Koneturvallisuus: Uuden konedirektiivin toiminnallinen turvallisuus & täytäntöönpano

Tiivistelmä

Tässä asiakirjassa käsitellään muutoksia, jotka liittyvät turvallisuuteen liittyvien ohjausjärjestelmien suunnittelua. EN 62061 ja EN ISO 13849-1 käsittelevät koneen ohjausjärjestelmän toiminnallista turvallisuutta, mutta niissä käytetään hieman erilaisia termejä ja tekniikoita suorituskyvyn määrittelyssä. Tavarantoimittajat voivat suosia tiettyä standardia ja monet käyttäjät ovat hämmentyneitä tavarantoimittajien antamista ristiriitaisista ohjeista. Tässä asiakirjassa selvennetään EN 62061 and EN ISO 13849-1 välisiä eroja ja painotetaan pääkohtia, jotka koneenrakentajien tulisi pitää mielessä.

Schneider Electric

998-2095-02-11-12AR0

Sisällys

1 Euroopan uusi konedirektiivi

Euroopan konedirektiivi 2006/42/EC, joka on julkaistu vuonna 2010, korvaa edellisen konedirektiivin 98/37/EC.

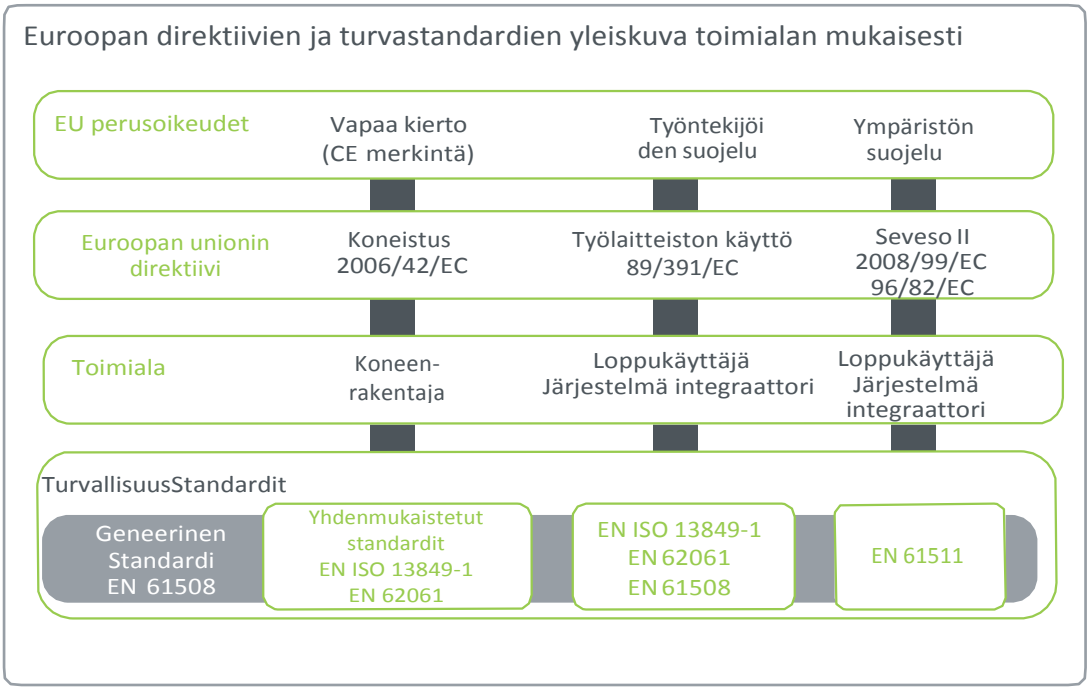
EN 954-1 käyttäjät tuntevat vanhan «riskikaavion», jota on käytetty luokkaan B, 1, 2, 3 tai 4 kuuluvien turvallisuutta koskevien sähköisten ohjauspiirien suunnittelussa. Käyttäjien oli arvioitava subjektiivisesti vamman vakavuus, kuinka usein riskille altistutaan ja sen välttämismahdollisuudet jokaisen turvallisuuteen liittyvän osan luokituksen määrittämiseksi. Kyseinen luokitus määrittelee turvapiirin käyttäytymisen vikatilanteessa, mutta se ei kerro vian ilmenemisen todennäköisyyttä.

Järjestelmissä käytettävän ohjelmoitavan ja ei-ohjelmoitavan elektroniikan määrän kasvun vuoksi turvallisuutta ei voida enää mitata luokituksin. Sen lisäksi aikaisemmat standardit eivät tarjoa tietoa virheen ilmenemistodennäköisyydestä.

