Toni Honkanen

Toiminnallisen turvallisuuden vaatimukset ja soveltaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Kone- ja tuotantotekniikka

Insinöörityö

13.5.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Toni Honkanen Toiminnallisen turvallisuuden vaatimukset ja soveltaminen 38 sivua + 1 liite 13.5.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Kone- ja tuotantotekniikka
Suuntautumisvaihtoehto	Koneautomaatio
Ohjaaja	Lehtori Heikki Paavilainen

Insinöörityössä selvitettiin standardien ISO 13849-1 ja EN 62061 asettamia vaatimuksia koneiden toiminnalliselle turvallisuudelle sekä niiden käytännön sovellutusmahdollisuuksia. Työssä selvitettiin myös, miten toiminnallinen turvallisuus saavutetaan Beckhoffin komponenteilla. Työn tilaajana oli Metropolia Ammattikorkeakoulu Oy.

Työn pohjana on käytetty standardeja ISO 13849-1 ja EN 62061, jotka määrittävät tietyt tavoitteet eri turvallisuustasojen saavuttamiseksi. Näistä tavoitteista selvitettiin, miten tietty turvallisuustaso milloinkin määritetään ja miten kyseiset tavoitteet saavutetaan. Lisäksi tutkittiin, kuinka turvallisuustasojen tavoitteet saavutetaan Beckhoffin TwinSAFE-turvaratkaisulla.

Avainsanat	toiminnallinen turvallisuus, turvallisuustaso

Author	Toni Honkanen
Title	Requirements and Application of Functional Safety
Number of Pages	38 pages + 1 appendix
Date	13 May 2015
Degree	Bachelor of Engineering
Degree Programme	Mechanical Engineering
Specialisation option	Machine Automation
Instructor	Heikki Paavilainen, Lecturer

In the Bachelor's thesis, the requirements set by the standards ISO 13849-1 and EN 62061 and also the practical application possibilities of these requirements were examined. It was also studied how the functional safety is met by using Beckhoff's components. The Bachelor's thesis was commissioned by Metropolia University of Applied Sciences.

This Bachelor's thesis is based on the analysis of the standards ISO 13849-1 and EN 62061, which define specific goals for achieving different security levels. From these goals it was discovered, how a specific security level was defined in each case and how those goals were met. In addition, it was examined, how the goals of the security levels were met by using Beckhoff's TwinSAFE safety solution.

Keywords	functional safety, security level

Sisällys

Käsitteet ja lyhenteet

CFF	Common Cause Failure; yhteisvikaantuminen. Jos samasta syystä aiheutuu useampia vikoja, on niitä tarkasteltava yksittäisinä vikoina.
CRC	Cyclic redundancy check; tiivistealgoritmi, jota käytetään havaitsemaan pieniä virheitä sekä korjaamaan siirron aikaisia tai säilytyksessä tapahtuneita virheitä.
DCavg	Diagnostic Coverage average; diagnostiikan kattavuuden keskiarvo, toisin sanoen järjestelmän valvonnan kattavuuden keskiarvo prosentteina, mitä voidaan arvioida muun muassa vika- ja vaikutusanalyysin avulla.
FSoE	Fail-Safe over EtherCAT; avoin kenttäväyläriippumaton turvallisuusprotokolla.
MTTFd	Mean Time To dangerous Failure; vaarallinen keskimääräinen vikaantumisaika vuosissa mitattuna; määritellään jokaiselle komponentille ja ohjausjärjestelmän kanavalle.
PFHd	Probability of dangerous Failure per Hour; Vaarallisen vikaantumisen keskimääräinen todennäköisyys yhden tunnin aikana.
PL	Performance Level; suoritustaso, jolla arvioidaan turvallisuuteen liittyvän ohjausjärjestelmän kykyä suorittaa turvatoiminto.
Plr	Required Performance Level; riskianalyysissä määritelty PL-taso, jolle turvallisuuteen liittyvän ohjausjärjestelmän osan suorittama turvatoiminto vähintään tulisi yltää.
PTE	Probability of dangerous Transmission Error; tiedonsiirron vaarallisten vikaantumisten todennäköisyys
SIL	Safety Integrity Level; turvallisuuden eheyden taso, jolla arvioidaan turvallisuuteen liittyvän ohjausjärjestelmän kykyä suorittaa turvatoiminto virheettä.

1 Johdanto

Tässä insinöörityössä määritetään koneiden toiminnallisen turvallisuuden standardien määrittämät vaatimukset ja niiden käytännön soveltamismahdollisuudet. Työn tarkoituksena on selvittää periaatteet ja käytännön sovellutukset, joilla toiminnallinen turvallisuus saavutetaan käyttäen Beckhoffin turvaratkaisua.

Automaation käyttö teollisuudessa on yleistynyt roimasti viime vuosikymmenen aikana. Tämä tarkoittaa, että yhä useampi joutuu nykyään työskentelemään automaatiolaitteiden parissa. Tämän seurauksena automaatiolaitteiden toiminnan turvallisuuden takaamisella on yhä enemmän merkitystä.

Työn lähtökohtana on kaksi yleisintä koneiden toiminnallisen turvallisuuden määrittämiseen käytettyä standardia: EN 62061 ja ISO 13849-1. Näiden standardien pohjalta oli tarkoitus selvittää, miten toiminnallinen turvallisuus määritellään, millaisia vaatimuksia toiminnalliselle turvallisuudelle esitetään, kuinka standardeja käytännössä sovelletaan ja mitä muuta toiminnallisen turvallisuuden soveltaminen vaatii.

2 Toiminnallisen turvallisuuden standardit

2.1 Yleistä

Koneturvallisuuden standardit jaetaan neljään eri tyyppiin niiden sovelluslaajuuden mukaan: A-, B1-, B2- ja C-tyypin standardeihin. A-tyypin standardit ovat perusstandardeja, jotka määrittelevät koneturvallisuuden perusfilosofian, ja niitä voi soveltaa kaikkiin koneisiin. Esimerkkinä A-tyypin standardista on SFS-EN ISO 12100 (Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen).

B-tyypin standardit ovat yleisiä koneturvallisuuden standardeja, jotka määrittelevät perustietoa yhdestä turvallisuusnäkökohdasta tai suojateknisestä laitteesta, ja niitä voidaan käyttää monessa koneessa. B-tyyppi jaetaan B1- ja B2-tyypin standardeihin, joista B1-standardit käsittelevät yksittäisiä turvallisuusnäkökohtia ja B2-standardit käsittelevät yksittäisiä turvalaitteita. Standardit ISO 13849-1 (Koneturvallisuus.

Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet) ja EN 62061 (Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus) ovat molemmat B1-tyypin standardeja.

C-tyypin standardit ovat kone- tai koneryhmäkohtaisia standardeja. Nämä standardit käsittelevät koneiden tai koneryhmien tietoja ja turvallisuutta. C-tyypin standardeja sovelletaan yleensä ensisijaisesti, jos vain on sopiva olemassa.

Molemmat B1-standardit, sekä EN 62061 että 13849-1, määrittävät vaatimuksia koneen turvallisuuteen liittyvien ohjausjärjestelmien suunnitteluun ja toteuttamiseen. Käyttämällä kumpaa standardia tahansa niiden soveltamistapojen mukaisesti, voidaan olettaa olennaisten turvallisuusvaatimusten tulevan täytetyksi. Taulukossa 1 on lyhyt yhteenveto molempien standardien soveltamisaloista.

Taulukko 1. Standardien EN/IEC 62061 ja ISO 13849-1 soveltamissuositukset

	Turvallisuuteen liittyvien ohjaustoimintojen toteutuksessa käytettävä teknologia	ISO 13849-1	IEC 62061
A	Muut kuin sähköiset, esim. hydrauliset	X	Ei käsitellä
B	Sähkömekaaniset, esim. releet ja/tai yksinkertainen elektroniikka	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL e	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
C	Monimutkainen elektroniikka, esim. ohjelmoitavat järjestelmät	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL d	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
D	A yhdessä B:n kanssa	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL e	X [c]
E	C yhdessä B:n kanssa	Rajoitettu nimettyihin rakenteisiin (ks. huomautus 1) ja enintään suoritustasolle PL d	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
F	C yhdessä A:n kanssa tai C yhdessä A:n ja B:n kanssa	X [b]	X [c]
X tarkoittaa, että kyseistä kohtaa käsitellään sarakkeen otsikossa mainitussa kansainvälisessä standardissa			
[a] Nimetyt rakenteet määritellään kohdassa 6.2, jotta voidaan esittää yksinkertaistettu lähestymistapa suoritustason määrälliseen arviointiin. [b] Monimutkainen elektroniikka: käytetään nimettyjä rakenteita standardin ISO 13849 tämän osan mukaisesti suosituskyvyn tasolle PL d asti tai mitä tahansa rakennetta standardin IEC 62061 mukaisesti. [c] Muissa kuin sähköisissä teknologioissa käytetään alajärjestelminä standardin ISO 13849 tämän osan mukaisia osia.			

Taulukosta 1 huomataan, että standardin ISO 13849-1 soveltamisalat on rajoitettu tiettyihin rakenteisiin toisin kuin EN 62061:n, mutta EN 62061 ei käsittele ollenkaan hydrauliikkaa tai pneumatiikkaa. On otettava myös huomioon, että vaikka ISO 13849-1 on rajoitettu tiettyihin rakenteisiin, sen käytännön soveltaminen on helpompaa, eikä niin

työlästä verrattuna EN 62061:een. Taulukossa 2 esitetään suoritustasojen ja turvallisuuden eheyden tasojen suhteutus.

Taulukko 2. Suoritustasojen (PL) ja turvallisuuden eheyden tasojen (SIL) suhteutus

Suoritustaso (PL)	Keskimääräinen vikaväli (vuotta)	Vaarallisen keskimääräisen vikaantumisajan todennäköisyys tuntia kohden (1/h)	Turvallisuuden eheyden taso (SIL)
a	1,14–11,4	$\geq 10^{-5} ... < 10^{-4}$	ei ole
b	11,4–38,1	$\geq 3x10^{-5} ... < 10^{-5}$	1
c	38,1–114	$\geq 10^{-6} ... < 3x10^{-5}$	1
d	114–1412	$\geq 10^{-7} ... < 10^{-6}$	2
e	1142–11416	$\geq 10^{-8} ... < 10^{-7}$	3

2.2 Standardien käytännön sovellutus

Standardit ISO 13849-1 ja EN 62061 tarjoavat turvallisuusvaatimukset ja ohjeistuksen periaatteisiin, joita käytetään turvallisuuteen liittyvien ohjausjärjestelmän osien suunnitteluun ja valmistukseen, mukaan lukien ohjelmiston suunnittelu. Standardeja voidaan myös käyttää, kun halutaan rakentaa turvaratkaisuja tietylle laitteelle tai kun halutaan laskea turvatoiminnoista saavutettu tai saavutettava turvallisuus.

2.2.1 ISO 13849-1

Kun halutaan saada turvallinen automaatiolaite/-kone, tulee turvallisuus ottaa huomioon jo laitteen tai koneen suunnitteluvaiheessa. Aluksi suunnitellaan kone ja sen toiminta. Suunnitellulle laitteelle tulee tehdä turvakartoitus, jolla tunnistetaan vaarakohdat. Kun koneelle ruvetaan määrittämään turvallisuutta ja turvatoimintoja, hyödynnetään standardia.

ISO 13849-1:n turvatoimintojen suunnitteluprosessi voidaan kuvata kuudella askeleella:

- Määritä turvatoiminnot.
- Arvioi vaadittava suoritustaso (PL_r).
- Suunnittele ja luo toteutus turvatoiminnoille.
- Määritä suoritustaso jokaiselle turvallisuuteen liittyvälle osalle.
- Tarkista, että vaadittava suoritustaso on saavutettu.
- Toteuta suunniteltu turvallisuuteen liittyvä ohjausjärjestelmän osien kokonaisuus.

Kaksi ensimmäistä askelta, eli turvatoimintojen määritys ja vaadittavan suoritustason arviointi, voidaan toteuttaa kahdella eri tavalla, joko:

- määritetään ohjausjärjestelmän vaarakohdille välttämättömät turvatoiminnot, tarkennetaan näiden toimintojen vaatimukset ja määritetään turvatoiminnoille vaadittava suoritustaso (PLr), tai
- määritetään ohjausjärjestelmälle suoraan korkein suoritustaso ja tämän jälkeen määritetään suoritustason täyttävät turvallisuustoiminnot.

Näistä kahdesta tavasta suoritustason määritys suoraan korkeimmalle tasolle on yleisempi toteutustapa. Näin toteutuksen suunnittelu ja komponenttien valinta helpottuu, kun otetaan suoraan korkeimman turvallisuustason komponentit ja suunnitellaan turvatoiminto korkeimman luokkarakenteen pohjalta, sen sijaan, että suunniteltaisiin ja arvioitaisiin juuri tarpeeksi turvallinen järjestelmä. Kuitenkin on huomattavasti työläämpää, jos valitaan suoraan korkein suoritustaso, sillä eritoten ohjelmoinnin ja johdotuksen työmäärä kasvaa huomattavasti. Lisäksi kustannusten määrä kasvaa, tosin kasvu ei ole merkittävä, ellei kyseessä ole sarjatuotanto.

