jamk.fi

Ohjausjärjestelmällä toteutettujen turvatoimintojen määrittely Protaconilla

Tapio Pekkarinen

Opinnäytetyö
Marraskuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), automaatiotekniikan tutkinto-ohjelma
Sähkövoimatekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Pekkarinen, Tapio	Opinnäytetyö, AMK	26.11.2017
	Sivumäärä 67	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Ohjausjärjestelmällä toteutettujen turvatoimintojen määrittely Protaconilla

Tutkinto-ohjelma

Automaatiotekniikan tutkinto-ohjelma

Työn ohjaaja(t)

Ari Kuisma, Veli-Matti Häkkinen

Toimeksiantaja(t)

Protacon Technologies Oy

Tiivistelmä

Automaation lisääntyminen koneiden ohjauksissa lisää tehokkuutta ja turvallisuutta kaikilla teollisuuden aloilla. Automaattisten järjestelmien luotettavuus on kuitenkin usein kyseenalaistettu turvallisuusmielessä. Koneiden turvallisuus on nykyään yhä enemmän ohjelmoitavien elektronisten laitteiden varassa, joka luo epävarmuutta. Turvallisuuteen liittyvien järjestelmien selkeä dokumentointi on tärkeässä asemassa automaation tuoman monimutkaisuuden vuoksi.

Opinnäytetyön konkreettisena tavoitteena oli kehittää Protacon Technologies Oy:lle toimintatapa ja malli, jolla dokumentoidaan turvatoimintojen toteutus projekteissa. Yrityksen aikaisempien projektien turvallisuuteen liittyvien järjestelmien dokumentointi on tehty vaihtelevilla tavoilla ja selkeä tapa toteutuksesta on jäänyt selvittämättä. Uudella dokumentointimallilla otetaan huomioon eri suunnitteluryhmien tarpeet turvallisten ohjausjärjestelmien suunnittelussa.

Teoriaosuuden tavoitteena oli perehtyä koneturvallisuuteen ohjausjärjestelmien osalta. Käytännön työn osuus toteutettiin Protaconin turvallisuusmäärittelyihin liittyvän projektin osana. Työssä käytettiin viimeisimpiä koneturvallisuuden standardeja tiedon oikeellisuuden varmistamiseksi.

Työn konkreettisena tuloksena saatiin yrityksen toimintatapoihin soveltuva turvajärjestelmien dokumentointimalli. Dokumentointimalli on suunniteltu ohjausjärjestelmä standardin osien SFS-EN ISO 13849-1 ja 13849-2 vaatimusten mukaiseksi dokumentoinnin osalta. Dokumentointimallia voidaan käyttää suunnittelussa pohjana projektista riippumatta sekä apuna mm. turvapiirien toiminnallisissa testauksissa.

Avainsanat (asiasanat)

Koneturvallisuus, ohjausjärjestelmä, turvatoiminto, turvallisuuteen liittyvä järjestelmä

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Pekkarinen, Tapio	Bachelor's thesis	26.11.2017
		Language of publication: Finnish
	Number of pages 67	Permission for web publication: X

Title of publication

Defining safety functions included in control system at Protacon

Degree programme

Electrical and Automation Engineering

Supervisor(s)

Kuisma Ari, Häkkinen Veli-Matti

Assigned by

Protacon Technologies Oy

Abstract

Increasing automation in machine control systems makes systems more effective and secure in all fields of industry. Reliability of automation systems is often questioned when it comes to the safety aspect of systems. Programmable electronic devices handle more and more safety data, which can cause insecurity in employees. Clear documentation of safety-related systems play an important role because of complicated automation systems.

The main objective of the project was to develop a procedure and model for safety-related documentation at Protacon. The company's safety documentation is implemented in various ways and it lacks a clear direction of how it should be done effectively. The new documentation model will pay attention to the needs of different design groups for successful planning.

The goals for the theory part of the thesis were to take a deeper look at control systems related to machine safety. The practical part of thesis was implemented as part of Protacon projects. The latest machine safety standards were applied during work to ensure that information is up to date.

The final result of the thesis was a documentation model suitable for the company's procedure of producing safety-related documentation. The documentation model is designed based on safety-related control systems standards SFS-EN ISO 13849-1 and 13849-2, which specify the most important issues related to the content of safety-related documentation. Regardless of project, the documentation model can be used as an example when starting to prepare safety-related documentation. It can also be used to help to understand safety circuits when carrying out functional testing for safety circuits.