Viime vuosina toiminnallisen turvallisuuden konsepti on tullut esiin seuraavasti: sillä viitataan Equipment Under Control (EUC) ja EUC-ohjausjärjestelmään. Toiminnallinen turvallisuus riippuu sähkö-/elektronisten/ohjelmoitavien elektronisten järjestelmien tai muun turvallisuuteen liittyvän järjestelmän oikeanlaisesta toiminnasta, sekä myös ulkoisista riskien hallinta laitteista. Toiminnallinen turvallisuus ei ole jonkun tietyn komponentin tai tietynlaisen laitteen ominaisuus, vaan se koskee koko EUC:tä ja sen ohjausjärjestelmää. Se koskee kaikkia osia, jotka osallistuvat toiminnallisen turvallisuuden toimintaan, esim. sisäänmeno kytkimiä, logic solvers kuten turvareleitä, turvaohjaimia ja turvallisuus PLC:tä (mukaan lukien niiden ohjelmistot ja laitteisto) sekä myös ulostulo laitteita kuten kontaktoreita ja nopeussäätöisiä laitteita / taajuusmuuttajia.

Termi asianmukainen toiminta tarkoittaa, että toiminta on asianmukaista eikä pelkästään mitä odotetaan sen olevan. Tämän vuoksi sopivien toimintojen valinta on aivan välttämätöntä. Aiemmin suunnittelijat yleensä valitsivat komponentteja EN 954-1 luokituksen ylimmältä tasolta sen sijaan, että he olisivat käyttäneet alemman luokituksen komponentteja, jotka olisivat ehkä olleet paremmin sopivia. Tämä johtui usein harhakäsityksestä, että EN 954-1 luokitukset olisivat hierakkisia, esim. että luokitus 3 olisi parempi kuin luokitus 2.

Uudet EN ISO 13849-1 ja EN 62061 standardit auttavat osoittamaan EN 954-1 standardin heikkoudet. Vaikka ne edelleen vaativat piiri arkkitehtuurin harkintaa kuten EN 954-1 standardissa, ne ottavat huomioon myös turvakomponenttien luotettavuuden ja piirin kyvyn havaita / diagnosoida vikoja sekä myös yleisin vian aiheuttajan mahdollisuuden. Jokaisen turvateknisen toiminnon suorituskyky on määritelty EN 62061 alla SIL:nä (Safety Integrity Level 1, 2 tai 3) tai EN ISO 13849-1 alla PL:nä (Performance Level (suorituskyky taso) a, b, c, d tai e).

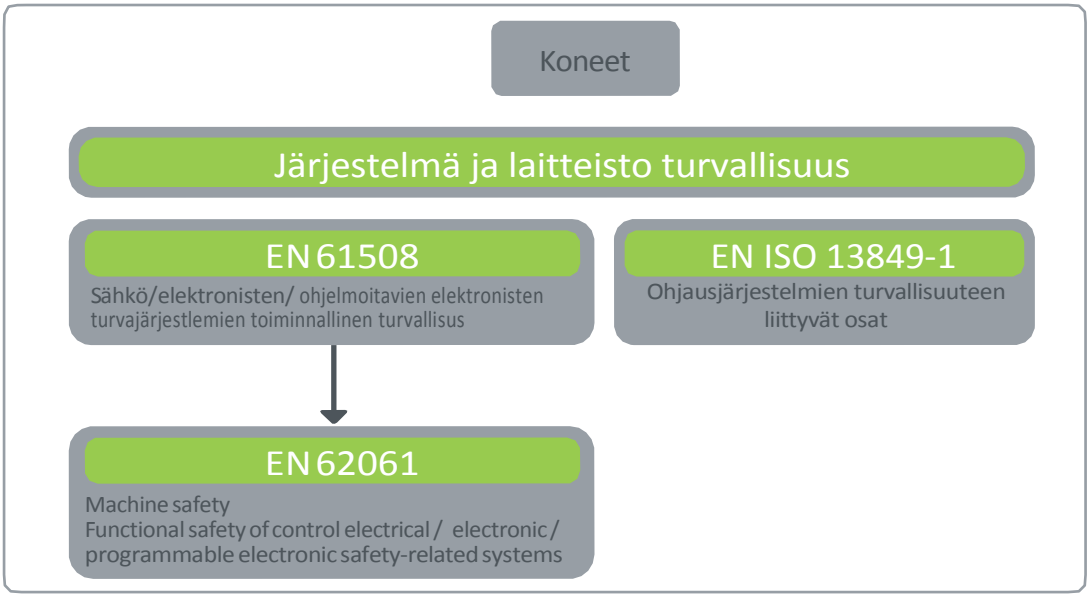


2 Lähestymistapana Toiminnallinen turvallisuus

Uusien toiminnallisen turvallisuuden standardien tarkoituksena on rohkaista suunnittelijoita keskittymään enemmän toimintoihin, jotka ovat välttämättömiä jokaisen yksittäisen riskin tapahtumismahdollisuuden alentamiseksi ja suoritukseen, joka vaaditaan jokaiselta toiminnolta, eikä ainoastaan luottaa tietyn komponentin toimintaan. Nämä standardit mahdollistavat entistä paremman turvallisuustason saavuttamisen koneen käyttöiän aikana.