Seuraavaksi suunnitellaan turvatoimintojen toteutus ja komponenttien valinta. Turvatoimintojen suunnittelussa määritetään, millainen luokkarakenne turvatoiminnolla on, minkä tasoinen diagnostiikan kattavuus, ja kuinka korkea kanavan vaarallinen vikaantumisaika on tavoitteena. Nämä tavoitteet määräytyvät turvallisuustasojen mukaan ja miten kyseinen turvallisuustaso halutaan saavuttaa. Turvatoimintojen suunnitelman perusteella valitaan komponentit ja järjestelmä ohjelmointia varten. Järjestelmän valinnassa tulee ottaa huomioon, voidaanko käyttää integroitua

järjestelmää ja kuinka kattava diagnostiikka halutaan. Komponenttien valinnan jälkeen turvatoiminnot tulisi toteuttaa teknisesti ja toteutetuille turvatoiminnoille tulisi arvioida suoritustasot (ks. kpl 2.3.1), joiden arvioinnissa otetaan huomioon:

- kanavan vaarallinen keskimääräinen vikaantumisaika (ks. kpl 2.3.3)
- diagnostiikan kattavuus (ks. kpl 2.3.4)
- luokka (ks. kpl 2.3.5)
- yhteisvikaantuminen (ks. kpl 2.3.6).

Arvioituja suoritustasoja verrataan jokaisen turvatoiminnon omaan vaadittuun suoritustasoon. Jos arvioitu suoritustaso on riittävä, varmistetaan, että kaikki muut turvatoiminnolta vaadittavat vaatimukset on täytetty. Laite ja turvatoiminnot toteutetaan ja ohjelmoidaan. Lopuksi suoritetaan testaus ja hyväksyntä.

2.2.2 EN 62061

Aluksi suunnitellaan kone ja sen toiminta. Suunnitellulle laitteelle tulee tehdä turvakartoitus, jolla tunnistetaan vaarakohdat. Kun koneelle ruvetaan määrittämään turvallisuutta ja turvatoimintoja, hyödynnetään standardia.

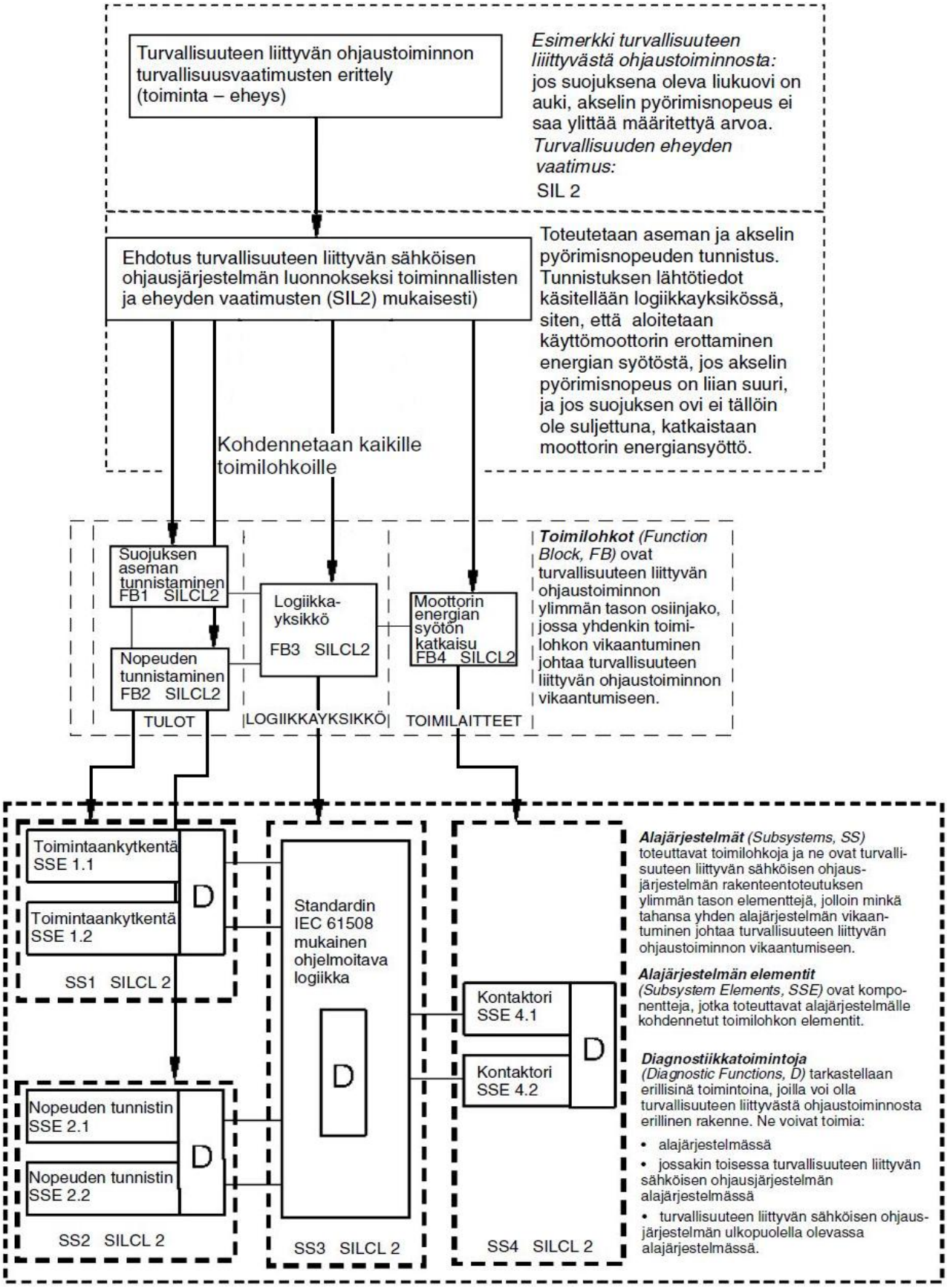
EN 62061-standardin turvatoimintojen sunnitteluprosessi kuvataan 8 askeleella:

- Aseta SIL-taso ja tunnista/päätä sähköisen ohjausjärjestelmän rakenne.
- Jaa jokainen turvatoiminto toimilohkoihin (esim. tulot, logiikka, lähdöt).
- Listaa turvallisuusvaatimukset jokaiselle toimilohkolle ja määritä toimilohkoille alajärjestelmät rakenteen sisällä.
- Valitse komponentit jokaiselle alajärjestelmälle.
- Suunnittele diagnostiikkatoimintojen toteutus.
- Määritä SIL-taso jokaiselle turvallisuuteen liittyvälle ohjausjärjestelmän osalle.
- Dokumentoi turvallisuuteen liittyvän sähköisen ohjausjärjestelmän rakenne.
- Suunniteltujen turvallisuuteen liittyvän ohjausjärjestelmien toteuttaminen.

Kuten standardin ISO 13849-1 kanssa, myös EN 62061:stä käytettäessä voidaan turvatoimintojen sunnittelua lähestyä kahdella eri tavalla, joko:

- määritetään ohjausjärjestelmän vaarakohdille välttämättömät turvatoiminnot, tarkennetaan näiden toimintojen vaatimukset ja määritetään turvatoiminnoilta vaadittava turvallisuuden eheyden taso (SIL), tai
- määritetään ohjausjärjestelmälle suoraan korkein turvallisuuden eheyden taso ja tämän jälkeen määritetään turvallisuuden eheyden tason täyttävät turvallisuustoiminnot.

Seuraavaksi turvatoimintojen turvallisuusvaatimukset eritellään ja kehitetään turvatoiminnolle turvallisuusvaatimusten mukainen käytännön toimintasuunnitelma. Tämän jälkeen turvatoiminto ja sen toimintasuunnitelma jaetaan toimilohkoihin (esimerkiksi tulot, logiikka, lähdöt), jotka vielä jaetaan alajärjestelmiksi. Kuvassa 1 on esitelty, kuinka toiminto jaetaan toimilohkoihin ja vielä alajärjestelmiin.



Kuva 1. Toiminnon jako toimilohkoihin ja vielä alajärjestelmiin

Alajärjestelmän muodostuttua, sen elementtien tilalle valitaan komponentit, jotka toteuttavat alajärjestelmälle kohdennetut tehtävät. Komponenttien valinnan jälkeen suunnitellaan diagnostiikkatoimintojen toteutus. Alajärjestelmille määritetään perusrakenteet ja lasketaan vaaralliset satunnaiset laitevikaantumiset (PFH_{DSS}).

Tämän jälkeen lasketaan yhteen jokaisen alajärjestelmän vaarallinen satunnainen laitevikaantuminen ja tälle saadulle arvolle määritetään saavutettu turvallisuuden eheyden taso taulukon 2 avulla. Saatua turvallisuuden eheyden tasoa verrataan vaadittuun turvallisuuden eheyden tasoon. Kun vaadittu turvallisuuden eheyden taso on kokonaisuudessaan saavutettu, dokumentoidaan turvallisuuteen liittyvän sähköisen ohjausjärjestelmän rakenne ja aloitetaan koneen sekä sen turvatoimintojen toteuttaminen. Kun kone on kokonaisuudessaan valmis, suoritetaan sen testaus ja hyväksytään se käyttöön.

2.3 EN ISO 13849-1

2.3.1 Suoritustaso (PL)

Standardi 13849-1 käyttää turvallisuuden arviointiin käsitettä ”suoritustaso” (PL), joka ilmaisee turvallisuuteen liittyvien ohjausjärjestelmän osien kykyä suorittaa turvatoiminto ennakoitavissa olosuhteissa. Jokaiselle turvallisuuteen liittyvälle ohjausjärjestelmän osalle ja/tai niiden yhdistelmälle, joka toteuttaa turvatoiminnon, on määritettävä suoritustaso arvioimalla seuraavia näkökohtia:

- vaarallinen keskimääräinen vikaantumisaika (MTTFd) jokaiselle yksittäiselle komponentille (ks. 2.3.3)
- diagnostiikan kattavuus (DC, ks. 2.3.4)
- yhteisvikaantuminen (CCF, ks. 2.3.6)
- rakenne eli ohjausjärjestelmän luokat (ks. 2.3.5)
- turvatoiminnon käyttäytyminen vikatilanteessa
- turvallisuuteen liittyvä ohjelmisto
- systemaattinen vikaantuminen; systemaattisten vikojen hallinta ja niiden välttäminen
- kyky toteuttaa turvatoiminto ennakoitavissa ympäristöolosuhteissa.

Tässä työssä esitetään suoritustason arvioinnin helpottamiseksi yksinkertaistettu menetelmä, joka perustuu viiteen nimettyyn rakenteeseen ja täyttävät määrätyt suunnittelukriteerit sekä käyttäytymisen vikatilanteissa.

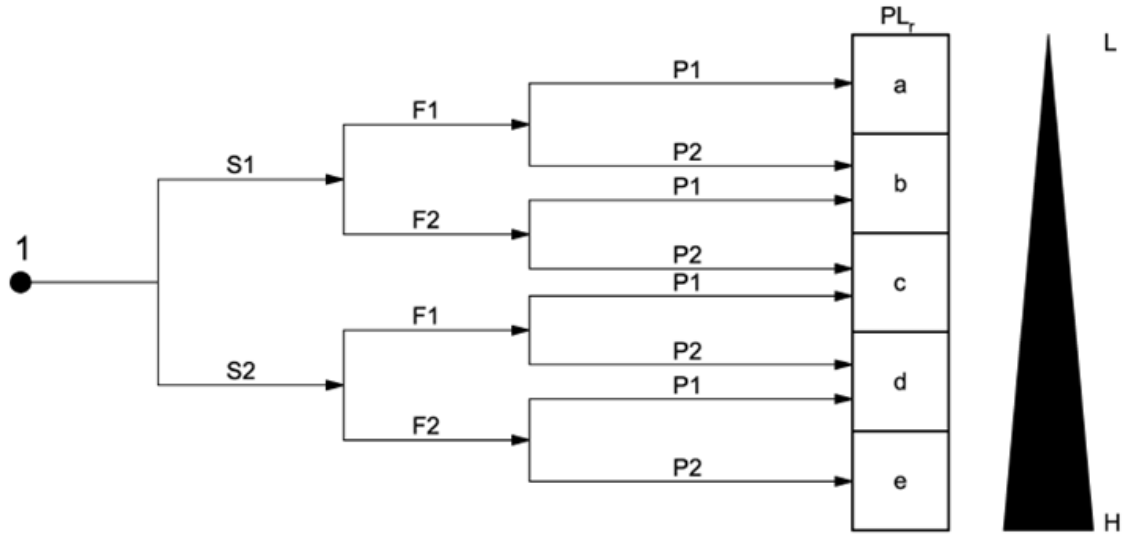
2.3.2 Vaadittavan suoritustason (PLr) määrittäminen

Vaadittava suoritustaso (PLr) ilmaisee, kuinka paljon turvallisuuteen liittyvien ohjausjärjestelmän osien riskiä on pienennettävä. Vaadittava suoritustaso on määritettävä jokaiselle ohjausjärjestelmän turvatoiminnolle, joka on toteutettu turvallisuuteen liittyvillä osilla ja se on dokumentoitava.

