Artikkelisarja turvallisen koneen suunnittelusta

Osa 5: Koneen ohjausjärjestelmän yksinkertaistettu suunnittelumenetelmä Sistema

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 5

Tämä kirjoitussarjan osa 5 perustuu standardissa ISO 13849-1 esitettävään koneen ns. yksinkertaistettuun ohjausjärjestelmän suunnittelumenetelmään. Tässä osassa 5 keskitytään turvatoimintojen luotettavuuden arviointiin ja siihen liittyvään laskentaan. Liitteessä 1 esitellään turvatoimintojen suunnittelutyökalu Sistema [IFA: Kirjallisuutta].

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 artikkelisarjan osassa 4 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 16 ”Viittauksia ja kirjallisuutta” standardit luetellaan standardin numerolla ja kirjallisuusviitteet luetellaan [nimilyhenteellä] hakasuluissa.

Suorat lainaukset on kirjoitettu *kursiivilla*.

2 Turvatoiminnon suunnittelu

Huom. Nimitys ”turvatoiminto” eroaa kaikista muista ”turvallisuuteen liittyvistä toiminnoista” siten, että ”turvatoiminto” tarkoittaa turvallisuuteen liittyvän sähköisen/elektronisen tai ohjelmoitavan elektronisen ohjausjärjestelmän toteuttamaa toimintoa, jonka vikaantuminen (esim. satunnaisvikaantuminen) tai virhe (esim. suunnittelu tai ohjelmointivirhe) voi aiheuttaa vaaraa henkilön terveydelle.

2.1 Turvatoimintojen suunnittelun etenemistapa

Turvatoimintojen yksityiskohtainen suunnittelu (mukaan lukien suoritustason arviointi) voidaan tehdä vasta kun ohjausjärjestelmään kuulumattomat koneeseen tarvittavat turvallisuustekniset toimenpiteet on suunniteltu (suunnittelun ensisijaisuusjärjestyksen vaiheet (osa 3 kohta 9.1 vaihe 1 ja kohta 9.2 vaihe 2 a). Koneen peruskonseptin ja luvuissa 6 ja 7 esitettävien ohjaustoimintojen suunnitteludokumenttien on oltava valmiina.

Standardissa ISO 13849-1 koneen turvatoimintojen suunnittelun etenemistapa perustuu lukuisiin liitteisiin ja siten toimenpiteiden järjestys ei vastaa tavanomaista turvatoimintojen suunnitteluprosessia. Osissa 1, 2 ja 3 koneen ohjaustoiminnot suunnitellaan standardin ISO 12100 mukaisessa järjestyksessä. Osat 4 ja 5 täydentävät turvatoimintojen suunnittelua teknisen raportin [ISO TR 22100-1] etenemistavan mukaisesti lähinnä satunnaisvikojen hallinnan osalta.

Kun suunnitellaan turvallisuuteen liittyviä ohjaustoiminoja, siinä voi olla monia erilaisia ohjaus-, valvonta-, varmistus- ym. toimintoja., joita käsitellään osan luvuissa 6 ja 7. Nämä toiminnot eivät kuulu tämän osan 5 tarkasteluun. Kuitenkin kaikkien toimintojen oikeellisuus on tarkistettava ja siinä yhteydessä on tarkistettava myös muiden kuin turvatoimintojen toimintojen mahdollisten vuorovaikutusten seurauksia turvallisuuteen liittyviin toimintoihin tai koneen toimintatiloihin.

Suunnittelutyökalu Sistema (liite 1) koskee turvatoimintojen suunnittelua vain turvatoiminnon suoritustason arvioinnin osalta, ja osan 5 etenemistapa vastaa Sisteman rakennetta (liite 1). Jos kaikki tarvittavat luotettavuustekniset lähtötiedot ovat käytettävissä, turvatoiminnon suunnittelutyökalu [Sistema: Kirjallisuutta] laskee suoritustason automaattisesti (liite 1). Sitä mukaa kuin alkuarvoja syötetään Sistemaan, laskennan tulokset nähdään reaaliaikaisesti niiltä osin kuin laskenta etenee.

Siten Sisteman iteratiivisessa suunnittelussa kannattaa varautua muutoksiin ja komponenttien vaihtamisiin. Kun suunnittelussa on syötetty kaikki tarvittavat lähtötiedot ja tehty Sisteman pyytämät valinnat, Sistema ilmoittaa välitulosten ohella turvatoiminnan saavuttamaan suoritustason PL ja vertaa sitä vaadittavaan suoritustasoon PLr. Lopullinen turvallisuuteen liittyvän ohjausjärjestelmän kelpuutus tehdään ohjelmiston ja laitteiston sekä niiden yhteisten testausten avulla.

Jotta turvatoiminto pienentäisi riskiä riittävästi, turvatoiminnon on saavutettava suoritustaso PL, joka täyttää osan 4 luvussa 7 määritetyn vaadittavan suoritustason PLr vaatimukset. Suunnittelijan tehtäväksi jää valita komponentit, joiden vikaantumis- ja diagnostiikkatiedot syötetään valittuun arkkitehtuuriin turvatoiminnon suoritustason laskemiseksi. Jos saatu suoritustaso ei täytä turvatoiminnolle vaadittavaa suoritustasoa PLr, on lähtötietoja ja/tai arkkitehtuurivalintaa muutettava ja tehtävä uusi laskenta.

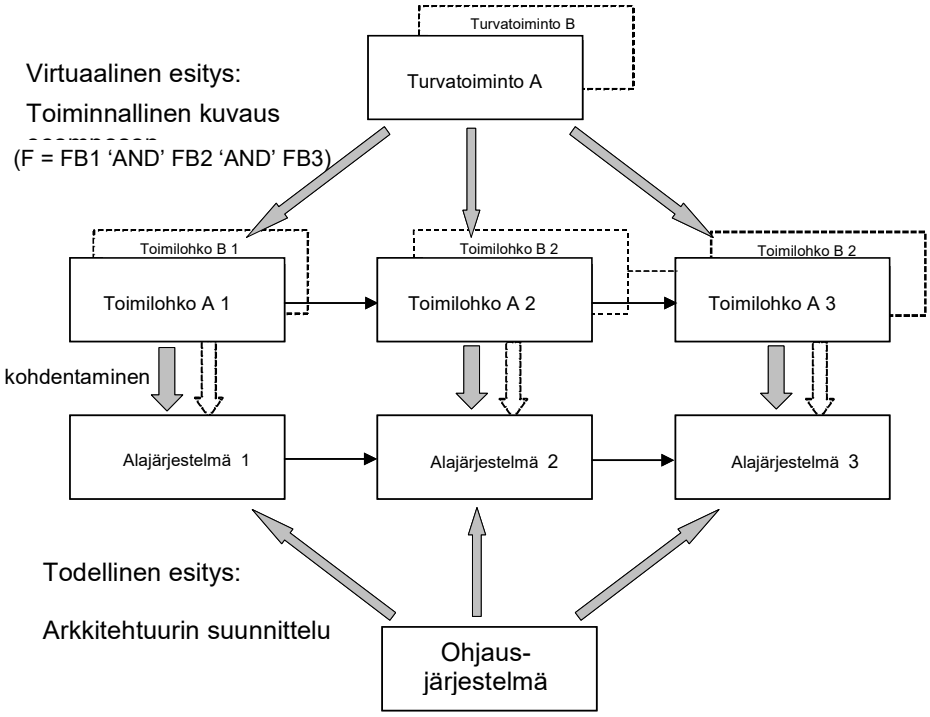
2.2 Turvatoimintojen suunnittelun standardit

Huom. Termillä ”lohko” on kaksi hieman toisistaan poikkeavaa merkitystä:

- toimilohkot kuvaavat järjestelmän osien loogisia toimintoja (*Function Block*, standardi IEC 62061), joita toteuttaman suunnitellaan alajärjestelmiä (*Subsystem*, kuva 1)
- alajärjestelmän kanavien lohkot ovat rakenneosia

Koneen ohjausjärjestelmän toteuttamien turvatoimintojen suunnittelu voidaan tehdä osassa 3 esitettävien standardien avulla:

Standardi 62061: Tässä standardissa turvatoiminto (*Safety Function*) muodostuu yhdestä tai useammasta toimilohkosta (*Function Block, FB*, kuva 1). Ne ovat ohjausjärjestelmän turvallisuuteen liittyviä toiminnallisia osia jotka on esitettävä sarjamuodossa: A1…A3 ja B1…B3. Jokaista toimilohkoa vastaavat turvatoiminnon toteuttavat fyysiset alajärjestelmät (*Subsystem, SS*): Alajärjestelmät 1, 2, 3. Alajärjestelmät koostuvat alajärjestelmän elementeistä (Subsystem Elements, SSE).



Kuva 1 Kahden turvatoiminnon A ja B jakaminen horisontaalisesti sarjamuotoisesti yhdistettyihin toimilohkoihin (*Function Block*) 1, 2 ja 3 ja tämän mallin toteutus sarjamuotoon yhdistetyillä alajärjestelmillä (*Subsystem*), jotka toteuttavat turvatoiminnon (IEC 62061 kuva 5).

Standardi ISO 13849-1: Vastaavasti myös standardin ISO 13849-1 mukaan turvatoiminnon toteuttavat sarjamuotoon yhdistetyt ohjausjärjestelmän turvallisuuteen liittyvän osat (*Safety Related Parts of Control System*, SRP/CS) (kuva 3).

Sistema-työkalussa [IFA: Kirjallisuutta] (liite 1) turvatoimintoa toteuttavat sarjamuotoon yhdistettyjä ohjausjärjestelmän turvallisuuteen liittyvän osia vastaavat alajärjestelmät (*SubBlock*)

Kaikissa edellä mainituissa menetelmissä tämä tarkoittaa sitä, että jos menetetään yksikin turvatoiminnon muodostaman sarjarakenteen osista, menetetään koko turvatoiminto. Turvatoiminnon luotettavuus ei voi olla korkeampi kuin ketjun heikoin lenkki ja muiden lenkkien parantaminen ei tätä tilannetta kompensoi.

Terminologinen vertailu suunnittelun hierarkioista:

IEC 62061	turvatoiminto (*Safety Function*) – toimilohko (*Function Block*) – alajärjestelmä (*SubSystem*) – alajärjestelmän elementti – (*Subsystem Element*)
ISO 13849-1 ja 2	turvatoiminto (*Safety Function*) − ohjausjärjestelmän turvallisuuteen liittyvät osat (*Safety Related Parts of Control System* – alajärjestelmä *SubSystem*) − kanava (*Channel*) – lohko (*Block*) – elementti (*Element*)
Sistema	turvatoiminto (*Safety Function*) − alajärjestelmä (*Safety Related Part of Control System*) − kanava (*Channel*) – lohko (*Block*) – elementti (*Element*)

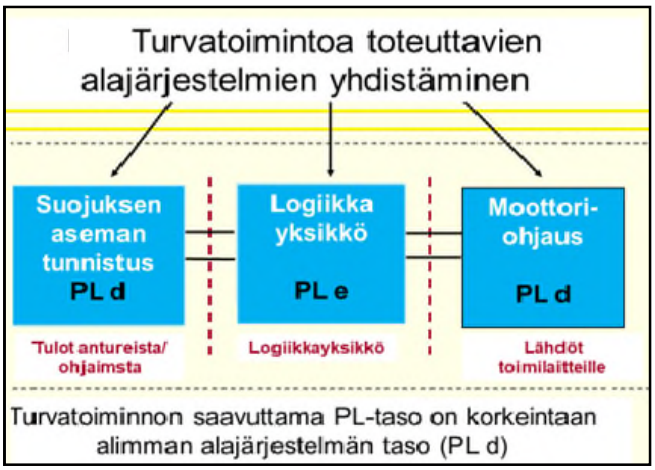
Seuraavassa käsitellään standardin ISO 13849 turvallisuuteen liittyvän toiminnon suoritustason määrittämistä yksinkertaistetulla menetelmällä. Tässä yhteydessä käytetään selkeämpää Sistema-työkalun menetelmää ja terminologiaa (liite 1).

Alajärjestelmien sisäisen rakenteen (arkkitehtuuri) muodostaa, jonka muodostaa (*Channel*, Ch) turva- ja diagnostiikkasignaalien siirtokanavien yhdistelmät. Tässä yksinkertaistetussa menetelmässä on etukäteen valittu konesovelluksiin sopivat arkkitehtuurit eli nimetyt rakenteet, *Designated Architectures*), jotka ovat yleisimmin käytössä koneautomaatiosovelluksissa. Nimetyillä rakenteilla on viisi erilaista vaihtoehtoista luokkaa eli kategoriaa (Cat.) B, 1, 2, 3 ja 4. Näiden suoritustasot PL on laskettu lähtöarvoista matemaattisesti valmiiksi 16 eri vaihtoehdolle (yhteensä 45 mahdollisesta).

Jokainen luokka koostuu kanavista, jotka puolestaan koostuvat lohkoista. Tässä yhteydessä lohko (*Block*, BL) ei tarkoita reaalista komponenttia eikä myöskään kuvan 1 ”toimilohkoa” /eikä luotettavuuslaskennassa käytettyä luotettavuuslohkoa. Tässä lohkot ovat loogisia yksikköjä, jotka kuvaavat turvatoiminnon loogisen rakenteen (kanavien avulla). Lohko puolestaan koostuu elementeistä (perusyksiköistä), jotka eivät muodosta mitään lohkon sisäistä rakennetta. Lohkolle voidaan laskea luotettavuusarvoja elementtien avulla (luku 3).

Edellisten rakenteellisten sääntöjen lisäksi suoritustason laskennan lähtöarvoina ovat komponenttien luotettavuus, diagnostiikan kattavuus ja yhteisvikaantumisen estämisen tehokkuus (luku 4).

Esimerkki kolmen alajärjestelmän muodostamasta kahdennettujen kanavien rakenteesta.



Kuva 2 Tyypillinen kolmen alajärjestelmän rakenne.

Kuvassa turvatoiminto D on jaettu kolmen toimilohkon sarjamuotoiseksi rakenteeksi. Kukin toimilohko on toteutettu kahdennettujen kanavien alajärjestelmällä (luokat 3 tai 4). Kuvassa 2 alajärjestelmien saavuttamat suoritustasot PL ovat vain esimerkkejä.

Alajärjestelmien toteutus voi olla tyypillisesti: tulot – logiikka – lähdöt, esimerkiksi:

- tuloyksikkö: esim. painikkeet, rajakytkimet, valoverhot ym.
- logiikka: esim. ohjelmoitava logiikkayksikkö (PLC)
- lähtöyksikkö: esim. kontaktori, taajuusmuuttaja, virtausventtiilit

turvasignaali kulkee anturista toimilaitteeseen kahdennettuna: ”turvasignaalin muodostaminen – signaalin muokkaus – signaalin ohjaustoiminto turvallisuuteen liittyvälle laitteelle” (kuvassa 2 rinnakkaiset kanavat on mahdollista toteuttaa myös yhdellä turvaväylällä).

Turvatoiminnon suoritustaso on korkeintaan PL d, mutta tarkempi tulos saadaan laskemalla alajärjestelmien PFH_d-arvot yhteen ja tarkistamalla tulosta vastaava suoritustaso PL.

3 Lohkokaaviot

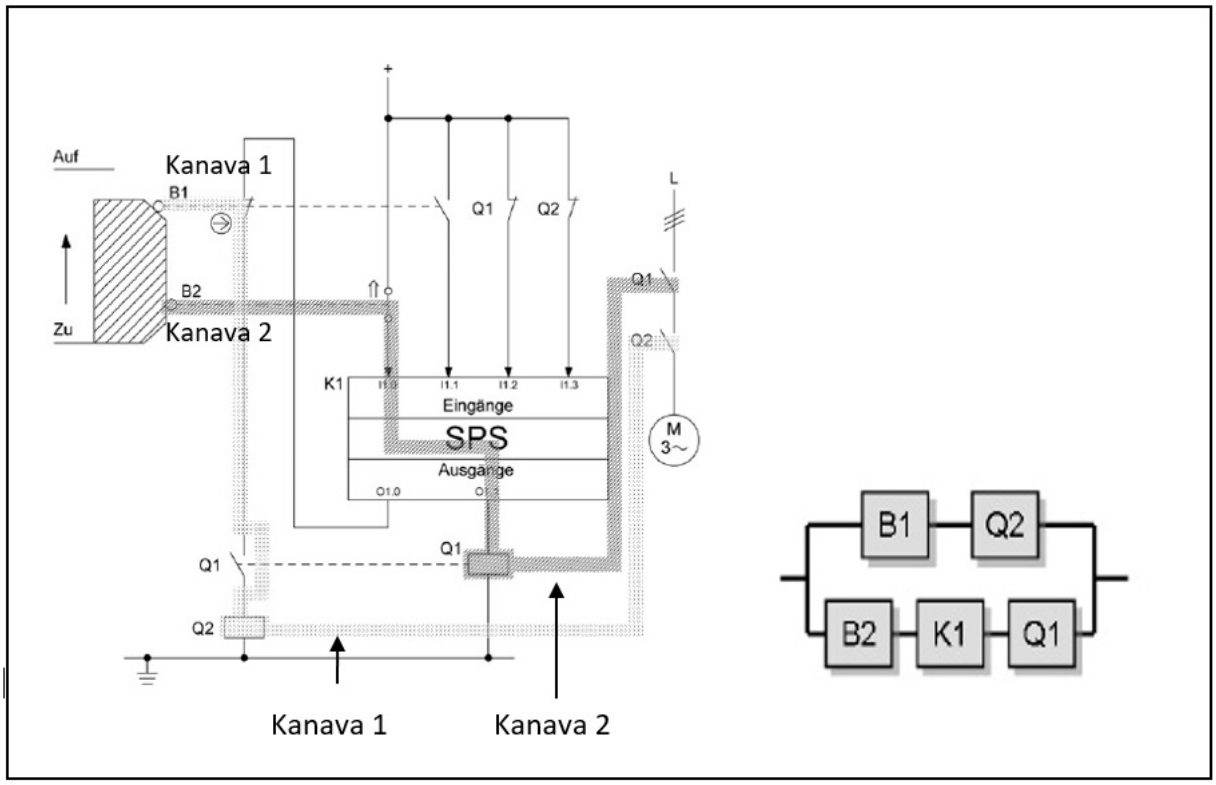
Luvun 2 mukaisesti turvatoimintoa toteuttava alajärjestelmä (SB tai SRP/CS) voi sisältää useita lohkoja.

