Artikkelisarja turvallisen koneen suunnittelusta

Osa 4: Turvallisuuteen liittyvien ohjausjärjestelmien suunnittelu

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 perusperiaatteita 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 soveltamissuosituksen 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 ratkaisuista. Epäselvissä tapauksissa on nojauduttava 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 4

Elektronisten ohjausjärjestelmien käyttöönotolla parannetaan koneen ominaisuuksia ja saadaan aikaisempaa kattavampaa tietoa paitsi ohjattavasta prosessista myös koneen omasta tilasta. Erään arvion mukaan noin puolet koneilla sattuneista työtapaturmista liittyy koneen hallinta-järjestelmän (hallintalaitteet ja ohjausjärjestelmä) virheelliseen toimintaan. Siten turvallisen koneen suunnittelu edellyttää laatuajattelun mukaista järjestelmällistä suunnittelua ja aikaisempaa parempaa osaamista ja kehittyneitä suunnittelu- ja testausmenetelmiä. Tässä artikkelisarjan osassa 4 käsitellään koneen tyypillisten turvallisuuteen liittyvien ohjaustoimintojen oikean toiminnan ja luotettavuuden varmistamista. Kirjoitus perustuu koneiden ohjausjärjestelmien uusimpiin turvallisuusstandardeihin.

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

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 käyttöönotettavaksi

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

Suorat lainaukset on kirjoitettu *kursiivilla*.

2 Koneautomaation turvallisuus

Automaatio on mahdollistanut erilaisten ja eri valmistajien koneiden yhdistämisen kokonaisiksi tuotantolinjoiksi ja automaattisiksi valmistusjärjestelmiksi (osa 1 kohta 2.2). Tämän seurauksena myös erilaisten koneiden valmistajat ovat verkostoituneet keskenään ja myös alihankkijoiden, laitetoimittajien ja palveluntuottajien muodostamiksi verkostoiksi (”ekosysteemi”). Koneautomaation turvallisuus on tullut aikaisempaa useamman koneen ja sen ohjaustoimintoja toteuttavien komponenttien suunnittelijoiden vastuualueille. Kuitenkin Euroopan talousalueella uuden koneen suunnittelussa ja valmistuksessa turvallisuuden kokonaisvastuu on edelleen koneen valmistajalla (osa 2 luku 2) ja kaikki koneen suunnittelussa ja toteuttamisessa mukana olevat osapuolet ovat kukin turvallisuusvastuussa omista tehtävistään.

Automaation käyttöönotto on nykyisin tärkein tekninen menetelmä paitsi tuotannon tehostamisessa, myös turvallisuuden edistämisessä ja etenkin niillä toimialoilla, joissa esiintyy merkittäviä turvallisuusriskejä. Monia vaaranalaisia prosesseja ei voida hallita turvallisesti ilman nykyaikaista automaatiota. Automaation avulla työntekijä saadaan pois teknisestä prosessista tai koneiden vaaravyöhykkeiltä, kun prosessia tai konetta ohjataan valvomosta tai suojatulta työasemalta (esim. metsäteollisuus, kaivosteollisuus jne.). Vaarallisia prosesseja ei voida hallita turvallisesti ilman nykyaikaista automaatiota.

Toisaalta automaattisten turvajärjestelmien käyttö edellyttää järjestelmän kokonaisturvallisuuden hallintaa, johon kuuluu vaatimukset turvallisuudesta, käyttövarmuudesta, kunnossapidettävyydestä, ympäristöturvallisuudesta, tietoturvallisuudesta ym. Siten eri alojen asiantuntijoiden toiminnot vaikuttavat muidenkin osapuolten toimintaan ja (osa 2 luku 4).

Automaatio tarjoaa koneiden turvallisuuden varmistamiseen myös uusia turvallistamisen menetelmiä ja välineitä (esim. valosähköiset turvalaitteet). Nämä ovat tarpeen varmistettaessa erityisesti jatkuvatoimisten automaattisten koneiden turvallisuutta. Näissä koneissa ongelmat keskittyvät säätö, korjaus- ja kunnossapitotoimintoihin, jolloin työntekijän on mentävä vaaravyöhykkeelle tai sen lähelle. Tämä aiheuttaa suuren riskin, jos vaarallinen prosessi tai kone on toiminnassa, mutta toisaalta pysähtyneen koneen odottamaton käynnistyminen voi aiheuttaa vielä suuremman riskin.

Koneiden turvallisuuden varmistamiseen tarvitaan useiden eri alojen asiantuntemusta kuten esimerkiksi mekaaninen ja hydraulinen suunnittelu, sähköistys, automaatiosuunnittelu, ohjelmistosuunnittelu, tietoturva jne. Koska kysymys on henkilöturvallisuudesta, turvallisuuteen liittyvän automaatiojärjestelmän laatuvaatimukset ovat korkeammat kuin ei-kriittisissä järjestelmissä.

Kun turvallisuuteen liittyvän automaation suunnittelussa ja toteutuksessa yhdistyvät koneturvallisuus, sähkötekniikka, tieto- ja tiedonsiirtotekniikat, ihminen-kone-vuorovaikutuksen näkökohdat jne., tarvitaan tämän kokonaisuuden hallintaan eri alojen ammattilaisten yhteistyötä. Jokaisen osapuolen toiminta, osaaminen, yhteistyö ja vastuurajat jne., on varmistettava turvallisuuden hallintajärjestelmän avulla heti suunnittelun alkuvaiheessa (kohta 4.1 ja osa 1 kohta 3.2). Tähän tarvitaan selkeitä menettelytapoja. Osapuolina monien pientenkin yritysten asiantuntijat ovat omalla erikoisalallaan mukana suunnittelemassa ja toteuttamassa suurempiakin

turvallisuuteen liittyviä ratkaisuja, ja siten he kuuluvat osaltaan verkostoituneen toiminnallisen turvallisuuden hallintajärjestelmään.

3 Elektroniset ohjausjärjestelmät

3.1 Elektronisten ohjusjärjestelmien kehitys

Teollisuudessa käytössä oleva tekniikka on muuttunut nopeasti uusien ohjelmoitavien valmistusjärjestelmien kehittämisen ja käyttöönoton seurauksena. 1960-luvulla digitalisointi valtasi alaa ja tietokonepohjaisia ratkaisuja alettiin ottaa käyttöön. Releohjauksien rinnalle tulivat vähitellen ohjauslogiikat, perinteiset ohjelmoitavat logiikat (PLC) sekä yksittäiset eristetyt tietokoneet. Näitä järjestelmiä on viimeisten parin vuosikymmenen aikana korvattu mikroprosessoreihin perustuvilla ohjelmoitavilla logiikoilla. Nämä ovat tyypillisesti modulaarisia laitteita tai piirikortteja, joita käytetään prosessinohjaukseen, digitaalisiin tuloihin ja -lähtöihin sekä analogisiin tuloihin ja lähtöihin, ihminen–kone -vuorovaikutukseen sekä tietoliikenteen liitäntöihin.

Uusien ohjelmoitavien valmistusjärjestelmien kehittämisen ja käyttöönoton seurauksena teollisuudessa käytössä oleva tekniikka on muuttunut nopeasti. Tyypillisiä järjestelmiä ovat kappaletavarateollisuuden valmistusjärjestelmät, joita ohjataan logiikoilla ja joissa on jatkuva-aikainen säätö yhdistettynä logiikalla ohjelmoituun työkiertoon. Toinen esimerkki on metsäkone, jossa voi olla useita erillisiä tietokoneita ohjaamassa laitteita CAN-väylän kautta.

Tänä päivänä valmistajakohtaiset käyttöjärjestelmät ja verkot kehitetään yhteen kytketyiksi sovelluksiksi (esim. prosessit, konelinjat, laitokset), joissa käytetään kaupallista tekniikkaa. Näitä järjestelmiä integroidaan tehdasjärjestelmien kesken (horisontaalinen integrointi) ja muiden liiketoimintasovellusten kanssa tietoliikenneverkkojen välityksellä (vertikaalinen integrointi).

Suljetuista valmistajakohtaisista verkoista siirrytään standardiverkkoihin, kuten Ethernet- ja Internet-verkkoteknologioiden käyttöön. Automaation viimeisinä vuosikymmeninä määrättyyn tarkoitukseen erikseen suunnitelluista laitteista siirrytään standardilaitteistoilla, -ohjelmistoilla ja -tiedonsiirtoteknologioilla toteutettuihin automaatioympäristöihin, joissa automaatio on toteutettu sulautetuilla ohjelmistoilla.

Mahdollisuudet erilaisten laitteiden ja ohjelmistojen yhdistämiseen lisääntyvät, mutta samalla tuotantojärjestelmien monimutkaisuus kasvaa. Tarve informaation laaja-alaiseen hyödyntämiseen sekä yritysten sisällä että yritysten kesken lisää paineita tietoverkkojen entistä laajempaan käyttöön. Automaatio edellyttää uusia suunnittelumenetelmiä ja tietokoneavusteisia työkaluja (koneen toimintojen mallintamiseen, ohjelmistokehitykseen, ohjelmistotestaukseen jne.)

Verkottumisella saavutettavien hyötyjen ohella verkottumiseen liittyy myös kasvava tarve turvallisuuden hallintaan. Kun uhkat ja verkkojen haavoittuvuudet ovat lisääntyneet, myös tarve suojata tietojärjestelmiä ja niihin kuuluvia automaatiojärjestelmiä ja -verkkoja on kasvanut.

Yhtenäiset, sovellusaluekohtaiset standardit ja ohjeet tietoturvasta sekä sen käytännön toteutuksesta kuitenkin puuttuvat. Monilla yrityksillä ei vielä ole kokonaisuuden hallintaan tarvittavaa osaamista tai selkeitä käytäntöjä. Koneen ohjausjärjestelmät ja erityisesti niiden elektroniset komponentit ovat herkkiä mm. ympäristöolosuhteille. Esimerkiksi järjestelmän

vikaantuessa tai käyttäjän virhetoiminnan johdosta voi syntyä tilanteita, joissa järjestelmää ei voi hallita. Tämän varalta ohjausjärjestelmän ohjelmistojen oikea toiminta ja riittävä luotettavuus on varmistettava kehittyneillä suunnittelu- ja testausmenetelmillä (luku 11).

Huom. Riskiä voidaan pienentää joko pienentämällä:

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

Riskin pienentämisessä käytetään tavallisesti molempia menetelmiä esimerkiksi siten, että ensin pyritään estämään vaaratilanne suunnittelemalla oikealla tavalla toimivia ja luotettavia laitteita ja niiden ohjaustoimintoja, sitten vaarallisen tapahtuman varalta rajoitetaan vaaravyöhykkeitä fyysisillä laiteilla ja sen jälkeen tarvittaessa lisätään ohjausjärjestelmän toteuttamia turvatoimintoja. Tässä kirjoitussarjassa keskitytään turvallisuuteen liittyvien ohjaustoimintojen suunnitteluun. Osan 3 robottiyksikön turvallistamisen useissa esimerkissä käsitellään mekaanisten suojusten osuutta kokonaisturvallisuuden varmistamisessa.

3.2 Elektroniikan ongelmia

Elektroniikan monimutkaisuus ja herkkyys lisäävät suuresti vaatimustasoa koneiden elektronisten ohjausjärjestelmien suunnittelussa verrattuna aikaisempiin ohjausjärjestelmäteknologioihin. Seuraavassa eräitä tärkeimpiä ominaisuuksia, mutta ei kaikki, mitkä on otettava huomioon:

Ohjelmoitavan elektroniikan ongelmia

- Monimutkaisuus, joka johtaa helposti suunnitteluvirheisiin: tarvitaan järjestelmällinen suunnitteluprosessi, kattavat testaukset ym.
- Herkkyys komponenttien vikaantumisille: tarvitaan komponenttien satunnaisvikaantumisten hallintaa, luotettavuusteknisiä menetelmiä ja niiden työkaluja (esim. Sistema)
- Huono ympäristöolosuhteiden sieto (poikkeukselliset lämpötilat, mekaaniset iskut, EMC-häiriöt jne.): käytetään testattuja komponentteja, vikaturvallisia ratkaisuja, yhteisvikaantumisten hallintaa
- Ohjelmistovirheet: tarvitaan kelpuutettuja ohjelmistokehitys- ja testaustyökaluja
- Langaton ohjaus ja etäohjaus: on otettava huomioon käyttörajoitukset.
- Järjestelmien yhteensopivuus: käytetään standardisoituja tuotteita, erilaisten ja eri-ikäisten järjestelmien yhteensovittamisessa tarvita huolellista räätälöintiä
- Tietoliikenneyhteyksien haavoittuvuus: tarvitaan tietoturvatietoisuutta, ohjelmallisia ja fyysisiä suojauksia
- Käyttöliittymät: käytetään ergonomiastandardeja.

Elektroniikkaan perustuvan automaation monimutkaisuuden ja herkkyyden vuoksi järjestelmän laatuvaatimukset ovat korkeat. Tämä koskee erityisesti turvallisuutta, jonka on oltava korkealla tasolla, mutta sama koskee myös järjestelmän luotettavuutta, käyttövarmuutta, kunnossapidettävyyttä, tietoturvallisuutta ym. laatutekijöitä (luku 4).

3.3 Ketä ohjausjärjestelmien turvallisuusvaatimukset koskevat?

Henkilöturvallisuuden vuoksi automaatiojärjestelmien laatuvaatimukset ovat korkeammat kuin sellaisissa muissa järjestelmissä, joissa ei ole kysymys henkilöturvallisuudesta (ei-kriittisissä

järjestelmissä). Muita vastaavia kriittisiä järjestelmiä (joita ei tässä käsitellä) ovat prosessiteollisuuden järjestelmät, joihin liittyy paitsi käyttäjien henkilöturvallisuus myös suuronnettomuusvaarat tai ”infrasysteemit” kuten esimerkiksi sähkö-, vesi-, liikenne- ym. turvallisuuteen liittyvät järjestelmät, jotka koskevat suuria ihmisjoukkoja.

Koneiden toimintojen turvallisuuden suunnittelu koskee

- yrityksiä, yksiköitä ja henkilöitä, jotka suunnittelevat, toteuttavat tai arvioivat ohjelmoitavalla elektroniikalla ohjattavia turvallisuuteen liittyviä koneen toimintoja ja niiden yhteyksiä muihin tietojärjestelmiin
- yrityksiä, jotka ovat alihankkijoina tai laitetoimittajina em. tahoille
- tutkimuslaitoksia, oppilaitoksia ym., jotka kehittävät nykyaikaisia turvallisuusmenetelmiä tai opettavat niitä.

Huom. Turvatoiminnon suoritusvaatimukset ovat aivan samat pienille ja suurille yrityksille, koska turvallisuusvaatimukset riippuvat ainoastaan siitä tunnistetun riskin pienentämisvaatimuksesta, joka kyseiseillä toimenpiteillä on tarkoitus saada aikaan.

Toiminnallisen turvallisuuden varmistamista tehdään järjestelmän koko elinkaaren ajan lähtien järjestelmän suunnittelusta, toteutuksesta ja käyttöönotosta edelleen järjestelmien käyttöön, kunnossapitoon ja järjestelmän muutoksiin. Kaikkien näiden elinkaaren vaiheiden hallintaan tarvitaan niitä kattava turvallisuuden hallintajärjestelmä ja eri vaiheisiin tarvitaan turvallisuuden erityisosaamista.

3.4 Osaamisen kehittäminen

Useimmiten koneen valmistajan teknisistä asiantuntijoista vain harvat ovat opiskelleet luotettavuustekniikkaa. Vaikka yksinkertaiset ohjaustoiminnot voidaan toteuttaa kokemuspohjaisesti yksinkertaisten käytännöllisten mallien ja muistisääntöjen avulla, järjestelmällisen suunnittelun mukana syntyvät dokumentit voivat jäädä tekemättä. Jos näin käy, koneen tilaaja ei voi varmistua koneen turvallisuudesta eikä voi huolehtia turvallisuusvastuustaan. Tällöin tilaaja ei voi vastaanottaa konetta ja koneen toimitus voi pahasti viivästyä. Kun jälkikäteen suunnitellaan koneen ohjaustoiminnot uudelleen toisella tavalla, jotta saataisiin aikaan tarvittava dokumentaatio, tehdään ainakin osittain kaksinkertainen työmäärä.

Osaamisen pitäminen ajan tasalla voi olla jatkuvana ongelmana, kun uusia ja edullisempia ohjausjärjestelmiä, komponentteja ja ohjelmistotyökaluja tulee koko ajan markkinoille. Ohjelmistojen koko ja niiden osuus tuotantojärjestelmän suunnittelussa kasvaa nopeasti. Siten koneiden ja prosessien turvallisuuden varmistamiseksi tarvitaan aikaisempaa enemmän ja parempaa koulutusta oppilaitoksissa, parempaa opastusta koneiden turvalliseen käyttöön ja kunnossapitoon työpaikoilla jne. Myös altistuminen tietoturvahyökkäyksille kasvaa. Tarvitaan tietoturvan hallintajärjestelmää ja siihen kuuluvia toimenpiteitä (liite 2).

Huom. Mikään yritys ei itse valmista automaattista turvallisuuteen liittyvää konetta kokonaan itse (osa 1 kohdat 2.3…2.5 ja osa 2 luku 4).

Koneen valmistajalle voi olla hyvin vaativaa, jos pyrkii suunnittelemaan turvallisuuskriittisen järjestelmän kokonaan tai mahdollisimman pitkälti itse ja käyttää siihen runsaasti resursseja. Realistisena vaihtoehtona on

- hankkia osaamista ja resursseja yrityksen ulkopuolelta tai
- ostaa ja räätälöidä koneeseen valmis ohjausjärjestelmä tai ainakin hankkia ohjausjärjestelmän keskeisimpiin toimintoihin valmiita testattuja laitteita ja komponentteja
- käyttää apuna erityistä automaatiointegraattoria ohjausjärjestelmän suunnitteluun, hankintoihin ja toteuttamiseen.

Siten koneen turvallisuuden suunnittelun alussa on huolellisesti eriteltävä koneen tarvittavat ominaisuudet ja sitten päätettävä mitä tehdään itse ja mitä komponentteja tai palveluita tai valmiita järjestelmiä hankitaan yrityksen ulkopuolelta (osa 1 kohdat 2.3…2.5 ja osa 2 luku 3).

Suomessa toiminnallisen turvallisuuden herättäjänä ovat olleet mm. kansainvälisten tilaajien tiukat turvallisuusvaatimukset sekä toiminnallisesta turvallisuudesta että sen dokumentoinnista.

> Toiminnallisen turvallisuuden ”isä” Ron Bell (UK) totesi toiminnallisen turvallisuuden koulutuksesta muutama vuosi sitten: ”Nykytilanne ei anna riittävän vankkaa perustaa pätevyyden saavuttamiseksi ja sen ylläpitämiseksi. Haluaisin nähdä nopeampaa kehitystä kansainvälisessä yhteistyössä standardin IEC 61508 ja sen sovellusstandardien (ml. konepuolen standardit) vaatimusten perustalta laadittaville pätevyysvaatimusten erittelyille siten, että niillä helpotettaisiin henkilöiden pätevyyden kehittämistä ja tukevia kursseja. Tässä tavoitteessa on erityisen tärkeätä internetin kautta saatavien etäopiskelukurssien kehittäminen. Eräitä aloitteita on jo toteutumassa tämän kehityksen nopeuttamiseksi.”

Toiminnallisen turvallisuuden kursseja järjestää ulkomailla mm. seuraavat tahot:

Yhdysvalloissa on toiminnallisen turvallisuuden koulutusohjelmia, joita ylläpitää kansainvälinen Automaatioseura ”*International Society of Automation, ISA*”. Koulutus tapahtuu etäopiskeluna ja siinä on kaksi tasoa:

- ”ISA84 SIS Fundamentals Specialist (ISA84 SFS)” (perusteet) ja
- ”ISA84 Safety Instrumented Systems (SIS) Expert” (erikoisasiantuntija).