Keywords/tags (subjects)

Machine safety, control system, safety function, safety-related system

Miscellaneous

Sisältö

Kuviot

Taulukot

Sanasto

ASi-väylä	Actuator Sensor Interface, anturointi- ja toimilaiteväylä
B_{10D}	Toimintajaksojen määrä, jossa 10 % komponenteista on vaarallisesti vikaantunut
DC	Diagnostiikan kattavuus
EFTA	Euroopan vapaakauppajärjestö
CENELEC	Eurooppalainen sähköalan standardisoimisjärjestö
HW	Hardware, laitteistosuunnittelu
I/O	Input/Output
IEC	Kansainvälinen sähköalan standardisoimisjärjestö
ISO	Kansainvälinen standardisoimisjärjestö
PL	Turvatoiminnon arvioitu suoritustaso
PLr	Turvatoiminnolta vaadittava suoritustaso
Profinet	Teollisuuden ethernet-standardi
SIL	Turvallisuuden eheystaso
SW	Software, ohjelmistosuunnittelu
TLJ	Turvallisuuteen liittyvä järjestelmä

1 Johdanto

1.1 Opinnäytetyön tavoitteet

Koneiden turvallisen toiminnan varmistaminen on hyvin tärkeä osa nykyaikaista teollisuuden prosessisähkösuunnittelua. Protacon Technologies Oy:llä on usean vuosikymmenen vahva kokemus mm. teollisuuden prosessisähköistys- sekä instrumentointisuunnittelusta. Yrityksen menestyminen kovasti kilpaillulla teollisuuden alalla vaatii monialaista osaamista sekä työn tuloksien positiivista näkyvyyttä esimerkiksi työpaikan työturvallisuuden osalta. Yhä useammat alan yritykset haluavatkin olla mukana ”nolla tapaturmaa” –hankkeessa. Koneturvallisuuden hallitsemista voidaankin sanoa nykyään yhdeksi tärkeimmistä asioista yrityksen julkisuuskuvaa ajatellen, jos haluaa menestyä markkinoilla. Protaconin vahva asiantuntijuus koneturvallisuuden saralla onkin varmasti yksi yrityksen menestystekijöistä.

Dokumentoinnin tärkeys koneturvallisuuden osalta on merkittävä. Selkeästi ja standardien mukaisesti suunnitellut sekä dokumentoidut turvallisuuteen liittyvät järjestelmät parantavat koneiden ja tehtaiden kokonaisturvallisuutta huomattavasti. Turvallisuuden parantuminen käy ilmi mm. monimutkaisten automaatiojärjestelmien dokumentoinnin selkeyttämisen seurauksena, joka johtaa turvallisuuteen liittyvien järjestelmien parempaan ymmärrykseen.

Tämän opinnäytetyön konkreettisena tavoitteena on kehittää Protaconille dokumentointimalli, jonka avulla saadaan yhtenäistettyä toimintatapoja eri suunnittelijaryhmien välillä turvallisuuteen liittyvien järjestelmien dokumentoinnissa ja suunnittelussa. Dokumentointimallin kehittämisen seurauksena saadaan tehostettua suunnittelua ja parannetaan yrityksen sisäistä yhteistyötä.

Raportin teoriaosuudessa käsitellään koneiden turvallisuuteen liittyvää yleistä asiaa, mutta pääpaino on niiden ohjausjärjestelmien turvatoimintojen vaatimuksissa ja

määrittelyiden tekemisessä. Käytännön osuus koostuu työn aiheena olevan dokumentointimallin kehittämisestä.

1.2 Protacon Technologies Oy

Protacon Technologies Oy on monialainen sähköalaan erikoistuneita suunnittelupalveluja tuottava yritys. Yrityksen suurimmat asiakkaat ovat pääosin kotimaisen teollisuuden parista sekä yhä kasvavissa määrin kansainvälisiltä markkinoilta. Protaconin vahvuuksia ovat erikoisosaaminen prosessi-, energia- ja konepajateollisuudesta sekä suurtenkin tehdasprojektien prosessi- ja instrumentointisuunnittelun hoitaminen aina esisuunnittelusta käyttöönottoon asti. Protacon tarjoaa palveluita myös mm. tehdas- ja laitossuunnittelusta, hydrauliikka- ja pneumatiikkasuunnittelusta sekä ohjelmistosuunnittelusta (Me olemme Protacon 2017).

Protacon Group Oy –konserni koostuu neljästä erillisestä osakeyhtiöstä. Emoyhtiönä toimii Protacon Group Oy, joka vastaa Protaconin operatiivisista toiminnoista. Protaconin Groupin tytäryhtiöitä ovat Protacon Technologies Oy, Protacon Solutions Oy ja Protacon Analyzes Oy:

- Protacon Technologies Oy tuottaa sähköistykseen liittyviä suunnittelupalveluja kattavasti monelle eri toimialalle.
- Protacon Solutions Oy on erikoistunut ohjelmisto- ja IT-puolelle ja tuottaa näin ollen ohjelmisto- ja IT-palveluja.
- Protacon Analyzes Oy tuottaa prosessianalyysipalveluita (Me olemme Protacon 2017).

Protaconilla on toimipisteitä Jyväskylän pääkonttorin lisäksi myös Jämsässä, Espoossa, Hollolassa, Kajaanissa, Kuopiossa, Kymenlaaksossa, Oulussa, Tampereella, Vaasassa ja Kiinassa Jiangyinissa. Protaconin koko liikevaihto oli vuonna 2016 n. 21 M€ ja henkilökuntaa oli n. 270 henkeä (Me olemme Protacon 2017).