Vanhassa EN 954-1 standardissa, luokitukset (B, 1, 2, 3 ja 4) sanelevat, kuinka turvallisuuteen liittyvät sähköiset ohjauspiirit käyttäytyvät vikatilanteessa. Suunnittelijat voivat seurata joko EN ISO 13849-1 tai EN 62061 osoittaakseen näiden yhdenmukaisuuden konedirektiivin kanssa. Nämä kaksi standardia ottavat huomioon tuleeko vika ilmenemään sekä sen ilmenemistodennäköisyyden.

Tämä tarkoittaa, että mitattavissa olevat, todennäköiset elementit noudattavat: koneenrakentajien tulee voida määrittää täyttävätkö heidän turvapiirit turvallisuus intefriteettitason (safety integrity level, SIL) tai suorituskykytason (performance level, PL) vaatimukset. Koneiston rakentajien ja suunnittelijoiden tulee olla tietoisia siitä, että turvapiireissä (kuten tunnistavat komponentit, turvalogiikan ratkaisut ja ulostulo laitteet kuten kontaktorit) käytettävien komponenttien valmistajien tulee antaa yksityiskohtaiset tiedot tuotteistansa.



Tämä tieto voi olla hankalasti ymmärrettävissä ja uusissa standardeissa on eri vaatimukset. Kaikkien numeroiden ja lyhenteiden ymmärtäminen voi olla vaikeaa.

Tässä ovat pääkohdat, jotka koneen rakentajien tulisi pitää mielessä EN ISO 13849-1 osalta:

• **Suorituskykytaso (PL):** piiri arkkitehtuuri määrittää tämän (EN 954-1:ssä olevien luokitusten B, 1, 2, 3, ja 4 kaltainen) kuten myös MTTFd ja DC. ISO standardi määrittää viisi (5) suorituskyky tasoa, jotka vaihtelevat PL a:sta (korkein vian ilmenemistodennäköisyys) PL e:hen (matalin vian ilmenemis todennäköisyys). Jos valmistaja antaa komponentille (kuten turvareleelle) tietyn PL luokituksen, tämä tarkoittaa, että se on korkein PL jonka komponenttiin kuuluva piiri voi saavuttaa.

• **Mean Time To Dangerous Failure (MTTFd)** on keskimääräinen aika ennen kuin komponentin vika aiheuttaa häiriön turvallisuus toiminnan. MTTFd on luokiteltu korkeaksi (30-100 vuotta), keskimääräiseksi (10-30 vuotta) tai matalaksi (3-10 vuotta). Huomio: jos komponentin MTTFd on 100 vuotta, se ei taakaa, ettei se rikkoudu aikaisemmin.

• **Diagnostic Coverage (DC)** on komponentin tai piirin kyky tunnistaa/diagnosoida sitä koskeva vika (esim. oikosulku). Mitä korkeampi DC on, sitä pienempi on todennäköisyys vaaralliseen laitteiston häiriöön.

• **Common Cause Failures (CCF)** ovat häiriöitä, jotka johtuvat joko yleisestä ongelmasta (esim. oikosulku) tai yksittäisestä erillisestä tapahtumasta. Yleisten vikojen estämiseksi voidaan tehdä toimenpiteitä esim. suunnittelija voi valita eri komponentteja käytettäväksi kaksikanavaisten järjestelmien eri tiloissa.