Lohkokaaviolla on tarkoitus kuvata järjestelmän loogista toimintaa. Järjestelmän (fyysinen) toteutus voi poiketa lohkokaaviosta, mutta arviointimenetelmä edellyttää, että järjestelmän turvallisuuteen liittyvät signaalit kulkevat loogisesti lohkokaavioissa (luku x).

Kun arvioidaan valmista järjestelmää, ensin etsitään kaikki turvasignaalin käyttämät signaalipolut (”datavuo”). Tarkastelusta poistetaan kaikki ne komponentit, jotka eivät kuulu turvasignaalin polkuun, ja tunnistetaan signaalien käyttämät alajärjestelmät sekä niiden kanavarakenne. Jos kanavarakenne ei ole minkään nimetyn rakenteen (luokan) mukainen, yritetään yhdistää kanavia luotettavuustekniikan menetelmillä [IFA [Kirjallisuutta]. Jos tämä ei onnistu, tätä standardin ISO 13849-1 mukaista yksinkertaistettua suunnittelu-/arviointimenetelmää ei kyseiseen sovellukseen voida käyttää ja tällöin voidaan siirtyä käyttämään esimerkiksi standardia IEC 62061 tai IEC 61508.

Esimerkki: Koneen turvatoiminnon lohkokaavion muodostaminen

Kone on varustettu ympäröivällä suojuksella (korkea aitaus) ja pääsy koneen vaaravyöhykkeelle voi tapahtua vain portin kautta. Mentäessä aitauksen sisäpuolelle kone ensin pysäytetään ja sitten vasta portti avataan. Jos portti avataan koneen käydessä, moottori pysähtyy välittömästi. Kone ei voi käynnistyä ennen kuin portti suljetaan ja kuittauksella varmistetaan, että ketään ei ole jäänyt aitauksen sisäpuolelle (robottiesimerkki osan 3 kohdassa 9.3). Vasta tämän jälkeen kone voidaan käynnistää. Kuvassa 8 portin toimintaankytkentä koneen ohjausjärjestelmään on kuvattu sähkökaaviolla ja siitä muodostetulla loogisella lohkokaaviolla.



Kuva 3 Turvatoiminnon toimintaankytkennän piirikaavio, jossa esitetään koneen toimintaan kytketyn portin kaksi rinnakkaista kanavaa: 1) pakkotoiminen rajakytkin B1 –> kontaktorin Q2 koskettimet, 2) rajakytkin B2 –> logiikka –> kontaktorin Q1 koskettimet. Vasemmalla on toimintaankytkennän lohkokaavio [IFA]

Kuvassa 3 vaaravyöhykkeelle johtavan portin asentoa (kiinni – auki) valvotaan ohjauspiirin kahdella rinnakkaisella kanavalla 1 ja 2.

- Kun portti avataan, kanavan 1 rajakytkimen B1 koskettimet avautuvat pakkotoimisesti, jolloin kontaktorin Q2 solenoidi avaa moottorin virransyötön koskettimet Q2 ja moottori pysähtyy. Logiikkayksikkö saa tästä tiedon toisesta pakkotoimisesti sulkeutuvasta koskettimesta.
- Samalla porttia avatessa kanavan 2 rajakytkimen B2 koskettimet avautuvat jousivoimalla, jolloin logiikka avaa kontaktorin Q1 solenoidin avulla moottorin virransyötön koskettimet Q1 ja näin varmistaa moottorin pysähtymisen. Logiikka valvoo kanavien toimintaa näiden tilavaihtojen avulla.
- Kun portti suljetaan, molempien kanavien rajakytkimet vaihtavat asentoa eli kanavan 1 rajakytkimen Q2 koskettimet menevät kiinni jousivoimalla ja kanavan 2 rajakytkinien koskettimet avautuvat pakkotoimisesti. Logiikka ohjaa kanavan 2 apukoskettimen Q1 itsepidolle ja moottori voidaan käynnistää.

Kuvan 8 vasemmalla puolella loogisten toimintojen rakenne on kuvattu lohkokaaviolla. Siinä turvatoimintoa (*Safety Function*, SF) ”toimintaankytkentä” toteuttavan alajärjestelmän (*Sub Block*, SB) kahdennetut kanavat (*Channel*, CH) on muodostettu sarjamuotoisesti yhdistetyistä komponenttien (toiminta)lohkoista (BL) (liite 1 kuva 3).

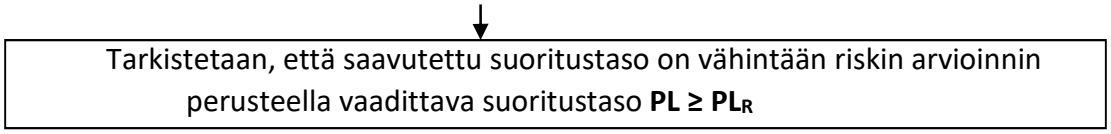
Yksinkertaistettu menetelmä (Sistema) on joustava erilaisten teknologioiden soveltamisessa. Siten ohjausjärjestelmän suunnittelijalla on mahdollisuus valita mikä tahansa nimetty rakenne ja siihen sopiva muuttujien yhdistelmä, kunhan vain turvatoiminnon suoritustaso PL saavuttaa vaadittavan suoritustason PLr.

4 Turvatoiminnon suoritustason arviointi

Tässä luvussa esitetään menetelmiä turvatoiminnolta vaadittavan suoritustason PLr määrittämiseen sekä tämän vaatimuksen täyttämiseen tarvittavan suoritustason PL saavuttamisen arvioinnin tai laskennan menetelmiä.
Taulukossa 1 esitetään suoritustason PL arvioinnin vaiheet.

Taulukko 1 Suoritustason PLr arvioinnin askeleet

Annetaan suoraan elementtien $MTTF_d$–arvot
↓
Annetaan suoraan tai lasketaan (osien laskenta menetelmä) lohkojen $MTTF_d$-arvot
↓
Annetaan suoraan tai lasketaan (osien laskenta menetelmä) kanavien $MTTF_d$-arvot
↓
Symmetrisoidaan mahdolliset rinnakkaiset kanavat Luokitellaan kanavien **$MTTF_d$-arvot**: matala, keskimääräinen, korkea
↓
Annetaan suoraan tai interpoloidaan DC_{avg} Luokitellaan **DC_{avg}-arvot**: nolla, matala, keskimääräinen, korkea
↓
Tarkistetaan yhteisvikaantumisen **CCF** kriteerit
↓
Annetaan valittu luokka **Cat.**
↓
Syötetään parametrien arvot pylväsdiagrammiin ja saadaan turvallisuuteen liittyvän ohjausjärjestelmän osan (alajärjestelmän) saavuttama **PL** = PFH_d
↓
Yhdistetään turvallisuuteen liittyvien ohjausjärjestelmän osien (alajärjestelmien) PL-tasot joko – tarkistamalla alimmalla PL-tasolla olevien osien (alajärjestelmien) lukumäärään ja tarkistamalla taulukosta koko turvatoiminnon **PL_{tot}** tai – laskemalla osien (alajärjestelmien) PFH_d-arvot yhteen ja tarkistamalla mille **PL_{tot}**-tasolle päädytään (**tot** = total, kokonaisarvo)



4.1 Nimetyn rakenteen (luokan) valinta

Yksinkertaistetussa menetelmässä suoritustasojen PL määrittämiseen tarvittava osien todennäköisyys on laskettu etukäteen jokaiselle nimetylle rakenteelle (luokalle) sekä muuttujien $MTTF_d$, DC_{avg} ja CCF yhdistelmille. Suoritustason laskenta perustuu Markovin ketjuihin ja sen numeeriset tulokset esitetään standardin liitteessä K.

Turvallisuuteen liittyvien ohjausjärjestelmien alajärjestelmien sisäisen kanavarakenteen muodostamiseen käytetään lohkokaavioita (luku 3) ja siihen liittyy muutamia sääntöjä (standardi ISO 13849-1 liite B muokattuna):

- määrätty turvatoiminta voidaan toteuttaa yhdellä tai useammalla turvallisuuteen liittyvällä peräkkäisellä tai rinnakkaisella ohjausjärjestelmän kanavalla (redundanssi)
- useampi turvatoiminta voi käyttää yhtä tai useampaa samaa turvallisuuteen liittyvää ohjausjärjestelmän kanavaa (kuvan 9 alajärjestelmien erilaiset luokat)
- yksittäinen turvallisuuteen liittyvä ohjausjärjestelmän kanava voi toteuttaa sekä turvatoimintoja että muita turvallisuuteen liittyviä toimintoja ja ”tavallisia” (turvallisuuteen liittymättömiä”) ohjaustoimintoja,
  - jos nämä toiminnot erotellaan riittävästi toisistaan tai
  - jos käyttötoimintoja käsitellään turvallisuuteen liittyvinä (osa 4 luku 6).

Nimetyt rakenteet perustuvat seuraaville oletuksille (standardin ISO 13849-1 kohta 4.5.4):

- ohjausjärjestelmän toiminta-ajan pituudeksi on ennakoitu 20 vuotta
- komponenttien vikaantumistaajuus on likimain vakio järjestelmän elinkaaren aikana

Jos alajärjestelmän (esim. kaupallisesti saatavilla oleva turvalaite) suoritustaso PL on tiedossa, sitä voidaan käsitellä suoraan ohjausjärjestelmän valmiina alajärjestelmänä, joka liitetään sellaisenaan sarjamuotoiseen rakenteeseen.

Nimetyt rakenteet eivät ole piirikaavioita, vaan loogisia toimintakaavioita. Siten kahdennettujen kanavien tapauksissa (luokat 3 ja 4) voi olla komponentteja, joiden sisäisessä rakenteessa on riittävästi redundanssia ja ne voidaan esittää kaaviossa yksittäisenä.

4.2 Turvatoiminnon arkkitehtuurin valinta

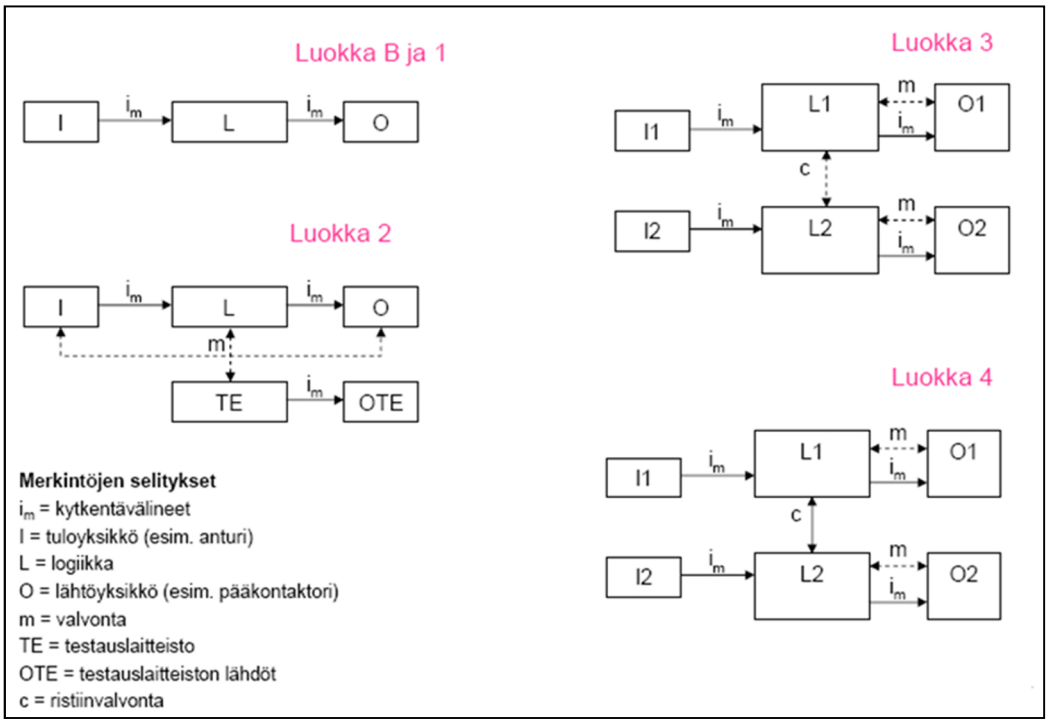
Arkkitehtuuriluokkien yleiskuvaukset esitetään standardin ISO 13849-1 kohdassa 6.2:

- luokka B on yksikanavainen perusrakenne, jossa käytetään tavallisia komponentteja. Vaarallinen vikaantuminen on suhteellisen todennäköistä ja yksikin vaarallinen vika aiheuttaa turvatoiminnan menettämisen. Kanavan $MTTF_d$ oltava vähintään 3 vuotta. Sovellusta vastaavia turvallisuuden perusperiaatteita on noudatettava. Suurin savutettavissa oleva suoritustaso on PL b.
- luokka 1 on yksikanavainen rakenne, jossa käytetään hyvin koeteltuja komponentteja. Vaarallisen vikaantumisen todennäköisyys on huomattavasti pienempi kuin luokassa B, mutta yksikin vaarallinen vikaantuminen aiheuttaa turvatoiminnan menettämisen. Samat

perusvaatimukset kuin luokassa B on täytettävä. Lisäksi tässä luokassa on käytettävä vain hyvin koeteltuja komponentteja (komponenteista on hyviä kokemuksia) ja noudatettava hyvin koeteltuja periaatteita, kohta 4.3.5). Suurin saavutettava suoritustaso on PL c.

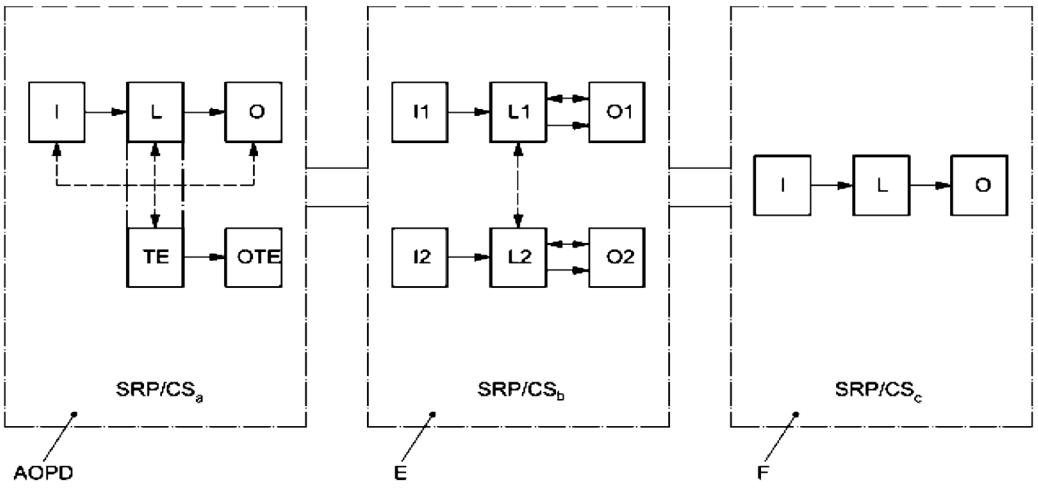
- luokka 2 on yksikanavainen rakenne, 9jota valvotaan esimerkiksi erillisellä testauskanavalla (diagnostiikkatoiminto). Turvatoiminnan menettämisen todennäköisyys riippuu valvonnan kattavuudesta ja valvonnan aikavälistä. Samat perusvaatimukset kuin luokassa B on täytettävä. Suurin saavutettava suoritustaso on PL d.
- luokka 3 on rinnakkainen rakenne ja siinä on rajoitetusti valvontaa. Yksi vikaantuminen ei vielä aiheuta turvatoiminnan menettämistä, mutta vika ei aina paljastu ja se voi seuraavan vikaantumisen kanssa johtaa turvatoiminnan menettämiseen. Yhteisvikaantumiset otetaan huomioon. Samat perusvaatimukset kuin luokassa B on täytettävä.
- luokka 4 on rinnakkainen rakenne ja kattava valvonta. Mahdollisimman monet vikaantumiset pyritään paljastamaan ja yhteisvikaantumiset otetaan huomioon. Samat perusvaatimukset kuin luokassa B on täytettävä.

Standardissa ISO 13849-2 esitetään tarkemmin ”turvallisuuden perusperiaatteet”, ”hyvin koetellut komponentit” ja ”hyvin koetellut turvallisuusperiaatteet” ja niiden noudattaminen eri luokissa B, 1…4 (kohdat 4.3.2 ja 4.3.5).



Kuva 4 Nimetyt rakenteet (luokat/kategoriat/Cat: B, 1, 2, 3 ja 4, standardin ISO 13849-1 kuvat 8…12)

Suunnittelijalla on mahdollisuus valita mikä tahansa nimetty rakenne ja siihen sopiva muuttujien yhdistelmä, kunhan vain saavutetaan vaadittava suoritustaso PLr. Siten menetelmä on joustava erilaisten teknologioiden soveltamiseen.



Merkintöjen selitykset

AOPD	aktiivinen valosähköinen turvalaite esim. valoverho)
E	elektroninen ohjauslogiikka
F	hydrauliikka
I, I1, I2	tuloyksikkö (esim. anturi)
L, L1, L2	logiikka
O, O1, O2, OTE	lähtöyksikkö (esim. pääkontaktori)
TE	testauslaitteisto

Kuva 5 Turvatoiminnon toteuttaminen turvallisuuteen liittyvän ohjausjärjestelmän kolmen alajärjestelmän (SB) avulla, jotka muodostavat sarjamuotoisen rakenteen.

Alajärjestelmät koostuvat kanavista, jotka kuvassa 5 muodostavat alajärjestelmän sisäiset nimetyt rakenteet luokissa 2, 4 ja 1 (standardin ISO 13849-1 kuva H.2). Yksinkertaisimmalla menetelmällä valitaan alimman suoritustason alajärjestelmän suoritustaso koko turvatoiminnon suoritustasoksi. Tarkemmalla laskennalla voidaan päätyä yhtä korkeammalle tai yhtä alemmalle tasolle.