2 Työmenetelmät ja tietoperusta

Opinnäytetyön tietoperusta koostuu lähes kokonaan koneturvallisuuden standardeista ja kaikki käytetty materiaali löytyi toimeksiantajalta. Tässä työssä käytettyjä standardeja ja kirjallisuutta ovat mm.:

- SFS-EN 60204-1 Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset
- SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet.
- SFS-EN 62061:2005. Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus.
- Tapio Siirilän & Katri Tytykosken kirjoittama Koneturvallisuuden käsikirja.

Käytännön osuus toteutettiin kehittämisprojektina. Työmenetelmänä käytettiin laadullista, eli kvalitatiivista menetelmää. Työpaikalla työtehtävien välityksellä havainnoimalla ja keskustelemalla kollegoiden kanssa saatiin kerättyä aineistoa käytännön osuuden toteuttamiseksi.

3 Koneiden turvallisuus: konedirektiivi ja standardit

Koneiden automatiikka on kehittynyt nopeasti 2000-luvulla. Kehitys on tuonut kuitenkin uusia haasteita koneturvallisuuden saralla; kone osaa tehdä sille tarkoitetun tehtävän nopeasti ja virheettömästi, mutta vika- tai häiriötilanteessa sen on myös toimittava turvallisesti. Tässä mukaan tulee ohjausjärjestelmien turvallisuus. Koneen käyttäjälle turvallinen työskentely-ympäristö luodaan työturvallisuutta koskevien lakien sekä koneturvallisuuteen liittyvien säädösten avulla.

Markkinoille saatettavien sekä käytössä olevien koneiden turvallisuutta säätelee Euroopan talousalueella konedirektiivi. CE-merkintä vuoden 1994 jälkeen valmistetussa koneessa merkitsee, että kone on valmistettu konedirektiivin vaatimusten mukaisesti. Ennen vuotta 1989 kaikki direktiivit olivat hyvin yksityiskohtaisia ja niiden ylläpitäminen osoittautui hankalaksi tekniikan kehittyessä

nopeaan tahtiin. Direktiivien osalta otettiin 1989 vuoden jälkeen käyttöön ”uusi lähestymistapa”, jonka tarkoituksena oli, että direktiivit säätävät vain yleiset vaatimukset ja tavoitteet turvallisuuden takaamiseksi. (Siirilä & Tytykoski 2016, 34.)

Vaatimuksille ja tavoitteille on kuitenkin oltava täsmennetyt arvot ja ohjeet saatavilla, jotta koneen valmistukseen ja käyttöönottoon tarvittavaa suunnittelua voidaan tehdä. Nämä tiedot löytyvät EU:n alueella käytettäville koneille eurooppalaisista standardeista. Standardit ovat EU:n ja EFTA:n tilaamia täsmennyksiä direktiiveille eurooppalaisilta standardoimisjärjestöiltä, jotka EU:n komissio hyväksyy, jos standardi täyttää hyväksyttävästi direktiivin vaatimukset. Suomessa standardien laatijana toimii Suomen Standardisoimisliitto SFS. (Siirilä & Tytykoski 2016, 88.)

Koneturvallisuuden standardien tehtävänä on täsmentää konedirektiivin vaatimuksia, ja niitä seuraamalla saavutetaan vaadittava turvallisuuden minimitaso koneen sekä niiden ohjausjärjestelmien suunnittelussa. Standardeista voidaan myös poiketa, mutta standardin esittämä turvallisuustaso on silti pystyttävä osoittamaan vaihtoehtoiselle tavalle. (Siirilä & Tytykoski 2016, 88-89.)

4 Ohjausjärjestelmän turvatoiminnot

4.1 Turvatoiminto

Koneen ohjausjärjestelmä on monimutkainen kokonaisuus, ja se voi sisältää useita eri turvatoimintoja. Turvatoiminto on toiminto, joka aktivoituessaan aiheuttaa koneiden vaarallisten osien pysähtymisen tai tekee niistä vaarattomia esimerkiksi rajoittamalla niiden nopeutta. Tärkeimpänä koneen ohjausjärjestelmällä toteutettavista turvatoiminnoista voidaan pitää varmistusta siitä, että kone on pysähdyksissä, kun ihminen tai jokin kehon osa on koneen vaikutusalueella. Siihen liittyy muutamien perusasioiden toiminnoista varmistuminen, esimerkiksi koneen käynnistys ja pysäytys, jotka on esitelty lyhyesti tässä luvussa. Lisäksi riippuu koneesta ja sen käyttötarkoituksesta, millaisia turvatoimintoja on sisällytettävä ohjausjärjestelmään. (Siirilä & Tytykoski 2016, 478.)