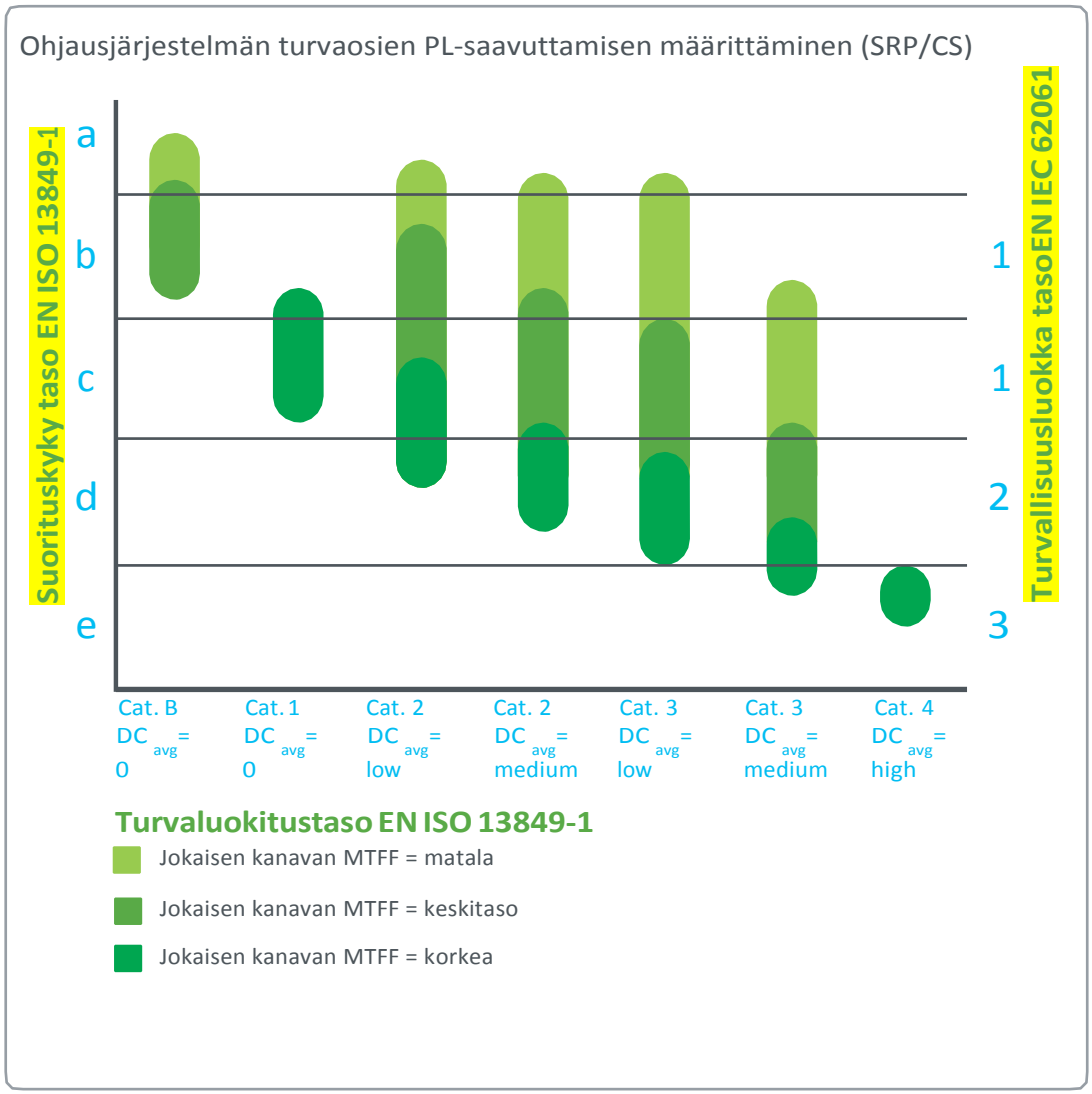
Avainkohdat EN 62061:

• **Safety Integrity Level (SIL)** on erillinen taso ohjausjärjestelmän turvallisuustason vaatimusten määrittämiseen. Standardissa on kolme (3) tasoa yhdestä (alin) kolmeen (ylin). Jos valmistaja antaa tietyn SIL tason komponentille (kuten turvallisuus PLC) silloin se on maksimi SIL turvallisuustaso, joka voidaan antaa millekään kyseistä komponenttia osajärjestelmänä käyttävälle järjestelmälle.

- **SIL Claim Limit (SILCL)** käytetään turvajärjestelmän osajärjestelmissä. Osajärjestelmä määritellään turvajärjestelmän tai -piirin osaksi, jonka vika hajottaa turvajärjestelmän. SILCL on korkein SIL turvallisuustaso, joka voidaan vaatia arkkitehtuuriesteille ja järjestelmälliselle turvallisuuseheydelle.applies to subsystems within a safety system.
- **Probability of Dangerous Failure per Hour (PFH)** on komponentin, osajärjestelmän tai kokonaisen turvajärjestelmän tai -piirin luottettavuuden mitta. Se vastaa MTTFd:ta EN ISO 13849-1:ssa.
- **Safe Failure Fraction (SFF)** alajärjestelmässä on turvavikojen keskimääräinen suhde plus osajärjestelmien vaaralliset havaitut viat osajärjestelmän kokonaiskeskiarvo vika-asteeseen.