Vaadittavan suoritustason määrittämiseksi tulee arvioida kolmea muuttujaa, jotka ovat seuraavat:

- Vamman vakavuus (S1, S2): vamman vakavuus määritetään sen mukaan, onko saatu vamma lievä (S1) vai vakava (S2) tai jopa kuolema.
- Vaaralle altistumistaajuus (F1, F2): vaaran altistumistaajuus määritetään sen perusteella, tapahtuuko vaaralle altistuminen useammin kuin kerran tunnissa (F2) vai ei (F1).
- Mahdollisuus välttää vaara (P1, P2): muuttuja P1 valitaan, jos tapaturma on mahdollista välttää tai sen vaikutusta voidaan vähentää merkittävästi, mutta jos vaaraa ei voida realistisesti välttää, olisi valittava muuttuja P2.

Näiden edellä mainittujen muuttujien avulla pystytään arvioimaan turvatoiminnolle vaadittava suoritustaso (PL_r) riskin arvioinnin perusteella käyttämällä apuna kuvaa 2.



Merkintöjen selitys

1 aloituskohta turvatoiminnon osuuden arvioimiseksi riskin pienentämisessä
L osuus riskin pienentämisessä pieni
H osuus riskin pienentämisessä suuri
PLr vaadittava suoritustaso

Riskiin liittyvät muuttujat

S Vamman vakavuus
S1 lievä (tavallisesti palautuva vamma)
S2 vakava (tavallisesti palautumaton vamma)
F vaaralle altistumistaajuus tai altistumiskesto
F1 harvoin...toisinaan tai lyhyt altistumisaika
F2 toistuvasti...jatkuvasti tai pitkä altistumisaika
P mahdollisuus välttää vaaraa
P1 mahdollista tietyissä olosuhteissa
P2 tuskin mahdollista

Kuva 2. Riskigraafi vaadittavan suoritustason PLr määrittämiseksi turvatoiminnolle

2.3.3 Kanavan vaarallinen keskimääräinen vikaantumisaika (MTTFd)

Kanavan vaarallinen keskimääräinen vikaantumisajan arvo ilmaistaan käyttäen kolmea eri tasoa (taulukko 3), ja se on otettava huomioon jokaiselle kanavalle erikseen (esim. yksittäiselle kanavalle tai redundanttisen järjestelmän jokaiselle kanavalle). Suurin käytettävä arvo on 100 vuotta.

Taulukko 3. Kanavan vaarallinen keskimääräinen vikaantumisaika (MTTFd)

	$MTTF_d$
Kunkin kanavan merkintä	**Kunkin kanavan vaihteluväli**
matala (low)	3 vuotta ≤ $MTTF_d$ < 10 vuotta
keskimääräinen (medium)	10 vuotta ≤ $MTTF_d$ < 30 vuotta
korkea (high)	30 vuotta ≤ $MTTF_d$ ≤ 100 vuotta
HUOM. 1 Kunkin kanavan $MTTF_d$ -arvojen vaihteluvälien valinta perustuu nykytekniikan mukaisista kenttähavainnoista saatuihin vikataajuuksiin ja ne muodostavat tietyntyyppisen logaritmisen asteikon, joka sopii logaritmiseen suoritustason asteikkoon. Todellisten turvallisuuteen liittyvien ohjausjärjestelmän osien jokaisen kanavan $MTTF_d$ -arvoja, jotka ovat alle kolme vuotta, ei oleteta esiintyvän, koska tämä tarkoittasi, että yhden vuoden kuluttua noin 30 % markkinoilla olevista järjestelmistä vikaantuisivat ja ne pitäisi korvata. Minkään kanavan $MTTF_d$ -arvoa yli 100 vuotta ei hyväksytä, koska suuria riskejä varten olevat turvallisuuteen liittyvät ohjausjärjestelmän osat eivät saisi riippua yksistään komponenttien luotettavuudesta. Turvallisuuteen liittyvien ohjausjärjestelmän osien vahvistamiseksi systemaattisia ja satunnaisia vikaantumisia vastaan olisi vaadittava täydentäviä keinoja kuten redundanssia ja testausta. Käytännön syistä vaihteluvälit rajoitetaan kolmeen. Jokaisen kanavan $MTTF_d$ -arvon rajoittaminen enintään 100 vuoteen koskee turvallisuuteen liittyvien ohjausjärjestelmän osien yhtä kanavaa, jotka toteuttavat turvatoiminnon. Korkeampia $MTTF_d$ -arvoja voidaan käyttää yksittäisille komponenteille (ks. taulukko D.1). HUOM. 2 Tässä taulukossa esitettävien rajojen tarkkuuden oletetaan olevan 5 %.	

Komponentin vaarallisen keskimääräisen vikaantumisajan arviointia varten tarvittavien tietojen hankinta tehdään seuraavassa prioriteettijärjestyksessä:

- käytetään valmistajan antamia tietoja
- käytetään ISO 13849-1 standardin liitteissä C ja D esitettäviä menetelmiä
- valitaan 10 vuotta.

Jos valmistaja on antanut vaarallisen vikaantumisajan PFH-arvona, voidaan siitä määrittää MTTFd-arvo seuraavalla kaavalla:

$$MTTFd = \frac{1 - DC}{PFH}$$

2.3.4 Diagnostiikan kattavuus (DC)

Diagnostiikan kattavuus ilmaistaan neljällä tasolla (taulukko 4).

Yleensä diagnostiikan kattavuuden arvioimiseen voidaan käyttää esimerkiksi vika- ja vaikutusanalyysiä (ks. IEC 60812). Tällöin kaikki asiaan kuuluvat viat ja/tai vikaantumistavat otetaan huomioon ja näin saatua ohjausjärjestelmän osien yhdistelmän suoritustasoa (PL) verrataan siltä vaadittavaan suoritustasoon (PL_r).

Diagnostiikan kattavuuden arvioimiseksi on myös yksinkertaistettu tapa. Standardissa ISO 13849-1 (liite E) esitetään taulukko esimerkkejä toimenpiteistä tulo- ja

lähtöyksiköille sekä logiikalle, mistä jokaiselle esimerkille on määritelty diagnostiikan kattavuus. Esimerkkien pohjalta voidaan arvioida diagnostiikan kattavuus jokaiselle tulolle, logiikalle ja lähdölle. Tämä taulukko löytyy tämän työn liitteestä 1.

Taulukko 4. Diagnostiikan kattavuus

DC	
Merkintä	**Vaihtelualue**
nolla (none)	DC < 60 %
matala (low)	60 % ≤ DC < 90 %
keskimääräinen (medium)	90 % ≤ DC < 99 %
korkea (high)	99 % ≤ DC
HUOM. 1 Useasta osasta koostuvan turvallisuuteen liittyvän ohjausjärjestelmän osan diagnostiikan kattavuudelle (DC) käytetään kuvassa 5, kohdassa 6 ja liitteessä E.2 keskimääräistä diagnostiikan kattavuutta (DC_{avg}).	
HUOM. 2 Diagnostiikan kattavuudelle valitut arvojen vaihteluvälit perustuvat avainarvoihin 60 %, 90 % ja 99 %, joita käytetään myös muissa standardeissa (esim. IEC 61508), joissa käsitellään diagnostiikan kattavuuden testauksia. Tutkimukset osittavat, että pikemminkin (1 – DC) kuin itse DC, on testauksen tehokkuudelle ominainen mitta. Avainarvoja 60 %, 90 % ja 99 % vastaavat (1 – DC) arvot muodostavat tietyntyyppisen logaritmisen asteikon, joka sopii logaritmiseen suoritustason asteikkoon. DC-arvoa 60 % pienemmällä arvolla on vain vähäinen merkitys testatun järjestelmän luotettavuuteen ja siksi se merkitään "nolla (none)". DC-arvoa 99 % suurempaa arvoa on hyvin vaikea saavuttaa monimutkaisilla järjestelmillä. Käytännön syistä vaihteluvälit rajoitetaan neljään. Tässä taulukossa esitettävien rajojen tarkkuuden oletetaan olevan 5 %.	

2.3.5 Luokat

Jokaisen turvallisuuteen liittyvän ohjausjärjestelmän osan on oltava tietyn luokan mukainen. Standardin ISO 13849-1 määrittelemiä, nimettyjä rakenteita eli luokkia on yhteensä viisi: B, 1, 2, 3 ja 4.

Luokat B, 1 ja 2 ovat yksikanavaisia, kun taas luokat 3 ja 4 ovat kaksikanavaisia, eli niissä on kaksi erillistä toisistaan riippumatonta, toimivaa kanavaa, jotka pystyvät suorittamaan turvatoiminnon. Tämä tekee luokaista 3 ja 4 kalleimmat toteuttaa, mutta niillä saadaan korkeimmat suoritustasot. Järjestelmän rakenteella on siis suuri merkitys sille, mihin suoritustasoon päädytään. Luokkien arkkitehtuuri yleensä kuvataan lohkokaavioesityksena (ks. kuva 3). Luokkarakenteiden määritelmät ovat seuraavat:

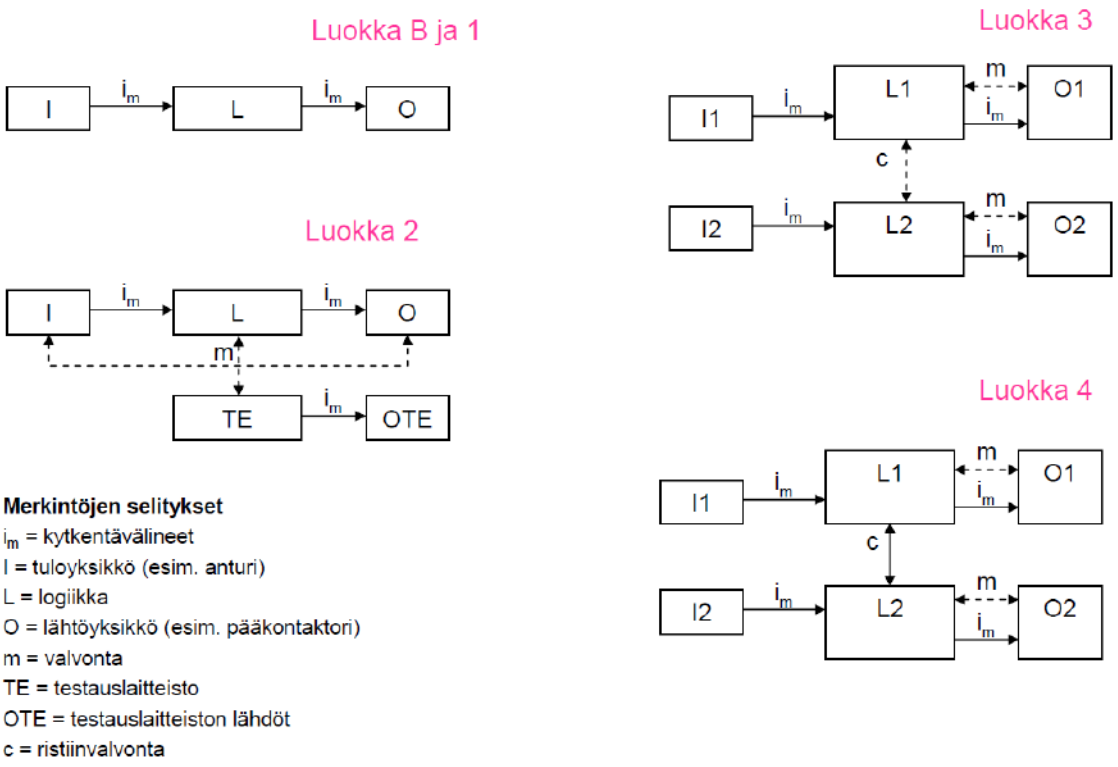
- Luokka B: yleisiä tuvallisuusperiaatteita (suojamaadoitus, eristyksen valvonta, jännitepiikkien vaimennus yms.) on noudatettava. Käyttö- ja ympäristöolosuhteet on otettava huomioon käytettävissä komponenteissa. Vaarallisten vikaantumisten välinen keskimääräinen aika, MTTFd-arvo, on oltava 3–30 vuotta.

- Luokka 1: on noudatettava luokan B vaatimuksia sekä hyvin koeteltuja komponentteja ja hyvin koeteltuja turvallisuusperiaatteita (ylimitoittaminen, pakkotoimisuus yms.). MTTFd on oltava 30–100 vuotta.

- Luokka 2: on noudatettava luokkien B ja 1 vaatimuksia, sekä koneen ohjausjärjestelmän on koetettava turvatoimintojen toimivuus tietyin väliajoin. MTTFd on oltava 3–100 vuotta vaaditun PL-tason mukaan ja yhteisvikaantumisen (CCF) todennäköisyys on oltava pieni (CCF-arvon määrittäminen; kpl 2.3.6).

- Luokka 3: on noudatettava luokkien B ja 1 vaatimuksia. Yksittäisen vian sattuessa ohjausjärjestelmän on pystyttävä suorittamaan turvatoiminto, ja mahdollisuuksien mukaan yksittäinen vika on havaittava. Useammat viat on aina havaittava. MTTFd on oltava 30–100 vuotta vaaditusta PL-tasosta riippuen. Dcavg, eli diagnostiikan kattavuuden keskiarvo on oltava vähintään 60–99 %, yhteisvikaantumisen (CCF) todennäköisyys oltava pieni.

- Luokka 4: on noudatettava luokkien B ja 1 vaatimuksia. Turvatoimintoa ei saa menettää vaikka järjestelmässä olisi yksi vika. Kaikkien vikojen on paljastuttava, eli vikoja ei saa kertyä järjestelmään, ilman että käyttäjä niistä tietää. Jos vikoja kuitenkin kertyy, ne eivät saa aiheuttaa turvatoiminnon menettämistä. Käytännössä tarkoittaa järjestelmän kahdennusta, sekä itse- että ristivalvontaa. MTTFd on oltava 30–100 vuotta, DCavg on oltava 99–100 % ja yhteisvikaantumisen (CCF) todennäköisyys on oltava pieni.