Konedirektiivi ohjeistaa ohjausjärjestelmien turvallisuudesta ja toimintavarmuudesta seuraavaa:

> *Ohjausjärjestelmät on suunniteltava ja rakennetta sellaisiksi, että ne estävät vaaratilanteiden syntymisen. Ennen kaikkea ne on suunniteltava ja rakennettava sellaisiksi, että*
> - *Ne kestävät tarkoitetut käyttörasitukset ja ulkoiset vaikutukset,*
> - *Ohjausjärjestelmän laitteisto- tai ohjelmistovika ei aiheuta vaaratilanteita,*
> - *Virheet ohjausjärjestelmän logiikassa eivät aiheuta vaaratilanteita*
> - *Kohtuudella ennakoitavissa oleva inhimillinen erehdys käytön aikana ei aiheuta vaaratilanteita*
>
> *Erityistä huomiota on kiinnitettävä seuraaviin seikkoihin:*
> - *Kone ei saa käynnistyä odottamattomasti,*
> - *Koneen ominaisarvot eivät saa muuttua hallitsemattomasti, jos tällainen muutos saattaa aiheuttaa vaaratilanteita,*
> - *Koneiden pysähtymistä ei saa estää, jos pysäytyskäsky on jo annettu,*
> - *Mikään koneen liikkuva osa tai koneen kiinni pitämä kappale ei saa pudota tai sinkoutua,*
> - *Minkään liikkuvan osan automaattinen tai käsikäyttöinen pysäyttäminen ei saa estyä,*
> - *Turvalaitteiden on pysyttävä täysin toimintakykyisinä tai annettava pysäytyskäsky,*
> - *Turvallisuuteen liittyviä ohjausjärjestelmän osia on käytettävä yhtenäisellä tavalla koneiden ja/tai puolivalmisteiden muodostamaan koko kokoonpanoon.*
>
> *Langattomassa ohjauksessa aikaansaatava automaattinen pysäytys, jos oikeita ohjaussignaaleja ei saada tai jos yhteys menetetään.* (Konedirektiivin 2006/42/EY soveltamisopas 2010, 168.)

4.2 Koneen käynnistys

Koneen käynnistymisen täytyy olla aina hallittu ja tietoinen tapahtuma. Käynnistyminen ei saa tapahtua hallintaelimeen vahingossa vaikuttamalla tai esimerkiksi sähkönsyötön palautuessa katkoksen jälkeen. Myöskään käsikäytöltä automaatille vaihtaminen, hätäpysäyttimen palauttaminen normaaliin tilaan tai turvalaitteeseen vaikutuksen loppuminen ei saa aiheuttaa käynnistymistä. Poikkeuksena edellisiin on täysin suojattu koneen rakenne, joka estää pääsyn

liikkuviin osiin tai koneen muihin vaarakohtiin. Tällöin vaaraa ei aiheudu odottamattomasta käynnistymisestä. (Siirilä & Tytykoski 2016, 479-480.)

4.2.1 Käynnistys suojuksilla ja valoverhoilla

Käynnistäviä suojuksia tai valoverhoja voidaan käyttää helpottamaan työtä. Niitä käytetään yleensä toistuvissa ja lyhyissä työnkierroissa, joissa toimintajakso on lyhyt ja ihminen toimii aktiivisena osana työnkiertoa. Yksi toimintajakso on työliikkeen aloituksen ja seuraavan aloituksen välinen aika. Vaatimukset ovat kuitenkin tällaisissa tapauksissa tiukemmat. Seuraavassa on eritelty yhteisiä vaatimuksia käynnistävien suojuksien ja valoverhojen käytölle Siirilän ja Tytykosken mukaan:

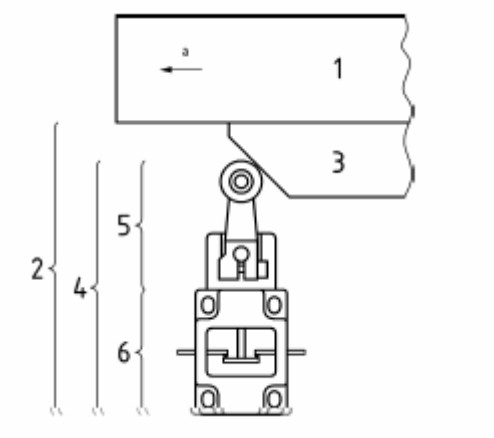
- Vaaravyöhykkeelle on pääsy vain tarkoitetuista kohdista.
- Valoverho tai suojus on suunniteltava oikean kokoiseksi suojausta vaativaan aukkoon nähden.
- Ensimmäinen toimintajakso käynnistetään käyttämällä normaalia käynnistystapaa.
- Koneen käyttöaika tällä käynnistyksellä kestää enintään yhden toimintajakson ja toimintajakso alle 30 sekuntia.
- Suojusten aukiololle tai valoverhojen vaikuttamiselle on asetettava maksimiajat.
- Suojus tai valoverho ei saa olla ainoa käynnistystapa. (Siirilä & Tytykoski 2016, 480.)

Suojuksille on seuraavia lisävaatimuksia:

- Kaikkien koneen suojusten on oltava toimintaankytkettyjä suojuksia, myös kiinteiden työkalulla irrotettavien ja avattavien suojusten.
- Suojuksen auki ja kiinnioloa valvottava vähintään kahdella toimintaankytkentälaitteelta tulevalta signaalilla.
- Suojus ei saa sulkeutua tahattomasti aukiasennosta kiinniasentoon ja aiheuttaa koneen käynnistymistä. (Siirilä & Tytykoski 2016, 481.)