Alimmissa luokissa B ja 1 suoritustaso perustuu pääasiassa laatuvaatimusten täyttämiseen ja vikaantumisten minimointiin rakenteellisilla keinoilla (systemaattisten virheiden estäminen, osa 4 luku 7). Luokassa 2 turvatoiminto varmistetaan sitä valvovalla diagnostiikka kanavalla, ja sitä korkeammissa luokissa 3 ja 4 edellisen lisäksi korkeampi suoritustaso perustuu kanavien kahdennuksiin ja erillisyyteen.

Yksinkertaistetulla menetelmällä voidaan suunnitella myös jonkin verran tässä esitettävistä nimetyistä luokista poikkeavia rakenteita ([Sistema] keittokirja). Tämän yksinkertaistetun menetelmän ulkopuolella voi konejärjestelmissä olla monimutkaisempia rakenteita (esim. useamman kanavan äänestäviä rakenteita), jolloin luotettavuuslaskennan ja arviointien apuna voidaan käyttää standardeja IEC 62061 tai IEC 61508-2.

Standardissa ISO 13849-1 esitettävän yksinkertaistetun menetelmän mukaan arkkitehtuurin valinnan jälkeen aloitetaan PL-tasojen arviointi etukäteen laskettujen mallien avulla.

Yksinkertaistetussa menetelmässä suoritustason PL arviointi tehdään erikseen jokaiselle alajärjestelmälle sen luokan ja siihen liittyvien muuttujien avulla. Näitä muuttujia ovat:

1. Kaikkien käytettävien komponenttien keskimääräinen vaarallinen vikaantumisaika (*Mean Time To Failure*, $MTTF_d$, standardin ISO 13849-1 liitteet C ja D).
2. Kaikkien komponenttien diagnostiikkatoimintojen tiedot ja niiden avulla alajärjestelmän diagnostiikan keskimääräinen kattavuus (*Diagnostic Coverage average*, DC_{avg}, standardin ISO 13849-1 liitteet E).
3. Redundanttisten (kahdennettujen) kanavien yhteisvikaantumisten estämisen menetelmät (*Common Cause Failure, CCF,* standardin ISO 13849-1 liitteet F).

Sistema tekee nämä laskennat automaattisesti reaaliajassa järjestelmän suunnitteluvaiheiden yhteydessä.

4.3 Komponentit - keskimääräisen vaarallisen vikaantumisen ($MTTF_d$) arviointi

Lisäämällä sarjamuotoiseen rakenteeseen hyviä komponentteja ei voida kompensoida heikompien komponenttien luotettavuutta, vaan päinvastoin hyvätkin komponentit voivat vikaantua ja siten ne heikentävät omalta osaltaan omalta ehkä pieneltä osaltaan koko sarjamuotoista yhdistelmää. Siten sarjamuotoisessa rakenteessa koko ohjaustoiminnan luotettavuus riippuu pääasiassa heikoimmasta lenkistä. Tämän vuoksi on tärkeää tunnistaa sarjamuotoisen rakenteen ”heikoin lenkki” ja tarvittaessa se on vaihdettava parempaan, ja jos se ei auta riittävästi, on muutettava koko alajärjestelmän rakennetta esimerkiksi kahdentamalla (redundanssi) tai lisäämällä diagnostiikkaa.

Koneen turvatoimintoa toteuttaa alajärjestelmien sarjamuotoinen rakenne. Jos turvatoiminto on vain yhden kanavan varassa, yhdenkin komponentin vaarallinen vikaantuminen voi aiheuttaa ohjausjärjestelmän turvallisuuteen liittyvän ainoan kanavan menettämisen, jolloin kyseinen alajärjestelmä ja siihen kuuluva turvatoiminto menetetään. Tämän vuoksi keskisuurilla ja suurilla riskitasoilla tarvitaan lisättäviä turvallisuuden varmistamisen menetelmiä, kuten kahdennuksia (redundanssi) ja erillisyyttä yhteisvikaantumisten estämiseen valvontaa sekä diagnostiikkaa paljastamaan vaarallisia vikaantumisia.

Huom. Ohjaustoimintojen turvallisuutta ei voi jättää pelkästään laskennallisen turvallisuuden varaan.

Tämä on tarpeen paitsi vaarallisten vikaantumisten estämiseen myös tukemaan turvatoimintoja (mm. pienentämällä turvatoimintojen vaateen taajuutta) ja samalla lisäämään käytettävyyttä (vähentämään prosessimuotoisen valmistuksen tarpeettomia pysäytyksiä).

Tässä tarkastellaan turvatoimintaa toteuttavien laitteiden satunnaisia laitevikaantumisia ja lähinnä sellaisia vaarallisia vikaantumisia, jotka voivat aiheuttaa turvatoiminnon suorituskyvyn alenemisen tai sen kokonaan menettämisen. Systemaattisesti vikaantuvia komponentteja tarkastellaan Luvussa 6 ja kohdassa 9.5.2.

Vikatarkasteluun tarvitaan hyvää osaamista

- ohjattavan kohteen tuntemus
- ohjattavan kohteen ja sen ohjausjärjestelmän kokonaisuuden ja siihen kuuluvien osien ja komponenttien toiminnan tuntemus
- osaamista komponenttien vikaantumismuotojen ja -taajuuksien arviointiin
- luotettavuuslaskennan perusteiden osaamista
- taitoa arvioida järjestelmän turvallisuuteen liittyvien vaatimusten lisäksi muitakin vaikutuksia (mm. ympäristövaikutukset).

Monimutkaisempien ohjausjärjestelmien arvioinnissa tehdään luotettavuuslaskelmia esimerkiksi vika- ja vaikutusanalyysien ja vikapuumenettelyn avulla. Tähän tarvitaan tietokoneavusteisia työkaluja sekä hyvää ammattitaitoa ja kokemusta niiden käsittelyssä.

Vaikka komponenteille arvioidaan keskimääräiset vaaralliset vikaantumisajat ja niiden avulla tehdään luotettavuuslaskentaa tai -arviointia, kaikille komponenteille ja niiden yhdistelmille on tehtävä systemaattisten vikaantumisten tarkistukset ja toteutettava sen osoittamat toimenpiteet systemaattisten vikaantumisten estämiseksi tai vähentämiseksi (kohta 4.3.2 ja osa 4 luku 7).

4.3.1 Vikaantumistaajuuksien laskenta

Turvatoimintaa toteuttavien laitteiden keskimääräinen vaarallinen vikaantumisaika on keskeisenä parametrina, kun saavutettua suoritustasoa PL verrataan riskin arvioinnin perusteella määritettyyn vaadittavaan suoritustasoon PLr.

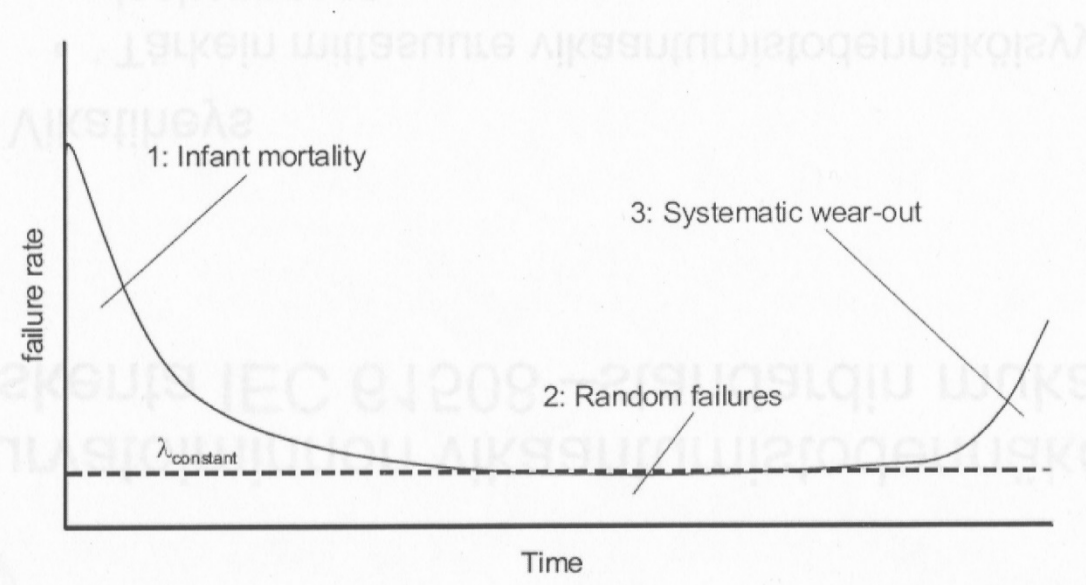
Keskimääräisen vaarallisen vikaantumisajan määritelmä (keskiarvottaminen): ”Keskimääräinen vaarallinen vikaantumisaika (*Mean Time To dangerous Failure*, $MTTF_d$) on keskimääräinen odotettavissa oleva aika vaarallisen vikaantumisen esiintymiseen (ISO 13849-1 kohta 3.1.25)”

Tämä määritelmä on sovellus luotettavuuden (*reliability*) määritelmästä.

Esimerkki: Seuraavilla esimerkeillä havainnollistetaan luotettavuustekniikan käsitteitä.

Todennäköisyys (*probability*) kuvaa tapahtuman esiintymismahdollisuutta lukuarvolla, joka on arvojen 1 ja 0 välissä: lukuarvo 1 tarkoittaa, että kyseinen ilmiö toteutuu aina ja lukuarvo 0 tarkoittaa, että ilmiö ei toteudu koskaan. Kaikki reaalimaailman ilmiöt ovat tällä välialueella. Teknisen järjestelmän jokainen fyysinen komponentti vikaantuu, jos vain aikaa kuluu riittävästi, joten komponentti vikaantuu todennäköisyydellä 1. Siten pelkkää todennäköisyyttä ei voi käyttää teknisten järjestelmien arvioinnissa, vaan on käytettävä käsitettä ”luotettavuus (*reliability*)”, joka tässä yhteydessä tarkoittaa keskimääräistä vaarallisen vikaantumisen todennäköisyyttä aikayksikössä MTTFd.

Tasaisella vikatiheydellä vikaantumisen mahdollisuus (todennäköisyys) on joka hetki yhtä suuri eli myös keskimääräinen vikaantumisaika on vakio. Tässä standardoidussa menetelmässä käytetään komponenttien tilastollisilla menetelmillä (B_{10d}-arvot) ja käyttökokemuksilla saatuja tietoja komponenttien epäluotettavuudesta (ISO 13849-2 luvut 4.3 ja 4.4).



Time = aika, failure rate = vikaantumistiheys, $\lambda_{constant} = \lambda_{vakio}$

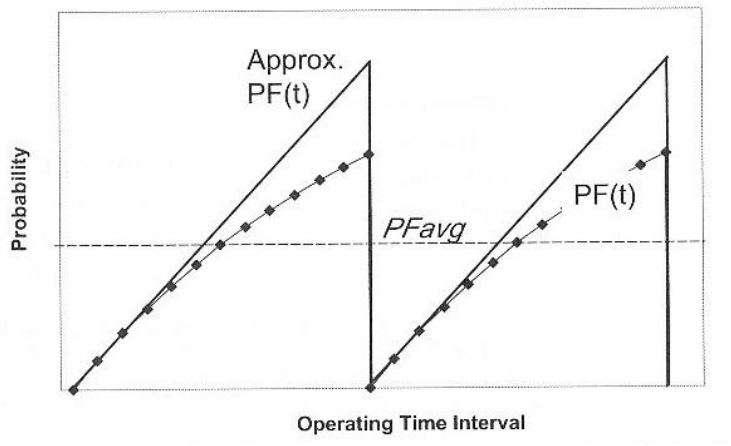
1. Infant mortality = Alkuajan vaaralliset vikaantumiset
2. Random failures = Satunaisvikaantumiset
3. Systematic wear-out = Systemaattiset kulumisvikaantumiset

Kuva 6 Komponentin epäluotettavuus käyttöajan funktiona (”kylpyammekäyrä”)

Tasaisella vikatiheydellä komponentin epäluotettavuus (epäluotettavuus = 1 − luotettavuus) on aluksi pieni ja kasvaa loppua kohden. Yksinkertaisuuden vuoksi oletetaan, että turvatoiminnon vikatiheys on vakio, eli riski sen menettämisestä pysyy samana koneen koko käyttöiän aikana. Tämä on perustelua, sillä useimmilla komponenteilla on niiden alkuvaiheessa todettujen ”lastentauti-vaiheen” jälkeen suhteellisen tasainen vikatiheys, joka alkaa kasvaa voimakkaammin vasta komponentin käyttöiän loppuvaiheessa (kuva 11).

Havainnollistamiseksi esimerkkinä lento-onnettomuuteen joutumisesta:

1. Mitä useammin matkustaa lentokoneella, sitä suuremmaksi käy todennäköisyys joutumisesta lento-onnettomuuteen (esim. n tapausta/1 000 000 lentoa).
2. Yksittäistapauksessa eli astuttaessa lentokoneeseen, lento-onnettomuuteen joutumisen todennäköisyys on joka kerta suunnilleen sama ja yhtä suuri kaikille matkustajille riippumatta heidän aikaisemmista lennoista eli edelleen n tapausta/1 000 000 lentoa (luku pienenee vähitellen, jos lentoturvallisuutta parannetaan).



Probability = todennäköisyys

Approx. PF(t) = vikaantumistodennäköisyyden likiarvo ajan suhteen

PFavg = vikaantumistodennäköisyyden keskiarvo

Operating Time Interval = Määräaikaistestausten välinen aika

Kuva 7 Vaarallisen vikaantumisen todennäköisyys pysyy tasaisella vikatiheydellä *PFavg* vakiona, mutta epäluotettavuus PF kasvaa ajan t kuluessa. Määräaikaistestauksella voidaan järjestelmä palauttaa lähelle alkuperäistä tilaa.

Erilaisten komponenttien ja niiden vikamuotojen vikaantumisajat vaihtelevat suuresti. Siten vikaantumisaikojen määrittäminen komponenttityypeille tai myös yksittäisille komponenteille on epävarmaa. Samasta syystä turvatoimintoa ei voi jättää ainoastaan luotettavaksi arvioitujen komponenttien varaan.

Standardisoiduilla menetelmillä vaarallinen vikaantumisaika voidaan kuitenkin arvioida tai laskea riittävän tarkasti suoritustason PL a…e määrittämiseksi. Tavallisesti koneen valmistaja hankkii tarvittavat komponentit ja saa niiden dokumentaation mukana komponentin vikaantumistiedot. Muussa tapauksessa koneen valmistajan on käytettävä muita tietolähteitä.

Esimerkiksi jos seurataan 100 komponentin vikaantumista ja todetaan, että niistä 10 vuodessa on vikaantunut 10 komponenttia, mutta vain yksi niistä 1 on vikaantunut vaarallisesti, $MTTF_d$ on keskimäärin suunnilleen 0,1 vuotta.

Tilaa vaihtavilla komponenttityypeillä (esim. anturi, rele, kytkin, kontaktori yms.) keskimääräinen vaarallinen vikaantumisaika voidaan määrittää testaamalla niitä siten, että kuormitetaan suurta määrää komponentteja niin kauan kunnes niistä 10 % on vaarallisesti vikaantunut. Tähän kulunut aika kerrotaan kymmenellä, jolloin saadaan keskimääräinen vaarallinen vikaantumisaika B10d. Koska vikaantumisajat ovat hyvin pitkiä tai tilavaihtoja tarvitaan tavallisesti vähintään useita satoja tuhansia, useimmiten käytetään likimääräisiä nopeutettuja testejä.

Keskimääräinen vaarallinen vikaantumisaika $MTTF_d$ arvioidaan tilaa vaihtaville komponentille testauksessa saadun tilavaihtojen lukumäärän $B10_d$ avulla. $B10_d$ tarkoittaa sitä tilavaihtojen lukumäärää, joka saadaan koepenkissä, kun 10 % komponenteista on vikaantunut vaarallisesti ja testaus lopetetaan eli sadasta komponentista 10 on vikaantunut vaarallisesti.

Komponentille arvioidaan komponentin tilavaihtojen kokonaislukumäärä Nop-lukuarvo (*Number of operations*, Nop) koneelle määritetyn elinkaaren aikana (esim. 20 vuotta), ja standardissa esitettävillä yksinkertaisilla laskukaavoilla saadaan komponentin keskimääräinen vaarallinen vikaantumisaika (standardin ISO 13849-1 liite C.4.2 mekaanisille, sähkömekaanisille ja pneumaattisille komponenteille).

Esimerkki Nop-lukuarvon laskennasta:

Esimerkki: (Standardin ISO 13849-1 liite C.4.2) Komponentti on käytössä 220 vuorokautta vuodessa, 16 tuntia työpäivässä ja tilanvaihto tapahtuu kerran viidessä sekunnissa. Komponentin valmistaja on määrittänyt komponentin kestävän keskimäärin 60 miljoonaa tilanvaihtoa. Kolmannen kaavan jakaja 0,1 tulee siitä, kun koepenkissä odotettiin 10 komponentin vikaantumista vaarallisesti ja tässä tapauksessa ensimmäinen riittää koko toiminnon vikaantumiseen.

$$n_{\mathrm{op}} = \frac{220\ \mathrm{T/J} \times 16\ \mathrm{h/T} \times 3600\ \mathrm{s/h}}{5\ \mathrm{s/jakso}} = 2{,}53 \times 10^{6}\ jaksoa/vuosi$$

$$T_{10\mathrm{d}} = \frac{60 \times 10^{6}\ jaksoa}{2{,}53 \times 10^{6}\ jaksoa/\mathrm{vuosi}} = 23{,}7\ vuotta$$

$$\mathrm{MTTF_d} = \frac{23{,}7\ vuotta}{0{,}1} = 237\ vuotta$$

Saavutetun suoritustason PL arviointimenetelmässä turvatoiminnan arviointi tehdään komponenttien keskimääräisen vaarallisen vikaantumisaika $MTTF_d$ hierarkian mukaan alhaalta ylöspäin. Laskennassa oletetaan, että vikataajuus on vakio (”kylpyammekäyrän” keskialue, kuva 11). Jos koko lohkon $MTTF_d$ -arvoa ei tunneta, laskenta tehdään kyseiseen elementtiin kuuluvien elementtien $MTTF_d$ -arvojen yhteenlaskulla.