B10 and B10d, joita käytetään yhdessä molempien standardien kanssa, ovat sähkömekaanisten komponenttien luotettavuusparametrejä. B10 on toimintojen määrä, jossa 10 % määrästä on epäonnistunut ja B10d on syklien määrä, jonka jälkeen 10 % määrästä on epäonnistunut vaarallisella tavalla.

MTTFd tai PFHd lukuja sähkömekaanisillle komponenteille ei ole julkaistu, koska virheasteet riippuvat upon the hourly actuation rate, joka on sovelluskohtainen. Suunnittelijat voivat kuitenkin käyttää B10 tai B10d tiedossa olevan koneen tietojen kanssa (esim. suojakytkimet voivat aktivoitua tietyn kerran per tunti koneen lastauksen aikana) osajärjestelmien, joissa on nämä komponentit, MTTFd:n ja PFHd:n laskemiseksi.



3 Kumpi standardi?

EN 62061 ja EN ISO 13849-1 koskevat koneen ohjausjärjestelmän toiminnallista turvallisuutta, mutta niissä käytetään hieman erilaisia termejä ja tekniikoita suorituskyvyn määrittelyssä. Tavarantoimittajat voivat suosia tiettyä standardia ja monet käyttäjät ovat hämmentyneitä heidän antamista ristiriitaisista ohjeista.

Kahden standardin välillä valitseminen ei ole ihanteellinen tilanne suunnittelijoille. Tämä voi johtaa ongelmien integraatioon komponenttien välillä ja voi vaikuttaa valmistajien, koneen rakentajien ja loppukäyttäjien suhteisiin. Euroopan komitea sähköteknisellä standardisoimiselle (European Committee for Electrotechnical Standardization, CENELEC) ja Euroopan standardointikomitealla (CEN) on selkeät ajatukset siitä, kuinka säännellä toiminnallista turvallisuutta koneita rakennettaessa. Molemmat ovat laatineet standardeja, jotka voivat tarjota vaatimustenmukaisuus olettamuksen koskien konedirektiivin vaatimuksia.

Molemmilla EN 62061 (CENELEC:n julkaisema) ja EN ISO 13849-1 (CEN:n julkaisema) on sama tavoite: poistaa fokus yksittäisten komponenttien toiminnasta ja sen sijaan keskittyä koko koneen toiminnalliseen turvallisuuteen. Molempien standardien tarkoituksena on vähentää vamman mahdollisuutta; oikein käytettynä ne usein laskevat konevian todennäköisyyttä.
Vaikka nämä standardit tarjoavat samanlaiset riskien vähentämistasot, ne pyrkivät siihen tavoitteeseen hyvin erilaisin tavoin.

Standardit käyttävät erilaisia termejä koskien piirien toiminnallisen turvallisuuden tasoja: EN 62061 määrittelee kolme (3) turvallisuusluokkaa (Safety Integrity Levels, SILs), kun taas EN ISO 13849-1 määrittelee viisi (5) suorituskyky tasoa (Performance Levels , PLs). Terminologiassa olevista eroista huolimatta, joitakin vaatimuksia (kuten vaarallisten vikojen ilmenemistodennäköisyys per tunti) on helppo vertailla. Joka tapauksessa standardit käyttävät erilaisia lähestymistapoja.

Molemmissa EN 62061 and EN ISO 13849-1 on vahvuuksia ja heikkouksia. Molempia vastaan ja puolesta on olemassa perusteita, jotka riippuvat sovelluksesta ja valmistajan henkilökohtaisista mieltymyksistä. Jos konekohtainen tyyppi-C ei määrittele SIL tai PL standardia käytettäväksi, suunnittelijat ovat vapaita valitsemaan kumpaa standardia he käyttävät. Niitä ei kuitenkaan saa sekoittaa yhteen järjestelmään.

Suunnittelijat, joille vanha luokitus EN 954-1 on tuttu voivat pitää EN ISO 13849-1 helpompana käyttää. Edeltäjänsä tavoin, standardi käyttää yksinkertaisemman näköistä ”riskikaaviota” yksittäiseltä turvatoiminnolta vaaditun suorituskyky tason (PL) määrittämiseen sen jälkeen, kun riskien arviointi on suoritettu EN ISO 12100 mukaisesti. Tämä tarkoittaa sitä, että turvatoimintoja voidaan osoittaa asianmukaisella suorituksella ja näin jokaista yksittäistä riskiä voidaan käsitellä erikseen. Riskikaavioin käyttö yksistään ei ole tehokasta; järjestelmän suunnittelijan tulee tehdä muitakin valintoja.