Kuva 3. Standardin ISO 13849-1 määrittelemien luokkarakenteiden lohkokaavioesitykset

Käytännössä luokan 3 ja 4 välinen ero jää valvonnan, eli diagnostiikan kattavuuden suuruuteen. Luokka 4 vaatii järjestelmältä käytännössä täydellistä vikojen automaattista valvontaa.

2.3.6 Yhteisvikaantuminen (CFF)

Yhteisvikaantumiseksi kutsutaan tilannetta, kun samasta syystä aiheutuvia, useampia vikoja käsitellään yksittäisenä vikana. Yhteisvikaantumisprosessilla määritetään, kuinka hyvin järjestelmä pystyy estämään yhteisvikaantumisen tapahtumisen. Tällä laadullisella prosessilla olisi käytävä läpi koko järjestelmä. Turvallisuuteen liittyvien ohjausjärjestelmän osien kukin osa olisi otettava tarkasteluun. Yhteisvikaantumisen tarkastelu on tarpeen ottaa huomioon vain järjestelmissä, joiden rakenne vastaa luokkia 2, 3 tai 4

Taulukossa 5 luetteloidaan toimenpiteet, niihin liittyvät pisteet ja tarvittava kokonaispistemäärä. Jokaisesta toimenpiteestä annetaan vain joko täydet pisteet tai ei mitään ja jos toimenpide toteutetaan vain osittain, niin silloin siitä toimenpiteestä ei anneta pisteitä ollenkaan.

Taulukko 5. Pisteytysprosessi ja yhteisvikaantumista estävien toimenpiteiden määrällinen arviointi

Nro	Yhteisvikaantumisen estävä toimenpide	Pisteet
1	**Erottelu/erottaminen**	
	Signaalireittien fyysinen erottaminen: – johdotuksen/putkituksen erilleen sijoittaminen – riittävät ilma- ja pintavälit painetuissa piirilevyissä	**15**
2	**Erilaisuus (diversiteetti)**	
	Erilaisten teknologioiden, toteutustapojen, fyysisten periaatteiden tai valmistajien komponenttien käyttö	**20**
3	**Suunnittelu, soveltaminen ja kokemukset**	
	Suojaustoimenpiteet ylijännitteelle, ylipaineelle, ylivirralle jne.	**15**
	Käytetyt komponentit ovat hyvin koeteltuja	**5**
4	**Arviointi ja analyysit**	
	Onko vika- ja vaikutusanalyysin tulokset otettu huomioon toteutuksessa yhteisvikaantumisen estämiseksi?	**5**
5	**Pätevyys ja koulutus**	
	Onko suunnittelu- ja ylläpitohenkilöstö koulutettu ymmärtämään yhteisvikaantumisen syyt ja seuraukset?	**5**
6	**Ymäristöolosuhteisiin liittyvät toimenpiteet**	
	Pneumaattiset- ja hydrauliset järjestelmät: väliaineen suodatus, imuilman laatu, paineilman kuivatus Sähköiset järjestelmät: EMC testi	**25**
	Muut vaikutukset Asiaankuuluvien ympäristövaikutusten sietokyky?	**10**
	Yhteensä	**100**

Kokonaispisteet (Vaaditaan luokilta 2, 3 ja 4)	**Toimenpiteet yhteisvikaantumisen välttämiseksi**
65 tai enemmän	Täyttää vaatimukset -> ei lisätoimenpiteitä
Vähemmän kuin 65	Ei täytä vaatimuksia -> valitaan lisätoimenpiteitä

2.3.7 Suoritustason arviointi

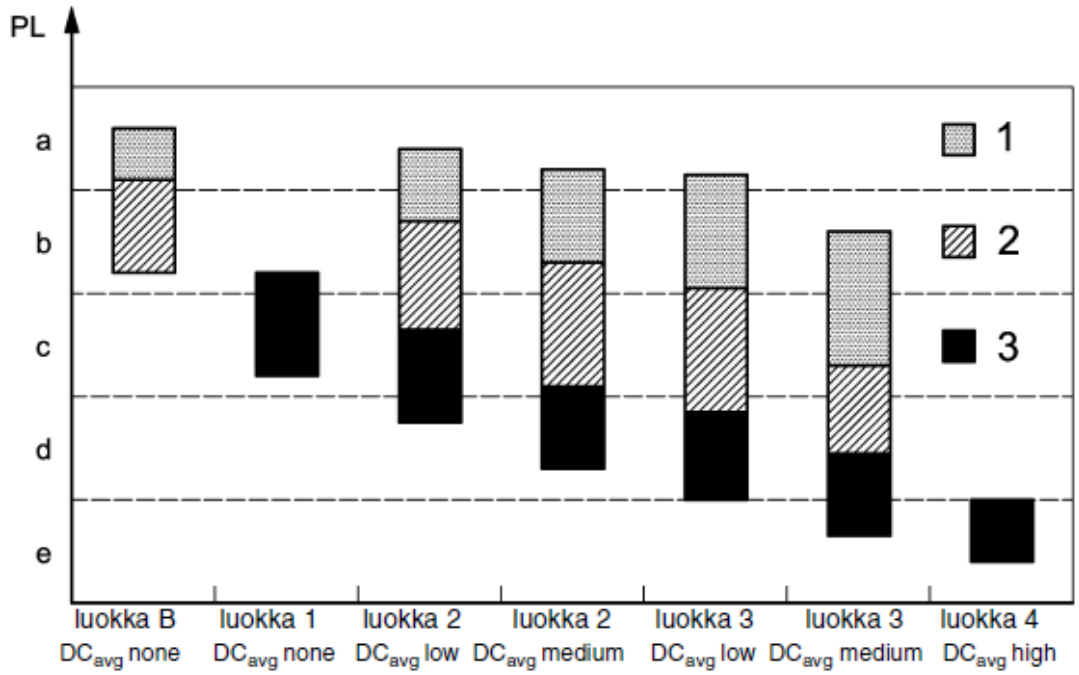
Suoritustaso voidaan arvioida ottamalla huomioon kaikki asiaan kuuluvat muuttujat ja laskentaan soveltuvat menetelmät. Tässä kohdassa kuvataan turvallisuuteen liittyvien ohjausjärjestelmän osien suoritustason arviointia varten yksinkertaistettu menetelmä, joka perustuu nimettyihin rakenteisiin.

Nimetyille rakenteille tehdään seuraavat tyypilliset oletukset:

- toiminta-aika 20 vuotta (ks. kuva 10)
- vikaantumistaajuus on vakio toiminta-aikana
- luokassa 2 vaateiden taajuus on enintään 1/100 testaustaajuudesta

Tässä menetelmässä luokkia pidetään rakenteina, joille on määritelty keskimääräinen diagnostiikan kattavuus (DCavg). Jokaisen turvallisuuteen liittyvän ohjausjärjestelmän osan suoritustaso riippuu rakenteesta, jokaisen kanavan vaarallisesta keskimääräisestä vikaantumisajasta (MTTFd) ja keskimääräisestä diagnostiikan kattavuudesta (DCavg). Myös yhteisvikaantumiset (CCF) olisi otettava huomioon.

Kuvassa 4 esitetään kunkin kanavan vaarallisen keskimääräisen vikaantumisajan (MTTFd) ja keskimääräisen diagnostiikan kattavuuden (DCavg) yhdistelmän avulla graafinen menetelmä turvallisuuteen liittyvän ohjausjärjestelmän osan saavuttaman suoritustason määrittämiseksi. Luokkien yhdistelmä (mukaan lukien yhteisvikaantumiset) ja DCavg määrittävät, mikä kuvan 4 pylväs on valittava. Kunkin kanavan vaarallisen keskimääräisen vikaantumisajan mukaisesti valitaan kyseisestä pylväästä yksi kolmesta erilaisella täyttökuviolla osoitetusta alueesta. Edellä mainitun alueen pystysuora sijainti määrittää saavutetun suoritustason, joka voidaan lukea pystyakselilta.



Merkitysten selitykset:

PL	suoritustaso
1	kunkin kanavan $MTTF_d$ = matala (low)
2	kunkin kanavan $MTTF_d$ = keskimääräinen (medium)
3	kunkin kanavan $MTTF_d$ = korkea (high)

Kuva 4. Luokkien, MTTFd- ja DCavg-arvojen keskinäinen suhde ja suoritustaso (PL)

2.4 EN/IEC 62061

2.4.1 Toiminnallisen turvallisuuden hallinta

Jokaiselle turvallisuuteen liittyvälle sähköisen ohjausjärjestelmän suunnitteluprojektille on laadittava toiminnallisen turvallisuuden suunnitelma. Sunnitelmassa on

- tunnistettava asiaankuuluvat toiminnot
- kuvattava politiikka, jolla täytetään määritetyt toiminnallisen turvallisuuden vaatimukset
- kuvattava strategia, jolla saavutetaan sovellusohjelmiston toiminnallinen turvallisuus kehittämistä, yhdistämistä, todentamista ja kelpuutusta varten.
- tunnistettava henkilöstö ja resurssit, jotka ovat vastuussa toimenpiteiden toteuttamisesta
- tunnistettava tai luotava menettelytavat ja resurssit merkityksellisten tietojen tallentamiseksi ja säilyttämiseksi, hyvä ottaa huomioon:
    - vaarojen tunnistaminen ja riskin arvioinnin tulokset
    - käytetyt laitteet ja niiden turvallisuusvaatimukset
    - ylläpidosta vastuussa olevat organisaatiot
    - menettelytavat
- kokoonpanon hallinnan strategia
- esitettävä todentamissuunnitelma, jossa on oltava:
    - todentamisen käyttöönoton yksityiskohdat
    - todentamisesta huolehtivien henkilöiden, osastojen ja yksiköiden yksityiskohdat
    - todentamisen strategioiden ja tekniikoiden valinta
    - testauslaitteiden valinta ja käyttö
    - todentamisen toimenpiteiden valinta
    - hyväksymiskriteerit
    - todentamisen tulosten arviointiin käytettävät menetelmät
- esitettävä kelpuutussuunnitelma, jossa on oltava:
    - kelpuutuksen käyttöönoton yksityiskohdat
    - koneeseen kuuluvien käyttötapojen tunnistaminen (esimerkiksi tuotantokäyttö, asetuskäyttö)
    - vaatimukset, joihin turvallisuuteen liittyvää sähköistä ohjausjärjestelmää verrataan kelpuutuksessa
    - kelpuutuksen tekninen strategia, esimerkiksi analyyttiset menetelmät tai tilastolliset testaukset
    - hyväksymiskriteerit
    - toimenpiteet, joihin on ryhdyttävä, kun epäonnistutaan hyväksymiskriteerien täyttämisessä.

2.4.2 Turvallisuuden eheyden tasojen (SIL) asettaminen

Turvallisuuden eheyden taso (SIL) on standardissa EN 62061 määritetty taso, joka määrittää turvallisuuden eheyden vaatimukset turvallisuuteen liittyville sähköisen ohjausjärjestelmän ohjaustoiminnoille. Turvallisuuden eheyden tasoja on neljä, mutta standardi EN 62061 ei tarkastele tasoa neljä (SIL 4), koska sillä ei ole merkitystä konesovelluksiin tavallisesti liittyvän riskin pienentämisvaatimusten yhteydessä. Turvallisuuden eheyden taso kolme on korkein ja taso yksi matalin.

Standardissa IEC/EN 62061 esitetään menetelmä turvallisuuden eheyden tason asettamiseksi, joka on tarkoitettu yleisesti sovellettavaksi, ja se perustuu riskin suuruuden laadulliseen määrittämiseen. Jokaista määrättyä vaaraa kohden olisi erikseen päätettävä turvallisuuden eheyden vaatimukset.

Riskin suuruuden arviointi

Riskin suuruuden arviointi tulisi tehdä jokaiselle vaaralle määrittämällä riskitekijät, jotka ovat

- vahingon vakavuus
- kyseisen vahingon esiintymistodennäköisyys, joka riippuu seuraavista muuttujista:
  - henkilön vaaralle altistumisen taajuus ja kesto (Frequency, Fr)
  - vaarallisen tapahtuman esiintymistodennäköisyys (Probability, Pr)
  - mahdollisuus välttää tai rajoittaa vahinkoa (Avoidance, Av).

Vahingon vakavuus (Se)

Vahingon vakavuutta arvioidaan tarkastelemalla palautuvia vammoja, palautumattomia vammoja ja kuolemantapauksia. Vahingon vakavuus luokka valitaan taulukosta 6 vammojen vakavuuden arvioinnin perusteella.

Taulukko 6. Vahingon vakavuuden (Se) luokittelu

Seuraukset	**Vakavuuden luokka (Se)**
Palautumattomat: kuolemantapaus, silmän tai käden menetys	4
Palautumattomat: murtuneet raajat, sormien menetys	3
Palautuvat: tarvitaan sairaanhoitoa	2
Palautuvat: tarvitaan ensiapua	1

Vakavuuden luokkien määritykset:

4) tarkoittaa kuolemantapausta tai merkittävää palautumatonta vammaa silloin, kun on hyvin vaikeaa jatkaa parantumisen jälkeen samaa työtä tai palata lainkaan työhön.