Standardin ISO 13849-1 liitteessä D.1 esitetään ”osien laskentaan perustuva menetelmä”. Yksinkertaisessa menetelmässä tunnistetaan kaikki esim. lohkon elementit ja elementtien MTTFd-arvot lasketaan yhteen käänteislukuina ja summa käännetään takaisin käänteisluvuksi koko lohkon $MTTF_d$-arvoksi. Tämän menetelmän virhemarginaali on turvallisempaan suuntaan, koska siinä ei oteta huomioon kanavarakennetta eikä diagnostiikkaa, jotka parantaisivat tilannetta

Esimerkki: Lohkon elementtien tai yksittäisen kanavan MTTFd -arvojen yhteenlasku:

- kaikki yhteenlaskettavat $MTTF_d$ -arvot käännetään vastaluvuiksi yhtälöllä $\lambda_d = 1/MTTF_d$, jossa (lamda d, *dangerous*) λ_d = vaarallisen vikaantumisen taajuus (epäluotettavuus)
- nämä taajuudet lasketaan yhteen ja saadaan λ_{dtot}
- saatu summa käännetään takaisinpäin vastaluvuksi käänteisellä yhtälöllä $MTTF_{dtot} = 1/\lambda_{dtot}$, jossa tot = summa (total).

On huomattava, että komponenttien keskimääräistä vaarallista vikaantumisaikaa mitataan $MTTF_d$-arvoilla, mutta turvatoiminnon sekä sitä toteuttavien alajärjestelmien suoritustasoa PFHd-arvoilla (standardissa ISO 61508 tämä merkitään nykyisin PFH), jolla mitataan, kuinka usein turvatoiminto menetetään. Vaikka molemmat mittaavat vikaantumista aikayksikköä kohden eli vikataajuutta, toisin kuin komponenttien osalta PFH_d-arvoilla mitataan paitsi komponenttien vikaantumisia, siinä

otetaan huomioon myös rinnakkaisen kanavarakenteen ja diagnostiikan osuus vikaantumisten taajuuden pienentämisessä.

Rajoituksia $MTTF_d$-arvojen määrittelyssä (30 % kohta 4.5.2 taulukko 4):

- alajärjestelmiin eivät kelpaa komponentit, joiden $MTTF_d$-arvot, jotka ovat alle kolme vuotta (vuoden kuluttua 30 % näistä komponenteista olisi vikaantuneita)
- kanavan $MTTF_d$-arvoa yli 100 vuotta ei hyväksytä, koska suurien riskien yhteydessä turvallisuuteen liittyvät ohjausjärjestelmän osat eivät saa riippua yksinomaan komponenttien luotettavuudesta.

Komponentin vaarallisen keskimääräisen vikaantumisajan tietolähteiden käytössä on seuraava ensisijaisuusjärjestys:

1. Käytetään valmistajan antamia tietoja. Valmistajan antamat tiedot ovat muita vaihtoehtoja tarkemmat, koska ne koskevat valmistajan itsensä valmistamia ja testaamia komponentteja tai laitteita. Ohjausjärjestelmien suunnittelijoiden on syytä vaatia komponenttien ja laitteiden toimittajilta tietoja komponenttien luotettavuudesta ja ominaisuuksista.
2. Käytetään julkisia tietokantoja, esim. internet. Standardin ISO 13849-1 kohdassa ”Kirjallisuus” on viitteet kahdeksaan erilaiseen tietokantaan.
3. Käytetään standardin ISO 13849-1 liitteissä C ja D esitettäviä likiarvoja. Niitä voidaan käyttää ainoana tietolähteenä vain matalan riskitason tapauksissa. Muutoinkin niitä tulkittava vain suuntaa-antavina eikä niitä ei ole syytä käyttää ilman tarkempaa arviointia komponentin ominaisuuksista ja soveltuvuudesta kyseisen turvatoiminnan toteutukseen.
4. Valitaan komponentin $MTTF_d$-arvoksi 10 vuotta. Tällöin oletetaan, että kyseessä on yleisesti käytetty standardisoitu teollisuuskomponentti. Tämä karkea arvio on mahdollista vain yksinkertaisissa järjestelmissä, joissa turvatoimintojen suoritusvaatimukset ovat vähäisiä.

4.3.2 Systemaattisesti vikaantuvat komponentit

Monien erityyppisten komponenttien vikaantumiset eivät ole satunnaisia, vaan niiden vikaantumiset ovat systemaattisia. Näitä ovat monet hydrauliset, pneumaattiset ja mekaaniset komponentit, mutta myös määrätyt sähköiset (ei-elektroniset) komponentit (osa 4 luvut 6 ja 7). Niiden pääasiallinen vikaantuminen voi johtua esimerkiksi kulumisesta, jolloin hyvällä rakenteella ja harvalla käyttötaajuudella keskimääräiset vikaantumisajat voivat nousta useisiin satoihin tai satoja tai jopa tuhansiin vuosiin.

Nämä tapaukset eivät sovellu käsiteltäväksi standardien mukaisilla suoritustason tai turvallisuuden eheyden tason menetelmillä. Nämä komponentit ovat yksinkertaisempia ja niiden luotettavuutta on helpompi arvioida kuin elektronisten komponenttien satunnaisvikaantumisia. Tämän vuoksi tämän tyyppisiä komponentteja käsitellään standardissa ISO 13849-1 erikseen ohjaustoiminnon tulo- ja lähtöyksiköiden toteutuksissa.

Systemaattisia vikaantumisia ei käsitellä todennäköisyyslaskennan (tilastollisilla) menetelmillä, vaan systemaattisten vikaantumisten estämisen rakenteellisilla menetelmillä. Luvussa 6 käsitellään

näiden komponenttien luotettavuuden parantamista paremmalla laadunhallinnalla ja rakenteellisilla menetelmillä.

Pääasiallisesti systemaattisesti vikaantuvia komponentteja käytetään turvatarkoituksiin esimerkiksi

- sellaisissa turvallisuuteen liittyvissä toiminnoissa, joita ohjataan sähköisillä, hydraulisilla, pneumaattisilla tai mekaanisilla osilla, mutta joissa ei ole elektronisia ohjaussignaaleja käsitteleviä yksiköitä kuten esim. logiikkayksiköitä (esimerkiksi hätäpysäytys pysäytystoiminnoilla 0 ja 1 (IEC 60201-1)
- osana ohjausjärjestelmän turvatoimintoa, joka toteutetaan elektronisilla ohjaussignaaleilla, (esimerkiksi hätäpysäytys pysäytystoiminnoilla 2 (IEC 60201-1) taajuusmuuttajan turvatoiminnoilla
- vikaturvallisuudella ja vikojen poissulkemisella varmistetuissa ohjaustoiminnoissa
- diagnostiikka- ym. vikaantumisen paljastumista lisäävissä toiminnoissa.

Huom. Elektroniset komponentit mukaan lukien kiinteästi ohjelmoidut logiikkayksiköt kuuluvat satunnaisesti vikaantuviin komponentteihin.

4.3.3 Turvatoiminnon tulojen ja lähtöjen yksinkertaistettu arviointi

Jos mekaanisille, hydraulisille ja pneumaattisille komponenteille on käytettävissä luotettavuustiedot, näiden komponenttien käyttöä turvatoiminnoissa voidaan arvioida ilman $MTTF_d$-laskentaa. Tällöin arviointi perustuu vain nimettyihin rakenteisiin, diagnostiikkaan ja yhteisvikaantumisten estämiseen (kuva 13).

	PFH_D (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	2*10-5	●	○	○	○	○
PL b	5*10-6	●	○	○	○	○
PL c	1,7*10-6	-	●2*	●1*	○	○
PL d	2,9*10-7	-	-	-	●1*	○
PL e	4,7*10-8	-	-	-	-	●1*
●	Applied category is recommended					
○	Applied category is optional					
-	Category is not allowed					

Kuva 8 Turvatoimintoa toteuttavien systemaattisesti vikaantuvien alajärjestelmien suoritustason arviointi tulo- ja lähtöyksikköjen tarkastelu taulukon avulla (ISO 13846-1: 2015 kohta 6.3 taulukko 7).

Vaatimuksia:

- PL-tasoissa a ja b on käytettävä hyvin koeteltuja komponentteja ja turvallisuuden perusperiaatteita.
- PL-tasolla c luokassa 1 määritetään käytössä T_{10d}-arvot, jotka perustuvat käytössä hyviksi todettuihin tietoihin (ks. seuraava luku)
- PL-tasolla c luokassa 2 testauskanavan $MTTF_d$-arvon on oltava vähintään 10 vuotta.
- PL-tasolla d luokassa 3 on käytettävä hyvin koeteltuja komponentteja ja turvallisuusperiaatteita.
- PL-tasolla e luokassa 4 on käytettävä hyvin koeteltuja komponentteja ja turvallisuusperiaatteita.

Luokissa 2…4 on tehtävä yhteisvikaantumisten estämisen toimenpiteet ja tarkastettava onko DC-arvo riittävä (matala tai keskimääräinen luokissa 2 ja 3 ja korkea luokassa 4)

Tällöin DC_{avg}-arvo voidaan laskemalla kaikkien komponenttien DC-arvojen aritmeettisena keskiarvona.

4.3.4 Turvakomponentit

Konedirektiivin tarkoittamilla turvakomponenteilla tarkoitetaan konedirektiivin liitteessä V lueteltuja tai niitä vastaavia koneen turvallisuuden varmistamiseksi tarkoitettuja turvallisuuteen liittyviä komponentteja, jotka kuuluvat soveltuvin osin konedirektiivin soveltamisalaan vaikka ne eivät ole koneita. Niiden vaatimustenmukaisuus on osoitettava samalla tavalla kuin varsinaisten koneiden.

Tätä ei pidä sekoittaa konedirektiivin liitteessä IV lueteltuihin koneisiin ja turvakomponentteihin, joille on tehtävä EU-tyyppitarkastus (konedirektiivin liite IX) ns. ilmoitetussa laitoksessa (Notified Body). Tämä vaatimus EU-tyyppitarkastuksesta koskee koneiden lisäksi kuitenkin myös muutamia em. liitteessä V mainittuja komponenttityyppejä, joille on tehtävä EY-tyyppitarkastus ns. ilmoitetussa laitoksessa (Notified Body, konedirektiivin liite XI). Näitä komponentteja ovat mm. määrätyt elektroniset turvasignaalin siirtokomponentit (esim. logiikkayksiköt), kaksinkäsinkäyttölaitteen logiikkayksikkö ja valosähköiset turvalaitteet).

4.3.5 Hyvin koetellut komponentit

Nimettyjen luokkien B, 1, 2 ,3 ja 4 vaatimuksissa on kohtia, jotka turvatoiminnon toteuttamisessa on otettava huomioon. Näitä ovat (ISO 13849-1 taulukko 10)

- luokka B, suurin saavutettava PL on b: Turvallisuuteen liittyvien osien on oltava asiaan kuuluvien standardien mukaisia ja kelpuutus on tehtävä noudattamalla sovellusta vastaavia turvallisuuden perusperiaatteita (*basic safety principles*).
- luokka 1, suurin saavutettava PL on c: luokan B vaatimusten lisäksi on noudatettava koeteltuja turvallisuusperiaatteita (*well-tried design principles*) ja on käytettävä hyvin koeteltuja komponentteja (*well-tried components*)
- luokka 2, suurin saavutettava PL on d: luokan B vaatimusten lisäksi on noudatettava hyvin koeteltuja turvallisuusperiaatteita (*well-tried design principles*)
- luokka 3, suurin saavutettava PL on d: luokan B vaatimusten lisäksi on noudatettava hyvin koeteltuja turvallisuusperiaatteita (*well-tried design principles*)
- luokka 4, suurin saavutettava PL on e: luokan B vaatimusten lisäksi on noudatettava hyvin koeteltuja turvallisuusperiaatteita (*well-tried design principles*)

Tämän lisäksi kaikissa luokissa on useita erityisvaatimuksia.

Hyvin koetellut komponentit luokassa 1 perustuvat hyvin koeteltujen turvallisuusperiaatteiden soveltamiseen ja/tai komponenttia koskeviin standardeihin. Hyvin koeteltu komponentti tietylle sovellukselle ei välttämättä sovi toisenlaiselle sovellukselle.

Hyvin koeteltu komponentti on ”*käytössä koeteltu: elementin tietyn konfiguraation käyttökokemukseen perustuva osoitus siitä, että vaarallisten systemaattisten vikojen todennäköisyys on tarpeeksi pieni, jotta jokainen kyseessä oleva elementtiä käyttävä turvatoiminto saavuttaa sen vaadittavan suoritustason (PLr) (lähde ISO 13849-1 kohta 3.1.39 ja 61508-4 kohta 3.8.18*”).

Standardin ISO 13849-2 liitteissä on esimerkkejä erityyppisillä teknologioilla toteutetuista tuvallisuuden perusperiaatteista, hyvin koetelluista turvallisuusperiaatteista, hyvin koetelluista komponenteista ja vikojen poissulkemisesta ja jokaisessa kohdassa luetellaan komponenttikohtaisia käytännön esimerkkejä vaatimusten täyttämisestä.

A. Mekaaniset komponentit:

Taulukoissa esitetään konkreettisia esimerkkejä:

- taulukko A.1: turvallisuuden perusperiaatteet
- taulukossa A.2: hyvin koetellut turvallisuusperiaatteet
- taulukossa A.3: hyvin koetellut komponentit
- taulukoissa A.4 ja A.5: vikojen poissulkeminen

B. Pneumaattiset komponentit:

- taulukko B.1: turvallisuuden perusperiaatteet
- taulukossa B.2: hyvin koetellut turvallisuusperiaatteet
- taulukoissa B.3…B.18: vikojen poissulkeminen

C. Hydrauliset komponentit:

- taulukko C.1: turvallisuuden perusperiaatteet
- taulukossa C.2: hyvin koetellut turvallisuusperiaatteet
- taulukossa C.3: hyvin koetellut komponentit
- taulukoissa C.4 ja C.12: vikojen poissulkeminen

D. Sähköiset komponentit

- taulukko D.1: turvallisuuden perusperiaatteet
- taulukossa D.2: hyvin koetellut turvallisuusperiaatteet
- taulukossa D.3: hyvin koetellut komponentit
- taulukoissa D.4 ja D.21: vikojen poissulkeminen.

Huom. Elektronisia komponentteja ei ole hyväksytty näihin luetteloihin.

Vikojen poissulkeminen

- vikojen poissulkeminen voi perustua vikojen esiintymisen tekniseen epätodennäköisyyteen
- yleiseen sovelluksesta riippumattomaan tekniseen kokemukseen
- sovelluksen ja sen erityisiin vaaroihin liittyviin teknisiin vaatimuksiin.

4.3.6 Turvakomponentit vs. standardikomponentit

Näin ollen muitakin kuin turvakomponentiksi nimettyjä tavallisia komponentteja voidaan käyttää myös turvatarkoituksiin edellyttäen, että saavutetaan riittävä turvallisuustaso ja konedirektiivin vaatimustenmukaisuus voidaan osoittaa.

Turvallisuuteen liittyvät vaatimukset koskevat komponentin rakennetta, toimintaa, testauksia ja soveltuvuutta määritettyihin käyttötarkoituksiin ja ympäristöolosuhteisiin (systemaattiset vikaantumiset, osa 4 luku 7). Muissakin tavallisissa eli standardikomponenteissa on erilaisia ja eritasoisia turvallisuuteen liittyviä ominaisuuksia, joten määrätyillä rajoituksilla voidaan myös ns. standardikomponentteja käyttää turvatarkoituksiin, mutta tässäkin tapauksessa on osoitettava, että saavutetaan tarvittava turvallisuustaso mukaan lukien vaadittava PL-taso.

Tarkempia tietoja standardikomponenttien käytöstä turvatarkoituksiin esitetään IFA:n [Kirjallisuutta] julkaisussa. Sen mukaan tarvittavan turvallisuustason saavuttamiseksi on tarkasteltava sitä arkkitehtuuria (nimettyjen rakenteiden luokat), jossa standardikomponentti tai -komponentteja on osana. Tässä on otettava huomioon (diagnostiikka) vaarallisten vikojen paljastuminen ja niiden taajuus/todennäköisyys. Yleisesti ottaen monimutkaisten elementtien (rakenneosien) tai alajärjestelmien tapauksessa riittävää systemaattista eheyttä ei kuitenkaan voida osoittaa ja siten standardikomponenttien käyttö näissä tapauksissa on poissuljettu.

Standardin ISO 13849-1 osassa 2 esitetään toiminallisen turvallisuuden saavuttamisen kelpuutus todennäköisyyksiin nojautuvalla menetelmällä. Jos koneen tai ohjausjärjestelmän valmistaja käyttää standardikomponentteja turvallisuuteen liittyvässä ohjausjärjestelmässä, tämän on tarkistettava standardikomponentin osalta samat vaatimukset kuin mitä turvakomponentin valmistaja on jo tehnyt valmistamalleen turvakomponentille.

Standardikomponentin kelpoisuuden tarkistaminen

- Turvallisuuteen liittyvät perusperiaatteet ja hyvin koetellut periaatteet (kohta 4.3.2 ja 4.3.5)
- Arkkitehtuurin valinta (nimetty rakenne, luokka, Cat. (kohta 4.2)
- Vikaantumissieto yksittäiselle vikaantumiselle (kohta 4.3.5)
- $MTTF_d$- ja DC-arvojen määrittäminen (kohdat 4.3 ja 4.5)
- Yhteisvikaantumisten arviointi (CCF, kohta 4.6)
- Systemaattiseen vikaantumiseen johtavien ympäristöolosuhteiden arviointi (ISO 13849-2 kohta 10)
- PL-tason arviointi (kohta 4.8)
- Ohjelmistovaatimukset (osa 4 luku 10)
- Dokumentaatiovaatimukset (osa 4 luku 13)
- ym.

Käytännössä voi olla ylivoimaista osoittaa, että tavallinen eli standardikomponentti täyttää kyseistä sovellusta koskevat turvallisuusvaatimukset yhtä hyvin kuin turvakomponenttien valmistaja, joka on huolehtinut turvallisuusvaatimusten täyttämisestä tuotekehityksen alusta alkaen ja tehnyt vaadittavat testaukset. usein standardikomponenteista ei ole saatavilla tarpeellisia tietoja, joiden perusteella voitaisiin arvioida sen soveltuvuus turvallisuustarkoituksiin.