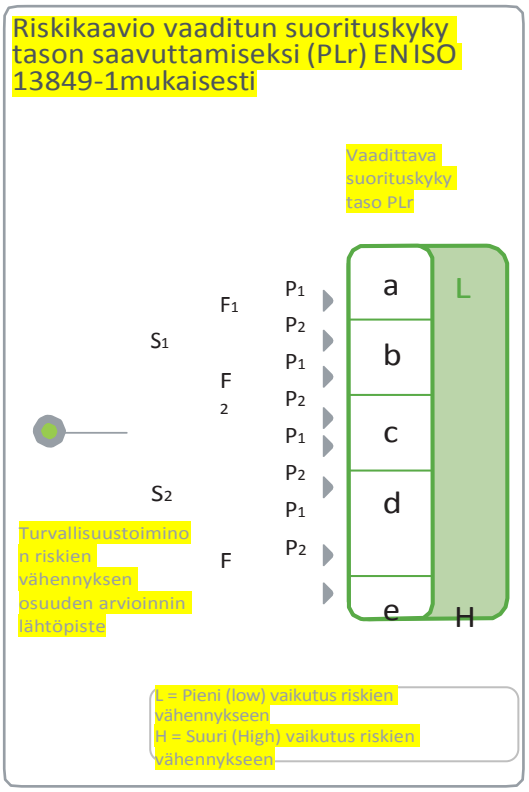
Järjestelmä arkkitehtuuri ei yksistään määritä suorituskykytasoa (Performance level, PL) vaan se perustuu myös Mean TIme to Dangerous Failure (MTTFd) ja Diagnostic Coverage (DC):n. Tämän lähestymistavan merkittävä etu on se, että suunnittelijat voivat käyttää yksinkertaisempia piirejä kunhan he valitsevat korkean luotettavuustason omaavia komponentteja, tai komponentteja, joilla on korkeat MTTFd luvut. Tämä johtuu siitä, että EN ISO 13849-1:ssä määritelyt PL:n viisi (5) tasoa ovat arvojoukko eivätkä erillisiä luokkia.

EN ISO 13849-1:n etu vanhoihin standardeihin nähden on se, että se voi tehdä suunnittelijoille turvallisuudesta kustannustehokkaampaa antamalla heille mahdollisuuden suunnitella turvapiirejä käyttämällä vähemmän mutta luotettavampia komponentteja. Esimerkiksi uudessa standardissa PLd voidaan saavuttaa käyttämällä joko luokituksen 2 yksikanavaista korkean luotettavuuden komponentteja tai luokituksen 3 kaksikanavaista arkkitehtuuria alhaisemman luotettavuustason omaavilla komponenteilla. Näin suunnittelijoilla on laajemmat mahdollisuudet valita.

Kehittäjien ja testaajien apuna on työkaluja (kuten SISTEMA Saksan ammatillinen turvallisuus ja terveys vakuutus instituutista, German Institute of Occupational Safety and Health Insurance), joita käytetään koneen turvallisuuden arviointiin EN ISO 13849-1 mukaisesti.

EN 62061 voi olla sopivampi järjestelmille, joilla on vankemmat vaatimukset toiminnallisen turvallisuuden hallintaan. Se tarjoaa enemmän ohjeita koskien organisaation vaatimuksia ja näin varmistetaan, että toiminnallinen turvallisuus saavutetaan ja ylläpidetään. Tämän lisäksi kyseinen standardi ottaa paremmin huomioon muutoksien vaikutukset, jotka johtuvat uuden laitteiston käyttöönotosta tai koneen käyttöiästä. Esimerkiksi käyttöönotosta huolehtivat insinöörit joutuvat ottamaan huomioon minkä tahansa muutoksen mahdolliset vaikutukset ja kuinka paljon ohjausjärjestelmää voi muuttaa ennen kuin vaaditaan uudelleen arviointi.

IEC-ISO työryhmä on kehittänyt kahden standardin vertailuasiakirjan. Kyseisen asiakirjan on julkaissut molemmat organisaatiot teknisenä raporttina, eli ei standardi-statuksen alla, mutta se on nopeammin julkaistavissa. Tämän yhteistyön perimmäisenä tavoitteena on kehittää yksi standardi, mutta se tulee kestämään useita vuosia.