3) tarkoittaa suurta tai palautumatonta vammaa silloin kun voi olla mahdollista jatkaa samaa työtä paranemisen jälkeen. Tähän voi myös kuulua suuri ja vakava, mutta palautuva vamma, esimerkiksi raajojen luunmurtumat.

2) tarkoittaa palautuvaa vammaa mukaan lukien vakavat viiltohaavat, pistohaavat ja vakavat ruhjeet, joihin tarvitaan sairaanhoitoa.

1) tarkoittaa vähäisiä vammoja mukaan lukien naarmut ja vähäiset ryhjeet, joissa hoitona tarvitaan ensiapua.

Haitan esiintymistodennäköisyys

Jokainen haitan esiintymistodennäköisyyden kolmesta muuttujasta (Fr, Pr, ja Av) olisi arvioitava toisistaan riippumattomasti. Jokaiselle riskitekijälle on tarpeen käyttää pahimman tilanteen oletusta sen varmistamiseksi, että turvallisuuteen liittyvään ohjaustoimintoon ei asetettaisi virheellisesti alempaa turvallisuuden eheyden tasoa kuin on tarpeen. Yleisesti ottaen suositellaan käyttöönotettavaksi työtehtäviin perustuvaan analyysiin tarkoitettua lomaketta varmistamaan, että vahingon esiintymistodennäköisyyden arvioinnissa on tehty tarvittavat tarkastelut.

Altistumisen taajuus ja kesto

Altistumistason määrittämiseksi on otettava huomioon seuraavat näkökohdat:

- tarve päästä vaaravyöhykkeelle ottaen huomioon koneen kaikki käyttötavat, esimerkiksi normaalitoiminta, kunnossapito
- pääsyn luonne, esimerkiksi materiaalin käsisyöttö ja asetus.

Olisi oltava mahdollista arvioida altistumisen keskimääräiset aikavälit ja sillä perusteella vaaravyöhykkeelle pääsyn keskimääräinen taajuus.

Olisi myös oltava mahdollista ennakoida altistumisen kesto, esimerkiksi onko se pidempi kuin 10 minuuttia. Jos kesto on lyhyempi kuin 10 minuuttia, altistumisen pistearvo voidaan pienentää alemmalle tasolle. Tämä ei koske altistumisen taajuuksia enintään kerran tunnissa, jolloin vähennystä ei tehdä millään keston pituudella.

Taulukosta 7 valitaan sopiva rivi altistumisen taajuudelle ja kestolle (Fr).

Taulukko 7. Altistumisen taajuuden ja keston luokittelu (Fr)

Altistumisen taajuus (kesto > 10 minuuttia)	Altistumistaso (Fr)
≤ 1 tunti	5
> 1 tunti…≤ 1 päivä	5
> 1 päivä…≤ 2 viikkoa	4
> 2 viikkoa…≤ 1 vuosi	3
> 1 vuosi	2

Vaarallisen tapahtuman esiintymistodennäköisyys

Vaarallisen tapahtuman esiintymistodennäköisyydelle olisi valittava luokka ”erittäin todennäköinen” kuvaamaan tavanomaisen tuotannon rajoituksia ja pahimman tilanteen tarkastelua. Käytettäessä mitä tahansa alemmista tasoista, vaaditaan myönteisiä tekijöitä (esimerkiksi hyvin määriteltävä sovellus ja käyttäjien ammattitaidon korkea taso). Taulukkossa 8 on taulukoitu tapahtuman todennäköisyysluokat ja niitä vastaavat todennäköisyystasot (Pr).

Taulukko 8. Todennäköisyyden (Pr) luokittelu

Tapahtuman todennäköisyysluokat	Todennäköisyystaso(Pr)
Erittäin todennäköinen	5
Todennäköinen	4
Mahdollinen	3
Harvoin	2
Ei oteta huomioon	1

Vahingon välttämisen tai rajoittamisen todennäköisyys

Tätä muuttujaa voidaan arvioida ottamalla huomioon koneen suunnittelijan näkökohdat ja koneen käyttötarkoitus, jotka voivat auttaa välttämään tai rajoittamaan vaaran aiheuttamaa vahinkoa. Näihin näkökohtiin kuuluvat esimerkiksi:

- vaarallisen tilanteen ilmaantumisen äkillisyys, nopeus tai hitaus.
- tilan antamat mahdollisuudet väistää vaaraa.
- komponentin tai järjestelmän luonne, esimerkiksi puukko on tavallisesti terävä, putki meijeriympäristössä on tavallisesti kuuma, sähkö on tavallisesti luonteeltaan vaarallista, mutta ei näkyvää.
- mahdollisuudet tunnistaa vaara, esimerkiksi sähköinen vaara: kuparijohtimen ulkonäkö ei muutu sen ollessa jännitteinen tai jännitteetön. Tämän tunnistamiseen tarvitaan mittalaite, jolla todetaan, onko sähkölaitte jännitteellinen. Ympäristöolosuhteet, esimerkiksi korkea melutaso voivat estää henkilöä kuulemasta koneen käynnistymisen.

Vaaran välttämisen tai rajoittamisen todennäköisyyden tasot on määritetty taulukossa 9 ja jokaisella tasolla on tasoa vastaava vaaran välttämisarvo (Av).

Taulukko 9. Vaaran välttämisen tai rajoittamisen tödennäköisyydet (Av)

Vahingon välttämisen tai rajoittamisen todennäköisyydet	Av
Mahdoton	5
Harvoin	3
Todennäköistä	1

Vahingon todennäköisyysluokka (Class, Cl)

Jokaiselle vaaralle ja tarvittaessa jokaiselle vahingon vakavuuden tasolle lasketaan taulukoista saadut pisteet yhteen (Fr, Pr ja Av) ja summaksi saadaan vahingon todennäköisyyden luokka ”Cl”.

ESIMERKKI: Jos on määritetty vaara, jolle on merkitty seuraavat muuttujat:

- Fr = 5, koska vaaralle altistutaan monta kertaa päivässä
- Pr = 4 eli todennäköinen, koska käyttäjien ammattitaito on korkea
- Av = 3, koska on mahdollista välttää vaara, mutta epätodennäköistä

Tällöin vaaralle saadaan vahingon todennäköisyyden luokaksi (Cl):

Cl = 5 + 4 + 3 = 12

Turvallisuuden eheyden tason (SIL) asettaminen

Turvallisuuden eheyden taso (SIL) asetetaan vamman vakavuuden ja vahingon todennäköisyyden luokan avulla taulukon 10 mukaan.

ESIMERKKI: Jos vaarana käytetään vahingon todennäköisyyden luokka-osiossa esimerkkinä ollutta vaaraa, jonka Cl = 12 ja tälle vaaralle määritetään vamman vakavuudeksi Se = 3, koska on olemassa sormen menettämisen riski. Tällöin taulukon 10 mukaan SIL-tasoksi asetetaan SIL 2.

Taulukko 10. Turvallisuuden eheyden tason asettamisen matriisi

Vahingon vakavuus (Se)	Luokka (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Mustat ruudut osoittavat turvallisuuteen liittyvälle ohjaustoiminnolle asetettavan turvallisuuden eheyden tason tavoitetta. Harmaat ruudut osoittavat, että suositellaan muiden (kuin sähköiseen ohjausjärjestelmään liittyvien) turvallisuustoimenpiteiden käyttämistä (Other Methods, OM).

2.4.3 Saavutetun turvallisuuden eheyden tason määrittäminen

Turvallisuuden eheyden tasoa, jonka turvallisuuteen liittyvä sähköinen ohjausjärjestelmä voi saavuttaa, on tarkasteltava erikseen jokaiselle turvallisuuteen liittyvän sähköisen ohjausjärjestelmän toteuttamalle turvallisuuteen liittyvälle ohjaustoiminnolle.

Saavutettu turvallisuuden eheyden taso määritetään turvallisuuteen liittyvän sähköisen ohjausjärjestelmän muodostavien alajärjestelmien vaarallisten satunnaisten laitevikojen todennäköisyyksien, rakenteellisten rajoitusten ja turvallisuuden systemaattisen eheyden avulla. Saavutettavan turvallisuuden eheyden tason on oltava pienempi tai yhtä suuri kuin alin mille tahansa alajärjestelmälle vaadittava turvallisuuden eheyden taso.

Turvallisuuteen liittyvän sähköisen ohjausjärjestelmän vaarallisen satunnaisen laitevikaantumisen todennäköisyys (PFH_D) saadaan laskemalla kaikkien alajärjestelmien vaarallisten satunnaisten laitevikaantumisten todennäköisyyksien (PFH_{DSS}) summa, ja niihin kuuluu tarvittaessa digitaalisten tietoliikenneprosessien tiedonsiirron vaarallisten vikaantumisten todennäköisyys (PTE):

$$PFH_D = PFH_{DSS1} + ... + PFH_{DSSn} + PTE$$

Tämä lähestymistapa perustuu toimilohkon määritelmään, jossa minkä tahansa toimilohkon vikaantuminen johtaa ohjaustoiminnon vikaantumiseen.

Saadun PFH_D-arvon avulla saadaan selvitettyä saavutettu SIL-taso käyttäen apuna taulukkoa 2.

Alajärjestelmän vaarallisen satunnaisen laitevikaantumisen (PFH_{DSS}) laskenta

Standardin 62061:n laskutapa perustuu alajärjestelmän perusrakenteen määrittämiseen. Tämä tarkoittaa, että jokaiselle alajärjestelmälle tulee valita jokin neljästä perusrakenteesta (A, B, C tai D) ja laskea vaarallinen satunnainen laitevikaantuminen (PFH_{DSS}) käyttämällä kyseiselle rakenteelle määritettyä kaavaa. Kuvissa 5-9 on eri alajärjestelmien loogiset esitykset. Alajärjestelmien perusrakenteiden suhteen tehdään oletus, että alajärjestelmien elementtien

vikataajuudet (λ) ovat vakioita ja tarpeeksi pieniä. Valmistaja on voinut myös määrittää valmistamilleen komponenteille vaarallisen satunnaisen laitevikaantumisen tai vikataajuuden arvon. Tämän perusteella voidaan käyttää seuraavia yhtälöitä:

$\lambda = 1/MTTF$

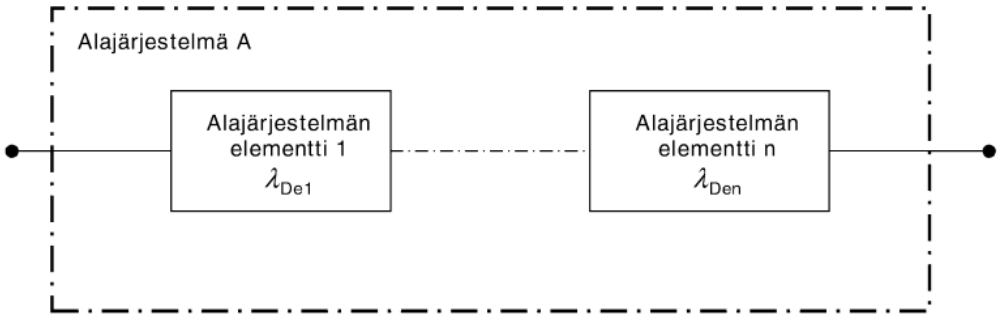
Sähkömekaanisille laitteille vikataajuus määritetään käyttämällä B_{10}-arvoa ja sovelluksen toimintajaksojen lukumäärää C seuraavasti:

$\lambda = 0{,}1 \times C/B_{10}$

Alajärjestelmän perusrakenne A: vikasietoisuus nolla, ilman diagnostiikkatoimintoa

$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den}$

$PFH_{DssA} = \lambda_{DssA} \times 1h$

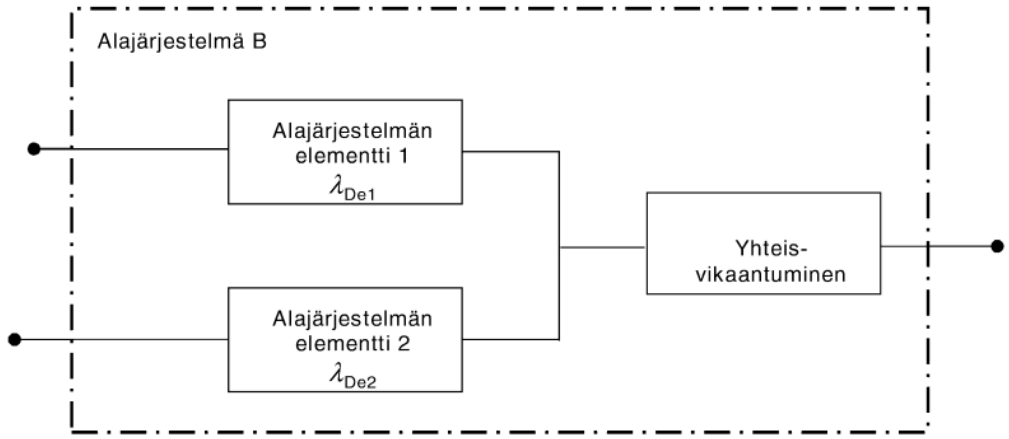


Kuva 5. Alajärjestelmän A looginen esitys

Alajärjestelmän perusrakenne B: vikasietoisuus yksi, ilman diagnostiikkatoimintoa