Myös kahdennettujen kanavien tapauksessa yhteisvikaantumiset voivat mitätöidä hyväksi lasketun tai arvioidun turvallisuustason (PL-tasot d ja e). Tähän liittyy ohjelmistovirheet ja niiden virheiden vaikutusten estäminen kahdennettujen ohjelmistojen erillisyydellä (*diversity*, kohta 9.3 ja 9.6).

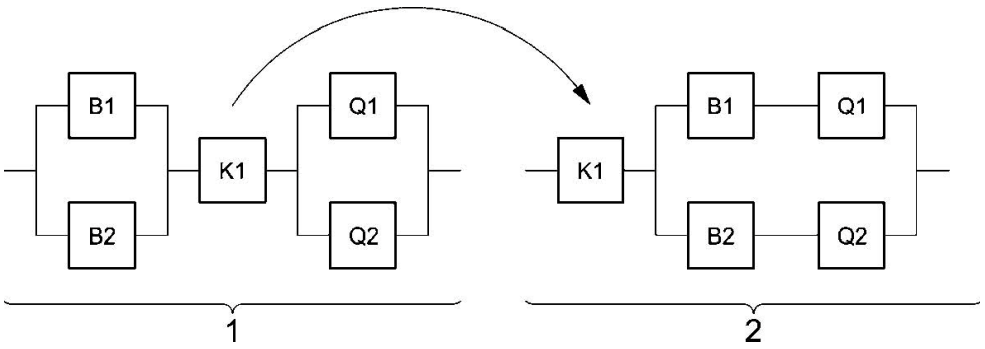
4.4 Kanavat turvatoiminnon rakenneosina

Jos rinnakkaisten kanavien $MTTF_d$-arvot eroavat toisistaan, tarvitaan kanavien ”symmetrisointia” ja siinä on kolme vaihtoehtoa:

1. Pahimman tapauksen oletuksen mukaan otetaan huonompi arvo molemmille kanaville.
2. Jos rinnakkaisilla kanavilla on samat $MTTF_d$-arvot, se tulee molempien kanavien yhteiseksi arvoksi.
3. Käytetään standardin ISO 13849-1 liitteessä D.2 esitettävää symmetrisoinnin yhtälöä, josta saadulla $MTTF_d$-arvolla voidaan korvata molempien kanavien $MTTF_d$-arvo yhdellä yhteisellä arvolla, joka on molempien kanavien $MTTF_d$-arvojen välissä.

Turvallisuuteen liittyvän ohjausjärjestelmän osan (alajärjestelmän) $MTTF_d$-arvo riippuu sen kanavarakenteesta (nimetyt rakenteet, luokat B, 1, 2, 3, ja 4).

Standardin ISO 13849-1 liitteessä H esitetään esimerkki kanavien yhdistelmän ”sieventämisestä”.



Kuva 9 Kanavajärjestelmän yksinkertaistaminen sieventämällä (ISO/DTR 23849-1 kuva 3)

Yhden kanavan alajärjestelmä voi olla vikasietoinen yhdelle vikaantumiselle (ks. IFAn keittokirja no.4). Tämä toteutuu, jos

- kaikki satunnaisvikaantumiset johtavat alajärjestelmän turvalliseen tilaan tai
- voidaan oikeuttaa (*justify*) vikojen poissulkeminen niiden erittäin pienen $MTTF_d$-arvon perusteella.

Tällöin ei myöskään tehdä diagnostiikan arviointia.

> **Esimerkki:** hätäpysäytyslaitteille, jotka ovat hätäpysytyslaiteen rakennetta ja toimintaa koskevan standardin IEC 60947-5-5 mukaisia ja joita ei käytetä muutoin kuin hätätilanteessa (standardin ISO 13849-2 taulukko D.8 ja BGIA Report 2/2008e, Section D2.5) a joiden systemaattiset vikaantumiset on muutoinkin minimoitu, ei tavallisesti tehdä suorituskyvyn arviointia. Hätäpysäytystoiminnon vaateen taajuus on useimmiten pieni, koska koneen aiheuttamia hätätilanteita saa syntyä mahdollisimman harvoin. Tällöin myös hätäpysäytystoiminnon suoritustason vaatimus PLr on matala. Varmuuden vuoksi standardissa ISO 13849-1 esitetään hätäpysäytystoiminnalle vaadittavaksi suoritustasoksi vähintään PL c.

Muille kanavarakenteille (ainakin luokissa 2, 3 ja 4) tehdään diagnostiikan kattavuuden arviointi ja sitä käytetään PL-tason arvioinnissa. Jokaiselle taulukon 1 alajärjestelmälle suurin sallittu $MTTF_d$-arvo on 100 vuotta.

Taulukko 2 Jokaisen kanavan keskimäärinen vaarallinen vikaantumisaika $MTTF_d$

Jokaisen kanavan merkintä	**Jokaisen kanavan vaihteluväli**
Matala	3 vuotta ≤ $MTTF_d$ ≤ 10 vuotta
Keskimääräinen	10 vuotta ≤ $MTTF_d$ ≤ 30 vuotta
Korkea	30 vuotta ≤ $MTTF_d$ ≤ 100 vuotta

Huom. Jos luokassa 4 on enemmän kuin 3 alajärjestelmää, suurin sallittu $MTTF_d$-arvo jokaiselle kanavalle on nostettu arvoon 2500 vuotta.

4.5 Diagnostiikan kattavuuden DC_{avg} arviointi

Tässä yhteydessä käsitellään koneen ohjausjärjestelmän satunnaisvikaantumisia, jotka voivat johtaa koneen virhetoimintoihin ja siten henkilö- ja esinevahinkoihin. Koska kaikkia vikaantumisia

ei voida kokonaan estää ainoastaan komponenttien luotettavuutta parantamalla, pyritään diagnostiikan kattavuutta parantamalla pienentämään myös muun tyyppisten vikaantumisten esiintymistä (esim. tuotantoprosessin hallintaan liittyviä vikaantumisia). Tämä voidaan tehdä vikadiagnostiikalla (ISO 13849-1 kohta 4.5.3 ja liite E), joka perustuu testauskanaviin ja logiikan omiin valvontatoimintoihin.

Diagnostiikan tehokkuutta mitataan diagnostiikan kattavuudella, jolla ilmaistaan kuinka monta prosenttia diagnostiikkamenetelmillä havaituista satunnaisten vaarallisten vikaantumisten taajuuksista saadaan paljastettua suhteessa kaikkiin satunnaisten vaarallisten vikaantumisten taajuuksiin (kuva 15). Myös ohjelmistolle tarvitaan sen oman toiminnan valvontaa (diagnostiikka, ISO 13849-1 liite J), mutta siinä on kyseessä systemaattisten vikaantumisten pienentämisestä eikä satunnaisvikaantumisten hallinta.

Jos koneen luotettavuus on huono, toistuvat pysäytykset vähentävät käyttövarmuutta (käytettävyyttä). Diagnostiikalla parannetaan luotettavuutta ja samalla myös käyttövarmuutta, jos diagnostiikan havaitessa virheen järjestelmä pysäytetään turvalliseen tilaan, ja ryhdytään korjaaviin toimenpiteisiin ennen kuin sattuu suurempaa vahinkoa ihmisille tai koneille, laitteille tai joissakin tapauksissa myös valmistettavalle työkappaleelle.

Diagnostiikka kohdistuu komponentin (Sistemassa elementti, lohko, kanava, alajärjestelmä) vikaantumisten paljastamiseen. Ylimmällä turvatoiminnan tasolla luotettavuutta arvioidaan vain turvatoiminnon menettämisen taajuudella.

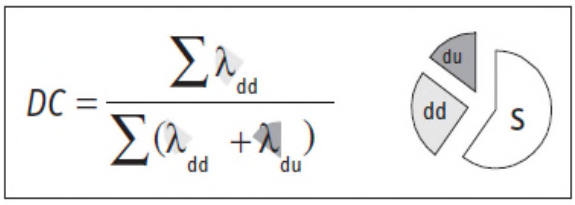
Pelkästään hyvillä komponenteilla päästää vain suoritustasoille a ja b systemaattisten vikaantumisten estämisen toimenpiteillä. Sen sijaan korkeammille suoritustasoille PL c, d ja e päästään, muiden turvallistamistoimenpiteiden lisäksi, soveltamalla diagnostiikkamenetelmiä. Turvallisuuteen liittyvässä järjestelmässä voi olla valmiina erilaista valvontaa ja diagnostiikkaa, mm. koneen käyttötoimintoihin tai prosessiin liittyvää valvontaa, joka voi paljastaa myös satunnaisvikaantumisia ja tämä voi samalla lisätä myös turvallisuutta.

Diagnostiikan kattavuutta voidaan arvioida esimerkiksi standardin IEC 60812 (vika- ja vaikutusanalyysi, *Failure Mode and Effect Analysis*, FMEA) avulla. Tavallisiin konesovelluksiin riittää yksinkertaistettu lähestymistapa diagnostiikan kattavuuden arvioimiseksi (standardin ISO 13849-1 liite E), jossa esitetään tyypillisille turvallisuuteen liittyville ohjausjärjestelmän osille ja komponenteille soveltuvia diagnostiikan kattavuuden arviointimenetelmiä.

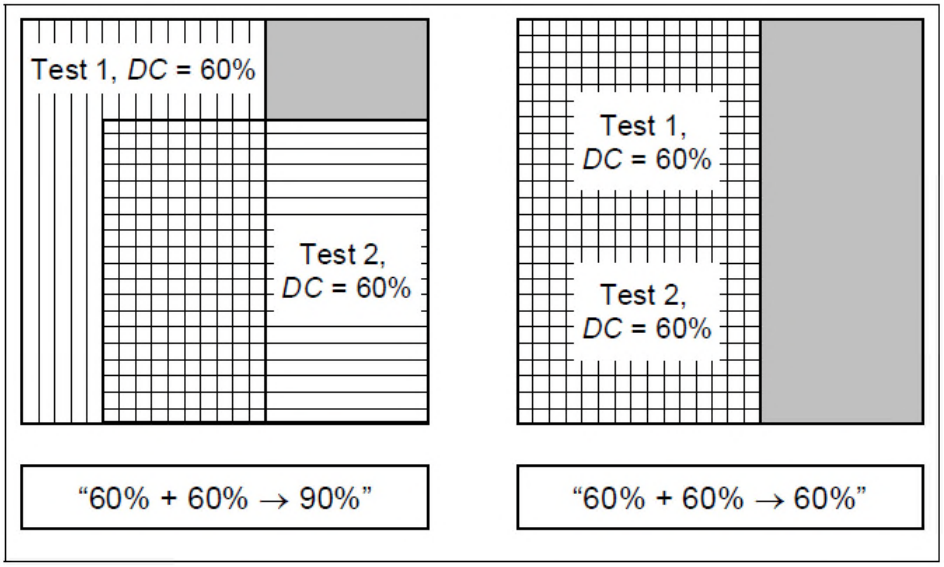
Diagnostiikan kattavuuden määritelmä:

”*Diagnostiikan kattavuus (Diagnostic Coverage, DC) on diagnostiikan tehokkuuden mitta, joka voidaan määrittää paljastuneiden vaarallisten vikaantumisten vikaantumistaajuuden ja kaikkien vaarallisten vikaantumisten vikaantumistaajuuden suhteena*” (standardin 13849-1 kohta 3.1.26).

Diagnostiikan kattavuus lasketaan vaarallisten vikaantumisten (λ_{DD}) suhteena kaikkiin vaarallisiin vikaantumisiin (λ_D).



Kuva 10 Diagnostiikan kattavuuden laskenta (BGIA Report 2/2008e, kuva E.1, [IFA])
DC = Diagnostiikan kattavuus (*Diagnostic Coverage*)
λ_{DD} = paljastuvien vaarallisten vikojen taajuus (DD = *Frequency of Dangerous Detected Faults*)
λ_{DU} = paljastumattomien vaarallisten vikaantumisten taajuus (DU = *Frequency of Dangerous Undetected Faults*)
S= turvalliset vikaantumiset (*Frequency of Safe faul*ts)



Kuva 11 Useamman diagnostiikkamenetelmän yhteensovittaminen: diagnostiikkamenetelmät voivat olla toisensa poissulkevia, toisiaan täydentäviä tai, kuten tässä kuvassa, toisiaan osittain täydentäviä (BGIA Report 2/2008e, kuva E.2 (Sistema: [IFA]). Tämä arviointi on tehtävä FMEA-menetelmällä (esim. IEC 61508-6)

Diagnostiikan kattavuus DC jaetaan yksinkertaisuuden vuoksi karkeasti neljään ryhmään (taulukko 2).

Keskimääräinen diagnostiikan kattavuus arvioidaan paljastuneiden vaarallisten vikaantumisten vikaantumistaajuuden ja kaikkien vaarallisten vikaantumisten vikaantumistaajuuden suhteena. Siten alajärjestelmän diagnostiikan keskimääräinen kattavuus DC_{avg} saadaan arvioitua sen kaikille turvallisuuteen liittyville rakenneosille määritettyjen diagnostiikan kattavuuksien DC avulla seuraavalla yhtälöllä :

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

Yhtälö pidentää erikseen jokaisen rakenneosan (komponentin) vikaantumisaikaa $MTTF_D$ diagnostiikan kattavuuden kertoimella DC.

Taulukko 3 Yksinkertaistettu arviointimenetelmä: Diagnostiikan keskimääräinen kattavuus DC_{avg} (standardin ISO 13849-1 taulukko 5)

Diagnostiikan keskimääräinen kattavuus DC_{avg}	
Nolla	DC < 60 %
Matala	60 % ≤ DC < 90 %
Keskitaso	90 % ≤ DC < 99 %
Korkea	99 % ≤ DC

Oletuksia diagnostiikan kattavuuden tasojen määrittämiselle yksinkertaistetussa arviointimenetelmässä:

- Diagnostiikan käsittelyssä käytetään logaritmityyppistä asteikkoa keskimääräisen paljastettujen vaarallisten vikojen λ_{dd} suhteessa kaikkiin vaarallisiin vikaantumisiin λ_d.
- Useasta osasta koostuvan turvallisuuteen liittyvän alajärjestelmän diagnostiikan kattavuudelle DC arvioidaan keskimääräinen diagnostiikan kattavuus DC_{avg}.
- Diagnostiikan kattavuuden DC_{avg}-arvoa 60 % pienemmällä arvolla on vain vähäinen merkitys testatun järjestelmän luotettavuuteen ja siksi sitä käsitellään arvona ”nolla”. DC_{avg}-arvoa 99 % suurempaa arvoa on hyvin vaikea saavuttaa monimutkaisissa järjestelmissä.

Lisävaatimuksia:

- Luokassa 2 (yksikanavainen valvottu rakenne) testauskanavan vaarallisen keskimäärisen vikaantumisajan on oltava suurempi kuin puolet (toiminnallisen) kanavan keskimääräisestä vaarallisesta vikaantumisajasta ($MTTF_{d,TE} > 0{,}5 \times MTTF_d$).
- Luokassa 2 turvatoiminnon vaateen on oltava pienempi kuin 1/100 testaustaajuudesta, mutta jos luokan 2 vaadetaajuus on pienempi tai yhtä suuri kuin 1/25 testaustaajuus (ks. ISO 13849-1:2015 kohta 4.5.4 ja liite K). Pahimman tapauksen arviointiin voidaan käyttää taulukossa K.1 luokassa 2 lueteltavia PFH_D -arvoja kerrottuna tekijällä 1,1.ö
- Testaus voi tapahtua juuri ennen turvatoiminnon vaadetta ja saada kone turvalliseen tilaan, jos koneen vaarallisen liikkeen pysähtymisaika on lyhyempi kuin henkilön aika ulottua vaarakohtaan (turvalaitteiden vähimmäisetäisyys ISO 13855).
- Luokassa 4 (PL e) useamman kuin kolmen alajärjestelmän tapauksessa jokaisen alajärjestelmän paras $MTTF_d$-arvo voi olla 2500 vuotta (ISO 13849-1 kohta 4.5.2).

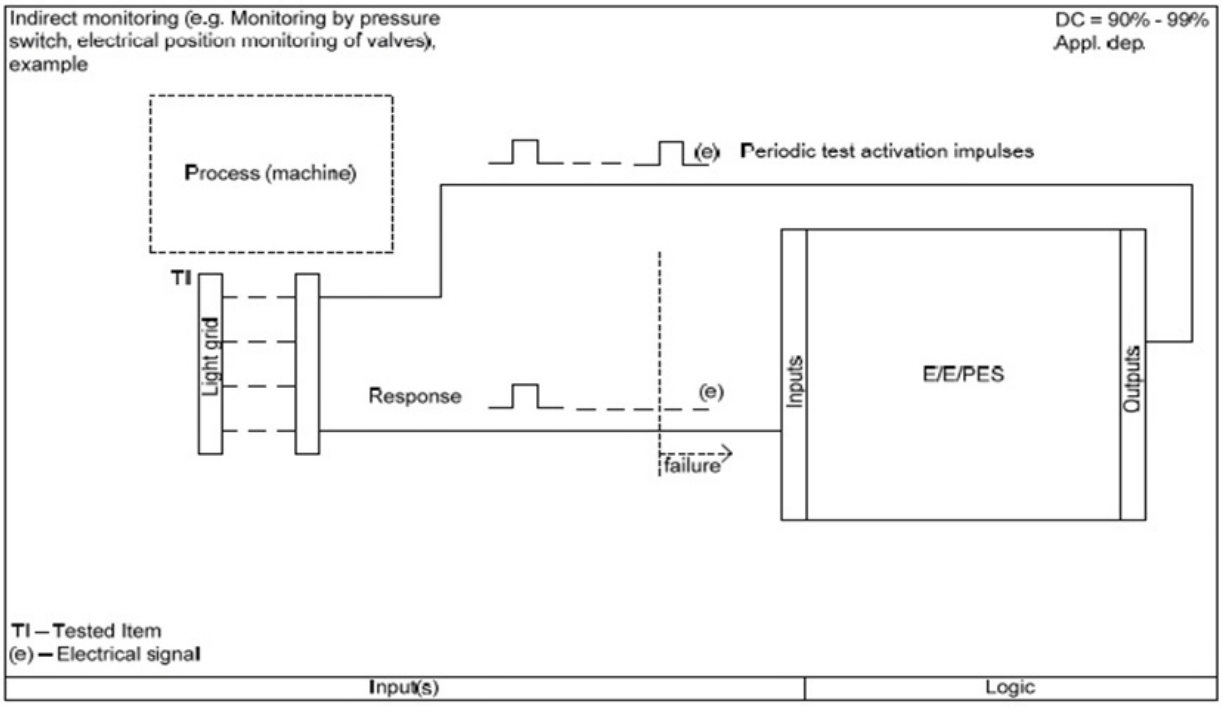
Vikaantumisen paljastuminen voidaan tehdä esimerkiksi automaattisella toimintojen valvonnoilla tai erikseen lisätyillä vikaantumisen (tai ohjelmistovirheen) havaitsemisen menetelmillä, esim.:

- testauskanavan testaussignaalin avulla
- kahden rinnakkaisen kanavan (jatkuvassa tuotannossa myös kahden rinnakkaisen koneen tai koneyhdistelmän) ristiinvalvonnan avulla (ks. IFAn raportit)

- prosessista saatavien tietojen avulla (esim. IoT)
- ohjelmiston toiminnan diagnostiikalla (esim. Watch-dog).