Vastaavaa koulutusta antaa vastaavasti kuin edellä myös kahdella tasolla myös saksalainen teknisen turvallisuuden valvontalaitos ”*Technischer Überwachungsverein, TÜV*”. Certified Machinery Safety Expert CMSE® on TÜV Nord’in sertifioima “Koneturvallisuuden asiantuntija tutkinto”:

- ”Functional Safety Engineer (FSeng)” ja
- ”TÜV Functional Safety Expert (FSExp)”.

Molemmat laitokset toimivat kansainvälisesti myös muualla.

Suomessa ”Toiminnallisen turvallisuuden insinöörin” viikon kursseja järjestää mm.

- Inspecta CMSE(R). Sertifioijana toimii TÜV Nord.
- FSCC (Functional Safety Certification Course) järjestäjänä Safety Advisor Oy. Sertifioijana toimii TÜV (SÜD).

Muutamat koulutusjärjestöt (esim. AEL) sekä ohjaus- ja turvajärjestelmien niiden komponenttien valmistajat ja maahantuojat järjestävät avointa koulutusta ohjausjärjestelmien suunnittelusta.

4 Laadunhallinnan järjestelmät

4.1 Turvallisuuden hallintajärjestelmä ja turvallisuussuunnitelma (Safety Plan)

Laadunhallinnan perusteita on käsitelty osassa 1 luku 3. Yrityksen turvallisuustavoitteiden asettamisen perustana on turvallisuussuunnitelma (*Safety Plan*) ja siinä osana erityisesti toiminnallisen turvallisuuden suunnitelma (osa 1 kohta 3.2, *Functional Safety Plan*). Turvallisuussuunnitelmien. toteutumista on seurattava ja poikkeamiin on puututtava.

Toiminnallisen turvallisuuden suunnitelma *(Functional Safety Plan)*

- Kehitetään turvallisuuskulttuuria
- Laaditaan osana tuvallisuuden hallintajärjestelmää toiminnallisen turvallisuuden ohjelma (Functional Safety Plan) ja sen noudattamista valvotaan
- Päätetään mitä ostetaan valmiina, mitä tilataan alihankintana, mitä tehdään itse
- Osapuolten huolellinen valinta ja yhteistyön koordinointi ja määritetään selkeät roolit/vastuut
- Henkilöstön ja alihankkijoiden turvallisuus- ym. osaamisen varmistaminen ja pätevyyden ylläpitäminen
- Turvallisuuden ja toiminnallisen turvallisuuden elinkaarten vaiheiden ja niihin liittyvien tehtävien suunnittelu ja koordinointi
- Tehdään toiminnallisen turvallisuuden elinkaaren mukaiset todentamiset ja lopuksi kelpuutukset.
- Valitaan sopivat ja kelpuutetut työkalut vaatimusten, dokumentaation ja versionhallintaan.
- Huolehditaan turvallisuuteen liittyvästä tiedonkulusta.

Yrityksen toiminnallisen turvallisuuden suunnitelma sisältää seuraavat tehtävät. Luettelon tehtäviä voidaan ottaa käyttöön soveltuvin osin toimialasta riippumatta.

Koneen valmistajan turvallisuuden ohjelma

Yritystason turvallisuuspolitiikka

Projektiin liittyvät turvallisuuden lähtökohdat
- Projektin nimi ja kuvaus
- Projektin aikataulu
- Projektin vastuuhenkilöt
- Projektin osapuolet ja niiden roolit
- Projektin elinkaarimalli ja sen vaiheet
- Projektiarkisto

Turvallisuuden hallintajärjestelmä ja siihen liittyvät muut järjestelmät
- Yleiset laatujärjestelmät (esim. ISO 9001)
- Dokumentaatiojärjestelmä
- Tuotetiedon hallintajärjestelmä
- Muutosten hallintajärjestelmä
- Ohjelmistojen versionhallintajärjestelmä
- Tietoturvan hallintajärjestelmä

Turvallisuusosaamisen varmistaminen
- Mitä tehdään itse ja mitä hankitaan muualta
- Alihankkijoiden valintaperusteet
- Turvallisuusosaamisen varmistaminen
- Omien työntekijöiden koulutus- ja työn opastusjärjestelmät
- Omien resurssien varmistaminen
- Ajalliset ja taloudelliset resurssit

Turvallisuuteen liittyvät elinkaarimallit
- Turvallisuuden varmistamisen elinkaarimalli ja sen vaiheiden kuvaukset
- Toiminnallisen turvallisuuden elinkaarimalli ja sen vaiheiden kuvaukset

Turvallisuuteen liittyvä lainsäädäntö
- Konedirektiivi/koneasetus
- Pienjännitedirektiivi ja vastaavat kansalliset säännökset
- Painelaitedirektiivi ja vastaavat kansalliset säännökset
- Muut direktiivit ja vastaavat kansalliset säännökset

Sovellettavat standardit ja ohjeet
- Eurooppalaiset yhdenmukaistetut standardit
- Muut standardit
- Konedirektiivin soveltamissuositukset
- Yrityksen ohjeet ja muut ohjeet

JATKUU

Valmistajan turvallisuusorganisaatio ja siihen liittyvät tehtävät, vastuut ja vastuunjako

- Laitostasolla
- Osastotasolla
- Yksikkötasolla
- Henkilötasolla

Muiden osapuolten vastuut ja niiden jakautuminen ja osaamisen varmistaminen

- Suunnittelijat ja niiden alihankkijat
- Laitetoimittajat ja niiden mahdolliset alihankkijat
  - sähkö- ja automaatiotoimittajat
  - muut toimittajat kuten palveluntuottajat (esim. suunnittelijat ja konsultit)

Koneen turvallisuuden perusperiaatteet

- Sovellettavat menettelytavat turvallisuuden varmistamiseen elinkaarivaiheiden mukaan
- Riskien tunnistamisen
- Riskien pienentämisen menettelytavat
- Vaatimustenmukaisuuden osoittamisen menetelmät

Toiminnalliseen turvallisuuteen liittyvä vastuunjako

- Laitostasolla
- Osastotasolla
- Yksikkötasolla
- Henkilötasolla

Toiminnallisen turvallisuuden varmistaminen

- Elinkaarivaiheiden mukaiset suunnittelun, todentamisen ja kelpuutuksen menettelytavat
- Turvallisuuteen liittyvien ohjaustoimintojen oikeellisuuden tarkistaminen
- Koneiden riskin arvioinnin tulosten käsittely turvatoimintojen määrittämistä varten
- Vaatimusmääritykset ja vaatimusten todentaminen turvallisuuteen liittyville ohjaustoiminnoille
  - turvatoimintojen oikean toiminnan varmistamisen menetelmät
  - turvatoiminnoilta vaadittavien PLr- ja SIL-tasojen määrittämisen menetelmät
  - turvatoimintojen saavuttamien PL- ja SIL-tasojen arvioinnin menetelmät
  - toiminnallisen turvallisuuden varmistamisen menetelmät katselmukset
  - todentamiset ja kelpuutus ja niiden testaukset

Käyttökokemusten kerääminen ja käsittely

- Koneturvallisuus
- Toiminnallinen turvallisuus.

Tarkempia vaatimuksia toiminnallisen turvallisuuden hallintajärjestelmistä esitetään standardeissa IEC 61508-1 luku 6 ja IEC 62061 luku 4.

4.2 Ohjausjärjestelmän turvallisuuden järjestelmällinen suunnittelumenetelmä

Kirjoitussarjan osissa 1…3 on kuvattu järjestelmällistä koneen turvallisuuden suunnittelua. Sen osana on järjestelmällinen koneen toiminnallisen turvallisuuden suunnittelu.

Vaikka elinkaaritarkastelu on otettu käyttöön ennen muuta toiminnallisen turvallisuuden suunnittelussa ja erityisesti ohjelmistokehityksessä (luku 10), elinkaaritarkastelua käytetään yhä

enemmän myös koko konejärjestelmien suunnittelussa (kohta 4.3). Käytettäessä elektronisia ohjausjärjestelmiä koneen toimintojen ohjauksessa koneen fyysisten ominaisuuksien ja elektronisten ohjaus- ja diagnostiikkatoimintojen vuorovaikutuksilla saadaan aikaan aikaisempaa parempaa koneen hallintaa ja siten myös parempaa turvallisuutta. Esimerkiksi koneen sovellusohjelmiston kehitystä varten on saatava tarkat tiedot koneen fyysisestä toiminnasta ja sen rajoituksista sekä muista mahdollisista ongelmista, mutta toisaalta sovellusohjelmiston avulla voidaan parantaa koneen toimintoja ja niiden luotettavuutta esimerkiksi lisäämällä sovellusohjelmistoon koneen tilaa ennakoivia ja tarvittaessa siihen reagoivia toimintoja (esim. IoT, liite 3).

Huom. Tässä kirjoituksessa ohjausjärjestelmän suunnittelu kuvataan standardissa ISO 13849-1 esitettävän yksinkertaistetun suunnittelumenetelmän ja siihen perustuvan ohjelmistotyökalun Sistema avulla (liite 1).

Koneen turvallisuuteen liittyvän ohjausjärjestelmän suunnittelu on toteutettava

- järjestelmällisellä lähestymistavalla (*Systems Approach,* osa 3 luku 2.2), jonka osana on toiminnallisen turvallisuuden suunnittelun elinkaaren vaiheistus ja
- kaikessa toiminnassa noudatetaan laadunhallinnan järjestelmien vaatimuksia ja valvotaan turvallisuusohjelman (Safety Plan) noudattamista (kohta 4.1).

Järjestelmällinen lähestymistapa perustuu kokonaisuuden jakamiseen osiin (moduuleihin tai Sistemassa alajärjestelmiin ja niiden lohkoihin ja elementteihin (IFA ”Kirjallisuutta” ja osa 5 liite1). Jokaisen osan on oltava riittävän pieni ja yksityiskohtainen, jotta sen tarkoitus, toiminnot ja perusominaisuudet ovat selkeät. Tämä on tarpeen vähintäänkin moduulitason tarkistuksia ja testauksia varten.

Järjestelmän osien dokumentoinnissa on selkeästi määritettävä mm. osan (moduulin) toiminta, ominaisuudet sekä liittyminen järjestelmän muihin osiin. Vasta tämän jälkeen testatuista ja dokumentoiduista moduuleista kootaan järjestelmän osia ja lopuksi osista koko järjestelmä.

Valmistustekniikan koneiden ohjaustoimintojen laajetessa ja monimutkaistuessa on syntynyt tarve siirtyä pitemmälle mallipohjaiseen suunnitteluun. Tällöin kone suunnitellaan sen toiminnallisen tietokonemallin avulla (”digitaaliset kaksoset”). Mallin avulla voidaan simuloida dynaamisesti koneen toimintoja tarkastelemalla tietokoneavusteisesti koneen tiloja ja tilasiirtymiä (tilakone, *state machine*), testata ohjelmistojen oikeellisuutta ja testata erityisesti koneen turvallisuuteen liittyviä toimintoja.

Jos yrityksellä ei ole kokemusta turvallisuuskriittisten tuotteiden valmistuksesta tai käsitellään järjestelmiä, joiden turvallisuuden todentaminen on hankalaa (esim. vaativia ohjelmistoja), on suositeltavaa hankkia valmiita sertifioituja komponentteja ja osajärjestelmiä. Turvallisuuteen liittyvien järjestelmien suunnittelun avuksi voidaan hankkia myös ulkopuolista asiantuntemusta palveluita, mutta tällöin on erityisesti syytä varmistaa alihankkijoiden turvallisuusosaamisen ajantasaisuus (kohta 3.4).

4.3 Ohjausjärjestelmän turvallisuuden suunnittelun elinkaarimalli ja sen vaiheet

Kohdassa 4.1 mainitussa toiminnallisen turvallisuuden suunnitelmassa (*Safety Plan*) määritetään strategiset, hallinnolliset ja tekniset toimenpiteet, joita tarvitaan koneen turvallisuuteen liittyvien toimintojen toteuttamisessa.

Tuotteen laadunhallintaan tarkoitetun elinkaaritarkastelun periaatteet syntyivät 1980-luvulla (Product Lifecycle Management, PLM). Tässä yhteydessä tarkastellaan koneen elinkaaren vaiheita vain koneen peruskonseptin suunnittelun vaiheita koneen käyttöönottoon ja tämä osa 4 keskittyy koneen toimintojen oikeellisuuden ja luotettavuuden varmistamiseen. Toiminnallisen turvallisuuden ja ohjelmistokehityksen hallintajärjestelmistä on yksityiskohtaiset kulkukaaviot ja selitykset standardissa IEC 61508-1 (”Toiminnallisen turvallisuuden hallinta”, luku 6, ”Kokonaisuuden turvallisuuden elinkaaren hallinta”, luku 7 ja ”Toiminnallisen turvallisuuden arviointi”, luku 8).

Elinkaaritarkastelulla on tarkoitus löytää suunnitteluvirheet mahdollisimman aikaisessa vaiheessa, jotta säästytään turhalta työltä, jota syntyy, jos suunnittelua jatketaan virheineen eteenpäin. Toiminnallisen turvallisuuden elinkaarimallissa koko suunnitteluprosessi jaetaan selkeästi hallittaviin osiin valmistettavan tuotteen suunnittelun elinkaaren vaiheisiin (*Safety Lifecycle, SLC*). Tämä lähestymistapa sopii hyvin teknisten järjestelmien turvallisuuden tarkasteluun, koska projektin elinkaaren eri vaiheissa on turvallisuuden kannalta erilaisia kohteita ja niihin liittyviä vaatimuksia ja menettelyjä. Myös osapuolet ovat mukana useimmiten vain muutamassa elinkaaren vaiheessa (kuva 1).

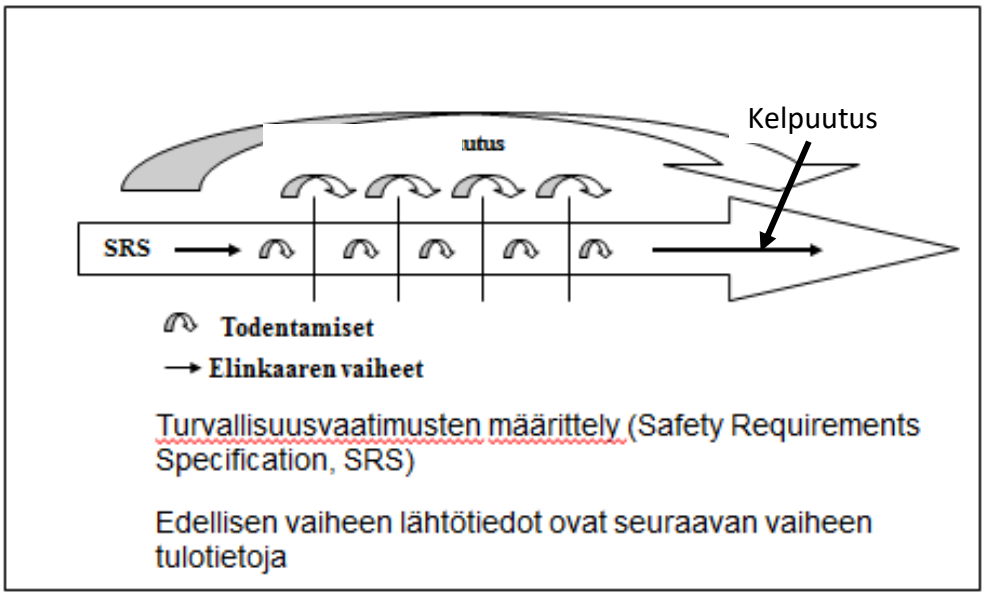
Tässä lähestymistavassa on olennaista, että elinkaaren jokaisessa vaiheessa on suunnittelu- ja todentamistehtäviä, joista huolehtivat nimetyt tahot ja henkilöt osapuolten työnjaon mukaan. Elinkaaren rajapinnoissa hallintaohjelmistot voivat huolehtia tietojen saatavuudesta, päivittämisestä ja tallennuksesta.

Toiminnallisen turvallisuuden elinkaarimalli on ohjausjärjestelmän suunnittelun runkona ja siinä on seuraavat turvallisuuden varmistamisen vaiheet:

- asetetaan ohjausjärjestelmälle toiminnallisen turvallisuuden vaatimukset (*safety requirements specification,* SRS)
- todennetaan (*verification*) elinkaaren peräkkäisten vaiheiden välissä toiminnallisten vaatimusten turvallisuusvaatimusten SRS täyttyminen
- ohjausjärjestelmän suunnittelun viimeisenä vaiheena on kelpuutus (*validation*), jossa tarkistetaan, että kaikki alussa määritetyt toiminnallisen turvallisuuden vaatimukset SRS on täytetty (esim. ohjelmiston testausten ja koneen toiminnallisten testausten avulla)
- kaikki elinkaaren vaiheet dokumentoidaan (mukaan lukien testaukset, niiden tulokset ja korjaavat toimenpiteet).

Suunnittelu tapahtuu turvallisuuden elinkaaren vaiheiden mukaan siten, että jokaisen vaiheen lopussa tehdään edellisen vaiheen todentaminen ennen siirtymistä seuraavaan vaiheeseen (kuva 1). Perusajatus on kuitenkin se, että joku muu käy läpi toisen henkilön tai työryhmän työn tulokset ja näin pyritään suhteellisen riippumattomasti löytämään mahdollisimman kattavasti virheet, jotta ne eivät kulkeutuisi suunnittelussa eteenpäin. Todentaminen voi olla auditointia, läpikäymistä,

parityöskentelyä tms. riippuen vaatimustasosta. Mitä suuremmat ovat vaatimukset, sitä tiukempaa riippumattomuutta tarvitaan. Lopuksi tehdään järjestelmän kelpuutus, jolloin tarkistetaan kelpuutussuunnitelman avulla, onko kaikki alun perin asetetut vaatimukset toteutettu.



Kuva 1 Elinkaarivaiheet ja todentamiset vaiheiden välissä

Jos merkittäviä virheitä on päässyt suunnittelun vaiheiden läpi kelpuutukseen saakka, voi olla tarpeen palata aikaisempiin suunnitteluvaiheisiin, käydä siitä alkaen vaiheet uudelleen läpi ja tehdä uudelleen kaikki todennukset. On selvää, että mitä useammin ja mitä pitemmälle alkuvaiheista lähtien joudutaan tekemään iteratiivisia kierroksia, sitä enemmän hukataan resursseja. Siksi ohjausjärjestelmän suunnittelun elinkaaren vaiheiden välissä tehtävät todennukset säästävät aikaa, vaivaa ja resursseja (kohta 4.3).

Elektroniikan käyttö koneiden ohjausjärjestelmissä on lisännyt dokumentointivaatimuksia. Ilman dokumentaatiota ei voi tehdä asianmukaista kunnossapitoa, muutostöitä tai modernisointia.

Jos koneen turvallisuuteen liittyvien ohjaustoimintojen suunnittelussa dokumentaatio ei ole täsmällistä ja kattavaa, ei voi käyttää elinkaarimallia eikä ohjelmistosuunnittelussa V-mallia. Jos lisäksi turvallisuuteen liittyvien ohjaustoimintojen suunnittelun alussa ei ole tehty vaatimusmäärittelyä, myös kaikki elinkaaren vaiheiden todentamiset ja valmiin koneen kelpuutus jäävät tekemättä. Tällöin koneeseen voi jäädä lukuisia erilaisia vaarakohtia ja epämääräisiä ratkaisuja.