$\lambda_{DssB} = (1 - \beta)2 \times \lambda_{De1} \times \lambda_{De2} \times T1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssB} = \lambda_{DssB} \times 1h$

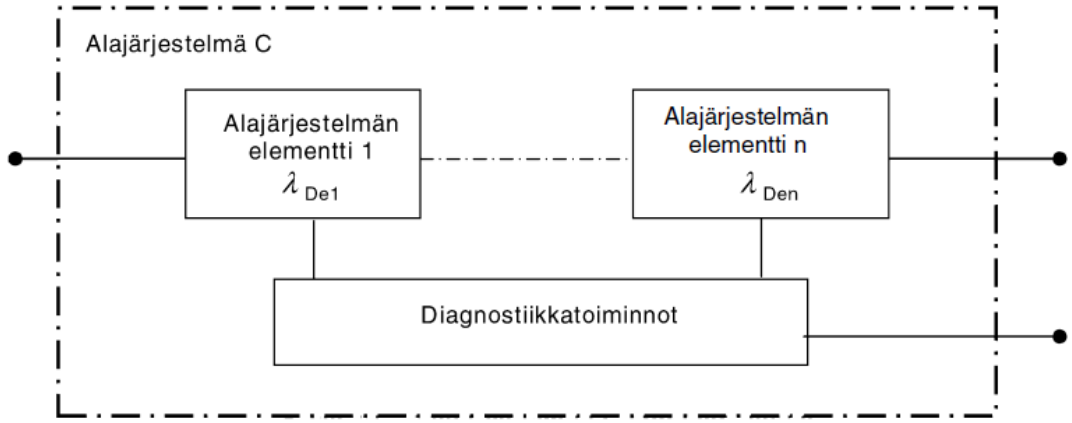


Kuva 6. Alajärjestelmän B looginen esitys

Alajärjestelmän perusrakenne C: vikasietoisuus nolla, diagnostiikkatoiminto

$\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + ...+ \lambda_{Den}(1 - DC_n)$

$PFH_{DssC} = \lambda_{DssC} \times 1h$

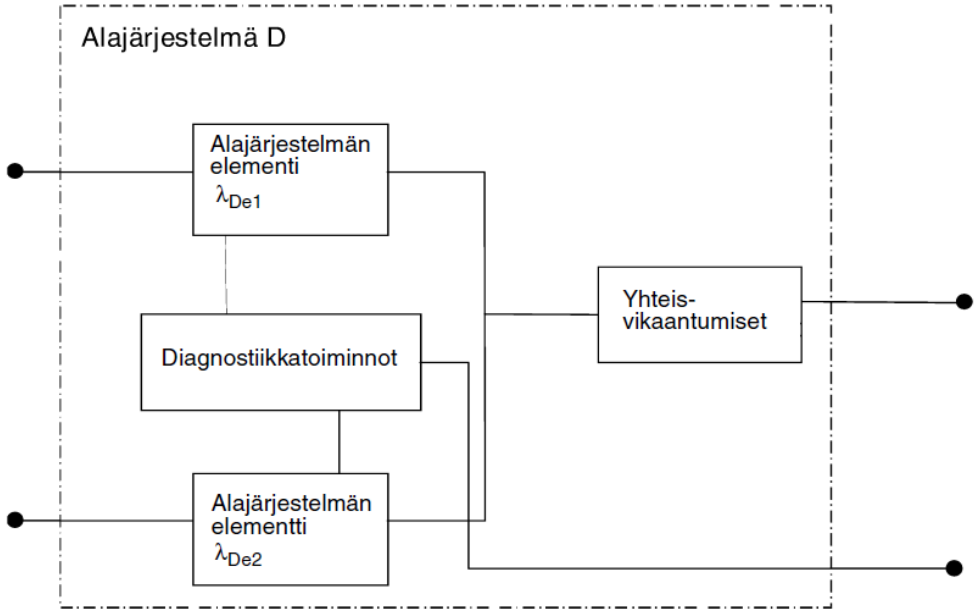


Kuva 7. Alajärjestelmän C looginen esitys

Alajärjestelmän perusrakenne D: vikasietoisuus yksi, diagnostiikkatoiminto

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times T_2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times T_1/2 \} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$



Kuva 8. Alajärjestelmän D looginen esitys

Yhteisvikaantumistekijän (β) arviointi

Tässä kappaleessa esitetään yksinkertainen lähestymistapa yhteisvikaantumisten arviointiin ja sitä voidaan soveltaa alajärjestelmien suunnitteluun.

Tämä yksinkertainen menetelmä toimii niin, että arvioitavaa järjestelmää arvioidaan taulukon 11 perusteella, pisteytetään järjestelmä ja lasketaan kokonaispistemäärä, jonka avulla määritetään yhteisvikaantumistekijän arvo taulukosta 12.

Taulukko 11. Kriteerit yhteisvikaantumistekijän arvioinnille

Kohde	Pisteet
Erillisyys ja erottelu	
Ovatko turvallisuuteen liittyvän sähköisen ohjausjärjestelmän yksittäisten kanavien signaalikaapelit reititetty erillisesti muista kanavista kaikissa kohdissa tai onko ne riittävästi suojattu?	5
Jos käytetään tietojen koodausta ja purkua, onko se riittävä signaalien siirtovirheiden paljastumiseksi?	10
Onko turvallisuuteen liittyvän sähköisen ohjausjärjestelmän signaalikaapelit ja energiansyöttökaapelit erotettu kaikissa kohdissa tai onko ne riittävästi suojattu?	5
Jos alajärjestelmän elementit voivat osaltaan vaikuttaa yhteisvikaantumiseen, onko ne järjestetty fyysisesti erotettuihin laitteisiin omissa paikallisissa suojakoteloissaan?	5
Erilaisuus ja varmennus	
Käytetäänkö alajärjestelmässä erilaisia sähköisiä teknologioita, esimerkiksi yhtenä elektroninen tai ohjelmoitava elektroninen rele ja toisena sähkömekaaninen rele?	8
Onko alajärjestelmässä käytetty elementtejä, joissa käytetään erilaisia fysikaalisia periaatteita (esimerkiksi suojuksen oven asennon tunnistavat elementit, joissa käytetään mekaanisia ja magneettisia tunnistustekniikoita)?	10
Käytetäänkö alajärjestelmissä hyväksi elementtejä, joissa on eriaikaisuutta toimintojen suorittamisessa tai vikamuodoissa?	10
Onko alajärjestelmän elementeillä diagnostiikkatestausta aikavälillä, joka on enintään yksi minuutti?	10
Monimutkaisuus, rakenne ja sovellus	
Onko alajärjestelmien kanavien ristiinkytkentä estetty lukuunottamatta tilannetta, jossa sitä on tarkoitus käyttää diagnostiikkatestaukseen?	2
Arviointi ja analysointi	
Onko vika- ja vaikutusanalyysin tulokset tutkittu yhteisvikaantumisten lähteiden määrittämiseksi ja onko etukäteen määritetyt yhteisvikaantumisten lähteet poistettu suunnittelun avulla?	9
Onko kenttälaitteiden vikaantumiset analysoitu ja tulokset otettu huomioon suunnittelussa?	9
Ammattitaito ja koulutus	
Ymmärtävätkö alajärjestelmän suunnittelijat yhteisvikaantumisten syyt ja seuraukset?	4
Ympäristöolosuhteiden hallinta	
Ovatko alajärjestelmän elementit soveltuvia toimimaan kaikissa tilanteissa niissä lämpötilan, kosteuden, korroosion, pölyjen, tärinän jne. rajoissa, joihin ne on testattu käyttämättä ulkoisten ympäristöolosuhteiden hallintaa?	9
Onko alajärjestelmien sähkömagneettisten häiriöiden sieto standardin liitteessä E esitettävien vaihteluvälien ja niiden rajojen mukainen?	9

Taulukko 12. Yhteisvikaantumistekijän määrittäminen

Yhteispisteet	Yhteisvikaantumistekijä (β)
< 35	10 % (0,1)
35 - 65	5 % (0,05)
65 - 85	2 % (0,02)
85 - 100	1 % (0,01)

3 Beckhoffin TwinSAFE-turvaratkaisu

3.1 TwinSAFE

TwinSAFE on Beckhoffin kehittämä turvaratkaisu EtherCAT-kenttäväylässä. TwinSAFE mahdollistaa turvakomponenttien käytön ja yhteensopivuuden mitä tahansa kenttäväylää käyttävän systeemin kanssa. Turvaratkaisun ja turvakomponenttien käyttäminen on välttämätöntä, jos halutaan saavuttaa standardien määrittämiä turvallisuustasoja. Turvakomponenttien tarjoamat turvaominaisuudet pitää kuitenkin ohjelmoida erikseen käyttöön. TwinSAFE ei saa haitata tai hidastaa koneen tai perusohjelman toimintaa millään tavalla, eikä perusohjelma saa vaikuttaa TwinSAFEn toimintaan millään tavalla.

3.1.1 Vaatimukset

Standardien vaatimia turvallisuustasoja ei voida saavuttaa tavallisilla EtherCAT-laitteistolla, vaan tarvitaan turvaratkaisu, kuten TwinSAFE. TwinSAFE-komponentit täyttävät vähintään EN 62061:n SIL 2-tason tai ISO 13849-1:n PL d-tason vaatimukset ja TwinSAFE:n käyttämä Safety over EtherCAT-kommunikaatiojärjestelmä täyttää siltä vaaditut standardit, jotka määritetään standardissa IEC 61784-3. Standardi IEC 61784-3 määrittää myös seuraavat virheoletukset kommunikaatiojärjestelmän verkostolle, jotka turvallisuusprotokollan tulee pystyä hoitamaan soveliain toimin:

- korruptio
- toisto
- vaihto
- häviö
- viive
- lisäys
- naamiointi
- viestien epäkelvoksi osoittaminen.

Safety over EtherCATin turvallisuusprotokolla pystyy vastaamaan standardin määrittämiin virheoletuksiin eri toimenpitein, jotka näkyvät taulukosta 13.

Taulukko 13. FSoE:n toimenpiteet eri virhetilojen havaitsemiseksi

Measure / Error	Sequence number	Watchdog	Connection ID	CRC calculation
Unintended repetition	☑			☑
Loss	☑	☑		☑
Insertion	☑			☑
Incorrect sequence	☑			☑
Corruption				☑
Unacceptable delay		☑		
Masquerade		☑		☑
Repeating memory errors in switches	☑			☑
Incorrect forwarding between segments			☑	

3.1.2 Turvakomponentit

Beckhoff valmistaa kolmen tyyppisiä turvakomponentteja: TwinSAFE-logiikkaohjaimia, TwinSAFE-tuloterminaaleja ja TwinSAFE-lähtöterminaaleja. Turvakomponentit voi vapaasti kytkeä muiden EtherCAT-terminaalien sekaan. Tavallisiin komponentteihin verrattuna, turvakomponenteissa on rakenteellisina eroina:

- 2 mikroprosessoria (tavallisessa vain 1)
- aina kaksikanavaisia
- rakenteellinen suunnittelu.

Ohjelmoitava logiikkaohjain on käytännössä pieni tietokone, jota käytetään reaaliaikaisten automaatioprosessien ohjaamiseen, kuten esimerkiksi NC-koneen. Ohjaamista varten logiikkaohjaimelle on kirjoitettava ohjelma, joka kirjoitetaan tietokoneella, ja valmis ohjelma siirretään logiikkaohjaimelle suoritettavaksi. TwinSAFE-logiikkaohjain on käytännössä hyvin samanlainen kuin tavallinen logiikkaohjain, mutta TwinSAFE-logiikkaohjain on välttämätön osa turvaratkaisua. Ilman TwinSAFE-

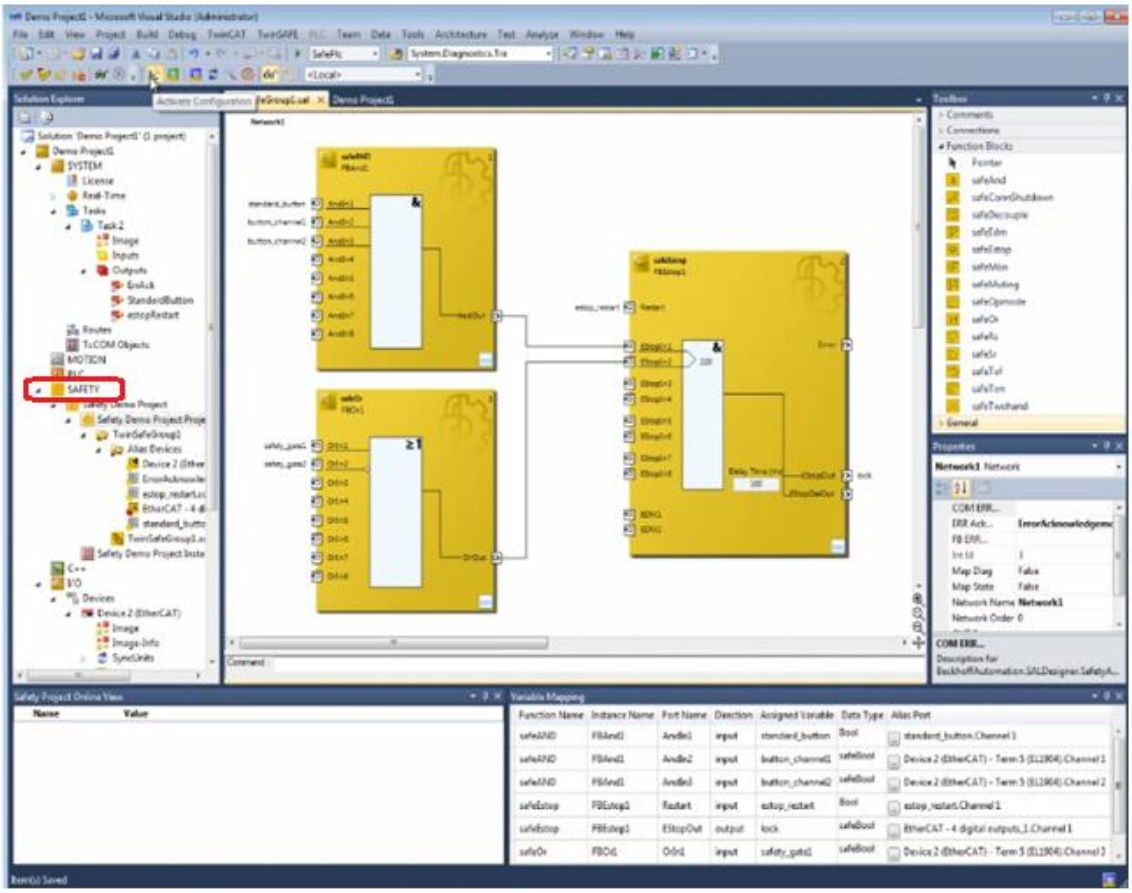
logiikkaohjainta ei TwinSAFEn tuomaa turvaratkaisua voida käyttää. Jos aiotaan siis hyödyntää TwinSAFEa, ensin valitaan TwinSAFE-logiikkaohjain.