- Suojuksen toimintaankytkentälaitetta ei saa ohittaa niin, että kone voi käydä sen aukiollessa.
- Vaarallisia toimintoja voidaan käyttää vasta kun suojus on suljettu. (SFS-EN ISO 14119:2013, 15.)

Toimintaankytkentälaitteella tarkoitetaan laitetta, joka lähettää ohjausjärjestelmään signaalin esimerkiksi suojuksen avautumisesta (ks. kuvio 1). Kuvion 1 toimintaankytkentälaitteen numerolla 5 merkitty osa taipuu vasemmalle suojuksen avautuessa ja näin järjestelmään saadaan tieto avautumisesta. (SFS-EN ISO 14119:2013, 12.)



Kuvio 1. Toimintaankytkentälaite (SFS-EN ISO 14119:2013, 12.)

Valoverhoille on puolestaan seuraavia lisävaatimuksia:

- Työtoiminto aktivoituu vasta vaadittavan manuaalisen toimenpiteen jälkeen, esimerkiksi työstettävän kappaleen asettamisen jälkeen.
- Valoverhoksi valittava tyypin 4 valoverho.
- Suoritustason PL täytyy olla korkeinta luokkaa eli PL e
- Valoverhoon vaikuttaminen vaarallisen työliikkeen aikana aiheuttaa välittömästi koneen pysähtymisen.
- Valoverholla, joka on tarkoitettu käden havaitsemiseen, on oltava 30mm tai parempi havaitsemiskyky. Vartalon tai jalan havaitsemiseen vastaava havaitsemiskyky on oltava vähintään 50mm.

- Alle 100ms vaikuttamisaika valoverhoon ei saa käynnistää konetta.
- Koneen pysähtymiseen kuluvaa aikaa on valvottava.
- Koneen turvalaitteina olevista valoverhoista voidaan käynnistämiseen käyttää vain yhtä valoverhoa. (Siirilä & Tytykoski 2016, 481.)

4.3 Koneen luotettava pysäytys

Pysähdyksissä oleva kone voidaan määritellä pysähtyneeksi vasta kun koneen liikkeen tai toiminnon mahdollistava tehonsyöttö on katkaistu ja liike tai toiminto on loppunut. Ohjausjärjestelmän turvatoimintojen tärkeimpiä varmistuksia onkin varmistus siitä, että kone on luotettavasti pysäytetty ja mahdollista käynnistää vasta vaadittavien kuittausten jälkeen, esim. käyntiluvan kuittauksen jälkeen. (Siirilä & Tytykoski 2016, 493.)

4.3.1 Turvalaitteella aiheutettu pysäytys

Koneen turvalaitteilla aiheutettu pysäytys on erityisen tärkeää henkilövahingoilta välttymisen kannalta. Turvalaitteilla varmistetaan, että henkilö ei pääse käsiksi koneen liikkuviin osiin vielä kun ne ovat liikkeessä. Tärkeää on myös se, että kone pysyy pysähtyneenä, kun ollaan vaarallisella alueella ja turvalaitteeseen vaikutetaan. Koneen toiminnallisuuden ja henkilöturvallisuuden kannalta valvotaan esimerkiksi sen nopeutta ja liikerataa. Raja-arvojen ylittäessä turvallisen rajan, kone pysähtyy. Turvalaitteen aiheuttaman pysäytyksen toteuttavan toiminnon suunnittelussa on otettava huomioon mm. koneen pysähtymiseen kuluva aika, koneen pysäytysluokan valinta ja liikkuvien osien hidastuvuus koneen ja prosessin turvallisuuden rajoissa. (Siirilä & Tytykoski 2016, 495.)

4.3.2 Pysäytysluokat

Standardin SFS-EN 60204-1 mukaan, koneen pysäyttämistoiminnot jaetaan pysäytysluokkiin 0, 1 ja 2 seuraavin perustein:

Luokka 0: Pysäytyskäskyn jälkeen koneen toimilaitteilta poistetaan heti tehonsyöttö ja koneen liikkuvien osien liike hidastuu ja pysähtyy hiljalleen itsestään. Tätä tapaa kutsutaan valvomattomaksi pysähtymiseksi.

Luokka 1: Pysäytyskäskyn jälkeen koneen toimilaitteille jää tehonsyöttö koneen liikkuvien osien hidastamista varten ja liikkuvien osien pysähtymisen jälkeen tehonsyöttö katkeaa toimilaitteilta. Tätä tapaa kutsutaan valvotuksi pysähtymiseksi.

Luokka 2: Pysäytyskäskyn jälkeen tehonsyöttö säilyy toimilaitteilla ja koneen liikkuvat osat hidastuvat ja pysähtyvät. Nopeaa liikkeen pysäytystä varten tehonsyöttö säilyy koko pysäytyksen ajan toimilaitteilla, eikä pysähtymisenkään jälkeen katkea. Kutsutaan myös valvotuksi pysähtymiseksi.

(Siirilä & Tytykoski 2016, 493-494; SFS-EN 60204-1:2006, 84.)