Esimerkkejä diagnostiikan toteuttamisesta (ISO 13949-1 taulukko E.1).

1. Suojuksen asemaa vaihtavan signaalin luotettavuustestaus
2. Tulosignaalien valvonta ilman dynaamista testausta
3. Tulosignaalien valvonta dynaamisen testauksen kanssa
4. Tulosignaalien ristiinvalvonta ja välitulokset
5. **Epäsuoravalvonta (kuva 12)**
6. Suora testaus
7. Vikaantumisten havaitseminen prosessitiedoista
8. Anturitoiminnan valvonta
9. Yksinkertainen ajan valvonta
10. Ajan ja logiikan valvonta
11. Testauslaitteen vasteajan valvonta
12. Yhden kanavan lähtötietojen valvonta ilman dynaamista testausta
13. Lähtötietojen ristiin valvonta ilman dynaamista testausta
14. Redundanttinen sulkukanava ilman toimilaitteen valvontaa
15. Redundanttinen sulkupolku yhden toimilaitteen valvonnan kanssa
16. Redundanttinen sulkupolku molempien toimilaitteiden valvonnan kanssa



Kuva 12 Esimerkki epäsuorasta valvonnasta, diagnostiikan menetelmä no. 5. Viitteessä [Johan Hedberg] esitetään vastaavat havainnollistavat toimintakaaviot myös muista diagnostiikan menetelmistä

Diagnostiikan kattavuus voidaan tehdä esim. FMEA-tarkastelun osana käsittelemällä komponenttien vaarallisia vikaantumisia (osa 4 luku 7) ja ottamalla huomioon myös kahden (tai useamman) toisistaan riippumattoman vian yhdistelmien tapauksia. Tämä voidaan tehdä tietokoneavusteisella ohjelmistotyökalulla.

Diagnostiikan arviointia varten voidaan tarvita myös yksinkertaisimpien komponenttien eli elementtien $MTTF_d$-arvot (liite 1 Sistema). Esimerkiksi hätäpysäytyslaitteen elementeille vaaditaan standardien mukainen rakenne, ne on asennettava ohjeiden mukaan ja vain niille sopivaan käyttötarkoitukseen, jolloin on otettava huomioon myös mahdolliset rajoitukset (esim. ympäristöolosuhteet kuten EMC, lämpötilat, tärinä jne., osa 4 kohta 7.2).

Sisteman-työkalu voi $MTTF_d$-arvojen laskennan rinnalla laskea samalla jokaiselle turvatoimintoa toteuttavalle osalle/alajärjestelmälle diagnostiikan kattavuuden arvon alhaalta ylöspäin alajärjestelmän lohkojen ja niiden muodostaman kanavan DC-arvojen avulla.

4.6 Yhteisvikaantumisen arviointi (CCF)

Yhteisvikaantumisen määritelmä: ”*Yhteisvikaantuminen (Common Cause Failure, CCF) on yksittäisestä tapahtumasta johtuva eri kohteiden vikaantuminen, jossa yksittäiset viat eivät ole toistensa seurauksia*” (standardin 13849-1 kohta 3.1.6 ja liite F).

Yhteisvikaantuminen tarkoittaa sitä, että redundanttiset kanavat vikaantuvat samasta syystä, eikä sitä, että kanavat vikaantuvat eri tavoilla samanaikaisesti. Yhteisvikaantumisten arviointi voidaan tehdä kvalitatiivisesti tunnistamalla kaikki vaaralliset vikaantumiset ja tutkimalla mitkä niistä voivat esiintyä samasta syystä (ISO 13849-1 liite F).

Yhteisvikaantuminen koskee vain redundanttisia järjestelmiä, joissa laitteistoredundanssi on tavallisesti tehty rinnakkaisilla (kahdennetuilla) kanavilla. Nimetyissä rakenteissa tämä tarkoittaa luokkia 2, 3 ja 4. Luokassa 2 toinen kanava on diagnostiikkakanava, jolloin turvatoiminnon menettäminen havaitaan, mutta sen tehokkuus riippuu diagnostiikan taajuudesta (kohta 4.5). Elektroniikassa ohjelmallinen redundanssi voi olla yhdessä signaalikanavassa, jossa redundanssi on toteutettu signaalin lisävarmistuksilla (esim. ”turvaväylät”).

Standardissa (ISO 13849-1 liite F) käytetään yksinkertaista pisteytysmenetelmää (taulukko F.1). Se perustuu painotettuihin kysymyksiin, jotka koskevat yhteisvikaantumisten estämiseksi käytettävien menetelmien toteutusta. Kysymysten painoarvoina annetut pisteet kuvaavat toimenpiteiden merkitystä yhteisvikaantumisten vähentämisessä. Tärkeimpiä toimenpiteitä ovat erilaisuuden (divergenssi) käyttäminen ja erityisesti EMC-häiriöiden hallinta. Saatujen yhteispisteiden perusteella arvioidaan, ovatko toteutettavat yhteisvikaantumisen menetelmät riittäviä.

Taulukko 4 Yksinkertaistettu arviointimenetelmä: Yhteisvikaantumisen kriteerien otsikot, standardissa ISO 13849-1 (liite F) ja IEC 62061 (x liite F) on tarkempi erittely yhteisvikaantumisista.

Luokissa 2,3 ja 4 yhteisvikojen vähimmäispistemäärä on 65.
Pisteiden maksimiarvo on 100:

Kriteerit	Pisteet
–Erottelu	15 p.
–Diversiteetti	20 p.
–Suunnittelu	15 p.
–Koetellut komponentit	5 p.
–FMEA	5 p.
–Ammattitaito	5 p.
–Ympäristöolosuhteet (EMC)	25 p.
–Muut	10 p.

Yhteisvikaantumisen menetelmien katsotaan olevan riittäviä luokissa 2,3 ja 4, jos saavutetaan vähintään 65 pistettä sadasta. Jos tätä ei saavuteta, ei myöskään voida saavuttaa korkeampia kaksikanavaisia suoritustasoja PL d ja e.

4.7 Turvatoiminnon saavuttaman suoritustason PL arviointi

Ohjausjärjestelmästandardeissa on samat taulukot, joissa on määritetty turvatoiminnon vaarallisten vikaantumisten suurimmat sallitut taajuudet jokaiselle vaadittavalle PLr-ja SIL-tasolle. Niiden avulla tarkistetaan turvatoiminnon saavuttaman PL-tason riittävyys.

Huom. Mitä korkeampi on turvatoimintoon liittyvä riski, sitä pienempi on vaadittavaa suoritustasoa PLr vastaava PFH_d-enimmäisarvo, joka asettaa rajan sille, kuinka usein enintään turvatoiminnon PL saa menettää.

Toisin sanoen jokaisen turvatoiminnon saavuttaman suoritustason PFH_d on oltava pienempi tai korkeintaan yhtä suuri kuin taulukossa 5 esitettävä vaadittavaa suoritustasoa PLr vastaava enimmäistaajuuden PFH_d-arvo. Sistema tekee tämän arvioinnin automaattisesti syöttötietojen avulla.

Taulukko 5 Turvatoiminnon (saavuttamat) suoritustasot PL (perustuu standardin ISO 13849-1 kohdan 4.2.2 taulukkoon 2).

Huom. <u>Taulukossa esitettäviä vikaantumistaajuuksia turvatoiminto ei saa ylittää!</u>

PL	SIl (TL.,	Vaarallisen vikaantumisen todennäköisyys (tuntia kohden) PFH_d
a	-	$10^{-5} \leq PFH_d < 10^{-4}$
b	1	$3 \cdot 10^{-6} \leq PFH_d < 10^{-5}$
c	1	$10^{-6} \leq PFH_d < 3 \cdot 10^{-6}$
d	2	$10^{-7} \leq PFH_d < 10^{-6}$
e	3	$10^{-8} \leq PFH_d < 10^{-7}$

Tavallisesti kuten taulukossa 5 riskien suuruuden ja taajuuksien käsittelyssä käytetään logaritmisia kymmenen kertaluokkien asteikkoja: 1, 10, 100, 1000, 10000 jne.

Standardissa IEC 62061 on vastaava taulukko SIL-tasoille. Konesovelluksiin keskeisesti kuuluva taso, joka vastaa tasoa SIL 1, on jaettu konesovelluksissa tarkemman arvioinnin saavuttamiseksi kahteen suoritustasoon PL b ja c.

SIL- ja PL-tasojen todennäköisyydet perustuvat lähtökohtaan, että työpaikoilla ei sallita enempää kuin keskimäärin kymmenesosa teollistuneissa maissa keskimäärin sattuvien työtapaturmien taajuudesta eli karkeasti arvioiden työtunnit työpaikalla olisivat työtapaturmien osalta noin 10 kertaa turvallisemmat kuin ihmisen elämässä keskimäärin (*As Low As Reasonably Practicable, ALARP*).

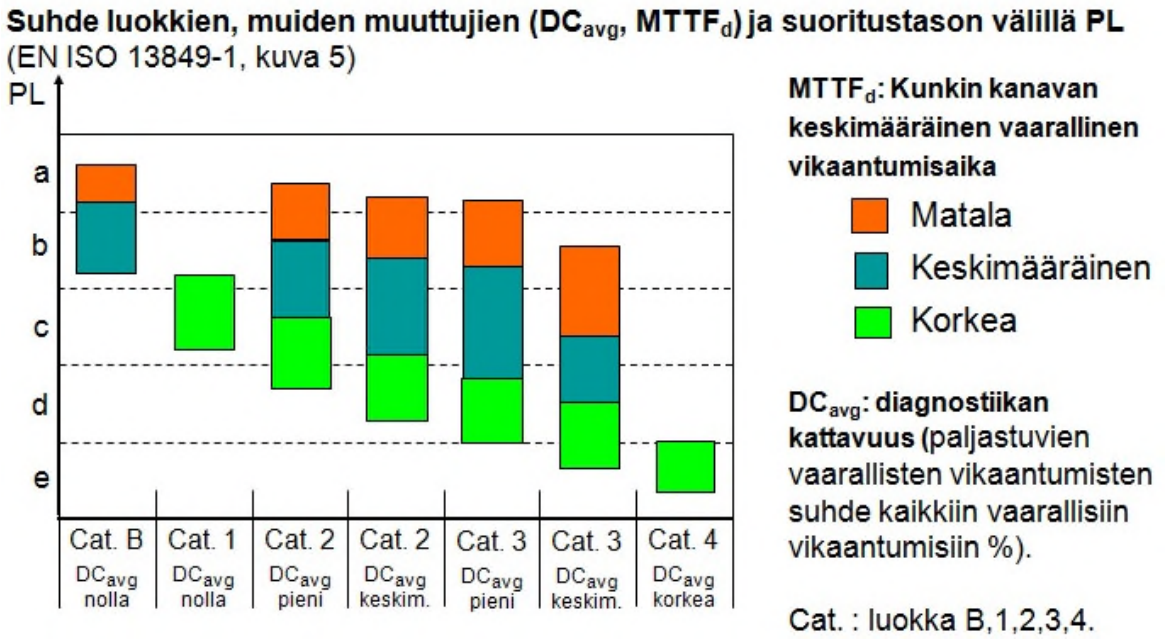
Standardissa ISO 13849-1 esitettävän yksinkertaisen menetelmän mukaan ohjausjärjestelmän turvallisuuteen liittyvän alajärjestelmän saavuttama suoritustaso PL määritetään ohjausjärjestelmän jokaisen turvallisuuteen liittyvän osan (SRP/CS) eli alajärjestelmän (SB) suoritustaso PL määritetään edellä kuvattujen nimettyjen rakenteiden ja niihin liittyvien muuttujien avulla.

1. alajärjestelmän nimetty rakenne: luokat B, 1, 2, 3 tai 4
2. alajärjestelmän komponenttien keskimääräisen vaarallisen vikaantumisajan ($MTTF_d$) arvot luokissa B, 1, 2, 3 ja 4: matala, keskitaso tai korkea
3. keskimääräisen diagnostiikan kattavuuden (DC_{avg}) arvot luokissa 1, 2, 3 ja 4: matala, keskitaso tai korkea
4. yhteisvikaantuminen (CCF): saavutetaanko 65 % pisteistä luokissa 2, 3 ja 4?

Näiden arvojen yhdistelmän avulla saadaan suoraan alajärjestelmän suoritustaso PL joko

a) graafisesti pylväsdiagrammin avulla (kuva 13)

b) taulukosta (ISO 13849-1 taulukko 2)
c) numeerisesti (ISO 13849-1 liite K) tai
d) tietokoneavusteisesti (liite 1, Sistema: [IFA]).



Kuva 13 Yksinkertaistettu menettelytapa alajärjestelmien saavuttaman suoritustason määrittämiseksi (ISO 13849-1 kuva 5)

Pylväsdiagrammissa (kuva 13) alajärjestelmien (SB) saavuttamat suoritustasot PL erilaisille parametriyhdistelmille (luokat) on laskettu muuttujien (edellä muuttujat 1…4) alkuarvojen yhdistelmistä Markovin ketjuilla. Diagrammi antaa suunnittelijalle joustavuutta erilaisiin vaihtoehtoihin, mikä helpottaa parametrien eri yhdistelmien valintaa vaadittavan suoritustason saavuttamiseksi. Koska saavutetun suoritustason PL määrittämisessä muuttujien avulla on lukuisia epävarmuustekijöitä, kaikki arviointivaiheet on tehtävä huolellisesti ja seurattava valintojen tuomien tulosten mielekkyyttä. Rajatapauksissa on valinta tehtävä turvallisempaan suuntaan, jos ei saada lisää näyttöä paremmasta vaihtoehdosta. Myös laskuvirheitä on huolellisesti vältettävä (esim. negatiivisten potenssien muuttaminen likiarvoiksi tai päinvastoin).

Pylväsdiagrammissa lähtökohtana saavutetun suoritustason PL määrittämiseen on $MTTF_d$-alueiden keskipisteet. Näistä pisteistä voidaan liikkua jonkin verran ylös- tai alaspäin kyseisellä $MTTF_d$-alueella riippuen riskin arvioinnin tarkkuudesta ja käytettyjen komponenttitietojen luotettavuudesta ym. Arkkitehtuurin rajoitukset on kuitenkin otettava huomioon eli erittäin hyvälläkään $MTTF_d$-arvolla ei voida ilman redundanssia (kahdennuksia)päästä korkeimmille suoritustasoille (PL d ja e).

Standardin ISO 13849-1 liitteen K taulukoiden avulla saadaan tarkempi tulos. Taulukoissa esitetään Markovin ketjuilla laskettujen suoritustasojen PL tarkat lukuarvot. Alajärjestelmän nimetyn rakenteen luokan, $MTTF_d$-arvon, DC_{avg}-arvon ja CCF:n avulla parametri ”vaarallisen vikaantumisen todennäköisyys tuntia kohden”, PFH_d (*Probability of Failure per Hour dangerous*) ilmaisee kyseisen alajärjestelmän suoritustason PL.

4.8 Suoritustason PL määrittäminen alajärjestelmien avulla

Kun kaikki turvatoimintoa toteuttavien alajärjestelmien saavuttamat PL-tasot on saatu määritettyä, voidaan määrittää turvatoiminnon saavuttama PL-taso yhdistämällä sarjamuodossa olevien alajärjestelmien PL-tasot koko turvatoiminnon yhteiseksi PL-tasoksi (ISO 13849-1 kohta 6.3). Tämä tehdään karkeasti siten, että valitaan turvatoiminnolle yksinkertaisesti alimman alajärjestelmän suoritustaso PL. Turvatoiminnan suoritustaso voi kuitenkin olla kertaluokkaa alempi, jos sarjamuotoisessa rakenteessa on useita samalla alimmalla suoritustasolla olevia alajärjestelmiä (taulukko 6, ISO 13849-1 taulukko 11).

Taulukko 6 Alajärjestelmien yhdistäminen turvatoiminnon PL-tason määrittämiseksi (standardi ISO 13849-1 Taulukko 11)

Suoritustason (PL) laskeminen sarjaan kytketyille turvallisuuteen liittyvien ohjausjärjestelmän osien kokonaisuuksille

HUOMAUTUS: Tähän taulukoon lasketut arvot perustuvat varmuusarvoihin kunkin suoritustason keskipisteessä

PL_{low}	N_{low}	⇒	PL
a	>3	⇒	Ei sallittu
	≤3	⇒	a
b	>2	⇒	a
	≤2	⇒	b
c	>2	⇒	b
	≤2	⇒	c
d	>3	⇒	c
	≤3	⇒	d
e	>3	⇒	d
	≤3	⇒	e

Tarkempi suoritustaso PL saadaan laskemalla alajärjestelmien PFH_d-arvot liitteestä K (ISO 13849-1 liite K), laskemalla ne yhteen ja vertaamalla lopputulosta taulukon 5 eri suoritustasojen raja-arvoihin.

4.9 Turvatoiminnon hyväksyminen ja todentaminen

Turvatoiminnon saavuttama suoritustaso merkitään seuraavasti ”ISO 13849-1:2015 PL c”. Alajärjestelmän suoritustasoon merkitään myös sen luokka: esim. ”ISO 13849-1:2015 luokka 3 PL d”

Turvatoimintojen todentamisessa tarkistetaan, että turvatoiminnot täyttävät kaikki niitä koskevat turvallisuusvaatimukset eli niiden oikean toiminnan ja luotettavuuden vaatimukset. Todentaminen dokumentoidaan ja se on osana koko ohjausjärjestelmän todentamista, mikä on edelleen osana koko koneen kelpuutusta (osa 4 luku 11). Lopuksi turvatoiminto hyväksytään, jos saavutettu suoritustaso PL on vähintään yhtä korkea kuin turvatoiminnalta vaadittava suoritustaso PLr (kohdat 4.8 ja 4.9).