Tulomoduuli on moduuli, joka yhdistää syöttölaitteen (esimerkiksi anturin) ohjelmoitavaan logiikkaohjaimeen. Toisin kuin tavallisella tulomoduuli, TwinSAFE-tulomoduulin jokaisen tulokanavan toiminta voidaan varmentaa ennen käyttöä ja niiden toimintaa voidaan monitoroida. Diagnostiikan suhteen, TwinSAFE-tulomoduuleissa on kommunikaation, prosessorien ja anturien monitorointi. Tulomoduuleissa on myös fail-safe-ominaisuus, joka tarkoittaa, että moduuli kytketään pois päältä automaattisesti järjestelmän havaitessa virheen.

Lähtömoduuli on moduuli, jolla yhdistetään toimilaite (esimerkiksi moottori) ohjelmoitavaan logiikkaan. Verrattuna tavalliseen lähtömoduuliin, TwinSAFE-lähtömoduuli monitoroi lähtökanavia, ja jos jonkinlainen virhe havaitaan yhdessäkään lähtökanavassa, turvalogiikan ohjausjärjestelmä toteaa järjestelmävirheen. Virheen havaitessaan, ohjausjärjestelmä järjestelmä odottaa ohjelmoidun viiveen ajan ja mikäli virhe ei poistu, järjestelmä suorittaa turvallisen sammutuksen. Diagnostiikkatoimintojen suhteen, TwinSAFE-lähtömoduulissa on pulssitustesti, kommunikaation, prosessorien, jännitteen ja lämpötilan monitorointi. Näillä diagnostiikkakeinoilla havaitaan oikosulut, yli- ja alijännite, lähdön ja prosessorien toimintavirhe, ylikuumeneminen ja johtojen ehjyys.

3.1.3 Ohjelmointijärjestelmä

TwinSAFEn ohjausjärjestelmä on integroitu Beckhoffin TwinCAT 3-ohjelmaan. Tämä mahdollistaa TwinSAFEn käytön järjestelmissä, joissa on jo tavallinen ohjelmoitu logiikka, käyttämällä yhtä ja samaa TwinCAT 3-ohjelmaa. Turvatoimintojen ohjelmointi tapahtuu safety-osiossa, kuten kuva 9 näyttää.



Kuva 9. Safety-osio ja turvatoiminnon visualisointi TwinCAT 3-ohjelmassa

TwinCAT-ohjelmaa voidaan siis käyttää ohjelmoimaan koko sen koneen toiminta, johon turvatoiminnot kehitetään. Tämä tekee koneesta täysin läpinäkyvän, mikä tarkoittaa, että koneeseen ei voi teoriassa ilmetä virhettä, mitä ohjelma ei pystyisi havaitsemaan. Jos jouduttaisiin käyttämään useampaa kuin yhtä ohjelmaa koneen ohjelmointiin ja käyttöön, niin ohjelmien väliseen kommunikaatioon syntyy sokeita pisteitä, josta kumpikaan ohjelma ei havaitse mahdollisen virheen ilmenemistä.

3.1.4 Safety over etherCAT

Safety over EtherCAT (FSoE, Fail-Safe over EtherCAT) on avoin turvallisuusportokolla, joka määrittää turvallisen kommunikaatiokanavan turvatun sekä perusinformaation lähetykseen samassa kommunikaatiosysteemissä aiheuttamatta rajoituksia lähetysnopeuteen, kiertoaikaan tai turvadatan kertasiirron määrään. missään kenttäväyläsysteemissä sen kenttäväyläneutraalin turvaprotokollan ansiosta. Tämä

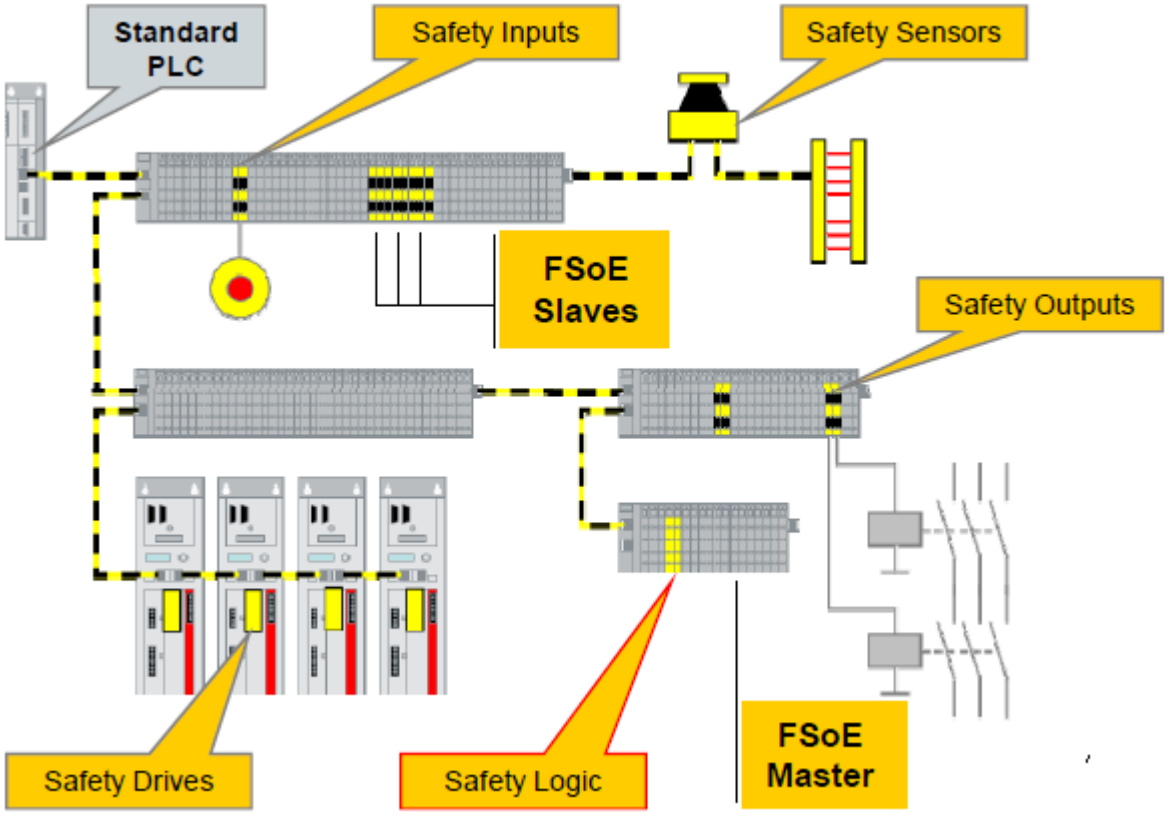
kommunikaatiokanava kulkee samaa kanavaa pitkin, kuin perusohjelman kommunikaatiokin.

Safety over EtherCAT on suunniteltu täyttämään EN 62061 SIL 3-tason vaatimukset. Standardi EN 62784-3 määrittää, ettei turvakommunikaatiokanava vaatisi enempää kuin 1 % koko PFD tai PFH arvosta. Tämä tarkoittaa, että jos esimerkiksi turvatoiminnolta vaaditaan SIL 3-tason turvallisuuden eheyden taso, niin turvakommunikaation PFH-arvon pitää olla alle 10^{-9} virhettä/h, mikä tarkoittaa 100 000 vuotta kommunikaatiota virheettä.

Kommunikaatiokierros

FSoE master lähettää *FSoE master framen*, joka sisältää safety-lähtöjen datan, FsoE:n määrittämää kommunikaatiokanavaa pitkin. Tämä frame kulkee aina *FSoE slaveille* asti, jotka vastaanottavat *master framen* tuomat tiedot ja lähettävät masterille *FSoE slave framen*. Tämä sisältää safety tulojen datan sekä ilmoituksen, milloin *FSoE master frame* kävi *FSoE slavella*. Kuvassa 9 on esimerkkikaavio, johon on merkitty *FSoE master* ja *FSoE slavet.*

Samalla hetkellä, kun *FSoE master* lähetti *master framen*, käynnistyi masterissa watchdog-ajastin, joka ajastaa, milloin *FSoE slave frame* saapuu masterille. Tällä tavoin määritetään, onko kommunikaatiossa viivettä ja että *FSoE master frame* käy jokaisella *FSoE slavella*. *FSoE master* lähettää uuden *master framen* vain, jos sekä *slave frame* saapui masterille että myös watchdog-ajastin ei havainnut ongelmia. *FSoE framessa*, turvadata jaetaan kahden bitin paloihin ja jokaista kahta bittiä turvadataa kohden on kaksi bittiä CRC-laskentaa, joka tarkastaa 2 bittiä turvadataa.



Kuva 10. Esimerkkikaavio ohjausjärjestelmästä

3.2 Turvallisuustason saavuttaminen TwinSAFE-turvaratkaisun avulla

Aluksi kone ja sen toiminto suunnitellaan, sitten tehdään riskianalyysi. Riskianalyysin avulla havaitaan vaarakohdat. Määritetään turvatoiminnot ja vaadittava suoritustaso (tai toisinpäin). TwinSAFE-turvaratkaisua ruvetaan varsinaisesti soveltamaan vasta kun turvatoimintojen rakennetta ja toteutusta ruvetaan sunnittelemaan. Turvatoiminnon rakenne määriytyy käytettävän standardin ja vaadittavan suoritustason mukaan.

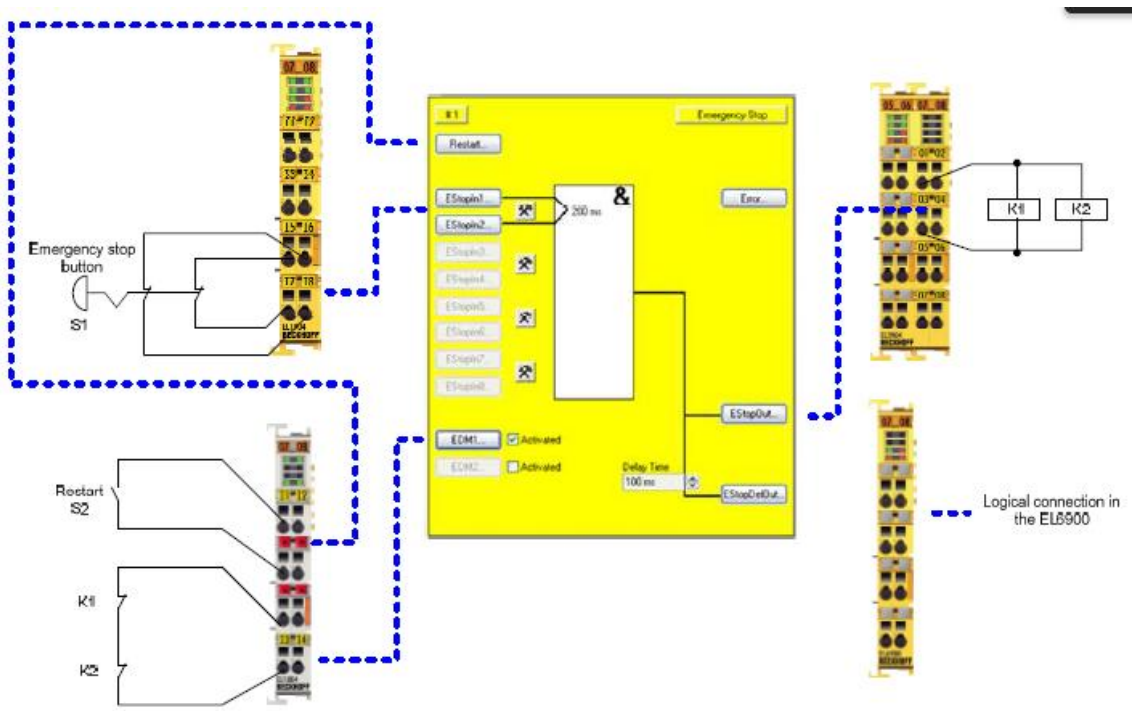
Beckhoff on tehnyt TwinSAFE-soveltamisohjeen nimeltä ApplicationGuideTwinSAFEen.pdf, josta löytyy 23 turvatoiminnon piiriesimerkkiä. Näille piiriesimerkeille on jo valmiiksi määritetty komponentit, lohkokaavioesitys, visuaalinen kytkentä, jossa myös ohjelmointiin tarvittava function block ja esimerkille on ennalta laskettu standardin 13849-1 mukainen, saavutettu turvallisuustaso. Soveltamisohjeesta löytyy myös jokaiselle käytetylle komponentille turvallisuustason määrittämisen kannalta olennaiset arvot, kuten vaarallinen vikaantumisaika ja diagnostiikan kattavuus.