Turvallisuuskriittisten järjestelmien suunnittelussa tarkka ja kattava dokumentaatio sekä täsmällinen versionhallinta ovat välttämättömiä (luku 13). Kaikki suunnittelun aikana syntyneet turvallisuuteen liittyvät dokumentit on tallennettava ja arkistoitava erikseen siten, että ne on helppo löytää myöhemmin jopa vuosienkin kuluttua esim. kunnossapitoa ja erityisesti ohjelmiston ylläpitoa varten. Kunnossapito on yksi pisimpään kestävistä tuotantolaitoksen elinkaaren vaiheista, joten järjestelmän valmistajan on laadittava kunnossapidon hallintajärjestelmän vaatimukset huolella.

5 Koneiden toiminnalliseen turvallisuuteen liittyvät standardit

5.1 Toiminnallisen turvallisuuden perusstandardi IEC 61508 osat 0…7

Jo 1980-luvun alkupuolella päädyttiin siihen, että monimutkaisten elektronisten ohjausjärjestelmien suunnittelu ja turvallisuuden varmistaminen on mahdollista vain turvallisuuden kokonaisuuden tarkasteluun soveltuvalla järjestelmällisellä (systemaattisella) lähestymistavalla. Tämä lähestymistapa perustuu turvallisuuden elinkaaren vaiheiden tarkasteluun, joka lähtee järjestelmän suunnittelusta, toteutuksesta, käyttöönluovutuksesta ja käyttöönotosta edelleen järjestelmän käyttöön, kunnossapitoon ja järjestelmän muutosten hallintaan (kohta 4.3).

2000-luvun alkuvuosina valmistuneessa toiminnallisen turvallisuuden yleisessä perusstandardissa IEC 61508 osat 1…7 esitetään vaatimuksia ja ohjeita sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallisen turvallisuuden suunnitteluun, toteutukseen, käyttöönottoon sekä käyttöön ja kunnossapitoon. Standardissa esitettävä järjestelmällinen ja elinkaaritarkasteluun perustuva lähestymistapa soveltuu kaikkien eri alojen turvallisuuteen liittyvien järjestelmien tarkasteluun.

5.2 Toiminnallisen turvallisuuden sovellusstandardit

Kaikki nykyiset koneiden turvallisuutta koskevat ohjausjärjestelmästandardit perustuvat toiminnallisen turvallisuuden käsitteeseen. Eri aloille on valmisteltu ja edelleenkin valmistellaan standardiin IEC 61508 perustuvia sovellusstandardeja. Valmiina on sovellusstandardeja muun muassa prosessiturvallisuuden (IEC 61511), koneiden ja konejärjestelmien (ISO 13849 ja IEC 62061) toiminnallisen turvallisuuden standardien lisäksi mm. rautateiden kulunohjauksen, lääketeollisuuden laitteiden ja monien muiden toimialojen automaatio- ja ohjausjärjestelmien turvallisuuden suunnitteluun. Uusimpiin sovellustandardeihin kuuluu autoalan toiminnallisen turvallisuuden suunnittelustandardi ISO 26262.

Toiminnallisen turvallisuuden vaatimuksia on lisätty myös useiden eri koneryhmien tai laitteiden omiin teknisiin standardeihin, esimerkiksi liikkuvien työkoneiden suunnittelustandardit ja ATEX-turvalaitteet. Siten elektronisten ohjausjärjestelmien käyttöönoton myötä myös toiminnallisen turvallisuuden käsite ja siihen liittyvät menettelytavat ovat tulleet laajalti käyttöön eri toimialueille.

Konejärjestelmien toiminnallisen turvallisuuden varmistamisen menetelmiä esitetään ohjausjärjestelmästandardeissa ISO 13849-1 ja -2 sekä IEC 62061 ja ne antavat hyvät lähtökohdat ohjausjärjestelmien suunnitteluun ja koneen turvallisuuden varmistamiseen sekä riittävät perusteet koneen vaatimustenmukaisuuden osoittamiseen.

Näissä kaikissa standardeissa vaadittava toiminnallisen turvallisuuden vaatimustaso riippuu sen riskin suuruudesta, jota on tarkoitus pienentää turvallisuuteen liittyvän ohjaustoiminnon avulla. Vaatimustason mittaamiseksi on luokiteltu neljä toiminnallisen turvallisuuden tasoa (Safety Integrity Level, SIL). Erityisesti konejärjestelmiä varten on räätälöity viisi suoritustasoa a…e (Performance Level, PL). Koneiden ohjausjärjestelmissä käytetään myös SIL-tasoja ja useimmiten koneiden elektronisten turvakomponenttien yhteydessä. PL- ja SIL-tasoja käytetään myös yhdessä.

5.2.1 Standardi IEC 62061

Koneiden ohjausjärjestelmien turvallisuusstandardi IEC 62061 on kattostandardin IEC 61508 pohjalta tehty sovellusstandardi konesektorille. Standardiin IEC 62061 on otettu koneita koskevia vaatimuksia standardista IEC 61508 jonkin verran muokattuna. Standardissa IEC 62061 esitetään lähestymistavat, vaatimukset ja menetelmät turvatoiminnoilta vaadittavan toiminnan ja luotettavuuden suunnitteluun. Standardissa esitetään arviointimenetelmiä sähköisten ja elektronisten ohjausjärjestelmien laitteiston satunnaisten ja systemaattisten vikaantumisten sekä yhteisvikaantumisten arviointiin sekä turvallisuuteen liittyvien ohjelmistojen kehittämiseen.

Standardissa luokitellaan vaatimukset turvatoiminnoille kyseisen turvatoiminnan aikaansaaman riskin pienentämisen mukaan, jota arvioidaan turvallisuuden eheyden tasoilla (*Safety Integrity Level*, SIL). Konesovelluksissa käytetään kolmea tasoa (SIL 1 on matalin ja SIL 3 korkein taso). Näitä tasoja vastaavat turvatoiminnon epäonnistumisen suurimmat sallitut taajuudet (todennäköisyydet) esitetään osan 5 kohdan 4.7 taulukossa 5. Standardissa IEC 62061 määriteltyä SIL 4 -tasoa ei käytetä koneiden yhteydessä, sillä se on asiaan kuuluva lähinnä suuronnettomuusvaarojen arvioinnissa.

Standardi soveltuu hyvin turvallisuuteen koneiden turvallisuuteen liittyvien sähköisten ja elektronisten ohjausjärjestelmien ja niiden komponenttien sekä ohjelmistojen suunnittelijoille ja toteuttajille. Laitteiston vikatarkastelut perustuvat vika-analyyseihin (esim. vika- ja vaikutusanalyysi tai vikapuuanalyysi) ja luotettavuuslaskenta perustuu standardissa IEC 61508 esitettäviin luotettavuustekniikan kaavoihin. Standardin käyttö edellyttää kokemusta ohjausjärjestelmien suunnittelusta ja todennäköisyyslaskennasta.

5.2.2 ISO 13849 osat 1 ja 2

Todennäköisyyslaskentaan perustuvat menetelmät voivat järjestelmän arkkitehtuurista riippuen olla varsin työläitä. Standardin IEC 62061 käyttö voi olla pienille ja keskisuurille koneenrakentajille liian suuritöistä ratkaistavan ongelman merkitykseen nähden. Standardissa ISO 13849-1 esitetään yksinkertaistettu menetelmä koneiden tavanomaisten ohjausjärjestelmien suunnitteluun ja arviointiin. Se perustuu valmiiksi laskettuihin, yleisesti konesovelluksissa käytettäviin turvatoimintoa toteuttaviin arkkitehtuurimalleihin.

Molemmissa standardeissa IEC 62061 ja ISO 13849-1 vaatimukset turvatoiminnolle luokitellaan sen aikaansaaman riskin pienentämisen mukaan. Standardissa ISO 13849-1 käsitellään vain turvallisuuteen liittyvien toimintojen tiheiden ja jatkuvien vaateiden toimintatapaa (ISO 13849-1 kohta 3.1.38), kun standardissa IEC 62061 käsitellään myös turvatoimintojen harvojen vaateiden toimintatapaa.

Turvatoiminnon suorituskykyä (*Performance Level, PL*) arvioidaan viidellä suoritustasolla a, b, c, d ja e (PL a on matalin ja PL e on korkein). Standardissa IEC 62061 koneiden turvatoiminnon suorituskykyä arvioidaan kolmella turvallisuuden eheyden tasolla 1, 2 ja 3 (kodat 8.1 ja 9.8).

ISO 13849 -standardisarjaan kuuluu myös ohjausjärjestelmien suunnittelun kelpuutusta käsittelevä standardi ISO 13849-2:2013. Siinä on laaja liiteosa, jossa esitetään turvallisuuden perusperiaatteet ja erilaisiin teknologioihin kuuluvien komponenttien tietoja (muun muassa

komponenttien vikamuotoja). Standardissa on myös esimerkki turvatoimintojen kelpuutuksesta sähköhydraulisen koneen turvatoimintojen analyysin avulla.

Standardi ISO 13849-1 on tarkoitettu koneiden suunnittelijoille ja niille, jotka yhdistävät ohjausjärjestelmiä koneeseen sekä muille, jotka ovat mukana turvallisuuteen liittyvän ohjausjärjestelmän suunnittelussa, toteutuksessa ja ylläpidossa. Standardi sopii varsinkin tilanteisiin, joissa koneenrakentaja toteuttaa turvatoimintoja valmiista laite- ja ohjelmistokomponenteista, joiden luotettavuuden niiden alkuperäinen valmistaja on varmistanut ja mahdollisesti myös osoittanut sertifioinnilla. Standardin käyttö edellyttää luotettavuustekniikan perusteiden ymmärtämistä, mutta se ei edellytä todennäköisyyslaskennan matemaattisten menetelmien erityisosaamista, kuten standardin IEC 62061 edellytetään sen käytössä monimutkaisempien arkkitehtuurien suunnitteluun.

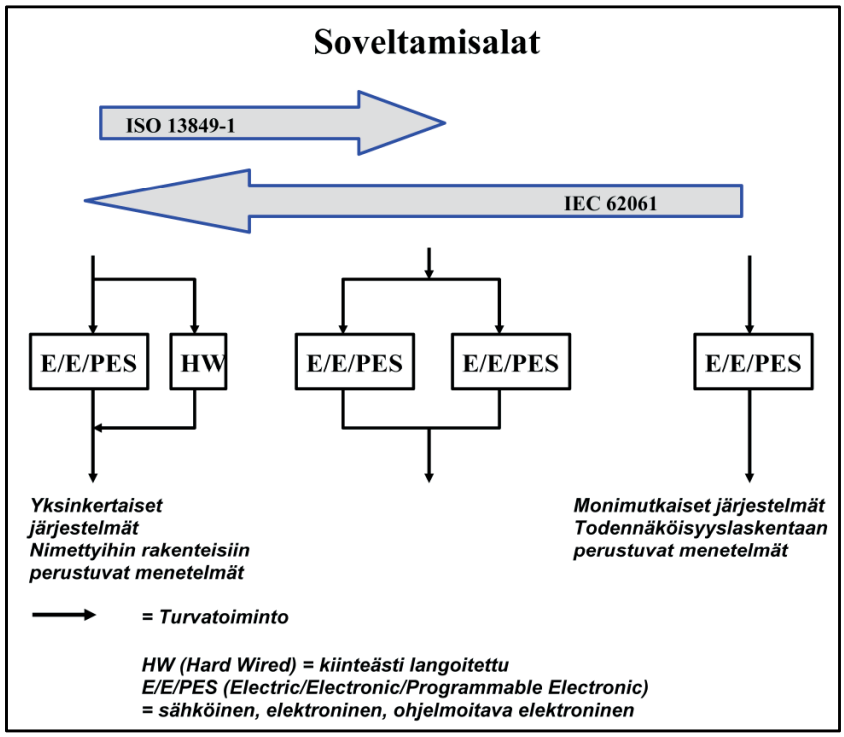
Standardi ISO 13849-1 on julkaistu 31.12.2015 ja seuraava painos on työn alla.

5.2.3 Valinta standardien ISO 13849-1 ja IEC 62061 välillä

Molempia standardeja ISO 13849 ja IEC 62061 voidaan käyttää koneiden ohjausjärjestelmien suunnittelussa. Niiden soveltamisalat ovat kuitenkin erilaiset (kuva 2):

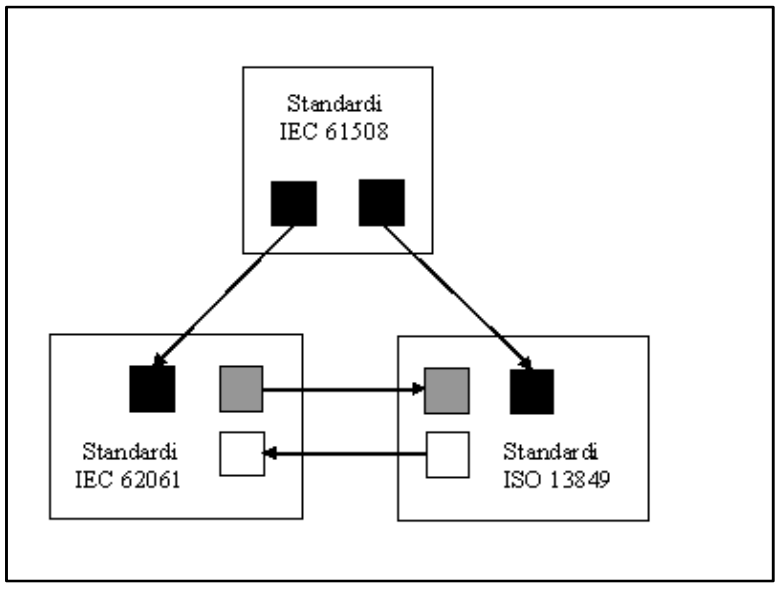
IEC 62061: Jos turvatoimintoja toteutetaan monimutkaisella arkkitehtuurilla tai laajalla ohjelmistolla, sovelletaan mieluummin standardia IEC 62061 kuin standardia 13849. Hyvin vaativiin turvallisuuskriittisiin konejärjestelmiin, joissa on sulautettuja ohjelmistoja, sovelletaan joko standardia IEC 62061 tai toiminnallisen turvallisuuden perusstandardia IEC 61508.

ISO 13849: Standardin ISO 13849-1 soveltamisalaan kuuluvat kaikki erilaiset teknologiat. Siten standardia voidaan soveltaa paitsi elektronisiin, sähköisiin tai sähkömekaanisiin ohjausjärjestelmiin ja myös ohjausjärjestelmän osina oleviin hydraulisiin, pneumaattisiin tai mekaanisiin järjestelmiin (esim. turvallisuuteen liittyvät mekaaniset ja hydrauliset laitteet). Standardissa ISO 13849-1 esitetään yksinkertaistettu menetelmä, jossa tyypillisille turvatoimintoja toteuttaville arkkitehtuureille esitetään valmiiksi lasketut mallit ja siten suunnittelijan ei niitä tarvitse itse laskea.



Kuva 2 Koneiden ohjausjärjestelmästandardien soveltamisalat

Esimerkiksi logiikkayksikön tai valosähköisen turvalaitteen valmistaja voi käyttää turvatoiminnon suunnittelussa standardia IEC 62061, ja käyttää valmiina alajärjestelmänä (tai komponenttina) kumman tahansa standardin IEC 62061 ja ISO 13849-1 mukaan suunniteltua alajärjestelmää (Kuva 3).



Kuva 3 Valmiiden alajärjestelmien yhteensopivuus

Monet koneiden elektronisten osien ja laitteiden valmistajat sertifioivat tuotteet standardien ISO 61508, ISO 13849 ja/tai IEC 62061 mukaan, jolloin ilmoitetaan sekä saavutettava suoritustaso PL että turvallisuuden eheyden taso SIL, mikä helpottaa tuotteiden yhteensopivuutta.

Suunnittelua helpottaa, jos käytetään määrätyille suoritustasoille hyväksyttyjä valmiita turvatoimintoratkaisuja tai niiden alajärjestelmiä tai jos yksittäisen turvatoiminnon toteuttamiseen voidaan käyttää luontaisesti turvallisia, esimerkiksi vikaturvallisia (*fail-safe*) ratkaisuja.

Kun toinen edellä mainituista ohjausjärjestelmien turvallisuusstandardeista on valittu, järjestelmän suunnittelu ja toteutus on tehtävä kaikilta osiltaan kyseisen valitun standardin mukaan (ei siis saa poimia eri standardeista sekaisin erilaisia vaatimuksia). Kuitenkin näiden kolmen standardin mukaan suunniteltua alajärjestelmää voidaan sellaisenaan käyttää alajärjestelminä (rakenneosina) kuvan 3 vaihtoehtojen mukaan.

6 Koneen turvallisuuteen liittyvät toiminnot

6.1 Toimintojen oikeellisuus

Kun koneisiin lisätään yhä enemmän erilaisia toimintoja, niiden riippuvuudet koneen hetkellisestä tilasta ja toimintojen välisistä loogisista yhteyksistä edellyttävät aikaisempaa enemmän koneen toimintojen oikeellisuuden varmistamista. Myöskään koneeseen lisätyt turvatoiminnot eivät toimi tarkoitetulla tavalla, jos koneen muiden ohjaustoimintojen vuorovaikutuksia ei ole varmistettu. Esimerkiksi autojen toiminnallisen turvallisuuden standardissa (ISO 26262) kuvataan menetelmiä paitsi riskin arviointiin myös toimintojen vuorovaikutuksen hallintaan (esimerkkinä mm. polttomoottorin ja ABS-jarrujen elektronisten ohjauksien ja säätöjen suunnittelu). Nämä menettelytavat voisivat olla hyödyllisiä myös muille sellaisille uuden tekniikan sovellusaloille, joissa toiminnallisen turvallisuuden varmistaminen on keskisenä osana suunnittelua.

Suuremmissa ja monimutkaisemmissa järjestelmissä koneen turvallisuuteen liittyviä toimintoja voi olla useiden kymmenien tai satojen logiikoiden varassa, jolloin on syytä käyttää mallipohjaista suunnittelua. Tätä tarvitaan muun muassa turvallisuuskriittisten ohjelmistojen kehittämiseen ja siihen liittyvään testaustoimintaan sekä koneen toimintojen ja tilasiirtymien oikeellisuuden varmistamiseksi (”digitaaliset kaksoset”). Myös tietoturva on viimeisten 10 vuoden aikana tullut olennaiseksi osaksi koneen turvallisuuden suunnittelua.

Huom. Tämä kirjoitussarja on rajattu koskemaan tyypillisten tavanomaisten valmistustekniikassa käytettävien koneiden ohjausjärjestelmien suunnittelua.

Automaattisen koneen kokonaisturvallisuus edellyttää koko suunnitteluprosessin hallintaa. Konejärjestelmän suunnittelussa on turvallisuus otettava mukaan yhtenä laatutekijänä muiden laatutekijöiden mukaan (käytettävyys, kunnossapidettävyys, ympäristöturvallisuus jne.).

Teknisten järjestelmien toiminnallisen turvallisuuden varmistamisessa on tavoitteena, että vaaranalaiset prosessit toimivat tarkoitetulla tavalla niin tavanomaisessa käytössä kuin myös poikkeustilanteissa. Toiminnallisen turvallisuuden lähestymistapa (Functional Safety) on osoittautunut parhaaksi menetelmäksi, kun varmistetaan monimutkaisten teknisten järjestelmien turvallisuutta.

Kun koneessa on merkittäviä vaaroja, koneen toimintojen turvallisuuden suunnitteluun tarvitaan konedirektiivin ja siihen liittyvien ISO- ja IEC-standardien suunnittelumenetelmiä, ja varsinkin silloin kun koneessa on

– monia toimintatapoja ja tiloja sekä niiden välisiä riippuvuuksia

- liityntöjä tehtaan muihin verkkoihin ja ulkomaailmaan
- monimutkainen arkkitehtuuri.