Standardin IEC 62061 mukaisessa menetelmässä saavutettavat SIL-tasot ja niiden yhdistäminen koko turvatoiminnon SIL-tasoksi lasketaan erikseen luotettavuuslaskennan kaavoilla ja menetelmillä ja lopuksi tarkistetaan, että saavutettu SIL ≥ vaadittava SIL.

Jos saavutettu suoritustaso ei ole riittävä, kyseisellä alajärjestelmien yhdistelmällä ei saavuteta vaadittavaa PLr-tasoa. Tällöin on palattava standardin ISO 13849-1 suunnitteluprosessin vaiheiden sopivaan lähtökohtaan ja on käytävä uudelleen läpi sitä seuraavat suunnitteluvaiheet.

Tällöin joku/jotkut tai kaikki alajärjestelmät on suunniteltava uudelleen eli on valittava parempia arkkitehtuureja ja/tai parempia komponentteja ja/tai kattavampaa diagnostiikkaa. Myös yhteisvikaantumisen ja systemaattisten vikaantumisten estämisen vaatimukset on tarkistettava. Tämä prosessi voidaan toistaa iteratiivisesti, kunnes saadaan kaikki vaatimukset täytettyä. Näitä turvatoimintojen riittävään suoritustasoon tähtääviä menetelmiä voi olla muun muassa:

- parempien osien tai komponenttien valinta: lisää luotettavuutta (käytössä koetellut komponentit, vikaturvalliset komponentit, vikojen poissulkeminen)
- parempi diagnostiikka: pienentää vikaantumistaajuutta (diagnostiikkakanava tai -laite)
- paremmin varmennetun rakenteen valinta: pienentää yhden vikaantumisen vaikutusta (redundanssi)
- yhteisvikaantumisten tehokkaampi estäminen: pienentää samasta syystä vikaantumisen taajuutta kahden kanavan arkkitehtuurissa (divergenssi)
- systemaattisten vikojen välttäminen (varmistukset, vikaturvallinen rakenne, vikojen poissulkeminen).

Sekaannusten ja virheiden välttämiseksi suositellaan turvatoiminnon suunnittelutyökalun käyttöä (liite 1, Sistema: [IFA]).

Turvallisuuskriittisten ohjelmistojen kehitystä käsitellään kohdassa 10.

5 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).

Koneiden ohjausjärjestelmien suunnittelun standardeja

- ISO 13849-1 (muutos tekeillä) Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat Osa 1: Yleiset suunnitteluperiaatteet (2015), Osa 2: Kelpuutus (2012)
- IEC 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset, 2018
- ISO 13850:2008 (uusittavana) Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet
- **SFS-EN ISO 12100:2010** Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen
- SFS-EN ISO 14119:2013 Koneturvallisuus, Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta

Sistema-työkalun soveltamisohjeita

Yleisesitys yksinkertaistetusta koneiden ohjausjärjestelmän turvallisuuden suunnittelumenetelmästä

- Hauke, M.; Schaefer, M.: Sicherheitsnorm (PDF, 3,3 MB) mit neuem Konzept. Revision der EN 954-1 (ISO 13849-1) vereinigt Kategorien mit Ausfallwahrscheinlichkeiten. O + P (2006) Nr. 3, S. 142-147.

Standardin 13849-1 soveltamisopas

- Functional safety of machine controls (BGIA Report 2/2008e) for the circuit examples of the Report (zip file): http://www.dguv.de/ifa/Publikationen/Reports-Download/BGIA-Reports-2007-bis-2008/BGIA-Report-2-2008/index-2.jsp

Yleisesitys Sistema-työkalun soveltamisesta

- Huelke, M.; Hauke, M.; Pilger, J.: Ein Tool zur einfachen Anwendung der Steuerungsnorm EN ISO 13849-1: SISTEMA (PDF, 849 kB). Software-Assistent SISTEMA -Safety Integrity Software Tool for the Evaluation of Machine Applications (A Tool for the Easy Application of the Control Standard EN ISO 13849-1): https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/sistema-kochbuecher/index.jsp

Sistema-työkalun käyttöohjeita (Cook books)

1. Toiminnallisesta piirikaavioista suoritustasoille – turvatoimintojen määrittäminen
   The SISTEMA Cookbook 1: From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA (PDF, 2.7 MB),
   Version 1.0 (EN)

2. Kirjastoverkon käyttö
   The SISTEMA Cookbook 2: Use of network libraries (PDF, 741 kB), Version 2.0 (EN)

3. Sistema-työkalun rinnakkaiskäyttö
   The SISTEMA Cookbook 3: Running several instances of SISTEMA in parallel (terminal server) (PDF, 675 kB)

4. Poikkeuksellisten arkkitehtuurien käsittely
   The SISTEMA Cookbook 4: When the designated architectures don't match (PDF, 648 kB), Version 1.0 (EN), and SISTEMA file with corresponding project examples (ZIP, 11 kB) (SSM file)

5. Esimerkki kirjasojen käytöstä
   The SISTEMA Cookbook 5: SISTEMA libraries (PDF, 2.2 MB), Version 2.0 (EN), and Example library (ZIP, 120 kB) (SLB)

6. Turvatoimintojen määrittely
   The SISTEMA Cookbook 6: Definitions of safety functions: What is important? (PDF, 1.0 MB), Version 1.0 (EN)

Liite 1 Koneen ohjausjärjestelmän yksinkertaistettu suunnittelumenetelmä Sistema

1 Sisteman esittely

Ohjausjärjestelmän suunnitteluun on kehitetty tietokoneavusteisia työkaluja helpottamaan suunnittelijoiden työtä. Standardin ISO 13849-1 pääasiallisen valmistelun tehnyt saksalainen työsuojelun tutkimuslaitos IFA (*Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung*, ent. BGIA) on kehittänyt ohjelmiston suunnittelumenetelmän Sistema auttamaan turvallisuuteen liittyvän ohjausjärjestelmän suunnittelua ja turvatoiminnon saavuttaman suoritustason PL arviointia. Myös useat muut ohjausjärjestelmien ja komponenttien valmistajat ovat julkaisseet vastaavia työkaluja (esim. SET/Siemens ja Pascal/Pilz).

SISTEMA-työkalun käytön edut

- Voidaan välttää suunnitteluvirheitä, koska suunnittelu tehdään vaihe kerrallaan ja siten voidaan varmistaa vaatimusten täyttyminen.
- Yhdenmukaisten käsitteiden käyttö vähentää väärinkäsityksiä ja karkeita virheitä.
- Yhdenmukaisten menetelmien käyttö lisää eri ratkaisujen vertailukelpoisuutta.
- Työkalun automaattisen laskennan avulla vältetään laskuvirheitä.
- Dokumenttien laadinta helpottuu.
- Vaatimustenmukaisuuden varmistaminen helpottuu niin asiakkaiden kuin viranomaistenkin suuntaan.

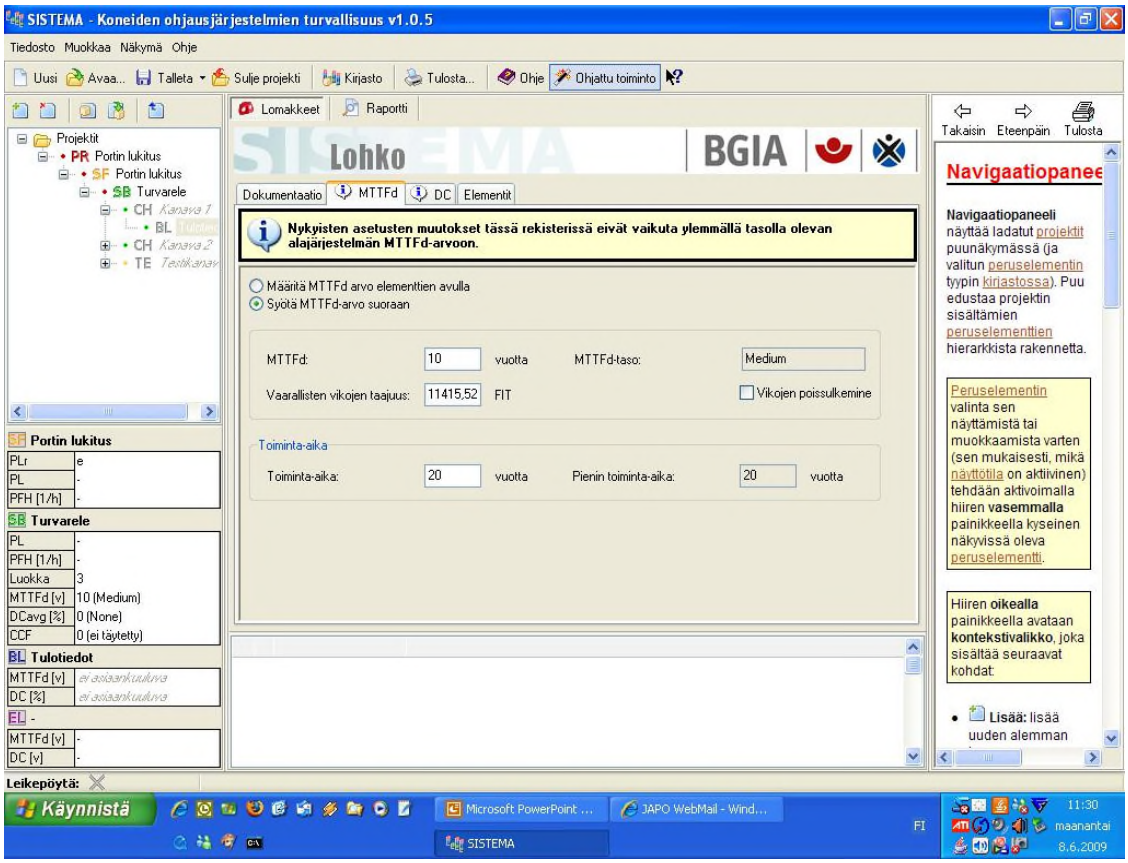
SISTEMAN avulla suunnitellaan ja samalla tarkistetaan, että turvatoiminnot toteuttavat vaadittavan suoritustason ja täyttävät turvallisuusvaatimukset. SISTEMA ohjaa myös ottamaan huomioon systemaattiset vikaantumiset. SISTEMAn päävaiheet perustuvat turvallisuuden elinkaaritarkasteluun.

Sisteman käyttö tukee järjestelmällistä suunnitteluprosessia ja nopeuttaa erilaisten vaihtoehtoisten ratkaisujen arviointia. Tietokoneavusteinen suunnittelutyökalu ei kuitenkaan korvaa ohjausjärjestelmän suunnitteluun tarvittavaa osaamista, vaan se on tarkoitettu tukemaan eri näkökohtien ja vaatimusten johdonmukaista läpikäymistä ja luotettavuusarvioiden tekemistä.

Jos Sistema-työkalua käyttää ilman perustietoja luotettavuustekniikasta, suunnittelija voi tehdä virheitä. Tätä varten elinkaaren turvallisuuden mallissa on elinkaaren vaiheiden välissä katselmukset, jossa toisen henkilön tai työryhmän työn tulokset on aina todennettava ennen siirtymistä turvallisuuden elinkaaren seuraavaan vaiheeseen.

IFA on laatinut ohjekirjan, jossa selostetaan luotettavuustekniikan perusteita, kuvataan SISTEMAn toimintaperiaatteet ja annetaan ohjeita ja useita esimerkkejä sen käytöstä (BGIA Report 2/2008e: [IFA]).

Sistemaa ylläpidetään ja sen toimintoja laajennetaan jatkuvasti. Sistema-työkalun käyttö edellyttää harjaantumista ja tutustumista Sisteman käyttöohjeisiin, joita voi ladata IFA:n verkkosivuilta. [Sisteman] voi ladata erikielisinä versioina, myös suomenkielisenä.



Sistema kuva 1. Turvallisuuteen liittyvän ohjausjärjestelmän suunnittelutyökalun Sistema päänäyttö: ylinnä päätoiminnot, vasemmalla yhäällä turvatoiminnon rakenne, keskellä työpöytä, oikealla aputoiminnot, vasemmalla alhaalla tulokset.

2 Sisteman rakenne

Lukujen 2, 3.2 ja 3.2 mukaisesti alajärjestelmän (*SubBlock*, SB) ja lohkon (*Block*, BL) toiminnalliset esitystavat ja niiden fyysiset toteutukset ovat seuraavat:

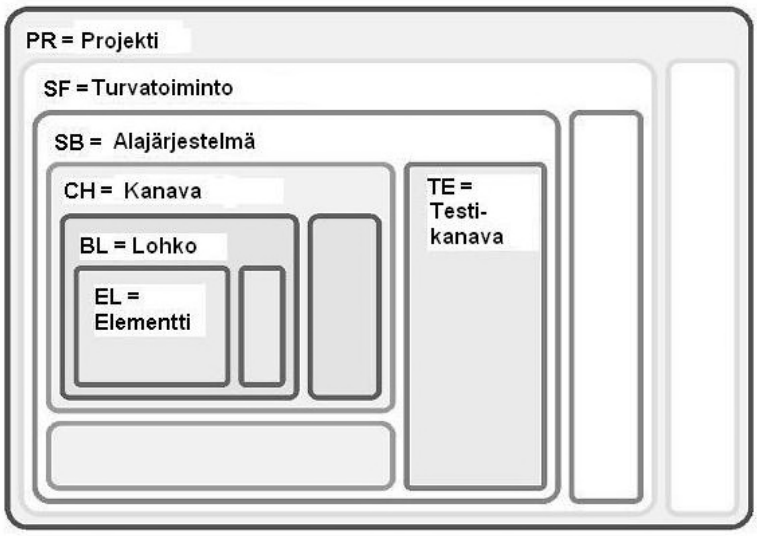
- Lohkot kuvaavat turvatoiminnon osien loogisia toimintoja
- lohko koostuu elementeistä (peruskomponenteista), jotka eivät muodosta järjestäytynyttä rakennetta.
- Alajärjestelmät kuvaavat turvatoiminnon sarjamuotoisen rakenteen erillisiä toiminnallisia yksikköjä
- alajärjestelmillä on turva- ja diagnostiikkasignaalien siirtokanavien määrätty nimetty rakenne (arkkitehtuuri).

Sisteman mukaisessa turvatoiminnon luotettavuuden arvioinnin (ja laskennan) menetelmässä tarvittavat parametrit:

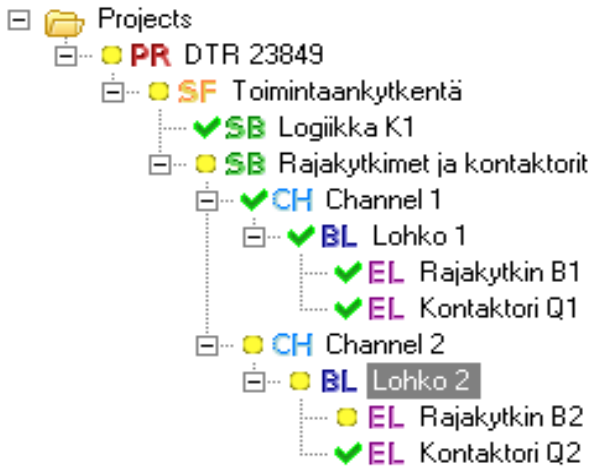
- $MTTF_d$ (*Mean Time To Failure, dangerous*)
- DC_{avg} (*Diagnostic Coverage, averige*)

- CCF (Common Cause Failure, dangerous)
- Luokka (*Category, Cat.*)
- sekä tiedot mahdollisista rajoituksista.

SISTEMAn yksinkertaistettu arviointimenetelmä perustuu eri tasoilla toimivien elementtien hierarkiaan (Sistema kuvat 2 ja 3).



Sistema kuva 2. SISTEMAn rakenneosien hierarkia. Suunnittelu lähtee ylimmältä tasolta alimmalle ja suoritustason laskenta alimmalta ylimmälle.



Sistema kuva 3. Sistema-työkalun ohjaustoiminnon suunnittelun hierarkkinen rakenne. Sisteman päänäytön kuva turvatoiminnon rakenteesta

Sistema kuvan 3 selitykset (ylhäältä alaspäin):

- Sisteman turvatoimintojen suunnitteluprojekti (*Project, PR*) koostuu turvallisuuteen liittyvistä toiminnoista
- turvatoiminto (Safety Function, SF) rakentuu ohjausjärjestelmän turvallisuuteen liittyvistä alajärjestelmistä, jotka muodostavat koko turvatoiminnalle sarjamuotoisen rakenteen

- alajärjestelmät (*Subsystem, SB*) muodostavat erityisen sisäisen arkkitehtuurin (nimetyn rakenteen eli luokan (kategorian, Cat.) B, 1, 2, 3 ja 4). Alajärjestelmät koostuvat kanavista.
- kanavat (*Channel*, CH) toteuttavat sarja- tai rinnakkaismuodossa loogisia toimintoja. Kanavat voivat olla toiminnallisia kanavia (esim. turvasignaalin siirto) ja testauskanavia (esim. vikailmoituksen siirto). Kanavat koostuvat lohkoista.
- lohkot (*Block, BL*) ovat kanavien loogisia yksikköjä. Lohkot koostuvat elementeistä.
- elementit (*Element, EL*) ovat lohkojen rakenneosia (esim. rajakytkimet, kontaktorit, taajuusmuuttajat), jotka eivät muodosta mitään keskinäistä rakennetta.

3 Turvallisuuteen liittyvän ohjausjärjestelmän rakenne ja suunnittelun vaiheet

Projektissa suunnittelu lähteen turvatoiminnon määrittämisestä edellä mainittuja tasoja (vaiheita) pitkin alaspäin. Sitä mukaa kuin käyttäjä tekee Sistemassa valintoja ja antaa parametrien arvoja, Sistema laskee automaattisesti syötettyjen tietojen perusteella ja näyttää sen hetkiset tulokset. Sistema ohjaa järjestelmällisesti prosessia alaspäin, pyytää jokaisessa vaiheessa tarvittavia tietoja ja esittää valinnoille vaihtoehtoja. Tämä tekee mahdolliseksi muuttaa tietoja ja seurata Sisteman antamia tuloksia. Näin suunnittelija voi kokeilla erilaisia vaihtoehtoja valitsemalla erilaisia nimettyjä arkkitehtuureja ja muuntelemalla niihin liitettävien komponenttien luotettavuuden ja diagnostiikan kattavuuden arvoja. Tulokset näkyvät välittömästi. Tällä tavoin voi helposti löytää suunnitelman heikoimmat kohdat ja ehdottaa niihin parannuksia.