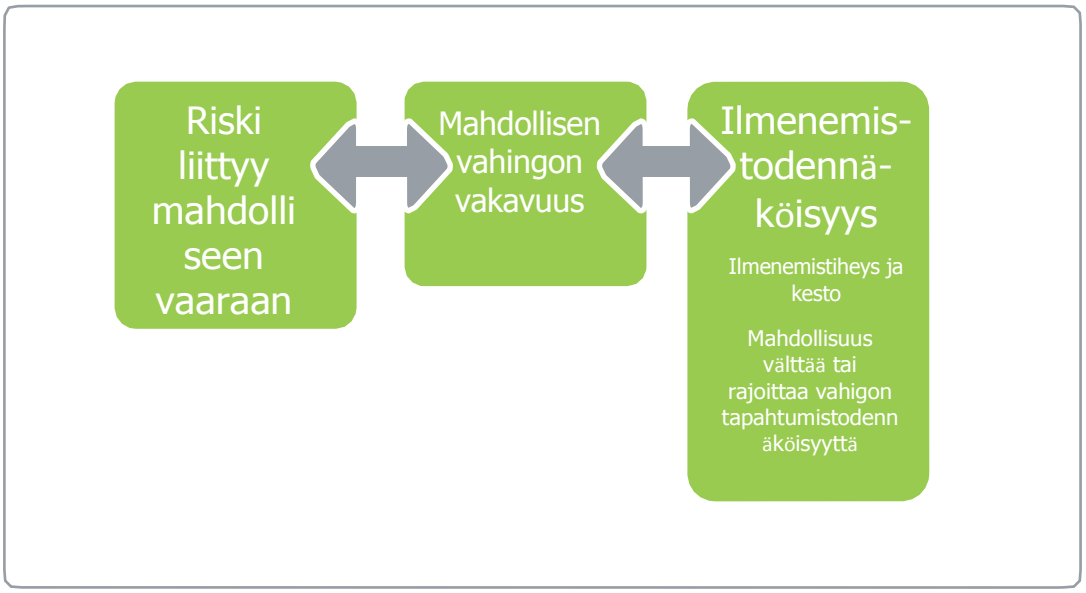
4 Toiminnallinen turvallisuus kontekstissa

Toiminnallinen turvallisuus on olennainen osa turvallisen ohjausjärjestelmän suunnittelua. Myös muita tekijöitä tulee ottaa huomioon ohjausjärjestelmää suunniteltaessa.

Vaikka toiminnallinen turvallisuus on tärkeä, se on merkityksellinen vain, jos muut tekijät ovat otettu huomioon toiminnallisen turvallisuuden laskelmien laittamiseksi kontekstiin. Tämä tarkoittaa koneen perussuunnittelun ja sen sähkölaitteiden sekä pneumaattisten ja hydraulisten laitteiden huomioon ottamista.

Toiminnallisen turvallisuuden standardit ovat hyödyllisiä vain perustavanlaatuisempien standardien kontekstissa kuten EN ISO 12100 (Koneturvallisuus – Yleiset suunnittelu periaatteet – Riskien arviointi ja riskien pienentäminen) ja EN 60204-1 (Koneturvallisuus – koneiden sähkölaitteet).

Vaikka EN ISO 13849-1 ja EN 62061 pidetään parempina ohjausjärjestelmän toiminnallisen turvallisuuden standardeina ne eivät poista riskien arvioinnin tarvetta ja riskien vähentämissuunnitelmaa turvallisuuteen liittyvän ohjausjärjestelmän suunnittelun alussa. Ne eivät myöskään korvaa hyvää turvallisuusteknistä käytäntöä.
Performance Levels (PLs) and Safety Integrity Levels (SILs) eivät ole täsmällisiä arvoja, vaan niitä tulisi käyttää suuntaa näyttävinä arvoina.