Tällöin koneen ohjausjärjestelmästä tulee monimutkainen ja siinä on laajoja ohjelmistoja.

Huom. Ohjelmoitavan elektroniikan monimutkaisuus johtaa helposti suunnitteluvirheisiin ja siksi tarvitaan turvallisuuden hallintajärjestelmiä ja systemaattisia suunnittelumenetelmiä.

Yksikertaisemmat koneet, joissa on vain pieniä riskejä, voivat käyttää yksinkertaisimpia valmiita dokumentoituja ratkaisuja, joita voidaan käyttää myös edellä mainittujen vaativampien järjestelmien osina.

Suunnittelun apuna on syytä käyttää aikaisemmin hyviksi osoittautuneita ratkaisuja. Tällöin voi suunnitteluun riittää aikaisempien dokumenttien ja saatujen kenttäkokemusten perusteella tehtävät muutos- ja päivitystehtävät. Tämä edellyttää, että aikaisemmat konetyyppi-ohjausjärjestelmä- ja ohjelmistoversiot on dokumentoitu riittävällä tarkkuudella ja tallennettu asianmukaiseen dokumentaation hallintajärjestelmään (*Product Data Management*, PDM). Tähän kuuluu muutostenhallinnan ja versionhallinnan menettelytavat.

6.2 Turvatoiminnot ja muut turvallisuuteen liittyvät toiminnot

Tavoitteena on saada useammalla erilaisella tekniikalla toteutettu turvallisuuteen liittyvien toimenpiteiden yhdistelmällä siedettävä jäännösriski (osa 3 luku 4.2 ja 9.4). Koneen peruskonseptissa on suunniteltu koneen erilaisia käyttötoimintoja ja tavallisesti jo siinä vaiheessa on huomattu, että monet niistä ovat turvallisuuteen liittyviä (osa 3 kohta 3.2). Siten jo tässä vaiheessa voidaan aloittaa myös koneen turvallisuuteen liittyvien ja myös koneeseen turvallisuuden parantamiseksi lisättävien ohjausjärjestelmän toteutettavaksi tarkoitettujen turvatoimintojen suunnittelu.

Pahimmat konetapaturmat johtuvat mekaanisesti liikkuvista osista (mekaaninen työ, osa 2 kohta 5.1). Pääasiassa mekaaniset turvallisuustekniset toimenpiteet eivät tavallisesti ole riittäviä ja syntyy tarve lisätä eri teknologioilla toteutettuja turvatoimintoja sekä etenkin ohjausjärjestelmän toteuttamia sähköisiä ja elektronisia turvatoimintoja.

Ohjaustoimintojen turvallisuuden suunnittelua jatketaan koneen peruskonseptin osalta yksilöimällä kunkin ohjausjärjestelmän toteuttaman turvallisuuteen liittyvän ohjaustoiminnon vaatimukset yksityiskohtaisesti. Eri tekniikoiden (sähkötekniikka, mekaniikka, hydrauliikka, pneumatiikka, jne.) toteuttamat toiminnot sovitetaan yhteen ja vaatimukset ohjelmistokehitykselle yksilöidään.

Koneen ohjaustoimintojen turvallisuuden suunnittelu aloitetaan siinä vaiheessa, kun

1. Koneen peruskonseptin suunnittelu on valmiina (osa 3 kohta 9.3) ja koneen riskin arviointi on tehty (osa 3 kohdat 4 …7)
2. Tunnistettujen ja arvioitujen riskien pienentäminen on jo suunniteltu käyttämällä ensin koneen luontaisen turvallisuuden kehittämistä (osa 3 kohta 9.1).
3. Koneen ohjausjärjestelmästä riippumattomien riskin pienentämistoimenpiteiden vaikutukset turvallisuuteen on jo suunniteltu (osa 3 kohta 9.2).
4. Koneen käyttöön liittyvien ohjaustoimintojen suunnittelu on riittävän pitkällä (luku 6)

Koska turvallisuuteen liittyvillä ohjaustoiminnoilla on suuremmat vaatimukset kuin turvallisuuteen täysin liittymättömillä toiminnoilla, on tarkoin eroteltava

- ohjausjärjestelmän toiminnasta riippumattomia, esim. yksinkertaisia) ohjaus- ja käyttötoimintoja
- ohjausjärjestelmän toteuttamat turvallisuuteen liittyvät toiminnot, jotka voivat olla
  - koneen peruskonseptissa olevia ohjausjärjestelmän toteuttamia, esimeriksi yhdistettyjä käyttö- ja turvatoimintoja tai
  - vasta koneen riskin arvioinnin tulosten perusteella koneeseen erikseen turvallisuuden parantamiseksi lisättäviä (varsinaisia) turvatoimintoja (osa 3 kohta 9.3).

Tällä luokittelulla on merkitystä koneen ohjaustoimintojen arviointiin ja siten turvallisuusvaatimuksiin ja toimintojen toteuttamiseen seuraavien selostusten mukaan.

Turvatoiminnot ovat tyypillisesti ohjausjärjestelmän toteuttamia turvallisuuteen liittyviä toimintoja, esimerkiksi turvasignaali syntyy tuloyksikössä, siirtyy logiikan muokkaamana lähtöyksikköön, joka ohjaa toimilaitteita. Turvatoimintoja voi olla koneen peruskonseptissa valmiiksi yhdistyneenä käyttötoimintoihin tai niitä on lisätty erikseen koneen riskin arvioinnin tulosten perusteella turvallisuuden varmistamiseksi.

Turvatoimintoja ovat esimerkiksi:

- turvalaitteen käynnistämät pysäytystoiminnot (*safe stop*)
- käsikäyttöinen kuittaustoiminto (*manual reset function*)
- käynnistys tai uudelleenkäynnistystoiminto (*start/restart function*)
- paikallisohjaustoiminto (*local control function*)
- passivointitoiminto (*muting function*)
- pakkokäyttöinen ohjaustoiminto (*hold-to-run function*)
- sallintalaitteen toteuttama toiminto (*enabling device function*)
- turvallisuuteen liittyvien tuloparametrien valvonta (*monitoring of parameterization and safety input values*)
- turva- ja käyttötoimintojen yhdistelmät (esim. kaksinkäsinkäyttölaitteet, *two-hand-control devices*)
- ym.

Näitä toimintoja arvioidaan luotettavuusteknisillä menetelmillä (standardi ISO 13849-1 ja -2, IEC 62061 ja esim. Sistema-suunnittelutyökalu liite 1).

Turvallisuuteen liittyviä toimintoja, eli muita kuin edellä mainittuja (varsinaisia) turvatoimintoja, ovat toiminnot, joiden luotettavuutta arvioidaan suoraan komponenttitietojen avulla. Näitä ovat ohjausjärjestelmästä (logiikasta) riippumattomat toiminnot, esimerkiksi yksinkertaiset tulo-lähtöyksikkö -toiminnot, vikaturvalliset toiminnot (*fail-safe function*) ja muut vikojen poissulkemisen avulla arvioitavat toiminnot.

> **Esimerkiksi** ohjausjärjestelmästä riippumattomia turvallisuutta parantavia toimintoja ovat paineastian mekaaninen varoventtiili tai rakenteeseen tarkoituksella tehty heikennys, jonka murtuminen voi tapahtua ilman vahinkoa tai tavallinen hehkulankasulake oikosulun varalta.

Huom. Seuraavia toimintoja ei tavallisesti arvioida luotettavuusarvioinnilla vaan systemaattisten virheiden ja vikaantumisten estämisen menetelmillä (luvut 6 ja 7).

Turvallisuuteen liittyviä toimintoja

- energian erottamis- ja purkamistoiminnot
- ohjaustavan valintatoiminto
- hätäpysäytystoiminto (ei ole turvatoiminto vaan täydentävä suojaustoimenpide (varotoimenpide, ISO12100 kohta 6.3.5).
- odottamattoman käynnistyksen estäminen
- turvallisuuteen liittyvien tuloparametrien valvonta
- loukkuun henkilön vapauttaminen ja pelastaminen
- vasteaika
- ym.

Jokaisen turvallisuuteen liittyvän ohjaustoiminnan oikea (tarkoitettu) toiminta yksilöidään tarkistamalla kaikki riskit, joita voi aiheutua sen väärästä toiminnasta (ei toimi, toimii väärällä hetkellä, toimii virheellisesti ym.).

Esimerkki: Vaarallinen tilanne voi syntyä työntekijän ollessa vaaravyöhykkeellä, jos esim.

- koneen pysäyttämisen jälkeen pysäytystoiminto ei vikaantumisen johdosta estä enää koneen vaarallisen liikkeen käynnistymistä
- kuittaustoiminto ei estä koneen liikkeen käynnistäminen väärällä hetkellä
- etäaseman lukitustoiminto ei estä päällekkäisiä vaarallisia ohjaustoimintoja
- koskettimien tai venttiilien virheellinen avautuminen, sulkeutuminen tai ajoitus sekoittaa koneen toimintoja vaarallisella tavalla jne.
- pakkotoimien kytkin ei toimi pakkotoimisesti tai ei palaudu alkuasentoon jne.

Useimmiten tarvitaan työntekijän pääsy koneen vaaravyöhykkeelle esim. säätö-, huolto-, ja korjaustöitä varten. Tällöin ulkoista suojausta täydennetään turvatoiminnoilla, joka on esimerkiksi ”kun sorvin suojus avataan, sorvin ja sen oheislaitteiden vaaralliset liikkeet pysähtyvät ja suojuksen ollessa auki, vaaralliset liikkeet eivät voi käynnistyä".

Tämä voidaan toteuttaa siten, että avattaessa suojus tai portti (lukinnalla tai ilman) portin toimintaankytkentä pysäyttää robotin vaaralliset liikkeet ja pitää ne paikoillaan, kunnes kaikki suojukset ja ovat uudelleen suojausasennossa ja portit suljettu. Ennen automaattiajon käynnistystä on työntekijän kuitattava, että vaaravyöhykkeellä ei ole ketään. Turvatoiminnan (esim. toimintaankytkentä) suoritustason PL on täytettävä turvatoiminnalta vaadittavan suoritustason PLr (kohta 8.1) vaatimukset.

Useiden erilaisten toimintojen vikaantumisen aiheuttamia vaaratilanteita voidaan usein estää lisäämällä koneeseen yksi kattava turvatoiminto, joka ohjaa koneen turvalliseen tilaan. Tavallisesti turvatoiminto pysäyttää kaikki koneen vaaralliset liikkeet tai muut toiminnot ja siten estää yhdellä kertaa kaikkien muiden toimintojen mahdollisten vikaantumisten aiheuttamat vaaralliset tilanteet, kuten esimerkiksi vaaravyöhykkeelle pääsyn valvonta. Myös sellaisia ohjaustoiminnon tai -toimintojen vikaantumisia, jotka voivat johtaa vaaratilanteeseen muiden toimintojen ja/tai koneen hetkellisen tilan yhteisvaikutuksista, on joko estettävä riittävästi tai lisättävä kattavia turvatoimintoja.

Jos turvatoiminto on luokkaa PL d ja se estää robotin kaikki vaaralliset liikkeet havaitessaan henkilön tulevan vaaravyöhykkeelle tai ollessa siellä, jolloin muut ohjaustoiminnot voivat olla alemmalla

suoritustasolla. Kuitenkin näiden toimintojen vikaantumiset lisäävät turvatoiminnon vaadetta ja voi vastaavasti olla tarpeen nostaa turvatoiminnon suoritustaso korkeammalle.

7 Ohjaustoimintojen systemaattisten vikaantumisten ja virheiden hallinta

Huom. Systemaattisen vikaantumisten ja virheiden arviointi on tehtävä sekä ohjausjärjestelmän toteuttamille (varsinaisille) turvatoiminnoille että myös muille turvallisuuteen liittyville ohjaustoiminnoille.

Systemaattisella vikaantumisella tarkoitetaan sellaisia vikaantumisia, jotka johtuvat järjestelmän suunnittelu- tai toteutusvirheistä. Systemaattiset virheet eroavat satunnaisista laitevikaantumisista mm. siinä, että ne ovat ajasta riippumattomia. Virhe voi olla järjestelmässä alusta alkaen tai vikaantuminen voi ilmaantua myöhemmin vasta poikkeustilanteessa, esim. kun järjestelmä vikaantuu. Ohjelmistovirheet ovat pääsääntöisesti suunnitteluvirheitä.

Systemaattiset virheet voivat aiheuttaa riskejä ja myös estää turvatoimintojen toimintaa vikatilanteessa esimerkiksi yhteisvikaantumisen seurauksena. Koska systemaattiset vikaantumiset ovat suunnittelu- ja toteutusvirheitä ja tavallisesti pysyviä, niiden merkitystä ei voi arvioida tilastollisilla menetelmillä. Systemaattisia vikaantumisia ja virheitä voidaan vähentää yrityksen laadun- ja turvallisuuden hallintajärjestelmillä, järjestelmällisellä suunnittelumenetelmällä (luku 4.2 ja osa 1 luku 3) ja hyvällä insinöörikäytännöllä (kohta 7.2).

7.1 Systemaattisten virheiden tunnistaminen

Seuraavissa analyysimenetelmissä voidaan paitsi arvioida vaarallisia tapauksia ja vikaantumisia myös analysoida niiden syitä. Jos käytettävissä on vikaantumistietoja, voidaan vikamuotojen esiintymistodennäköisyyksien avulla laskea ei-toivottujen tapahtumien todennäköisyyksiä.

- tapahtumapuu/vikapuu (*Fault Tree Analysis*, FTA): pahimman tapahtuman ”*worst case*”.
  - menetelmässä kartoitetaan kaikki ei-toivotut tapahtumat
  - selvitetään osien ja komponenttien vikaantumisketjut, jotka voivat johtaa ei-toivottuun tapahtumaan (”ja”, ”tai”, ”ei” portit).
- tarvittavia tarkistus-, testaus- ja läpikäyntitoimenpiteitä esitetään standardissa ISO 13849-2, näitä voivat olla:
  - on-line testaukset
  - simulointi
  - toiminnalliset testaukset jne.
  - materiaalivalintojen ja ylimitoituksen tarkistukset
  - erillisyyden (*divergence*) tarkistus
  - jne.
- HAZOP (*Hazard and Operability Study*) poikkeamatarkastelu, jota käytetään lähinnä prosessiteollisuudessa pääasiassa prosessiteollisuudessa (standardi IEC 61511-3).

Standardin ISO 13849-1 liitteessä G kuvataan systemaattisia virheitä. Standardissa 13849-2 on tarkempia tietoja komponenteista ja turvallisuuteen liittyvän järjestelmän kelpuutuksen yhteydessä tarkistettavista asioista. Virheen lähteenä voi olla:

- puutteellinen riskin arviointi
- puutteellinen vaatimusmäärittely
- komponenttien virheellinen valinta
- virheellinen rakenne
- ohjelmistovirheet.

Systemaattisilla virheillä tarkoitetaan järjestelmän vikoja, jotka tulevat suunnittelun ja toteutuksen mukana tehdyistä virheistä tai muista puutteellisuuksista. Tyypillisiä suunnitteluvirheitä ovat mm.:

- turvallisuusvaatimusten täyttämättä jättäminen
- järjestelmän toimintalogiikan virheet (esim. luotettavuuslaskennan virheet)
- ohjelmointivirheet
- puutteellinen ohjelmistotestaus
- riskin arvioinnin parametriarvojen virheellinen valinta (esim. vaarallisen tapahtuman todennäköisyys)
- virheellisten tai perustelemattomien komponenttien arvojen käyttö
- poikkeaminen turvajärjestelmän hierarkiasta (esim. alajärjestelmärakenne, sarjamuotoisuus)
- ympäristövaikutusten aliarviointi (esim. lämpötila, EMC, epäpuhtaudet)
- tietoturvan laiminlyönnit
- jne.

Suunnitteluvirheiden lisäksi voi hyvinkin suunniteltu toiminto vikaantua tai muutoinkin lakata toimimasta toteutuksessa tulleiden virheiden johdosta, esimerkiksi:

- väärät komponenttivalinnat (esim. komponenttien yhteensopimattomuus)
- komponenttien langoitusvirheet (esim. kahdennuksen menettäminen virheellisellä kytkennällä)
- johdotusten kytkentävirheet (esim. väärät kiinnittimet, virheellinen maadoitus, pakkotoimisuuden kadottaminen)
- jne.

7.2 Varmistuksia ja menetelmiä

Systemaattisten vikaantumisten välttämisestä standardissa ISO 13849-1 esitetään huomioon otettavia näkökohtia, mm.:

- turvallisuuteen liittyvä ohjelmisto: ISO 13849-1 kohta 4.6 ja liite J
- systemaattiset vikaantumiset: ISO 13849-1 liite G
- ympäristöolosuhteet: ISO 13849-1 liite G
- turvatoiminnan käyttäytyminen vikatilanteissa: ISO 13849-1 kohta 6
- käyttöön liittyvät näkökohdat (ihminen-kone -rajapinta).

Standardissa IEC 60204 esitetään koneiden sähkölaitteita koskevia vaatimuksia, jotka liittyvät koneiden turvallisuuteen ja monilta osin myös koneen toiminnalliseen turvallisuuteen.

Sähköistykseen liittyvät virheet:

- käytetään lepovirtaperiaatetta (jännitteen hävitessä koskettimet avautuvat ja esim. moottori tai venttiili ohjautuu turvalliseen tilaan)

- menetelmät jännitteen katkeamisen, jännitteen vaihteluiden, ylijännitteen ja alijännitteen vaikutusten estämiseksi

Tietotekniikkaan liittyvät virheet:

- turvallisuuteen liittyvissä ohjausjärjestelmän ohjelmien suorituksen valvonta virheellisten ohjelmajaksojen paljastamiseksi (esim. ”vahtikoira (*watch dog*)” -diagnostiikka)
- menetelmät tietoliikenteen aiheuttamien virheiden vaikutusten tai muiden virheiden hallintaan (esim. turvaväylät)
- teollisuuden automaatio- ja ohjausjärjestelmien tietoturvan hallinta ja menetelmien käyttö esim. standardisarjan IEC 62443 mukaan
- vikaantumisten paljastaminen automaattisilla testauksilla (esim. turvatoiminnan vaade ≤ 100 x testausväli) redundanttisen laitteiston testaukset (esim. diagnostiikka ristiinvalvonnalla)

Rakenteelliset menetelmät:

- erilaiset laitteistot (erilaisuus, *divergence*)
- pakkokäyttöinen toimintatapa
- pakkotoiminen ohjaus (esim. kytkimen tai releen koskettimien avautumisen mekaaninen ohjaus)
- suora avaustoiminto vikaantumismuotoja suuntaamalla (esim. valitaan todennäköisin vikaantumismuoto turvalliseen suuntaan (turvallisen vikaantumisen periaate, *fail safe principal*)
- ylimitoitus sopivalla kertoimella, jos valmistaja voi osoittaa, että pienempi kuormitus tai komponentin ylimitoitus voi parantaa luotettavuutta, ja jos ylimitoitusta sovelletaan, olisi käytettävä varmuuskerrointa vähintään 1,5
- menetelmät fyysisen ympäristön hallintaan ja sen vaikutusten välttämiseen (esimerkiksi lämpötila, kosteus, vesi, tärinä, pöly, korroosiota aiheuttavat aineet, sähkömagneettinen yhteensopivuus).

Tärkeitä kohtia sähkölaitteiden systemaattisten vikojen estämiseksi esitetään standardissa IEC 60204-1.

Pienillä riskitasoilla voidaan käyttää erillisiä koneen ohjausjärjestelmistä riippumattomia turvatoimintoja. Komponenttien laadun on kuitenkin oltava riittävä kyseiseen käyttötarkoitukseen, elinikävaatimus on täytettävä ja systemaattisen vikaantumiset on estettävä.