Suunnittelu etenee vaiheittain alaspäin kunnes kaikki tarvittavat valinnat on tehty Sistemaan ja sinne on syötetty kaikki suoritustason PL määrittämiseen tarvittavat tiedot (kohta 4.8).

Suunnittelun/laskennan vaiheet:

1. Turvatoiminto sisältää alajärjestelmiä (kohta 4.8):
   - Turvatoiminnon saavuttama suoritustaso saadaan yhdistämällä alajärjestelmät sarjamuotoiseksi rakenteeksi joko Sisteman avulla, standardin ISO 13849-1 liitteen K avulla tai kuvan 6 graafin avulla. Turvatoiminnon PFH_d-arvo saadaan laskemalla alajärjestelmien PFH_d-arvot suoraan yhteen (ei käänteislukuja!). Turvatoiminnon vaarallisen vikaantumisen taajuudelle PFH_d on asetettu enimmäisarvo, jota ei saa ylittää (kohta 4.7 taulukko 5).
2. Alajärjestelmät sisältävät kanavia (kohta 4.4): Jokaisella alajärjestelmillä on jonkin nimetyn arkkitehtuurin mukainen kanavarakenne:
   - yksittäinen kanava ilman diagnostiikkaa (luokat B ja 1) tai diagnostiikan kanssa (luokka 2)
   - kahdennetut kanavat diagnostiikan kanssa ja yhteisvikaantumisten estämisen tarkistus (luokat 3 ja 4). Kahden kanavan tapauksessa kanavat yhdistetään yhdeksi kanavaksi todennäköisyyslaskennan kaavan avulla (symmetrisointi 4.4).

   Alajärjestelmän saavuttama suoritustaso PL arvioidaan kanavien $MTTF_d$-arvojen asemesta vaarallisen vikaantumisen todennäköisyydellä tuntia tai vuotta kohden (*Probability of Failure per Hour (year), dangerous,* PFH_d), koska alajärjestelmän vaarallisen vikaantumisen voi aiheuttaa monet muutkin syyt kuin komponentin vikaantuminen.
   - Kanavien $MTTF_d$ ja DC_{avg} -arvojen ja nimettyjen rakenteiden avulla voidaan laskea kunkin alajärjestelmän PFH_d-arvo. Luokissa 3 ja 4 on tarkistettava CCF (yhteisvikaantumisen estäminen).

Huom. Mitä <u>suurempi</u> $MTTF_d$, sitä parempi komponentti ja mitä <u>pienempi</u> PFH_d, sitä parempi alajärjestelmä tai turvatoiminto.

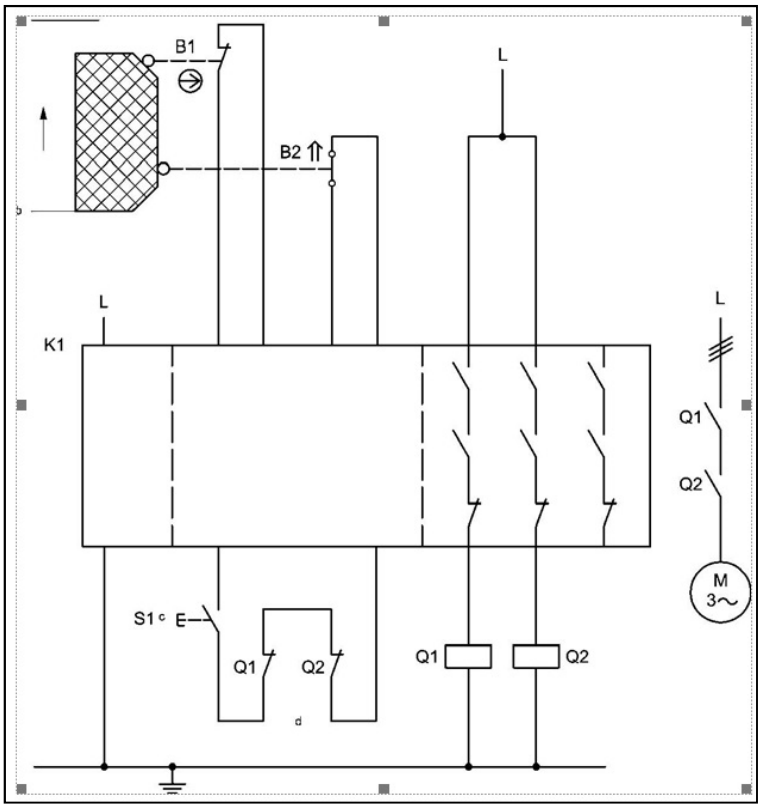
3. <u>Kanavat sisältävät lohkoja</u> (kohta 4.4):
   - Yksittäinen kanava sisältää lohkoja. Yksittäisten kanavien $MTTF_d$ -arvot saadaan laskemalla $MTTF_d$-arvon summa niiden käänteislukujen avulla ”osien laskentaan perustuvalla menetelmällä, kohta 4.3.1). Standardissa ISO 13849-1 kohdassa C.4.2 esitetään komponenttien testauksen tuloksena saadun B_{10}-arvon käyttöä turvatoiminnon suunnittelussa (myös Sistemassa voidaan käyttää komponenttien B10-arvoja).
   - Jos kanavan diagnostiikan kattavuutta DC_{avg}-arvoa ei tunneta, lasketaan tai arvioidaan kohdassa 4.5 esitettävillä diagnostiikan kattavuuden arvioinnin menetelmillä.
4. <u>Lohkot sisältävät elementtejä (kohta 4.3.1)</u>:
   - Lohko sisältää elementtejä. Jos <u>lohkon</u> $MTTF_d$-arvoa ei tunneta, se voidaan laskea elementtien $MTTF_d$-arvon summa niiden käänteislukujen avulla (osien laskentaan perustuva menetelmä, kohta 4.3.1).
   - Jos lohkon diagnostiikan kattavuutta DC_{avg} ei tunneta, se lasketaan tai arvioidaan osan 4 kohdassa 3.5 esitettävillä diagnostiikan kattavuuden arvioinnin menetelmillä.
5. <u>Elementit</u>:
   - Elementit eivät muodosta mitään rakennetta, niillä on vain keskimääräinen vaarallinen vikaantumisaika $MTTF_d$ (”epäluotettavuus”, kohta 4.3.1).

Esimerkki turvatoiminnon suoritustason PL määrittämisestä

Esimerkki: Turvalaitteen toimintaan kytkentä (standardin ISO 13849-1 soveltaminen, Draft Technical Raport DTR 23849)

Esimerkki on tarkoitettu havainnollistamaan standardin ISO 13849-1 mukaisten alajärjestelmien soveltamista ohjausjärjestelmän suoritustason arvioinnissa. Esimerkki perustuu turvatoimintoon: ”***avattavan suojalaitteen asennon valvonta***”, jolle on aikaisemmin määritetty riskin arvioinnin perusteella vaadittava suoritustaso PL_r e).

Suojus suojausasennossa (aktivoituna)



Liite 1 kuva 1 — Avattavan portin toimintaankytkentä turvayksikön (logiikka) avulla

Turvatoiminto

Turvatoimintona on turvallisuuteen liittyvä pysäytystoiminto, jonka käynnistää suojuksen avaaminen (nuolen suuntaan).

Toiminnallinen kuvaus

Liikkuvin koneenosien aiheuttama henkilövahingon riski on estetty avattavalla suojuksella. Suojuksen avaaminen tunnistetaan kahdella rajakytkimellä B1 ja B2 ja valvonta tapahtuu turvalogiikan K1 avulla. Turvalogiikka ohjaa kahta kontaktoria Q1 ja Q2, joiden avaaminen estää tai keskeyttää koneen vaaralliset liikkeet.

Suojuksen rajakytkimien B1 ja B2 toimintaa valvotaan logiikan K1:n avulla tarkoituksena vian havaitseminen. Kontaktorien Q1 ja Q2 vikaantuminen havaitaan K1:n testauksessa käynnistyksen

yhteydessä. Käynnistyksen mahdollistava valvontasignaali tulee konetta käynnistettäessä vain, jos kontaktorit Q1 ja Q2 olivat aikaisemmin avautuneet, joten suojuksen fyysistä testausta suojusta avaamalla ja sulkemalla ei tarvita.

Turvatoiminto säilyy huolimatta minkä tahansa toimintaankytkennän komponentin vikaantumisesta, koska toimintaa valvotaan kahden rajakytkimen avulla joka kerta suojusta avattaessa tai suljettaessa. Kun logiikkayksikkö havaitsee vikaantumisesta johtuvan epäloogisuuden, kone pysäytetään kahdennetun kontaktorin avulla.

Vain useamman kuin kahden vian kertyminen kahden peräkkäisen käynnistämisen välisenä aikana voi johtaa turvatoiminnon menetykseen.

Muut suojaustoimenpiteet

- turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita on noudatettu (esim. syöttövirtaa kontaktoreille Q1 ja Q2 on pienennetty 50%) ja muutoinkin täytetään luokan B vaatimukset
- virtapiirien suojaukset (esim. kosketussuojaus) toteutettu
- rajakytkimien ohittaminen (väärinkäyttö) on estetty
- B1 on pakkotoiminen rajakytkin (IEC 60947-5-1 liite K)
- syöttöjohtimet rajakytkimiin B1 ja B2 on sijoitettu erilleen ja ne on suojattu.

Turvallisuuteen liittyvä lohkokaavio

Luokka 4 voidaan saavuttaa vain, jos eri suojalaitteiden useita mekaanisia rajakytkimiä ei kytketä sarjamuotoisella rakenteella (eli ei peräkkäisesti), sillä muuten vikoja kytkimissä ei voida havaita.

Kaksikanavaiset tulo- ja lähtöelementit yhdistetään loogisen lohkokaavion alajärjestelmään K1. Laitetason lohkokaavion mukaisesti alajärjestelmien järjestys on periaatteessa keskenään vaihtokelpoinen. Sen vuoksi suositellaan, että alajärjestelmät, joilla on samanlainen rakenne, ryhmitellään yhteen kuten osan 3 kohdan 4.4 kuvassa 9.

Lisäksi suoritustason PL:n laskemista voidaan yksinkertaistaa rajoittamalla kanavan $MTTF_d$-arvo 100 vuoteen.

Vikaantumistodennäköisyyden laskenta

Osien valmistajien antamat tiedot:

Alajärjestelmä 1 (K1)

- Logiikkaa käsitellään yhtenä valmiina alajärjestelmänä. Valmistaja on vakuuttanut, että turvalogiikka K1 täyttää PL e luokan 4 vaatimukset. ’
- Valmistaja ilmoittaa turvalogiikan K1 vikaantumistodennäköisyyden arvoksi 2,31 x 10^{-9} /tunti, mikä riittää suoritustasolle PL e).

  Alajärjestelmä 2: Kanava 1 (B1/Q1) ja kanava 2 (B2/Q2)

- Rajakytkimet B1 ja B2: Molempien rajakytkimien vikaantumistaajuus (vikaantumistodennäköisyys) lasketaan samalla tavalla seuraavasti: Ensin lasketaan rajakytkimien tilavaihtojen lukumäärä vuotta kohden (n_{op}-arvo): oletusarvot ovat tilavaihtojen välinen aika 900 sekuntia (15 minuuttia), käyttöaika 24 työtuntia vuorokaudessa ja 365 työpäivää (Sistema laskee tämän automaattisesti, kun syötetään em. tiedot):

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\frac{s}{h}}{t_{cycle}} = \frac{365d/y \cdot 24h/d \cdot 3600s/h}{900\frac{s}{cycle}} = 35040\frac{cycles}{y}$$

Tulokseksi saadaan n_{op}-arvo 35 040 tilavaihtoa vuodessa.

Huom. B_{10d}-arvo ilmaisee ajan, joka saadaan kunnes koepenkissä 10 % koekappaleista on vikaantunut. Seuraavissa kaavoissa kerroin 0,1 tulee siitä, että kymmenestä vikaantumisesta jo ensimmäisen tilavaihdon vikaantuminen on vaarallinen vikaantuminen.

Näiden arvojen avulla saadaan rajakytkinten B1 ja B2 keskimääräisen vaarallisen vikaantumisen ajaksi eli $MTTF_d$-arvoiksi:

- Rajakytkin B1: Valmistajan antama B_{10d}-arvo 1 000 000 tilavaihtoa

$$MTTF_{d,B1} = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{1000000\ cycles}{0{,}1 \cdot 35040\ \frac{cycles}{y}} = 285\ y \qquad T_{10d,B1} = \frac{B_{10d}}{n_{op}} = \frac{1000000 cycles}{35040 cycles/y} = 28{,}5 y$$

Koska kyseessä on arvo, jolloin 10 komponenttia sadasta on vikaantunut ja ensimmäinen vikaantunut komponentti aiheuttaa vaarallisen tapahtuman, jaetaan $MTTF_d$-arvo kymmenellä:

- Rajakytkin B2: Valmistajan antama B_{10d}-arvo rajakytkin B2 on 500 000 tilavaihtoa.

$$MTTFd, B2 = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{500000 cycles}{0{,}1 \cdot 35040 \frac{cycles}{y}} = 143 y \qquad T_{10d,B1} = \frac{B_{10d}}{n_{op}} = \frac{500000 cycles}{35040 cycles/y} = 14{,}3 y$$

(**Huom.** virhe: pitää olla $T_{10d,,B2}$)

Huom. Rajakytkimen B2:n T_{10d}-arvo on 14,3 vuotta mikä tarkoittaa, että B2 on korvattava ennakoidusti komponentin vaihdolla, jos tavoitteena pidetään 20 vuoden toiminta-aikaa.

- Kontaktorit Q1 ja Q2 sisältävät mekaanisesti toisiinsa liitettyjä kosketinelementtejä (standardi IEC 60947-5-1, Liite L).

Kontaktorien B_{10d}-arvot vastaavat induktiivisen kuormituksen alaisena (AC 3) 1 000 000 toimintajaksoa (valmistajan arvo). Jos oletetaan, että 50 % vikaantumisista on vaarallisia, B_{10d}-arvo saadaan kaksinkertaistamalla B_{10d}-arvo:

$$MTTF_{d,Q1/Q2} = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{2000000 cycles}{0{,}1 \cdot 35040 \frac{cycles}{y}} = 571 y \qquad T_{10d,Q1/Q2} = \frac{B_{10d}}{n_{op}} = \frac{2000000 cycles}{35040 cycles/y} = 57{,}1 y$$

Koska kyseessä on arvo, jolloin 10 komponenttia sadasta on vikaantunut ja ensimmäinen vikaantunut komponentti aiheuttaa vaarallisen tapahtuman, jaetaan $MTTF_d$-arvo kymmenellä:

$MTTF_d$ lasketaan erikseen molemmille kanaville käyttämällä sarjamuotoisten (peräkkäisten) komponenttien yhdistämisen yhtälöä, jossa laskenta tehdään käänteislukujen avulla:

$MTTF_d = 1/\lambda_d$, jossa λ_d on vaarallisen vikaantumisen taajuus

$\lambda_{dtot} = \lambda_{d1} + \lambda_{d2} + \ldots + \lambda_{dn}$ tot = *total* (yhteensä)

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \qquad \frac{1}{MTTF_{d,Ch1}} = \frac{1}{285y} + \frac{1}{571y} = \frac{1}{190y} \qquad \frac{1}{MTTF_{d,Ch2}} = \frac{1}{143y} + \frac{1}{571y} = \frac{1}{114y}$$

Tällöin saadaan kanava 1 $MTTF_{d,Ch1}$-arvoksi 190 vuotta ja kanavan 2 $MTTF_{d,Ch2}$-arvoksi 114 vuotta (Ch = kanava). Standardin ISO 13849-1 mukaisesti molempien kanavien $MTTF_d$-arvo on rajoitettu 100 vuoteen ja tässä tapauksessa, kun molempien kanavien $MTTF_d$-arvot ovat tämän rajoituksen jälkeen yhtä suuret (100 vuotta), ei ole tarpeellista suorittaa kanavien yhdistämistä symmetrisointi kaavan avulla.

Diagnostiikan kattavuuden arviointi

DC_{avg}: Rajakytkimien B1 ja B2 *DC*-arvo 99% perustuu logiikan K1 valvontaan, jossa seurataan suojuksen aiheuttamien avaamisten/sulkeutumisten toimintaa. Kontaktoreille Q1 ja Q2 DC-arvo 99 % saadaan tavallisesta K1:n valvonnasta käynnistyksen aikana. Ilmoitetut *DC*-arvot vastaavat DC_{avg}-arvoa jokaiselle alajärjestelmälle. DC_{avg}-arvo lasketaan yhtälön E.2 mukaisesti. Koska jokainen yksittäinen *DC*-arvo on 99 %, myös DC_{avg}-arvo on 99 %.

Riittävät toimenpiteet yhteisvikaantumisia vastaan alajärjestelmissä B1/B2 ja Q1/Q2 tehdään seuraavasti: erottaminen (15 p), hyväksi todetut komponentit (5 p), suojaus ylijännitettä vastaan jne. (15 p) ja ympäristöolosuhteet (25 p ja 10 p) tekee yhteensä 70 pistettä

Toiminta-aika: standardin ISO 13849-1 yksinkertaistetussa lähestymistavassa oletetaan 20 vuoden toiminta-aika.

Alajärjestelmä B1/ Q1/B2/Q2 vastaa luokkaa 4 korkealla $MTTF_d$-arvolla (100 vuotta) ja korkealla DC_{avg}-arvolla (99%). Tämä johtaa vaarallisen vikaantumisen keskimääräiseen todennäköisyyteen 2,47 x 10^{-8} tuntia kohti (katso standardin taulukko K1). Alajärjestelmän K1 lisäämisen jälkeen vaarallisen vikaantumisen keskimääräinen todennäköisyys on 2,70 x 10^{-8} tuntia kohti. Tämä vastaa suoritustasoa PL e.