Nopeussäädetyille sähkökäytöille on olemassa omat pysäytysluokat standardin SFS-EN 61800-5-2 mukaan:

STO: Safe torque off. Pysähtymiseen käytetään vääntömomentin aiheuttavan tehon poistamista koneelta. STO:n ollessa päällä, kone pysähtyy hiljalleen koneen raja-arvoista riippuen. Verrattavissa pysäytysluokkaan 0.

SS1: Safe stop 1. Konetta hidastetaan sovelluksesta riippuen tarpeeksi paljon, jonka jälkeen sen liikettä aikaansaava teho kytketään pois. Verrattavissa pysäytysluokkaan 1.

SS2: Safe stop 2. Pysäytyskäskyn jälkeen liikkuvien osien nopeus hidastetaan sopivaan arvoon ja sen jälkeen koneen liike estetään ulkoisilla tehoilla. Verrattavissa pysäytysluokkaan 2.

SOS: Safe operating stop eli turvallinen tuotantopysäytys. Koneen liikkuvien osien liike estetään ulkoisilla tehoilla niin, että liike ei ole mahdollista. (Siirilä & Tytykoski 2016, 495.)

4.3.3 Hätäpysäytys

Hätäpysäytyksellä lisätään koneen käyttäjän turvallisuutta, mutta se ei suoranaisesti ole turvatoiminto. Hätäpysäytystoiminto on tarkoitettu turvallisuutta lisääväksi toiminnoksi ja se ei saa olla ainut pysäytystapa. (SFS-EN ISO 13850:2015, 8.)

Hätäpysäytystoiminnolla ei saa myöskään heikentää muiden turvatoimintojen toimivuutta ja sen täytyy olla koko ajan saatavilla, toimintakunnossa sekä toimia ensisijaisesti koneen tilasta riippumatta. Hätäpysäytyksen jälkeen pysäytetty kone tai koneet on tarkastettava ennen hätäpysäyttimen palauttamista normaaliin tilaan. Palauttaessa hätäpysäytintä, kone ei saa lähteä uudelleen käyntiin, vaan palautuksella sallitaan ainoastaan koneen uudelleenkäynnistys. Hätäpysäytyslaitteen hallintaelimen on oltava punainen ja sen taustan keltainen, jos taustan käyttö on mahdollista. (SFS-EN ISO 13850:2015, 11-13.)

Kuvio 2 Standardin IEC 60417-6538 mukainen hätäpysäytyksen symboli (SFS-EN ISO 13850:2015, 13.)

Hätäpysäytys toteutetaan pysäytysluokkien 0 tai 1 mukaan, sekä niihin verrattavissa olevien STO:n tai SS1:n mukaisesti. Riskinarvioinnin perusteella valitaan, kumpi luokka käy paremmin tilanteeseen. Esimerkiksi 0 luokassa täytyy huolehtia, että koneen liikkuvat osat hidastuvat tarpeeksi ennen kuin henkilö ehtii vaarakohtaan.

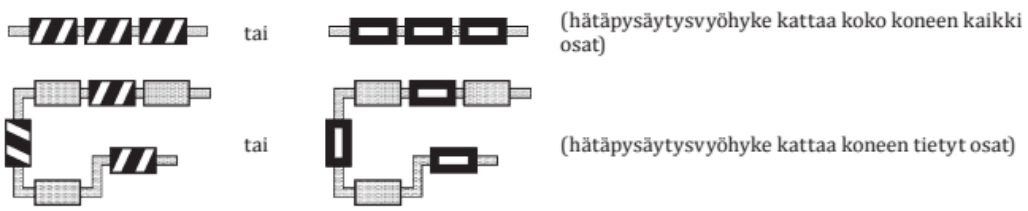
Toisaalta, hidastuvuus ei saa olla liiankaan nopea, sillä tietyissä prosesseissa tämä saattaa aiheuttaa vahinkoa koneelle itselleen tai sen ympäristölle. (SFS-EN ISO 13850:2015, 10.)

Hätäpysäytystoiminto kattaa yleensä tietyn hätäpysäytysvyöhykkeen (ks. kuvio 3) ja vyöhyke voi olla esimerkiksi tuotantolinjan osa tai koneryhmä. Vyöhykkeet määritellään standardin SFS-EN ISO 13850:2015 mukaisesti ottamalla seuraavat asiat huomioon:

> *a) Koneen fyysinen sijoittelu perustuen koneen näkyvissä oleviin alueisiin*
> *b) Mahdollisuus tunnistaa vaaratilanteet (esim. näkyvyys, äänet, hajut)*
> *c) Tuotantoprosessiin liittyvät turvallisuusvaikutukset*
> *d) Ennakoitavissa oleva vaaratekijöille altistuminen*
> *e) Mahdolliset lähistöllä olevat vaaratekijät.*
> (SFS-EN ISO 13850:2015, 9.)