Turvatoiminnoissa on käytettävä turvakomponentteja ja suositellaan valittavaksi sertifioituja turvakomponentteja. Jos näitä ei ole saatavilla, olisi valittava standardin mukaisia komponentteja. Tällöin saadaan myös tiedot komponentin ominaisuusista.

Joka tapauksessa turvallisuuteen liittyvien komponenttien oikean toiminnan ja luotettavuuden parantaminen paremmalla suunnittelulla voi olla pitkälti riittävää esim. valitsemalla hyvin testattuja komponentteja, ylimitoituksella, vikojen poissulkemisella, valitsemalla luonnostaan turvallisuutta tukevia toimintoja (fail-safe- ratkaisut), mekaanisilla lukituksilla ja muilla systemaattisen vikaantumisten hallinnan menetelmillä (luku 7). Turvallisuuteen liittyvien toimintojen suunnittelusta ja toteutuksista on tehtävä selkeät dokumentit.

Standardin ISO 13849-2 liitteissä A…E esitetään tyypillisiä komponenttien vikaantumisia. Yksittäisille sähkömekaanisille komponenteille (Sistemassa alimman tason elementtejä), esim. johdotukset, liittimet, painikkeet jne., ei määritetä $MTTF_d$- eikä DC-arvoja, vaan niiden turvallisuus varmistetaan hyvien komponenttien valinnalla, systemaattisten virheiden estämisellä ja hyvällä ”insinööritaidolla” (osa 4 luku 7 ja standardi IEC 60204-1).

Standardin 61508-2 liitteissä esitetään tarkemmin turvallisuuteen liittyvien järjestelmien ja niiden komponenttien vikaantumisia ja toimenpiteitä sekä tekniikoita: liitteessä A käytön aikaisia vikaantumisia ja niiden hallintaa ja liitteessä B systemaattisia vikaantumisia ja niiden estämistä.

8 Turvatoimintojen suunnittelu

Koneiden turvallisuuden suunnittelu perustuu koneturvallisuuden perusstandardiin ISO 12100. Siinä määritetään myös koneen ohjaustoimintojen suunnitteluperiaatteet. Turvatoimintojen suunnittelussa nojaudutaan koneen riskin arvioinnin tuloksiin (osa 3 kohta 6.3). Sen mukaan koneen valmistajan on huolehdittava siitä, että koneen riskin arvioinnin tulokset saadaan käyttöön turvatoimintojen suunnittelua varten.

Standardissa ISO 13849-1 esitetään yksinkertaistettu menetelmä ohjausjärjestelmän toteuttamien turvatoimintojen suorituskyvyn arviointiin. Osassa 5 käydään läpi em. standardin mukaisen turvatoimintojen suunnittelumenetelmän keskeisiä vaiheita.

Turvatoiminnon suunnitteluvaiheet seuraavissa luvuissa

Vaadittavan suoritustason arviointi

7	Turvatoiminnon vaadittavan suoritustason PLr määrittäminen
7.1	Vaadittavan suoritustason PLr määrittäminen riskigraafin avulla
7.2	Vaadittavan suoritustason SIL määrittäminen riskimatriisilla
7.3	Vaadittavan suoritustason PLr määrittäminen suoraan B- ja C-tyypin standardien avulla

Saavutetun suoritustason arviointi

8	Turvatoiminnon saavuttaman suoritustason PL arviointi
8.1	Alajärjestelmien saavuttamien PL-tasojen arviointimenetelmä
8.2	Turvatoiminnon saavuttaman PL-tason arviointi
8.3	Nimetyt rakenteet (arkkitehtuuri)
8.4	Lohkokaaviot (kanavat)
8.5	Komponentit
8.5.1	Satunnaisvikaantumiset
8.5.4	Diagnostiikan kattavuus
8.5.5	Yhteisvikaantuminen (yhteisestä syystä vikaantuminen)
8.6	Saavutetun suoritustason todentaminen
8.7	Turvatoiminnon hyväksyminen ja todentaminen

Huom. Kun turvatoimintoja suunnitellaan käytännössä esim. Sistema-työkalulla, suunnitteluvaiheiden järjestys voi vapaasti muuttua iteratiivisessa suunnitteluprosessissa.

8.1 Turvatoiminnon vaadittavan suoritustason PLr määrittäminen

Tässä luvussa esitetään kaksi menetelmää turvatoiminnon vaadittavan suoritustason PLr määrittämiseen.

Turvatoimintoja toteuttavien järjestelmien vikaantumisella on keskeinen merkitys turvatoiminnan luotettavuudelle. Seuraavassa standardin ISO 13849-1 mukaisessa menetelmässä arvioidaan turvallisuuteen liittyvän toiminnon suorituskyvyllä PL (*Performance Level*). Turvatoiminnon saavuttama suoritustaso PL (a…e) kuvaa turvatoiminnon menettämisen enimmäistaajuutta.

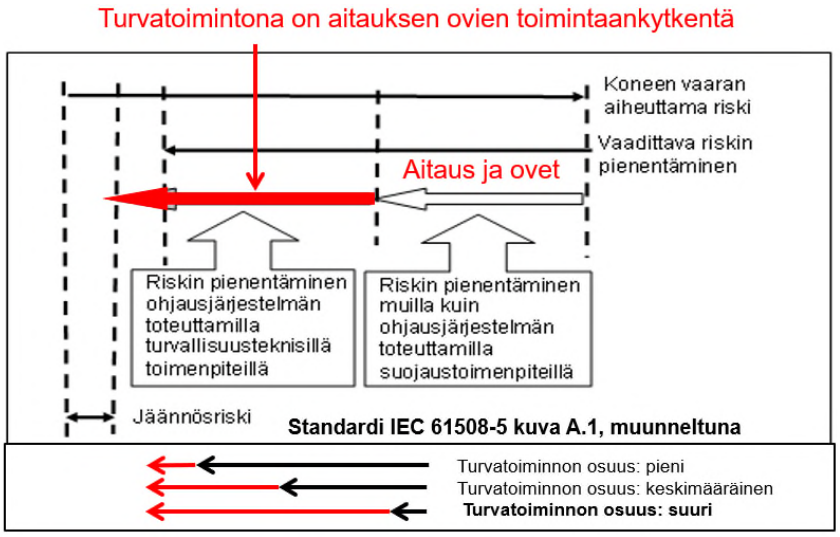
”Suoritustaso PL a…e (*Performance Level*) on erillinen taso, jota käytetään määrittelemään turvallisuuteen liittyvien ohjausjärjestelmän osien kyky suorittaa turvatoiminta ennakoitavissa olevissa olosuhteissa (ISO 13849 kohta 3.1.23)”.

Koneen ohjausjärjestelmän toteuttaman jokaisen turvallisuuteen liittyvän toiminnon oikea toiminta on varmistettava ja toiminnon luotettavuuden on oltava riittävä. Tällaisen turvatoiminnon aikaan saamiseksi turvallisuuteen liittyvän ohjaustoiminnon on saavutettava riittävä suorituskyky PL suhteessa sen riskin suuruuteen, joka seuraisi turvatoiminnon vikaantuessa (epäonnistuessa). Siten koneen turvallisuuteen liittyviltä toiminnoilta vaadittavan suoritustasojen PLr vaatimus on suhteessa sen riskin suuruuteen, jota on tarkoitus pienentää riittävästi.

Vaadittavan suoritustason PLr määrittämisen aluksi kaikki koneen ohjausjärjestelmän toteuttamat koneen turvallisuuteen liittyvät ohjaustoiminnot (luku 6) yksilöidään, määritetään ja dokumentoidaan riittävällä tarkkuudella. Jos peruskonseptin suunnittelun yhteydessä ei ole vielä tarkistettu kaikkien toimintojen ja koneen tilojen logiikka (ml. keskinäiset riippuvuudet), on tässä vaiheessa tehtävä nämä tarkistukset ja korjattava turvallisuuteen vaikuttavat ristiriidat ja muutoinkin poistettava tarpeettomat epäloogisuudet. Samoin voidaan alustavasti laatia ohjeet toimintojen toiminnallisiin testauksiin ja kunnossapitoon.

Ennen vaadittavan suoritustason määrittämisen menetelmien käyttöä selvitetään, onko ohjausjärjestelmästä riippumattomat eli muut kuin sähköisen/ohjelmoitavan ohjausjärjestelmän toteuttamat turvallisuustekniset toimenpiteet suunniteltu, esimerkiksi mekaaniset aitaukset ja suojukset, liikealueen mekaaniset rajoittimet ym. (osa 3 kohta 9.2). Nämä riskin pienentämisen toimenpiteet voidaan parhaassa tapauksessa ottaa huomioon, kuten esitetään kuvan 4 riskiä kuvaavan nuolen alkupään valkeana osuutena.

Seuraavaksi valitaan kaikki ohjausjärjestelmän toteuttamaksi suunnitellut turvallisuuteen liittyvät toiminnot, joille on tehtävä PLr-tason määritys. Muiden turvallisuuteen liittyvien ohjausjärjestelmästä riippumattomien toimintojen, joille ei tarvitse arvioida suoritustason vaatimuksia, varmistaminen tehdään systemaattisten virheiden vähentämisen tai pienentämisen menetelmillä (kohta 6.2).



Kuva 4 Ohjausjärjestelmän osuus koneen riskin pienentämisessä

Kuvassa 4 riskin pienentämistä kuvaavan nuolen punainen osuus kuvaa turvatoiminnolta vaadittavaa suoritustasoa PLr. Mitä pidempi on punaisella merkitty osuus, sitä korkeammalla on vaadittava suoritustaso Pr. Tätä havainnollistaa kuva 4: jos turvatoiminnon osuus (punainen nuoli) on hyvin pieni, esim. alle 10 % koko nuolen pituudesta, voidaan vaadittavaa PLr-tasoa alentaa enintään yhdellä kertaluokalla, esim. tasosta PLr e tasoon PLr d tai tasosta PLr d arvoon PLr c. jne. Jos vaatimustasoa PLr pienennetään tällä perusteella, tämä on tarkasti perusteltava ja dokumentoitava.

Kun lisäksi huolehditaan systemaattisten vikaantumisten estämisestä (luku 7), tämä tukee myös osaltaan vaadittavan PLr-tason saavuttamista. Siten se voi myös kompensoida mm. mahdollisia epävarmuuksia PLr-tason määrittämisessä esimerkiksi riskigraafin ja sen parametrivalintojen valinnassa (osa 3 luku 6.2).

Kaikkia muitakin ohjausjärjestelmän toteuttamia ohjaustoimintoja, mukaan lukien myös jo koneen peruskonseptissa suunnitellut turvallisuuteen liittyvät ohjaustoiminnot, käsitellään samalla tavalla kuin erikseen turvatarkoituksia varten lisättyjä turvatoimintoja ”ikään kuin niitä ei vielä olisi” (osa 3 kohta 3.2). Ohjausjärjestelmästä riippumattomia ohjaustoimintoja käsitellään kohdassa 6.2 ja luvussa 7.

8.2 Vaadittavan suoritustason PLr määrittäminen riskigraafin avulla

Tavallisesti turvallisuuteen liittyvältä toiminnolta vaadittava suoritustaso PLr määritetään riskin arvioinnin tulosten perusteella. Standardin mukaisen menetelmän etuna on sen helppokäyttöisyys. Haittana on riskiparametrien asteikon karkeajakoisuus, esimerkiksi vahingon toteutumisen seurauksissa on valittavana vain kaksi vaihtoehtoa ja niiden välille osuu suuri osa vahingoista.

Vaadittavan suoritustason PLr määritelmä (standardin kohta 4.3) eroaa saavutetun suoritustason määritelmästä: ”*Vaadittava suoritustaso (Required Performace Level) PLr on sovellettava suoritustaso, jolla on tarkoitus saavuttaa vaadittu riskin pienentäminen kullekin turvatoiminnolle (standardin ISO 13849-1 kohta 3.1.24).*”

Sen sijaan ”*Suoritustaso PL a…e (Performance Level) on erillinen taso, jota käytetään määrittelemään turvallisuuteen liittyvien ohjausjärjestelmän osien kyky suorittaa turvatoiminta ennakoitavissa olevissa olosuhteissa (ISO 13849-1 kohta 3.1.23)*” (osa 5 luku 4).

Standardin ISO 13849-1 liitteessä A kuvassa A.1 (tämän standardin kuva 5) riskigraafi ohjausjärjestelmän toteuttamien turvatoimintojen vaadittavien suoritustasojen PLr a…e määrittämiseen. Se perustuu määrätyn vaaran aiheuttaman riskin suuruuden arviointiin sen jälkeen, kun koneen riskin pienentäminen on tehty ohjausjärjestelmästä riippumattomilla toimenpiteillä (esim. aitaukset, suojukset, mekaaniset rajoittimet ym. (osa 3 kohta 9.2).

Standardin riskigraafi on hyvin yksinkertainen ja siksi korkean riskitason sovelluksissa on suositeltavaa käyttää tarkempia menetelmiä, esim. jos riskinä on useamman hengen menetys tai suuronnettomuusvaara (osa 3 kohta 7).

Standardin 13849-1 liitteen A riskin arviointimenetelmä perustuu määrätyn riskin kolmeen riskitekijään (S, F ja P, kuva 5):

1. Vahingon toteutumisen seurausten vakavuus (S1, S2) luokitellaan ”Seurausten vakavuuden” mukaan.
2. Vahingon todennäköisyys luokitellaan kahden muuttujan avulla:
   - ”Vaaralle altistumisen taajuus ja/tai kesto” (F1, F2) ja
   - ”Mahdollisuus välttää vaaraa” (P1, P2)

Tavanomaisten koneiden liikkuvien osien riskin arvioinnissa muuttujat ”Seurausten vakavuus S1/S2” ja ”Mahdollisuus välttää vaaraa P1/P2” on tavallisten koneiden osalta suhteellisen helppo määrittää, koska niissä seuraukset ovat useimmiten vakavat (konevoimalla liikkuvat osat) ja vaaraa ei voi välttää (nopeasti liikkuvat osat) eli valintana on usein S2 ja P2.

Sen sijaan riskin arvioinnin merkittävimpänä epävarmuustekijänä on useimmiten muuttuja F ”Altistumisen taajuus ja kesto F1/F2”. Muuttuja F kuvaa henkilön olemista vaaravyöhykkeellä (taajuus ja kestoaika) eli vaaratilannetta, jossa on vahingon mahdollisuus. Standardin ISO 13849-1 kohdan A.2.2 mukaan, jos kertyvä altistusaika ei ylitä 1/20 kokonaiskäyttöajasta ja taajuus ei ole suurempi kuin kerran 15 minuutissa, muuttujalle F1 voidaan valita arvo F1.

Vaaran välttämisen todennäköisyys ja vaarallisen tapahtuman todennäköisyys on yhdistetty parametriin ”mahdollisuus välttää vaaraa, P” (ISO 13849-1 kohta A.2.3). Tapaturma sattuu, jos vaarallisen tilanteen aikana vahingon ”laukaisee” vaarallinen tapahtuma esim. koneen vikaantumisen tai työntekijän virhetoiminnan johdosta, jolloin tämän tapahtuman esiintymistaajuus voidaan joskus arvioida pieneksi. Tämä on mahdollista, jos vaarallisen tapahtuman mahdollisuutta on ajan mittaan pystytty poistamaan muilla varotoimenpiteillä tai se on kokemusten mukaan saatu riittävän pieneksi. Tässä tapauksessa vaaralliseen tapahtuman tai turvatoiminnan vikaantumiseen vaikutus voidaan ottaa osittain huomioon, jos siitä saadaan riittävät tiedot tilanteen arvioimiseksi.

Standardin ISO 13849-1 mukaan, jos vaarallisen tapahtuman todennäköisyys voidaan perustellusti arvioida pieneksi (esimerkiksi alle 10 % koko taajuudesta), voidaan suoritustasoa pienentää yhdellä tasolla (yhdellä kertaluvulla). Esimerkiksi koneen käyttäjän turvallisuus on tavallisesti kokonaan (yli 90 %) valoverhon toiminnan varassa, jolloin ei edellä mainittua turvatoiminnolta

vaadittavan suoritustason alentamista voi tehdä. Myös jatkuvasti vaarakohtaan pääsyyn käytettävän portin toimintaankytkennän osuus koko riskin pienentämisestä pitkälti yli 10 % vaadittavasta turvatoiminnosta, jolloin myös toimintaankytkentälaitteen turvatoiminnan osuudeksi tulee koko riskin pienentäminen. Sama koskee valoverhoa, joka on välittömästi käyttäjän turvana,

Huom. Myös standardin IEC 62061 liitteen A riskimatriisissa on riskitekijänä lisänä edellä mainittu ”vaarallisen tapahtuman todennäköisyys” (kohta 8.3).

Standardin ISO 13849-1 liitteessä A (kuva 5) esitetään tarkempia ohjeita riskitekijöiden valintaan. Valitsemalla riskigraafista muuttujien (S, F ja P) mukaan polku standardissa esitettävien ohjeiden avulla päädytään vaadittavalle suoritustasolle (PL_r a…e).

Osan 3 kohdassa 6.1.2 kuvassa 2 esitettävässä esimerkissä robottiyksikkö oli aluksi lähes suojaamaton, vaikka työntekijä joutui menemään usein vaaravyöhykkeelle. Riskigraafilla määritettiin koneen odottamattoman vaarallisen liikkeen aiheuttaman riskin suuruus. Siksi riskigraafin tuloksena tuli vaatimus koko robottiyksikön uudelleensuunnittelusta ja toteutuksesta. Ensin koneen riskiä pienennettiin ohjausjärjestelmästä riippumattomilla turvallisuusteknisillä toimenpiteillä ja vasta sitten alettiin suunnitella turvatoimintojen vaatimuksia.

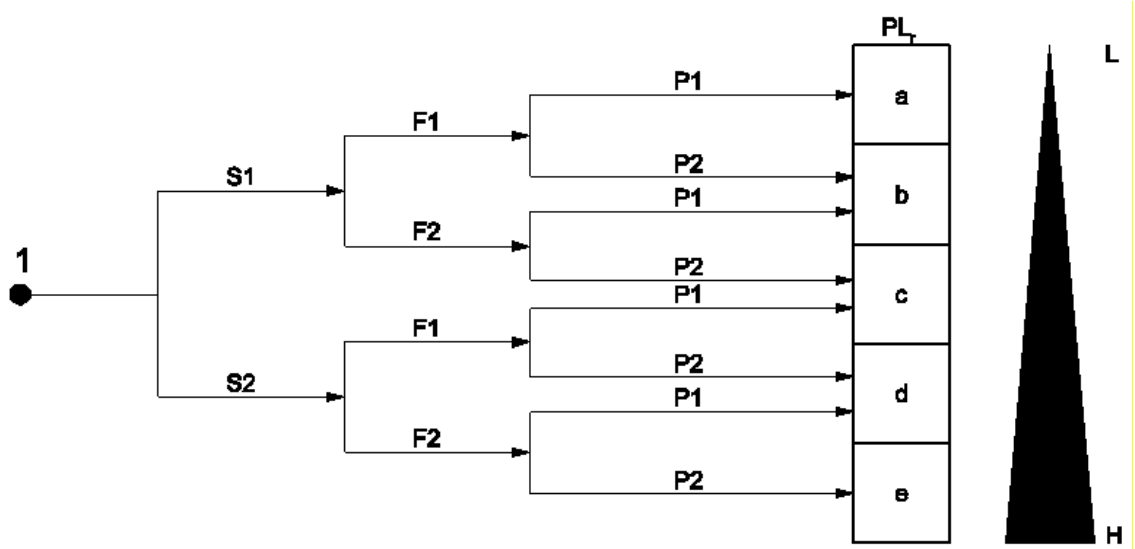
Oletetaan, että robottiyksikkö on suunniteltu uudelleen ja ohjausjärjestelmästä riippumattomat turvallisuustekniset toimenpiteet kuten asianmukaiset aitaukset, portit ja suojukset ovat valmiina, ja odottamattoman käynnistymisen toimenpiteet on toteutettu mekaanisilla, hydraulisilla, pneumaattisilla laitteilla (standardi ISO 10218-2). Vasta näiden toimenpiteiden jälkeen arvioidaan vaatimukset turvallisuuteen liittyville toiminnoille.