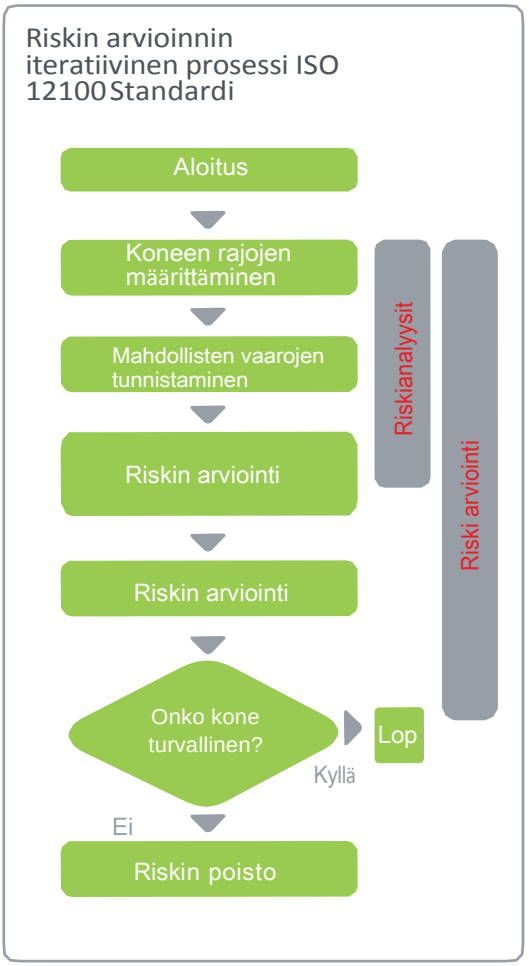


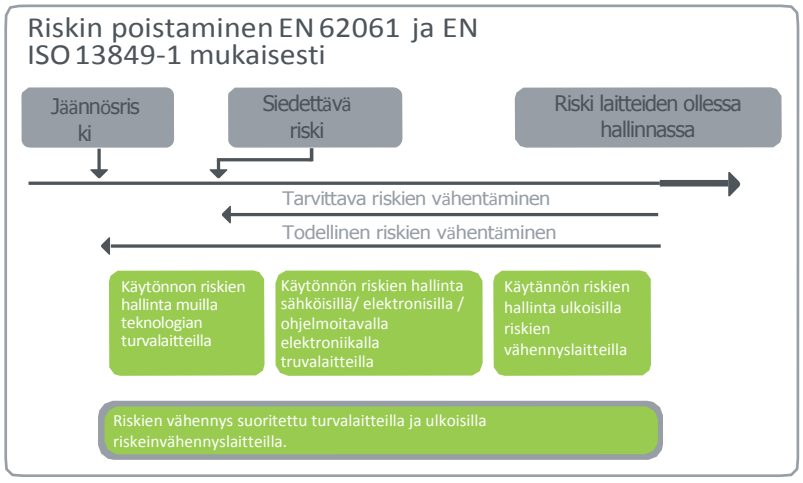
Riskiarviointi ja niiden vähentäminen tulee suorittaa EN ISO 12100 mukaisesti. Pääpaino on riskien vähentämisessä siinä marine kuin se on kohtuudella mahdollista. Riskien vähennys hierarkkia voidaan kuvata kolmella vaiheella.

- **Vaihe 1:** vaaran poistaminen, jos mahdollista (lähtökohtaisesti turvallinen suunnittelu) EN ISO 12100 mukaisesti. Esimerkiksi: suoja esteen asettaminen käyttäjän suojaksi liikkuvalta osalta.
- **Vaihe 2:** suoja vaaroja vastaan kohdissa, joissa sen huomioon ottaminen suunnittelussa ei ole käytännöllistä. Esimerkiksi: suojatoimenpiteiden käyttöönottaminen turva ohjausjärjestelemän kautta, esim. suojat turvakytkimillä tai avaimet aukot, jotka ovat suojattu valoverholla.
- **Vaihe 3:** täydentävien suojatoimenpiteiden käyttöön ottaminen. Esimerkiksi: henkilöstön kouluttaminen, varoitusmerkinnät, käytön ohjaaminen ja henkilökohtaiset suojavarusteet.

Käyttäjien tulee toistaa tämä riskiarviointi jakso ja sen jälkeen riskien vähentäminen riskien vähentämiseksi siedettävälle tasolle, ja varmistaa, että uusia riskejä ei ole tullut esiin.

Riskien vähennys prosessi voi vaatie turvallisuusteen liittyvien ohjausjärjestelmien käyttämistä, jotka ovat suunniteltu EN ISO 13849-1 ja EN 62061. Koneen kokonaisturvallisuus riippuu myös muiden standardien käytöstä, kuten EN 60204-1, joka on täydelliselle sähkölaitteistolle.





Selkeä ja lyhyt opas jossa on näiden kahden toiminnallisen turvallisuuden standardin vaatimukset yksityiskohtaisesti ja siinä on konkreettisia esimerkkejä, on ladattavissa Schneider Electricin sivuilta kohdasta Machine Safety.

Lisätietojen saamiseksi, käy osoitteessa:
http://www.schneider-electric.com/sites/corporate/en/solutions/oem/machine-safety/machine-safety.page

Schneider Electric Industries SAS

Head Office
35 rue Joseph Monier
92506 Rueil-Malmaison Cedex- France
Tel.: +33 (0)1 41 20 70 00
www.schneider-electric.com

WPB2110604EN

03/2012