Hätäpysäytysvyöhykkeisiin jakamiselle on määritelty standardissa tiettyjä ehtoja:

> - *Hätäpysäytysvyöhykkeiden on oltava selkeästi määriteltyjä ja tunnistettavia*
> - *Hätäpysäytyslaitteiden on oltava helposti yhdistettävissä hätäpysäytystä vaativaan vaaraan.*
> - *Hätäpysäytysvyöhykkeen on oltava tunnistettavissa jokaisen hätäpysäytyslaitteen käyttöpaikalta.*
> - *Hätäpysäytyslaitteeseen vaikuttaminen ei saa aiheuttaa lisävaaraa (-vaaroja) tai kasvattaa riskiä (riskejä) millään hätäpysäytysvyöhykkeellä*
> - *Hätäpysäytyslaitteeseen vaikuttaminen yhdessä hätäpysäytysvyöhykkeessä ei saa estää hätäpysäytystoiminnon käynnistämistä toisessa hätäpysäytysvyöhykkeessä*
> - *Koneen käyttöä koskevissa tiedoissa on oltava tiedot hätäpysäytyslaitteen vaikutusvyöhykkeestä*
>
> *Silloin kun se on käytännössä mahdollista, eri hätäpysäytysvyöhykkeisiin vaikuttavia hätäpysäytyslaitteita ei saa sijoittaa lähelle toisiaan* (SFS-EN ISO 13850:2015, 9-10.)



Kuvio 3. Esimerkki hätäpysäytysvyöhykkeistä (SFS-EN ISO 13850:2015, 9.)

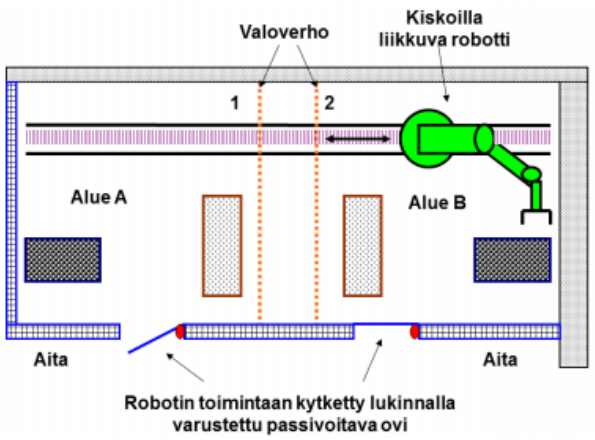
4.4 Kuittaus

Kuittausta tarvitaan esimerkiksi hätäpysäyttimien normaaliin tilaan vapautuksen jälkeen, että konetta voidaan taas käyttää. Kuittauksen tarkoituksena on poistaa järjestelmään jäänyt pysäytyskäsky ja sallia koneen käynnistys erillisestä käynnistyksen hallintaelimestä. Ennen järjestelmään jääneen SEIS-komennon kuittausta on syytä tarkistaa, että kone on käyntikunnossa ja kukaan henkilö ei ole sen vaara-alueella. Yleensä kuittauspaikalta on oltava hyvä näkyvyys koko vaaravyöhykkeelle. Vaaravyöhykkeeltä ei saa ylettyä kuittauspainikkeeseen niin, että sinne voi jäädä ilman turvatoimintojen aktivoitumista. Jos vaaravyöhykkeelle ei ole ollenkaan näköyhteyttä kuittauspainikkeen luota, on käytettävä useampaa kuin yhtä painiketta. Kuittauspainikkeen on oltava sinisen värinen ja on huolehdittava myös, että se on aina tunnistettavissa helposti. (Siirilä & Tytykoski 2016, 508-509.)

4.5 Passivointi

Passivoinnilla tarkoitetaan toimintoa, joka keskeyttää hetkellisesti turvatoiminnon normaalin toiminnan. Passivointi on tarpeen tietyissä sovelluksissa, joissa turvatoiminto on ohitettava työliikkeen loppuun saattamiseksi tai suurten konejärjestelmien turvalliselle vyöhykkeelle on päästävä aiheuttamatta toisella vyöhykkeellä olevien koneiden pysäytystä. Liikkeen loppuunsaattamisen esimerkkinä ovat mm. puristimet ja leikkurit, jotka vaativat kappaleen asettamisen työstötasolle ja siitä pois. (Siirilä & Tytykoski 2016, 509.)

Kuviossa 4 on esimerkki passivoinnin toteutuksesta yhdenlaisen konejärjestelmän osalta. Alueella A on turvallista toimia robotin ollessa B alueella. Suunnittelussa on kuitenkin otettava huomioon, ettei alueelta B pääse sinkoutumaan esineitä alueelle A, ja turvallisen alueen mahdolliset muut koneet ovat pysähdyksissä tai hyvin koteloituja. Robotin ollessa alueella B, alueen A oven lukko on avattavissa eli passivoituneena. Alueella A oleva henkilö ei vaikuta näin ollen alueella B toimivaan robottiin, jos ovi on aukaistu. Oven kiinni laittaminen henkilön ollessa alueen A sisällä ei saa aiheuttaa robotin pääsyä sinne, vaan erillinen kuittaus vaaditaan aitauksen ulkopuolelta varmistamaan, että ketään ei ole enää vaara-alueella. (Siirilä & Tytykoski 2016, 511-512.)