Edellä mainituista turvallisuusteknisistä toimenpiteistä huolimatta portista voi mennä vaaravyöhykkeelle. Tämän riskin suuruutta on tarkoitus pienentää turvatoiminnolla ja sen toteuttamiseksi on päätetty estää portin toimintaankytkentälaitteella pääsy vaaravyöhykkeelle koneen käydessä tai ollessa käyntivalmiina.

Tämän turvatoiminnon suoritustason määrittämiseksi arvioidaan jäljellä olevan riskin suuruus ennen kuin turvalaite on toiminnassa, jotta saadaan selville sen riskin suuruus, jota turvalaitteen on pienennettävä riittävästi (osa 3 kohta 4.2 ja luku 9). Pienennettävän riskin suuruus on suhteessa portin toimintaankytkennältä vaadittavaan suoritustasoon PLr (osa 5 taulukko 5) eikä alkuperäiseen osassa 3 määritettyyn koneen riskiin.

Tässä esimerkissä arvioidaan turvatoiminnolta (portin toimintaankytkennältä) vaadittava suoritustaso standardin ISO 13849-1 liitteessä A.1 olevalla riskigraafimenetelmällä (kuva 5).

Huom. Tämän riskigraafin parametrit ovat osittain erilaiset kuin osan 3 kohdassa 6 esitettävän riskin suuruuden arvioinnin riskigraafi).



Selite

1	aloituskohta turvatoiminnon osuudenarvioimiseksi riskin pienentämisessä
L	osuus riskin pienentämisessä pieni
H	osuus riskin pienentämisessä suuri
PL_r	vaadittava suoritustaso
Riskimuuttujat:	
S	vamman vakavuus
S1	lievä (tavallisesti palautuva vamma)
S2	vakava (tavallisesti palautumaton vamma tai kuolema)
F	vaaralle altistumisen taajuus ja/tai kesto
F1	harvoin...toisinaan ja/tai lyhyt altistumisaika
F2	toistuvasti...jatkuvasti ja/tai pitkä altistumisaika
P	mahdollisuus välttää vaaraa tai rajoittaa vahinkoa
P1	mahdollista tietyissä olosuhteissa
P2	tuskin mahdollista

Kuva 5 Vaadittavan suoritustason määrittäminen riskigraafin avulla (standardin ISO 13849-1 liite A kuva A.1)

Esimerkki: Robottiyksikön toimintaankytkennältä vaadittavan suoritustason PLr määrittäminen standardin ISO 13849-1 mukaisella riskigraafilla.

Valitaan riskimuuttujat liitteen A ohjeiden mukaan:

- seurausten vakavuus S: S2
- taajuus tai altistumisaika F: F1 tai F2
- mahdollisuusvaaran välttämiseen P: P2

Jos tässä esimerkissä oletetaan, että kone on modernisoitu ja sen liitännät robotin ohjausjärjestelmään tarkistettu ja testattu, jolloin voidaan valita F1 ja riskigraafissa päädytään vaadittavalle suoritustasolle PLr d.

Jos robottiyksikön ohjausjärjestelmään liittyvän käytetyn työstökoneen vikataajuus suuri, valitaan altistumisaika F2, jolloin päädytään vaadittavalle suoritustasolle PLr e. Tällöin turvallisuus voi olla näiltä osin varmistettu, mutta koneen käytettävyys voi huonontua.

8.3 Vaadittavan suoritustason SIL määrittäminen riskimatriisilla

Taulukossa 1 on vertailun vuoksi standardin IEC 62061 liitteessä A esitettävä riskimatriisi turvatoiminnolta vaadittavan SIL-tason määrittämiseen. Standardin IEC 62061 liitteessä A esitetään tarkempia ohjeita riskitekijöiden valintaan. Toisin kuin kohdassa 8.2 PL-tason määrittämisen menetelmässä, tässä SIL-tason määrittämisessä on mukana riskitekijänä ”Vaarallisen tapahtuman todennäköisyys Pr”.

Taulukko 1 Vaadittavan suoritustason määrittäminen riskimatriisin avulla (standardin IEC 62061 kuva A.3 muokattuna)

Seuraukset	Vakavuus Se	Luokka Cl 3-4	5-7	8-10	11-13	14-15
Kuolema, näön tai käden menetys	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Palutumaton, sormen menetys	3			SIL 1	SIL 2	SIL 3
Palautuva, sairaanhoiti	2				SIL 1	SIL 2
Palautuva, ensiapu	1					SIL 1

Taajuus ja kesto Fr		Vaarallisen tapahtuman todennäköisyys, Pr		Vältettävyys Av.	
<= 1 tunti	5	Erittäin todennäköinen	5		
> 1 t - <=päivä	5	Todennäköinen	4		
>1 päivä - <=2 viikkoa	4	Mahdollinen	3	Mahdoton	5
>2 vko - <=1 vuosi	3	Harvoin	2	Mahdollista	3
> 1 vuosi	2	Ei huomioitava	1	Todennäköistä	1

Standardin IEC 62061 mukaisessa menetelmässä riskitekijöiden arvot (pisteet) muodostavat logaritmimuotoiset asteikot, joissa on kaksi viiden, yksi neljän ja yksi kolmen pistearvon vaihtoehdon mahdollisuudet. Siten menetelmä on näiltä osin tarkempi kuin standardin ISO 13849-1 riskigraafi, jossa on valittavana kolmelle riskitekijälle arvo vain kahdesta vaihtoehdosta.

Haittapuolena ovat esimerkiksi vaarallisen tapahtuman viiden eri vaihtoehdon ohjeet ja tauluko 1 tekstit, jossa ainakin suomenkieliset sanamuodot ovat kovin epämääräisiä. Esimerkiksi riskimuuttujan Pr arvoa 4 pistettä vastaava termi ”todennäköinen” on merkityksetön, koska kaikki muutkin arvot ovat enemmän tai vähemmän ”todennäköisiä”, Kokemuksen mukaan useimmiten valitaan keskiarvo ”mahdollinen”. Standardin liitteessä A esitetään tarkempia ohjeita riskitekijöiden valintaan.

Robottiesimerkki: robottiyksikön toimintaankytkennältä vaadittavan suoritustason SIL määrittäminen standardin IEC 62061 mukaisella matriisimenetelmällä

Tässäkin esimerkissä tarkastellaan, kuten edellisessäkin esimerkissä, samaa vaaratilannetta (osa 3 luku 6.1). Esimerkissä arvioidaan vaatimukset portin toimintaankytkennälle standardin IEC 62061 liitteessä A olevan riskigraafimenetelmän siinä esitettävien ohjeiden mukaan:

Valitaan riskimuuttujat em. liitteessä A esitettävien ohjeiden mukaan:

- vakavuus (*Sequence*) Se: 4
- taajuus ja kesto (*Frequency*) Fr: 5
- vaarallisen tapahtuman todennäköisyys: (*propabiblity*) Pr: 4 tai 2
- vältettävyys (*Availability*) Av: 5

Kun muut pisteet paitsi vakavuus lasketaan yhteen, saadaan yhteensä 14 pistettä eli vaadittava SIL-taso on SIL 3, joka vastaa suunnilleen suoritustasoa e. Jos tässäkin tapauksessa robottiyksikkö modernisoidaan samalla tavalla kuin osan 3 kohdassa 10 esitetään, ja vaarallisen tapahtuman todennäköisyyden arvioidaan olevan ”harvoin” eli 2 pistettä, vaadittava SIL-taso pysyy edelleenkin tasolla SIL 3, mikä vastaa suoritustasoa e.

8.4 Vaadittavan suoritustason PLr määrittäminen suoraan B- ja C-tyypin standardien avulla

Riskin pienentämisen toimenpiteiden suunnittelussa voidaan käyttää B- ja C-tyypin standardeja, jos niitä voidaan soveltaa kyseisiin koneisiin ja ne kattavat kaikki asiaan liittyvät vaatimukset (ISO TR 22100-2 ja osa 3 luku 8).

Esimerkki: Robottiyksikön toimintaankytkennältä vaadittavan suoritustason PLr määrittäminen suoraan robottiyksikön standardin ISO 10218-2 vaatimusten mukaan

Osan 3 luvun 9 esimerkissä robottiyksikön suunnittelussa voidaan käyttää C-tyypin standardia teknisen raportin ISO 10218-2, jossa esitetään myös robottiyksikön toiminalliset vaatimukset. Seuraava teksti perustuu robottiyksikköstandardiin:

”*5.2.2 Suoritustasovaatimukset*

Ohjausjärjestelmän turvallisuuteen liittyvät osat on suunniteltava siten, että ne ovat standardissa ISO 13849-1:2006 kuvattavan suoritustason PL = d ja luokan 3 mukaisia, tai ne ovat standardissa IEC 62061:2005 kuvattavan turvallisuuden eheyden tason SIL 2, laitteiston vikasietoisuuden 1 ja määräaikaistarkastuksen aikavälin enintään 20 vuotta mukaisia.”

Näin ollen ohjausjärjestelmän turvallisuuteen liittyvien osien (alajärjestelmien) vaadittava suoritustaso on PLr d luokka 3 (jos riskin arvioinnista ei muuta johdu).

9 Piirikaavioiden suunnittelu

Ohjausjärjestelmän rakentaminen ja asennus on tehtävä noudattamalla hyvää insinöörikäytäntöä (engineering) ja ottamalla huomioon erityisesti sähkötekniset näkökohdat (systemaattiset virheet, luku 7).

Kun on valittu kaikki tarvittavat komponentit ja niiden dokumentit voidaan laatia turvallisuuteen liittyvien ohjaustoimintojen piirikaaviot. Siinä on erityisesti tarkistettava, että turvatoimintojen toteutus täyttää sille suunnitellut vaatimukset (esim. arkkitehtuurin edellyttämät kahdennukset on langoitettu oikealla tavalla ja tähän tarkoitukseen sopiviin komponentteihin, diagnostiikkatoiminnot ja niiden taajuudet ja ajoitukset tarkistetaan, yhteisvikaantumisen estämisen vaatimusten toteuttamisesta huolehditaan ym.).

10 Ohjelmiston kehittämisen perusvaatimukset

Kaikki ohjelmiston elinkaareen (ohjelmiston kehittämiseen, koodaukseen, testaukseen, konfigurointiin, parametrointiin ja muutoksiin) kuuluvat toimenpiteet on dokumentoitava (liite 3). Tavoitteena on, että ohjelmisto on selkeä ja yksikäsitteinen eli se on

- ymmärrettävä (loogiset kuvaukset, algoritmit)
- testattava

- jäljitettävä
- ylläpidettävä.

Toiminnallisen turvallisuuden suunnitelmassa (Safety Plan) on määriteltävä ohjelmiston kehittämisen strategia ja siihen kuuluvat ohjelmiston

- todentamiset (eri kehitysvaiheiden erittelyjen vaatimusten täyttyminen)
- testaukset (testaussuunnitelma)
- kelpuutus (täyttääkö koko järjestelmä turvallisuuserittelyn vaatimukset)
- muutosten hallinta ja ylläpito.

Ohjelmistokehityksen perustana on oltava laatujärjestelmä, joka täyttää standardisarjan ISO 9000 perusvaatimukset. Lähtökohtana on virheiden välttäminen ohjelmiston turvallisuuden elinkaaren aikana (”puolustuksellinen ohjelmointi”). Turvatarkoituksiin suositellaan testattujen (ja mieluummin sertifioitujen) ohjelmistomoduulien käyttöä.

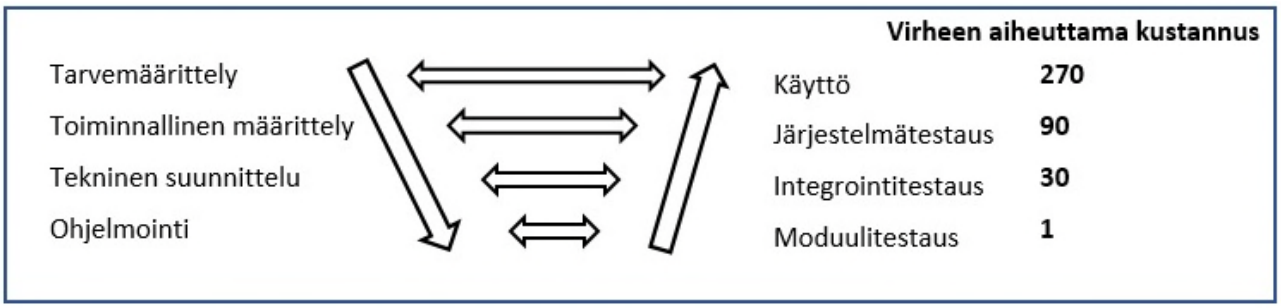
Ohjelmistokehityksen virheiden hallinta

Jo vuonna 1986 todettiin ohjelmistokehityksen virheiden kustannuksista (Softplan):

- mitä aikaisemmin virhe tehdään, sitä myöhemmin se havaitaan
- mitä myöhemmin virhe havaitaan, sitä kalliimpaa on sen korjaaminen
- mitä myöhemmin virhe korjataan, sitä todennäköisemmin se korjataan väärin.

10.1 Ohjelmistokehityksen V-malli

Ohjelmistokehityksen virheiden hallinnan tehostamiseksi koneen suunnittelu tehdään elinkaarimallin alkuosan mukaan. Tässä turvallisuuden elinkaarimallissa eri vaiheiden välissä tehdään auditointia, tarkastuksia ja/tai turvallisuuteen liittyvien toimintojen ja dokumenttien läpikäyntiä, joilla pyritään löytämään ajoissa elinkaaren edellisen vaiheen virheet, ja ne pyritään korjaamaan ennen kuin siirrytään seuraavaan suunnitteluvaiheeseen. Tällä tavoin estetään mahdollisimman kattavasti suunnitteluvirheiden kulkeutuminen elinkaaren loppuun ja kelpuutukseen liittyviin järjestelmätestauksiin (kuva 6).



Kuva 6 Ohjelmistokehityksen V-malli ja virheen aiheuttama kustannus (Softplan).

Turvallisuuskriittisten järjestelmien suunnittelussa käytetään toiminnallisen turvallisuuden (ohjelmistokehityksen) elinkaarimallia (*Functional Safety LIfecycle*, SLC, kohta 3.3). Sen mukaan erityisesti ohjelmistokehityksessä on otettu käyttöön elinkaarimallista kehitetty V-malli (kuva 7),

joka on nykyisin laajalti käytössä eri versioina ja jota käsitellään myös uusissa koneiden toiminnallisen turvallisuuden sovellusstandardeissa (kohta 4.3).

10.2 Sulautetun ohjelmiston kehitys

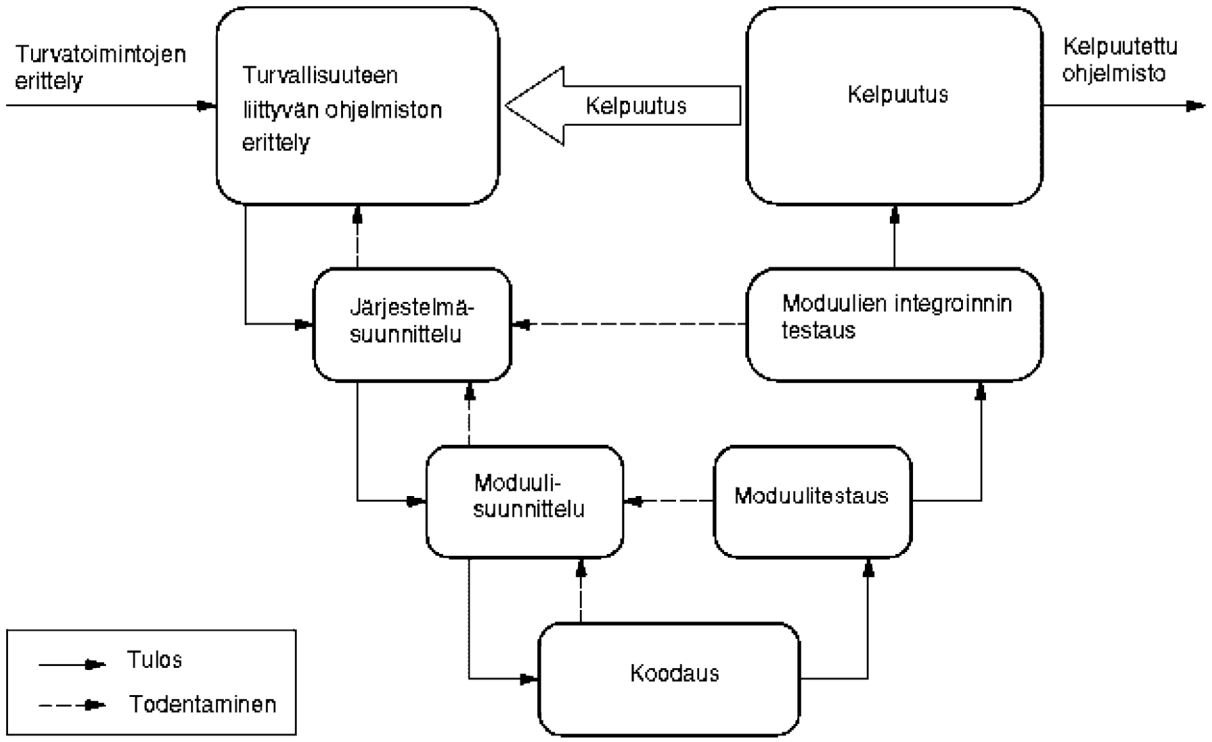
Standardissa IEC 61508-3 esitetään sulautettujen ohjelmistojen kehittämistä koskevia laatuun ja turvallisuuteen liittyviä vaatimuksia ja ohjeita. Standardissa ISO 13849-1 on hyvin lyhyesti esitettynä eräitä perusperiaatteita sulautettujen ohjelmistojen ja erityisemmin sovellusohjelmistojen kehittämiseen. Standardissa IEC 62061 on huomattavasti laajempi liite 6.11 konejärjestelmiin liittyvien sulautettujen ohjelmistojen sekä sovellusohjelmistojen turvallisuuden suunnittelusta.

Sulautettuja ohjelmistoja tehdään useimmiten rajoittamattoman käskykannan ohjelmointikielellä (*Full Variable Language, FVL*, esim. C-kielet, Java) ja korkeammilla suoritustasoilla on nojauduttava standardiin IEC 61508-3.

Standardissa ISO 13849-1 esitetään sulautetulle ohjelmistolle perusvaatimukset kaikille suoritustasoille sekä lisävaatimuksia korkeammille suoritustasoille (ISO 13849-1 kohta 4.6.2).

Perusvaatimukset kaikille suoritustasoille

- ohjelmiston turvallisuuden elinkaaren toimenpiteiden suunnitelma
- todentaminen, kelpuutus jne., ks. V-malli, (kuva 7)
- ohjelmiston spesifikaatio ja dokumentointi
- rakenteinen (modulaarinen) ohjelmointi
- systemaattisten vikaantumisten hallinta
- satunnaisten laitevikaantumisten hallinta ohjelmiston avulla
- toiminnalliset testaukset
- muutosten hallinta.



