien suojusten suunnittelun ja rakenteen yleiset periaatteet, 2015
- ISO 11161 + A1 Koneturvallisuus. Valmistusjärjestelmien koneyhdistelmät. Perusvaatimukset, 2010
- ISO 13855 Koneturvallisuus. Suojausteknisten laitteiden sijoitus ottaen huomioon kehon osien lähestymisnopeudet, 2010
- ISO 13857 Koneturvallisuus. Turvaetäisyydet yläraajojen ja alaraajojen ulottumisen estämiseksi vaaravyöhykkeille
- ISO 14119 Koneturvallisuus. Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta, 2013
- ISO 13850 Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet, 2015

Pääsy- ja kulkuteitä koskevia standardeja

- ISO 14122-1...4 Koneturvallisuus, Koneiden kiinteät kulkutiet:
- Osa 1 Pääsytien valinta ja yleiset vaatimukset
- Osa 2 Työskentelytasot ja kulkutasot
- Osa 3: Portaat, porrastikkaat ja suojakaiteet
- Osa 4: Kiinteät tikkaat

Koneen hallintalaitteita koskevia ergonomia standardeja

- Koneturvallisuuden, ergonomian ja käytettävyyden standardit:
<https://slideplayer.fi/slide/11136995/>

Sähkölaitteiden IEC-standardeja

- IEC 61511-3 Toiminnallinen turvallisuus – turva-automaatiojärjestelmät prosessiteollisuussektorille – Osa 3: Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiselle
- IEC 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset, 2018
- IEC 61508-5 Turvallisuuteen liittyvien sähköisten/elektronisten/ohjelmoitavien elektronisten järjestelmien toiminnallinen turvallisuus – Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi

Kirjallisuutta

- Tapio Siirilä: Turvalaitteen passivointi, Metstan verkkosivut
- Tapio Siirilä: Suojuksen kytkentä koneen toimintaan, Metstan verkkosivut
- Tapio Siirilä ja Katri Tytykoski: Koneturvallisuuden käsikirja, Inspecta, 2016, 720 s.
- Valvomo, suunnittelun periaatteet ja käytännöt, Suomen Automaatioseura ry., Helsinki 2010