Jos soveltamisohjeesta löytyy soveltamiskelpoinen esimerkki, voidaan suoraan siirtyä turvatoiminnon ohjelmointiin ja varsinaiseen toteutukseen. Soveltamisohjeen esimerkkejä voi yrittää soveltaa, jos esimerkit eivät täysin vastaa haluttua. Muutoin tulisi soveltaa standardien käytännön sovellutuksia (ks. 2.2) tai konsultoida valmistajaa.

ESIMERKKI:

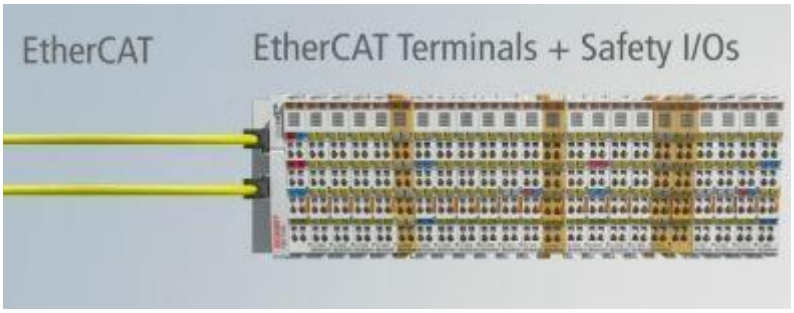
Halutaan hätäseis-turvatoiminto, jolle on asetettu turvallisuusvaatimukseksi suoritustaso PL d. Beckhoffin soveltamisohjeessa on ensimmäisenä esimerkkipiirinä hätäseis-turvatoiminnon variantti, joka on suoritettu luokkarakenteella 3 ja täyttää suoritustason PL d, jonka laskennallinen määritys löytyy myös ohjeesta. Tämän variantin toteuttamiseen tarvitaan EL1904 digitaalinen TwinSAFE tulomoduuli, EL2904 digitaalinen TwinSAFE lähtömoduuli, EL 6900 TwinSAFE logiikkaohjain, jokin vapaasti valittava vähintään 2-kanavainen tulomoduuli, hätäseis-painike ja kaksi kytkintä.

Kuvasta 11 huomataan, mihin kanaviin hätäseis-painike ja kytkimet johdotetaan. Kuvasta myös selviää, että turvatoiminnon ohjelmointiin ei tarvita muita function blockeja kuin Emergency Stop ja katkoviivoin kerrotaan, minkä tulo- tai lähtökanavan muuttuja liitetään mihinkin function blockin funktioon.



Kuva 11. Visuaalinen kytkentä, jossa myös ohjelmointiin vaadittu function block esillä.

Turvatoiminnon ohjelmointi tapahtuu TwinCAT 3-ohjelmassa safety-alavalikossa. Käytönnössä eri moduulit voidaan vapaasti kytkeä minne tahansa järjestelmää, kuten kuvasta 12 näkyy, joten moduulien sijoittamisella ei ole merkitystä toimintaan. Tämän jälkeen hätäseis-painike ja kytkimet liitetään moduulien kanaviin, otetaan turvatoiminnon ohjelma käyttöön ja turvatoiminto on valmis testattavaksi.



Kuva 12. Esimerkki terminaalien järjestyksestä

4 Yhteenveto

Standardit ISO 13849-1 ja EN 62061 antavat tarkat vaatimukset eri suoritustasojen saavuttamiseksi ja monet muuttujat onkin otettava huomioon aivan yksittäisten komponenttien tasolla. Tosin standardien vaatimukset riippuvat täysin siitä, kuinka turvallinen kyseessä olevasta laitteesta halutaan.

Standardien käytännön soveltaminen ja turvallisuustasojen saavuttaminen turvaratkaisun avulla paljastui odotettua työläämmäksi ja pidempikestoiseksi prosessiksi, koska nämä prosessit täytyy suorittaa jokaiselle koneen turvatoiminnolle erikseen. Jotkut laite- ja komponenttivalmistajat ovat laskeneet komponenteilleen eri arvoja, esimerkiksi vaarallisen vikaantumisen keskimääräisen todennäköisyyden tai vikaantumistaajuuden. Nämä arvot helpottavat ja nopeuttavat suuresti toimilaitteen saavuttaman turvallisuustason määrittämistä käytännössä.

Insinöörityötä pystyisi kehittämään eteenpäin selvittämällä, kuinka turvallisuustasot saavutettaisiin eri kenttäväylissä sekä miten turvatoimintojen ohjelmointi toteutetaan. Kuitenkin seuraava järkevä kehitysaskel olisi selvittää turvatoimintojen ohjelmointi TwinCAT-ohjelmalla, jolloin tämä tutkielma kattaisi turvallisuustason saavuttamisen TwinSAFE-turvaratkaisun avulla kokonaisuudessaan.

Insinöörityössä määritettyjä standardien käytönnön soveltamismahdollisuuksia pystytään käyttämään koneen toiminnallisen turvallisuuden implementointiin, pois lukien turvatoimintojen ohjelmointi ja testausvaiheet.

Lähteet

SFS-EN ISO 13849-1: Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki: Suomen Standardisoimisliitto. 28.12.2009.

SFS-EN 13849-1: Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Helsinki: Suomen Standardisoimisliitto. 27.3.2006.

Beckhoff Oy [PDF-tiedosto]. TwinSAFE Application Guide. Saatavissa: http://download.beckhoff.com/download/Document/TwinSAFE/ApplicationGuideTwinSAFEen.pdf

Beckhoff Oy [PDF-tiedosto]. TwinSAFE. Saatavissa: http://download.beckhoff.com/download/document/catalog/main_catalog/english/Beckhoff_TwinSAFE.pdf

Beckhoff Oy [multimedia presentaatio]. The safety solution for EtherCAT. saatavissa: http://www.beckhoff.com/english/highlights/FSOE/soe_presentation.htm?title=The+safety+solution+for+EtherCAT

EtherCAT Technology Group [PDF-tiedosto]. Safety over EtherCAT overview. saatavissa: http://www.ethercat.org/download/documents/Safety_over_EtherCAT_Overview.pdf

Avainasiakaspäällikkö Jukka Uotilan haastattelu. Beckhoff Oy. Hyvinkää. 29.4.2015

Liite 1. Yksinkertaistettu tapa diagnostiikan kattavuuden määrittämiseksi

Tässä liitteessä on standardin ISO 13849-1 yksinkertaistettu menetelmä diagnostiikan kattavuuden määrittämiseksi. Taulukossa on esimerkkejä, joiden perusteella voidaan arvioida turvatoiminnolle diagnostiikan kattavuus.

Taulukko 14. Esimerkkejä diagnostiikan kattavuudesta

Toimenpide	Diagnostiikan kattavuus (DC)
Tuloyksikkö	
Tulosignaalien dynaamisten muutosten aikaansaama jaksottainen testauksen käynnistys	90 %
Mielekkyyden tarkistus (esim. käyttämällä sulkeutuvia ja avautuvia mekaanisesti yhdistettyjä koskettimia)	99 %
Tulojen ristiinvalvonta ilman dynaamista testausta	0...90 % riippuen kuinka usein sovelluksessa tapahtuu signaalin tilamuutos
Jos oikosulkuja ei voida paljastaa, tulosignaalien ristiinvalvonta yhdessä dynaamisen testauksen kanssa, (useille I/O-yksiköille)	90 %
Tulosignaalien ja logiikan (L) väliarvojen ristiinvalvonta ja ohjelman suorituksen tilapäinen looginen ohjelmallinen valvonta sekä pysyvien vikojen ja oikosulkujen paljastaminen (useille I/O-yksiköille)	99 %
Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta)	90...90 % riippuen sovelluksesta
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99 %
Vikojen paljastuminen prosessin kautta	0...90 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle PL_r e.
Anturien joidenkin ominaisuuksien valvonta (vasteaika, analogisten signaalien vaihtelualue, kuten sähköinen vastus, kapasitanssi)	60 %

Taulukko 14 (jatkuu)

Toimenpide	Diagnostiikan kattavuus (DC)
Logiikka	
Epäsuora valvonta (esim. painekytkimen suorittama valvonta, toimilaitteiden aseman sähköinen valvonta)	90...99 % sovelluksesta riippuen
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99 %
Logiikan toiminnan yksinkertainen tilapäinen valvonta (esim. ajastinvahti, jolloin liipaisukohdat ovat logiikan ohjelmassa)	60 %
Logiikan toiminnan tilapäinen ja looginen valvonta ajastinvahdilla, jolloin testauslaitteet tarkistavat logiikan käyttäytymisen mielekkyyttä	90 %
Käynnistyksen itsetestaus piilevien vikojen paljastamiseen logiikan osissa (esim. ohjelma ja datamuistit, tulo- ja lähtöportit, rajapinnat)	90 % (riippuen testaustekniikasta)
Valvontalaitteiden reaktiokyvyn tarkistus (esim. ajastinvahti), joka tehdään pääkanavalla käynnistyksen yhteydessä tai kun tulee vaade turvatoiminnolle tai kun ulkoinen signaali vaatii turvatoimintoa tuloihin liitettävien laitteiden kautta	90 %
Dynaaminen periaate (kaikkien logiikan komponenttien on vaihdettava tilaa "PÄÄLLE – POIS – PÄÄLLE" kun turvatoimintoa vaaditaan), esimerkiksi releillä toteutettu toimintaankytkennän ohjauspiiri	99 %
Kiinteä muisti: yhden sanan pituinen varmenne (8 bittiä)	90 %
Kiinteä muisti: kahden sanan pituinen varmenne (16 bittiä)	99 %
Muuttuva muisti: RAM-testin suorittaminen käyttämällä redundanttista dataa, esimerkiksi lippuja, markkereita, vakioita, ajastimia ja näiden datojen ristikkäinen vertailu	60 %
Muuttuva muisti: käytettävien datan muistipaikkojen luettavuus- ja kirjoittamiskyvyn tarkistus	60 %
Muuttuva muisti: RAM-komponenttien valvonta muunnellulla Hamming-koodilla tai RAM-komponentin itsetestaus (esim. "galpat" tai "Abraham")	99 %
Prosessointiyksikkö: itsetestaus ohjelmallisesti	60...90 %
Prosessointiyksikkö: koodattu prosessointi	90...99 %
Vikojen paljastuminen prosessissa	0…99 % sovelluksesta riippuen, tämä menetelmä ei ole riittävä vaadittavalle suoritustasolle PL_r e.

Taulukko 14 (jatkuu)

Toimenpide	Diagnostiikan kattavuus (DC)
Lähtöyksikkö	
Yhden kanavan lähtöjen valvonta ilman dynaamista testausta	0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan signaalia
Lähtöjen ristiinvalvonta ilman dynaamista testausta	0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan signaalia
Lähtöjen ristiinvalvonta dynaamisella testauksella ilman oikosulkujen paljastumista	90 %
Lähtösignaalien ja logiikan (L) väliarvojen ristiinvalvonta sekä ohjelman suorituksen tilapäinen looginen ohjelmallinen valvonta sekä pysyvien vikojen ja oikosulkujen paljastaminen (useille I/O-yksiköille)	99 %
Redundanttinen signaalin sulkupolku ilman toimilaitteen valvontaa	0 %
Redundanttinen signaalin sulkupolku yhden toimilaitteen valvonnalla joko logiikan tai testauslaitteen avulla	90 %
Redundanttinen signaalin sulkupolku toimilaitteiden valvonnalla joko logiikan tai testauslaitteen avulla	99 %
Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta)	90...99 % sovelluksesta riippuen
Vikojen paljastuminen prosessin kautta	0...99 % sovelluksesta riippuen, tämä menetelmä ei ole riittävä vaadittavalle suoritustasolle PL_r e.
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99 %
HUOM. 1 Muita arviointimenetelmiä diagnostiikan kattavuudelle: katso esimerkiksi standardin IEC 61508-2:2000 taulukot A.2...A.15.	
HUOM. 2 Jos logiikalle vaaditaan diagnostiikan kattavuutta "keskimääräinen (medium)" tai "korkea (high)", on muuttuvalle muistille, kiinteälle muistille ja prosessointiyksikölle kullekin sovellettava vähintäänkin yhtä toimenpidettä, jolla saadaan diagnostiikan kattavuus tasolle 60 %. Tässä taulukossa lueteltujen toimenpiteiden lisäksi voi olla myös muita käytettävissä olevia toimenpiteitä.	