Kuva 7 Ohjelmistokehityksen V-malli (standardin ISO 13849-1 kuva 6)

Sulautettujen ohjelmistojen vaatimuksia

Sulautetuille ohjelmistoille on edellä esitettyjen kaikkia suoritustasoja koskevien vaatimusten lisäksi korkeammilla suoritustasoilla PL c ja d seuraavat vaatimukset:

- dokumentointi ohjelmiston koko turvallisuuden elinkaaren aikana sekä kaikkien dokumenttien arkistointi
- ohjelma- ja konfiguraatioversioiden hallinta
- turvallisuusvaatimusten ja -suunnittelun rakenteinen (modulaarinen) erittely
- soveltuvien ohjelmointikielten käyttö
- varmennettujen (sertifioitujen) tietokoneavusteisten työkalujen käyttö
- turvallisuuteen liittymättömän ohjelmiston erottaminen
- rajoitetut moduulien koot ja niiden täydellisesti määritetyt rajapinnat
- suunnittelu- ja koodausstandardien käyttö
- koodauksen todentaminen läpikäymällä tai katselmoimalla ohjausdataa kulkukaavioanalyysien avulla
- laajennettu toiminnallinen testaus, esimerkiksi ”harmaalaatikko” -testaus, suorituskyvyn testaus tai simulointi
- muutosten jälkeinen vaikutusanalyysi ja soveltuvat toimenpiteet.

Standardin ISO 13849-1 liitteessä J esitetään esimerkki sulautetun ohjelmiston turvallisuus-elinkaaresta ja toimenpiteistä suoritustasolle PL d.

Redundanttisissa rakenteissa on huomattava, että korkeampi suoritustaso voidaan saavuttaa vain, kun myös redundanttisten laitteiden ohjelmistot ovat erillisiä.

Turvallisuuteen liittyvän sulautetun ohjelmiston, joka on tarkoitettu korkeimmalle vaadittavalle suoritustasolle PLr e, on oltava standardin IEC 61508-3 kohdan 7 (ohjelmiston turvallisuuden elinkaari) mukainen, mikä vastaa turvallisuuden eheyden tasoa SIL 3.

10.3 Sovellusohjelmiston suunnittelu ja kehitys

Standardissa ISO 13849-1 esitettävä yksinkertaistettu ohjelmistokehityksen elinkaarimalli sopii myös sovellusohjelmiston kehittämiseen (ISO 13849-1 kohta 4.6.3).

Turvallisuuteen liittyvän sovellusohjelmiston suunnittelumenetelmät ja ohjelmointikielet on valittava siten, että turvallisuuteen liittyville ohjaustoiminnoille saadaan vaadittava turvallisuuden eheyden taso SIL tai suoritustaso PL. Turvallisuuteen liittyvän ohjelmiston kehittämisessä on käytettävä rajoittamattoman käskykannan kielten asemesta rajoitettujen käskykantojen ohjelmointikieliä (*Limited Variable Language, LVL*, esim. toimilohkokielet, tikapuukielet).

Käytettäessä rajoittamattoman käskykannan kieliä on täytettävä edellä esitettävät kaikki sulautettuja ohjelmistoja koskevat vaatimukset, jolloin myös voidaan saavuttaa kaikki suoritustasot PL a…e. Käytettäessä modulaariseen lähestymistapaan soveltuvia rajoitetun käskykannan ohjelmointikieliä, voidaan saavuttaa kaikki suoritustasot PL a...e. Nojautumalla standardiin ISO 13849-1 voidaan päästä korkeimmalle suoritustasolle PL e vain käyttämällä rajoitetun käskykannan kieliä.

Perusvaatimukset sovellusohjelmistolle ovat likimain samat kuin sulautetuille ohjelmistoille. Standardissa ei eritellä tarkemmin lisävaatimuksia eri suoritustasoille, vaan lisävaatimukset kohdennetaan tehostetusti kasvavan vaatimustason mukaan suoritustasoille c, d ja e.

Sovellusohjelmiston kehittämisen vaatimuksia ja tehtäviä

- ohjelmiston turvallisuuteen liittyvän dokumentaation katselmointi (esim. turvatoiminnot, suorituskyky kyseisessä sovelluksessa, laitteiston rakenne, ulkoiset häiriöt).
- työkalujen, ohjelmakirjastojen ja kielten valinta (esim. työkalujen ja toimilohkokirjastojen kelpuutus, suositellaan rajoitetun käskykannan kielten alajoukkoja).
- ohjelmiston suunnittelussa noudatettavat puolustuksellisen ohjelmoinnin tekniikat, puolimuodolliset kuvausmenetelmät, rakenteinen (modulaarinen) ohjelmointi ja mm. toimilohkojen rajoitukset ja virheiden havaitsemistekniikat.
- turvallisuuteen liittyvän ja liittymättömän sovellusohjelmiston yhdistämisen ehdot (esim. sovellusohjelmiston koodaus eri toimilohkoihin, loogisen yhdistämisen välttäminen).
- ohjelmiston toteutus ja koodaus (esim. käytettävä koodaussääntöjä ja symbolisia muuttujia, tietojen eheyden ja mielekkyyden tarkistukset, simulointi).
- testaussuunnitelma (esim. ”mustalaatikko” -testaus, ajoitustoiminnot, raja-arvojen analyysit, tulojen ja lähtöjen testaukset).
- dokumentoinnin on oltava saatavilla olevaa, luettavaa ja ymmärrettävää (esim. kaikki elinkaareen ja muutoksiin kuuluvat toimenpiteet on dokumentoitava, toiminnalliset kuvaukset,

tulojen ja lähtöjen kuvaukset, version tunnus ja käytettyjen kirjastotoimilohkojen version tunnus, kommentit).
- todentaminen (esim. katselmointi, tarkastus, läpikäynti).
- konfiguraation hallinta (esim. proseduurit, varmuuskopiot, arkistoidaan ohjelmistomoduulit ja todentamisen tai kelpuutuksen tulokset sekä työkalun konfiguraatiot).
- muutokset (esim. vaikutusanalyysit, elinkaarimalliin kuuluvat toimenpiteet, käyttöoikeudet, valvonta, muutoshistoria).

Turvallisuuteen liittyvän ohjelmistokehityksen perusperiaatteena on rakenteinen (modulaarinen) ohjelmointi eli sovelluksen toiminnan modulaarisuus sekä ohjaustietojen tarkat määritykset moduulien tuloille ja lähdöille.

Sovelluksen toimintojen toteuttaminen aloitetaan ohjelmiston toimintojen sekä tulojen ja lähtöjen kartoituksesta. Rakenteellisen ohjelmoinnin mukaan ensin laaditaan ohjausjärjestelmän ja sen moduulien sisäisen rakenteen ja toiminnan kattava kuvaus sekä erittely liitännöistä ja vuorovaikutuksista (ohjelmisto ja laitteisto). Ohjelmointi toteutetaan ensisijaisesti valmiilla (sertifioiduilla) toimilohkoilla, jotka otetaan turvallisuustarkoituksiin kelpuutetuista toimilohkokirjastoista.

Ohjelmoinnissa käytetään puolimuodollisia menetelmiä data- ja ohjelmavuon hallintaan (esim. tilakaaviot ja ohjelman vuokaaviot). Ohjelmoinnissa olisi otettava huomioon toimilohkojen rajoitettu koko ja yksikäsitteisyys siten, että toimilohkoilla olisi vain yksi tulokohta ja yksi turvallisuuteen liittyvä lähtö. Ohjelmistoon kehitetään systemaattisten virheiden paljastamisen menetelmiä (esim. datatyyppien sekoittuminen, epätäydellisesti nimetyt liitännät, epäselvä dynaamisen muistin jakaminen yms.). Turvallisuuteen liittyvän ja liittymättömän datan välillä ei saa olla mitään turvallisuuden eheyttä vaarantavaa loogista yhteyttä. Ohjelmistossa on oltava datan eheyden ja mielekkyyden testauksia (esim. vaihteluvälien tarkistukset).

Ohjelmiston koodaus olisi tehtävä hyväksyttävien koodausohjeiden mukaan. Koodauksessa olisi otettava huomioon, että koodi on helposti luettavissa, ymmärrettävissä ja testattavissa ja (esim. symbolisten muuttujien käyttö yksityiskohtaisten laitteisto-osoitteiden asemesta).

Sovellusohjelmiston testaus tehdään testaussuunnitelman mukaan, johon kuuluu muun muassa sovellusohjelmiston jakaminen helposti hallittaviin yksiköihin, testaustapausten ja testaustyyppien erittelyt sekä testausympäristön, työvälineiden ja testausohjelmien kuvaukset sekä testauskriteerit.

Sovellusohjelmiston testauksella on todennettava, että kaikki sovellusohjelmiston alajärjestelmät tai ohjelmistomoduulit toimivat oikealla tavalla toistensa suhteen ja niiden perustana olevan sulautetun ohjelmiston suhteen. Tarkoituksena on varmistaa, että ohjelmisto suorittaa sille tarkoitetut toiminnat, mutta ei suorita mitään tarkoittamattomia toimintoja, jotka voisivat vaarantaa jonkin turvatoiminnan.

Testaussuunnitelmassa määritetään testaustoiminnot ja hyväksymiskriteerit sekä tarvittavat työkalut. Turvallisuuselinkaaren vaiheiden mukaisia testauksia ovat moduulien testaus (mm. rajapinnat), moduulien yhdistämisen testaus (integraatiotestaus, mm. ohjelmiston ja laitteiston vuorovaikutus) ja lopuksi koko sovellusohjelmiston toiminnallinen testaus.

Kattavillakaan ohjelmiston testauksilla ei voi paljastaa kaikkia ohjelmistovirheitä. Testaustapaukset on valittava ja suunniteltava siten, että erityisesti turvatoiminnot tulevat riittävästi testatuiksi. Testauksilla on varmistettava, että kaikkien sovellusohjelmistojen moduulien jokainen haarautuma suoritetaan ja rajoilla olevat tiedot hallitaan. Testaukseen kuuluu sallittujen ja kiellettyjen tietoalueiden rajojen sekä ääriarvojen tarkistukset. Lisäksi on varmistettava, että ohjelmasekvenssit ja niiden synkronointiehdot ovat oikealla tavalla toteutetut. Jos testauksen yhteydessä havaitaan virhe, virheen syyt ja korjaavat toimenpiteet on otettava mukaan testausten tulosten dokumentaatioon.

Sovellusohjelmiston yhdistämisen testauksen tarkoituksena on testaussuunnitelman mukaan määrittää, toteuttaako ohjelmiston alajärjestelmien ja moduulien yhdistelmä oikealla tavalla kaikki ohjelmistovaatimusten erittelyssä vaaditut toiminnot. Suunnittelu- ja kehittämisvaiheessa määritetyillä testauksilla varmistetaan myös sovellusohjelmiston, sulautetun ohjelmiston ja laitealustan yhteensopivuus.

Kaikille ohjelmiston muutoksille tehdään turvallisuuden vaikutusanalyysi, jolla tarkistetaan ne ohjelmistomoduulit, joihin on vaikutettu. Muutetuille moduuleille tehdään uudelleen todentamisen ja tarvittaessa myös uudelleensuunnittelun toimenpiteet.

Ohjelmiston konfiguraation hallitsemiseksi sovellusohjelmiston versio on varmistettava ja ohjelmiston todentamisen sekä kelpuutuksen tulokset on dokumentoitava.

10.4 Ohjelmistopohjainen parametrointi

Ohjelmistopohjaisessa parametroinnissa (muuttujien asettaminen) esiintyvät virheet voivat johtaa turvatoiminnan menettämiseen (ISO 13849-1 kohta 4.6.4). Ohjelmistopohjaisen parametroinnin menettelytavat on kuvattava ohjelmiston turvallisuusvaatimusten määrittelyssä. Vaatimusten täyttyminen on todennettava. Parametroinnin menettelytavat on kuvattava ohjelmiston turvallisuusvaatimusten spesifikaatiossa.

Tietojen eheys

Kaikkien parametrointiin käytettävien tietojen eheys on säilytettävä. Tämä saadaan aikaan tietojen ja tietoliikenteen valvonnalla (esim. tietojen eheys ennen tiedonsiirtoa, tulotietojen rajoitukset, tiedonsiirtovirheiden ja epätäydellisen tiedonsiirron paljastaminen). Ohjelmistoon syötettävien parametrien tiedonsiirron onnistumisesta on saatava vahvistus palautteen avulla.

Työkalut

Parametrointi on tehtävä käyttämällä siihen soveltuvaa työkalua, jonka tavallisesti toimittaa ohjausjärjestelmän tai sen alajärjestelmän toimittaja. Parametroinnin työkalussa on oltava esto ilman valtuuksia tehtäville muutoksille (esimerkiksi salasana).

- parametroinnin työkalujen on oltava varmennettuja (sertifioituja)
- työkalulla on oltava oma tunniste (nimi, versio jne.).
- työkalussa on oltava esto ilman valtuuksia olevan muutoksen tekemiselle, esimerkiksi käyttämällä salasanaa.
- tulotietojen voimassa oleva alue (minimi, maksimi ja edustavimmat arvot)

Tietojen vahvistus

Parametrien asettamisessa on oltava ohjelmistoon syötettävien parametrien vahvistus joko

- lähettämällä muutetut parametrit takaisin parametroinnin työkaluun tai
- vahvistamalla muulla tavalla parametrien eheys ja lisäksi
- vahvistus tiedonsiirron onnistumisesta (esim. parametroinnin työkalun automaattisella tarkistustoiminnalla).

Systemaattiset virheet

Systemaattisten virheiden välttämiseksi on seuraavien moduulien oltava erillisiä:

- koodaukseen ja koodin purkuun käytettyjen ohjelmistomoduulien tiedonsiirto- ja takaisinsiirtoprosessit
- käyttäjille tarkoitettujen turvallisuuteen liittyvien parametrien visualisointi.
- Datan lähetys- ja vastaanottoprosessin koodaukseen ja koodin purkuun käytettävien ohjelmistomoduulien sekä ohjelmistomoduuleissa, joita käytetään turvallisuuteen liittyvien muuttujien näyttämiseen käyttäjälle, on vähintäänkin käytettävä toiminnallisen erillisyyden (*divergence*) vaatimukset systemaattisten virheiden välttämiseksi.

Todentaminen

Seuraavia todentamistoimenpiteitä on sovellettava ohjelmistoon perustuvassa muuttujien asettamisessa:

- jokaisen turvallisuuteen liittyvän muuttujan oikean asettamisen todentaminen (minimi, maksimi ja edustavat arvot)
- todentaminen, että turvallisuuteen liittyvien muuttujilla on ohjelmoitu tarkistus, esimerkiksi käyttämällä epäsopivia muuttujien arvoja
- todentaminen, että ilman valtuuksia tehtävät turvallisuuteen liittyvien muuttujien muutokset on estetty
- todentaminen, että muuttujiin liittyvä data tai signaalit luodaan ja prosessoidaan siten, että viat eivät voi johtaa turvatoimintojen menettämiseen.

Dokumentointi

Parametroinnin dokumenteissa on esitettävä riittävät tiedot (esim. etukäteen määritellyt parametrijoukot), jotta tunnistettaisiin:

- ohjausjärjestelmään liittyvät parametrit
- henkilöt, jotka tekevät parametrointia
- muut perustiedot kuten parametroinnin päivämäärä.

11 Kelpuutus

Ennen koneen luovutustestauksia tehdään ohjausjärjestelmän toiminnallisuuden kelpuutus tarkistamalla ovatko ohjausjärjestelmän suunnittelun alkuvaiheissa määritetyt koneen toimintoihin liittyvät turvallisuusvaatimukset täytetty. Kelpuutus tehdään koneen turvallisuuteen liittyvien toimintojen suunnittelun yhteydessä laadittavien kelpuutusohjeiden mukaan osana koko koneen turvallisuuden kelpuutusta

Turvallisuuteen liittyvien ohjausjärjestelmän osien toteuttamat turvatoiminnot ja niiden saavuttama suoritustaso on kelpuutettava kelpuutussuunnitelman mukaan. Valmiin ohjausjärjestelmän kelpuutusta käsitellään lyhyesti standardin ISO 13849-1 Luvussa 8 ja tarkemmin standardissa ISO 13849-2. Kelpuutuksella on osoitettava, että jokaisen turvatoiminnan toteuttavien osien yhdistelmä täyttää standardin ISO 13849-1 kaikki asiaan kuuluvat vaatimukset. Kelpuutukseen kuuluu tarkastuksia, läpikäyntejä ja testauksia.

Laitteiston vaarallisia satunnaisvikaantumisia käsitellään kvantitatiivisilla menetelmillä, ohjelmistovirheitä käsitellään puoli-kvantitatiivisilla tai kvalitatiivisilla menetelmillä ja systemaattisia vikaantumisia käsitellään vain kvalitatiivisilla menetelmillä (standardin ISO 13849-1 liite G).

Toiminnallisen turvallisuuden suunnittelun alussa asetetut turvallisuuteen liittyviä vaatimuksia joudutaan usein tarkistamaan ja täydentämään suunnitteluprosessin kuluessa. Toiminnallisen turvallisuuden suunnittelun jälkeen tehdään järjestelmän kelpuutus, jossa tarkistetaan, että järjestelmä täyttää sille asetetut vaatimukset. Useiden vaatimusten kohdalla tarvitaan testauksia ja testausvaatimukset tulee tehdä muiden vaatimusten mukana ja niitäkin voidaan täsmentää suunnittelun aikana.

Kelpuutuksen käytännön esimerkki esitetään standardin ISO 13849-2:2013 liitteessä E.

Systemaattisten virheiden tarkistus perustuu niiden menetelmien läpikäyntiin, joilla systemaattiset virheet on pyritty poistamaan. Tarkistusten perustella tapahtuva systemaattisten virheiden edelleen vähentäminen voi edellyttää muutoksia suunnittelussa, tuotannossa ja organisaatiossa.

Systemaattisten virheiden analyysimenetelmiä ovat mm. vika- ja vaikutusanalyysi, tapahtumapuu/vikapuu sekä HAZOP poikkeamatarkastelu (luku 7).

Vika- ja vaikutusanalyysi, VVA (*Failure Mode and Effect Analysis*, FMEA) on tärkein menetelmä koneiden ohjausjärjestelmien vaatimustenmukaisuuden tarkistamisessa. Se perustuu standardiin IEC 60812 (vastaava SFS 5438 on kumottu vuonna 2006). Sen työvaiheet ovat seuraavat:

- kartoitetaan kaikki turvallisuuteen liittyvät ohjausjärjestelmän osat ja komponentit
- selvitetään niiden vikamuodot
- tarkistetaan vikamuotojen vaikutus ohjausjärjestelmän toimintaan (turvallisuuteen)
- selvitetään osien, laitteiden ja komponenttien vikatiheydet
- huolehditaan systemaattisista virheistä (luku 7).

12 Kunnossapito-ohjeet

Aikaa myöten syntyvät poikkeamat määritetystä suorituskyvystä voivat johtaa turvallisuuden heikkenemiseen ja jopa vaaratilanteeseen. Ohjausjärjestelmän kunnossapito on tarpeen sen osien suorituskyvyn säilyttämiseksi. Koneen mukana käyttäjille toimitettaviin tietoihin kuuluu turvallisuuteen liittyvien ohjausjärjestelmän osien kunnossapito-ohjeet mukaan lukien ohjeet mahdollisista määräaikaisista tarkastuksista ja testauksista (esim. komponenttien vaihtovälit, ISO 13849-1 luku 9).

13 Tekninen dokumentaatio

Osan 1 kohdassa 4.2.3 käsitellään EU:n talousalueella koneen vaatimustenmukaisuuden osoittamiseen vaadittavista dokumenteista ja sen liitteessä 1 esitetään luettelo näistä koneen tilaajalle toimitettavista dokumenteista. Tässä osassa 4 (toiminnallinen turvallisuus) esitetään erityisesti turva-automaatioon liittyvää teknistä dokumentaatiota.

Koneen suunnitteluprosessin eri vaiheissa syntyvät tiedot on dokumentoitava ja päivitettävä. Turvallisuuden elinkaarimallin mukaisessa suunnitteluprosessissa edetään turvallisuuden vaatimusmäärittelystä kelpuutukseen turvallisuuden elinkaaren vaiheiden mukaan. Katselmuksilla todennetaan kulloisenkin vaiheen tuloksena syntyneet dokumentoidut tiedot ja ne toimivat tulotietoina seuraavalle suunnitteluvaiheelle. Näin alkuperäiset vaatimukset, testaussuunnitelmat ja muu dokumentaatio täsmentyvät ja täydentyvät suunnittelun edetessä. Tällöin suunnittelun loppuvaiheessa dokumentaatio on valmiina aineistona muun muassa teknisten asiakirjojen, käyttö- ja kunnossapito-ohjeiden laadintaa varten, ja ne ovat myös myöhemmin kunnossapidon ja mahdollisesti tehtävien muutostöiden ja modernisointien perustana.

Standardin ISO 13849-1 luvussa 10 esitetään tiivistetysti luettelo valmiissa dokumentaatiossa esitettävistä turvallisuuteen liittyvistä tiedoista. Sen mukaan suunniteltaessa turvallisuuteen liittyvää ohjausjärjestelmän osaa suunnittelijan on dokumentoitava alajärjestelmille vähintäänkin seuraavat tiedot:

Alajärjestelmän dokumentaatio (ISO 13849-1 kohta 10)

- 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 ($MTTF_d$, DC, CCF ja toiminta-aika)
- toimenpiteet systemaattisen vikaantumisen estämiseksi
- käytetyt teknologiat
- kaikki tarkastelussa mukana olleet turvallisuuteen liittyvät viat
- vikojen poissulkemisen perustelut (ISO 13849-2)
- suunnittelun loogiset perustelut (esim. huomioon otetut viat, poissuljetut viat)
- ohjelmistoa koskeva dokumentaatio
- kohtuudella ennakoitavissa olevan väärinkäytön estämisen toimenpiteet.

Konedirektiivin määrittelemään turvallisuuteen liittyvät dokumentit on erikseen merkittävä tai arkistoitava erillisenä muista tiedoista, jotta ne voidaan hakea, koota ja toimittaa viranomaiselle niitä pyydettäessä. Toimitettaessa koneita Euroopan talousalueella tekninen tiedosto on oltava saatavilla toimivaltaisia kansallisia viranomaisia varten vähintään 10 vuotta koneen valmistamisesta tai sarjavalmisteisen koneen viimeisen kappaleen valmistamisesta lähtien.

Tuotetietojen dokumentaatio on laajempi kuin konedirektiivin määrittelemä valmistajan ”tekninen tiedosto” myös turvallisuuteen liittyvien tietojen osalta, koska tuotetietoihin kuuluu kaikki suunnitteluprosessin aikana syntyneet tiedot. Yleensä tämä dokumentaatio on tarkoitettu valmistajan omiin tarkoituksiin eikä sitä toimiteta koneen käyttäjälle, mutta sen osat voivat olla tarpeen käyttäjille esim. muutostöitä ja modernisointia varten.

Yhteenveto ohjausjärjestelmän turvallisuuteen liittyvistä dokumenteista esitetään liitteessä 4.

14 Muutosten hallinta

Standardissa ISO 13849-1 käsitellään järjestelmän muutoksia lyhyesti vain sovellusohjelmiston osalta (standardin ISO 13849-1 kohta 4.6.3 j).

Standardin IEC 62061 kohdassa 9.3 on tarkempia vaatimuksia muutosten hallintaan ja seuraavassa niistä muutamia tärkeimpiä kohtia.

Muutosten hallinnan vaatimuksia

- muutostarve on perusteltava ja tehtävä muutossuunnitelma. Ennen muutostyön aloittamista on muutostyön kriittisyyden perusteella tehtävä sopivalla organisaatiolla päätös muutostyön toteuttamisesta. Käyttöoikeuksia muutosten tekemiseen on valvottava ja muutoshistoria on dokumentoitava.
- muutostyön jälkeen on tehtävä uudelleen tarpeelliset todentamisen toimenpiteet ja vahvistettava turvallisuusvaatimusten määrittelyn voimassaolo sekä laitteiden että ohjelmiston osalta.
- turvallisuuteen liittyvään sovellusohjelmistoon tehtyjen muutosten jälkeen on tehtävä vaikutusanalyysi, jolla tunnistetaan kaikki ne ohjelmistomoduulit, joihin muutoksilla on vaikutettu.
- muutosten dokumentoinnin oltava kattava, yksikäsitteinen ja jäljitettävissä (esim. ohjelmiston konfiguraation dokumentointi ohjelmiston kehittämisen aikana).
- vastuisiin liittyvät tiedot on dokumentoitava:
- muutosten perustelut ja hyväksyntäpäätökset
- kaikkien hyväksyttyjen muutosten yksityiskohtien ja henkilöiden valtuuksien dokumentointi.
- dokumentaatio on säilytettävä huolellisesti ja varustettava yksilöllisillä tunnuksilla.

15 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

Ohjausjärjestelmästandardeja

- ISO 9001 Laadunhallintajärjestelmät. Vaatimukset. 2015
- 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 korjauksia 2016 ja 2017, osa 2: Kelpuutus, 2012
- IEC 62061 Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus 2005, korjauksia 2012 ja 2013
- IEC 61508 Turvallisuuteen liittyvien sähköisten/elektronisten/ohjelmoitavien elektronisten järjestelmien toiminnallinen turvallisuus. Osat 1, 2 , 4, 5 ja 7 julkaistiin vuonna 2010, osa 3-1 vuonna 2016 ja osat 0 ja 6 vuonna 2011
- IEC 61511 Toiminnallinen turvallisuus – turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 0: 2010, osat 1 ja 2: 2017, ja osa 3: 2016
- IEC 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset 2016, korjaus 2018

Muita standardeja

- ISO 9001 Laadunhallintajärjestelmät. Vaatimukset 2015
- ISO 10218-2 Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 2: Robottijärjestelmät ja niiden yhdistelmät 2011
- ISO 22100-1 Koneturvallisuus. Osa 1: Miten B-tyypin ja C-tyypin standardit liittyvät standardiin
- ISO 26262 Road vehicles – Functional safety 2011
- ISO 13855 Koneturvallisuus. Suojausteknisten laitteiden sijoitus ottaen huomioon kehon osien lähestymisnopeudet 2010

- IEC 62443-1-1 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit 2013
- IEC 60812 Analysis techniques for system reliability. Failure modes and effects analysis (FMEA and FMECA) 2018
- IEC 61025 Fault Tree Analysis, FTA 2006

Kirjallisuutta

- IFA (ent. BGIA) – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung:
  - SISTEMA-suunnittelutyökalu: suomenkielinen versio on vapaasti ladattavissa rekisteröitymällä työkalun käyttäjäksi osoitteessa: www.dguv.de/bgia/13849.
  - Käsikirja: Functional safety of machine controls. BGIA Report 2/2008e
  - Ohjeita Sistema-työkalun käyttöön: Sistema cook books
  - Standardikomponentit turvatarkoituksiin: Thomas Bömer, Dr Michael Schaefer Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung
- Johan Hedberg, Andreas Söderberg, Jan Tegehall, SP Report, “How to design safe machine control systems – a guideline to EN ISO 13849-1”, SP Technical Research Institute of Sweden (SP)
- Tapio Siirilä ja Katri Tytykoski: Koneturvallisuuden käsikirja, Inspecta, 2016
- Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta, Suomen Automaatioseura ry
- Matti Sundquist toim. Teollisuusautomaation tietoliikenne, turvaväylät, Inspecta, Espoo 2008

Liite 1 Koneautomaation tietoturva

Lyhennelmä: Teollisuusautomaation tietoturva, Suomen Automaatioseura ry, [Kirjallisuutta]

Ongelma: Helppokäyttöisyys x Tietoturva = Vakio

- **Koneiden tietoturvan kehitys**
  - aikaisemmin tietoturva toteutettiin erottamalla järjestelmät toisistaan
  - nykyisin käytetään avoimia protokollia, TCP/IP jne., joita ei ole suunniteltu riittävän tietoturvallisiksi
  - langaton ohjaus tuo mukanaan lisää tietoturvaongelmia

- **Esimerkkejä vahingoista**
  - henkilövahingot
  - energianjakelun keskeytyminen
  - laitevahingot
  - liikesalaisuuksien vuotaminen
  - ympäristövahingot
  - tuotannon keskeytykset
  - valvonnan/hallinnan menetys
  - maineen menetys
  - lain rikkomukset

- **Laskentakapasiteetin rajoitukset**
  - tarkat ajoitusvaatimukset
  - korkeammat turvallisuus ja tietoturvavaatimukset
  - laskentakapasiteettia vaativien salausalgoritmien käyttö ei tavallisesti ole mahdollista

- **Tietoturvatietoisuus**
  - yleinen virheellinen käsitys: tietoturva on vain tekniikkaa
  - paras ratkaisu on tietoturvatietoisuus yhdistettynä sopivaan tekniikkaan
  - johdon sitoutuminen on välttämätön edellytys tietoturvalle
  - luotava tietoturvakulttuuri

- **Tietoturvan järjestämisen ongelmia**
  - alihankinta (työnjako eri puolten kesken)
  - ulkoistaminen (osaaminen, erilaiset järjestelmät)
  - tunnistaminen (käyttöliittymien ongelmat)
  - valtuuttaminen (ajantasaisuus)
  - tilojen valvonta (fyysiset suojaukset)

- päivitysten hallinta (päivitysten todentaminen)
- sähköposti ja internet (henkilöiden vastuut)
- huoltohenkilöstö (etäohjaukset, muistitikut).

Liite 2 Esineiden internet (*Internet Of Things*, IoT)

1. IoT -teknologian vaikutuksia automaation turvallisuuteen

Lähtökohtaisesti IoT:n vaikutukset (kuten myös automaation ja etäohjauksen vaikutukset) ovat myönteisiä, mutta niiden mukana tulee myös haitallisia vaikutuksia. Erityisesti henkilöturvallisuuden osalta negatiiviset vaikutukset riippuvat siitä, minkälaisia konkreettisia vaaroja ohjattavissa -järjestelmissä voi muutoinkin esiintyä. Seuraavassa esitetään näkökohtia esineiden internetin soveltamisesta turvallisuuskriittisiin järjestelmiin.

Esineiden internet on uusi vaihe tuotannon koneellistaminen ja automatisoinnissa. Jokaisessa kehitysvaiheessa on ollut tarpeen tunnistaa myös uusien koneiden ja tuotantojärjestelmien haitallisia ominaisuuksia kuten konkreettisia turvallisuus- ja terveysvaaroja, ja on tullut tarve kehittää menetelmiä niiden poistamiseksi tai riittäväksi pienentämiseksi.

Seuraavassa esitetään koneturvallisuuden kehitysvaiheita ja ongelmia:

- Koneellistaminen (ulkoisen energian käyttöönotto)
  - ongelmana ovat koneiden fyysiset vaaratekijät, esim. liikkuvat koneenosat aluksi suojaamattomina ja sittemmin ne siirrettiin kulkuesteen taakse. Nykyisin turvallisuus varmistetaan suunnittelusta lähtien (standardissa ISO 12100 esitetään koneen turvallisuuden suunnitteluperiaatteet ja sen lisäksi käytettävissä on laaja koneturvallisuusstandardien tietoaineisto)
- Koneautomaatio (sähköisten ohjausjärjestelmien käyttöönotto, esim. säätötekniikka, releteknіikka)
  - edellisten tehtävien lisäksii koneautomaation mukana on koneen toimintojen oikeellisuuden ja luotettavuuden varmistaminen tulleet tärkeiksi turvallisuustoimenpiteiksi, joilla varmistetaan oikeat ohjaustoiminnot ja niiden luotettavuus (nykyisin tähän on käytettävissä koneiden ohjausjärjestelmien suunnittelustandardit ja lukuisat sähkötekniset standardit)
- Digitaalitekniikka
  - edellisten tehtävien lisäksi digitaalisten järjestelmien käyttöönotto ja verkottuminen on tuonut edellisten toimintojen lisäksi elektronisten ohjausjärjestelmien toiminnan varmistamisen, tietoturvahyökkäysten torjumisen ja inhimillisten virhetoimintojen vähentämisen tehtävät
- IoT, koneiden ja laitteiden tiedon keruu ja hyväksikäyttö, tekoäly ja muut oppivat järjestelmät
  - edellisten lisäksi ongelmana algoritmien mahdolliset vaikutukset turvallisuuteen, esim. vikaantumisten ja virhetoimintojen ennaltaehkäisyn (analytiikka), järjestelmän päätöksenteko ristiriitaisessa tilanteessa, algoritmien avoimuus, tietosuoja, tekijänoikeudet, yksityisyyden suoja ym.

2. IoT:n mahdollisia myönteisiä vaikutuksia konejärjestelmien turvallisuuteen

Edellytyksenä on eri osapuolten tietojen avoimuus, järjestelmien yhteensopivuuden varmistaminen (standardit) sekä osaamisen parantaminen kehitysalueina ohjelmointi, testaus, analytiikka, robotisaatio.

- parempi kokonaisuuksien hallinta: verkottunut etäohjaus ja -valvonta, logistiikan parantaminen jne.
- teknisten järjestelmien toimintojen parantaminen: mm. käynnissäpidon parantaminen, toimintojen optimointi
- parempi ennakoitavuus (parantaa turvallisuutta): poikkeustilanteiden ennakointi (esim. vaaratilanteet), käyttövarmuuden lisääminen ennakoivalla kunnossapidolla (esim. huoltotarpeiden määrittäminen ajoissa koneen osien kulumisen seurannalla, toimenpiteiden ajoitusten optimointi, ohjauksen mobiiliratkaisut jne.

3. IoT:n mahdollisia negatiivisia vaikutuksia konejärjestelmien turvallisuuteen

IoT:n negatiiviset vaikutukset kone- ja laiteturvallisuuteen on otettava huomioon, jos

- kyseisessä lopputuotteessa on konkreettisia (esim. fyysisiä) riskejä käyttäjien tai muiden lähistöllä olevien ihmisten turvallisuudelle ja terveydelle
- kyseistä laitetta tai järjestelmää ohjataan tai sen toimintaan vaikutetaan etäohjauksella ja -valvonnalla
- ohjaus, valvonta tai toimintaan vaikuttaminen voi tapahtua kokonaan tai osittain itsenäisillä algoritmeilla ilman ihmisen valvontaa ja/tai ohjausta

Järjestelmien ja laitteiden vaaratekijöitä:

- sähkölaite tai kone: sähköisku, valokaari/tulipalo
- toiminnallinen turvallisuus: vaaraa aiheuttava toimintojen käynnistys, pysäytyksen esto tai pysäytys, toiminnon tai toimintatavan muuttaminen (esim. ohjauksen kaappaaminen) ym.

Kuluttajiin kohdistuvia riskejä:

- väestöön ja kuluttajiin voi kohdistua IoT:n vahingollisia tai haitallisia haavoittuvuuksia:
- tarkoituksellinen kiusan- tai vahingonteko (palvelunesto, tietojen tai rahan varastaminen, kiristys, maineen pilaaminen tms.) seuraavista järjestelmistä ja niiden laitteista:
  - infrajärjestelmät: sähkönjakelu, liikenteen ohjaus, varoitus- ja hälytysjärjestelmät, sairaala-automaatio, rakennusautomaatio (kulunohjaus ja -valvonta, lämmitys ja ilmastointi, ym.)
  - kulutustavarat: kodinkoneet, sähkölaitteet, henkilökohtaiset apuvälineet, (terveydenhoitolaitteet) jne.

4. Johtopäätöksiä

IoT:n vaikutukset teknisten järjestelmien turvallisuuteen voivat olla sekä positiivisia että negatiivisia. Siten kysymyksen selventämiseksi tarvitaan aiheen rajausta tarkastelemalla mitä vaikutuksia (positiivisia ja negatiivisia) IoT-tekniikka voi tuoda käyttäjien fyysiseen turvallisuuteen,

esim. vaikutukset turva-automaatioon ja tietoturvaan (haavoittuvuudet, palautumisaika aikakriittisissä järjestelmissä ym.).

Fyysisen turvallisuuden ja terveyden osalta analyysi ja priorisointi on aloitettava erilaisten koneiden, laitteiden ja järjestelmien konkreettisten riskien tunnistamisella ja sen jälkeen niihin tehtävillä fyysisten riskien arvioinneilla (riskin suuruus) ja tietoturvan arvioinneilla.

Liite 3 Luettelo koneen ohjausjärjestelmän dokumenteista ja käyttäjälle toimitettavista tiedoista

Tämän osan 4 luettelo täydentää osan 1 liitteessä 1 esitettävää luetteloa koneen tilaajalle toimitettavista dokumenteista. Tämä luettelo ei ole tyhjentävä, vaan se on tarkoitettu havainnollistamaan koneen dokumentaation kattavuutta. Epäselvissä tapauksissa on nojauduttava alkuperäisiin dokumentaatiovaatimuksiin.

Koneen käyttö- ja ohjaustoimintojen turvallisuuden dokumentointi

- koneen hallintalaitteiden ergonomiset vaatimukset:
  - koneen käynnistäminen (odottamattoman käynnistyksen estämisen toimenpiteet)
  - pysäytys (turvalliseen tilaan saattaminen)
  - toimintatavan valinta (turvatoiminnot automaattisesti mukaan)
  - energiansyötön häiriöt (tehonsyötön valvonta)
  - ohjauspiirin häiriöt (ohjausjärjestelmän luotettavuus)
  - ohjelmistot (oikeellisuus ja helppokäyttöisyys).

Koneen turvatoimintojen ja muiden turvallisuuteen liittyvien ohjaustoimintojen kuvaukset (osa 4)

- toimintojen loogiset tarkastelut
- toimintojen luotettavuustarkastelut:
  - kokonaisuuden turvallisuuteen liittyvä dokumentaatio
  - turvallisuuden elinkaaren vaiheiden dokumentaatio:
  - sähköiseen ohjausjärjestelmään liittyvä dokumentaatio
  - ohjelmistoon liittyvä dokumentaatio.
- luettelo käytetyistä turva-automaatiota koskevista standardeista ja muista teknisistä ohjeista (esim. tehdasstandardit) mm.: turvajärjestelmän
  - suunnitteluun
  - toteutukseen
  - todentamisiin
  - kelpuutukseen
  - edellisten toimenpiteiden edellyttämiin testauksiin
  - käyttöön
  - muutoksiin jne.
- sovellusohjelmiston moduulien yhdistäminen laitteisiin:
  - testaustulokset
  - testausten kriteerien saavuttaminen.

Käyttäjälle toimitettavat tiedot

- järjestelmän kunnossapito-ohjeita:
  - kunnossapitohistoria
  - rutiinit kuten varaosien vaihtaminen.
- kunnossapitomenetelmät
- tarvittavat työvälineet

- tarkastukset
- tarvittava ammattitaito ja vastuunjako
- tarvittavat piirustukset, dokumentit ym.
- ym.

Turvajärjestelmän asennus- ja kunnossapito-ohjeet (turvallisuusohje/turvallisuuskäsikirja, *Safety Manual*) ja siihen liittyvä dokumentaatio

- työkaluihin ja –menetelmiin liittyvä dokumentaatio.
- sopimuksista johdettava dokumentaatio:
  - turva-automaatioon liittyvät sopimuskohdat ja niihin liittyvä dokumentaatio
- standardiviittaukset (suositukset vs. sitovat) ja niissä olevat dokumentointivaatimukset.