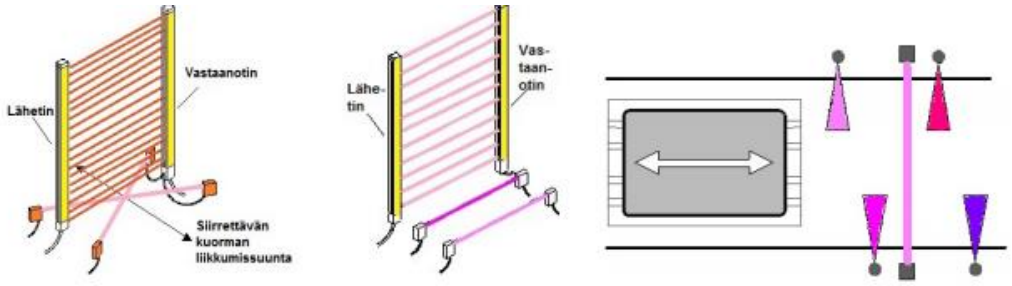
Kuvio 4. Esimerkki konejärjestelmän vyöhykkeistä (Siirilä 2014, 7.)

Passivointia saa käyttää osana ohjausjärjestelmän normaaleja turvatoimintoja vain, jos koneen normaali käyttö sitä jatkuvasti vaatii. Vähemmän tarvittava passivointi voidaan sisällyttää ohjausjärjestelmään, mutta sen käyttöä täytyy hallita esimerkiksi suojaamalla toiminto mekaanisen lukinnan tai salauksen taakse. (Siirilä & Tytykoski 2016, 515.)

Haastavan passivoinnista tekee juuri yhden tai useamman turvatoiminnon ohittaminen niin, että se on turvallisesti toteutettu ja niin, ettei vaarallisia tapahtumia ei pääse syntymään. Passivoinnin myötä menetetty turvatoiminto onkin korvattava muulla tavalla, jotta turvallisuuden taso ei laske. Järjestelmän täytyy osata erottaa ihminen ja työstettävä tai kuljetettava kuorma toisistaan niin, että ihminen ei

pysty kulkemaan kuormalle tarkoitetulle vaara-alueelle ja vahingossa passivoida turvatoimintoa. Passivointiantureiden oikein sijoittamisella voidaan myös varmistaa, että vaara-alueelle ei ihminen pääse kulkemaan aiheuttamatta turvatoiminnon aktivoitumista. (Siirilä & Tytykoski 2016, 516.)

Passivointitapahtumaa on hyvä valvoa, että voidaan toteuttaa oikein ja turvallisesti toimiva passivointi. Valvonnalla tarkoitetaan kuorman etenemistä ja sijaintia seuraavia antureita, jotka on nykyään helppo toteuttaa älykkäillä turvalaitteilla tai ohjausjärjestelmän avulla. Valvonta helpottaa erilaisten kuormien tunnistuksessa ja näin ollen estää esimerkiksi ihmisen pääsyn vaara-alueelle. Yksi tapa on valvoa antureilta tulevia signaaleja ja ohjausjärjestelmä tarkkailee näiden signaalien oikeaa aktivoitumisjärjestystä (ks. kuvio 5). (Siirilä & Tytykoski 2016, 517.)



Kuvio 5. Passivointiantureiden sijoittelutapoja (Siirilä 2014, 12.)

5 Ohjausjärjestelmien turvallisuuden määrittely

5.1 Turvatoimintojen turvallisuuden määrittely

Turvatoiminnot nimensä mukaisesti suojelevat henkilöitä ja tuotannon jatkuvuutta koneista mahdollisesti aiheutuvilta vaaroilta sekä inhimillisiltä virheiltä. Ohjausjärjestelmät saattavat myös vikaantua, eikä se saa vaikuttaa turvatoiminnon toimivuuteen. Vikaantumisen aiheuttamien häiriöiden ja mahdollisten vaaratilanteiden vuoksi ovat eri standardisoimisjärjestöt kehittäneet koneiden ohjausjärjestelmien suunnittelua eri näkökulmista tarkastelevia standardeja. IEC:n standardi 62061 käsittelee ohjausjärjestelmien turvallisuutta turvallisuuden eheystasoina, ja standardi ISO 13849-1 ohjausjärjestelmien suoritustasoina sekä

luokkina. Meneillään on pyrkimys, jossa edellä mainitut standardit on tarkoitus yhdistää yhdeksi standardiksi. (Siirilä & Tytykoski 2016, 560.)

Käytettävä standardi valitaan yleensä seuraavin perustein:

- suunnittelukokemuksen perusteella
- käytettävän teknologian mukaan
- asiakkaan tottumusten mukaisesti
- suunnittelukohteessa aikaisemmin toteutetulla tavalla. (SFS 5974. 2011, 10.)

Tässä opinnäytetyössä esitellään kaksi erilaista tapaa tehdä turvallisuusmäärittelyjen kuvaus koneen ohjausjärjestelmille ja niiden turvatoiminnoille. Ensimmäisenä on esitelty suoritustasoihin perustuva määrittely luvussa 5.2 ja luvussa 5.3 eheystasoihin perustuva määrittely.

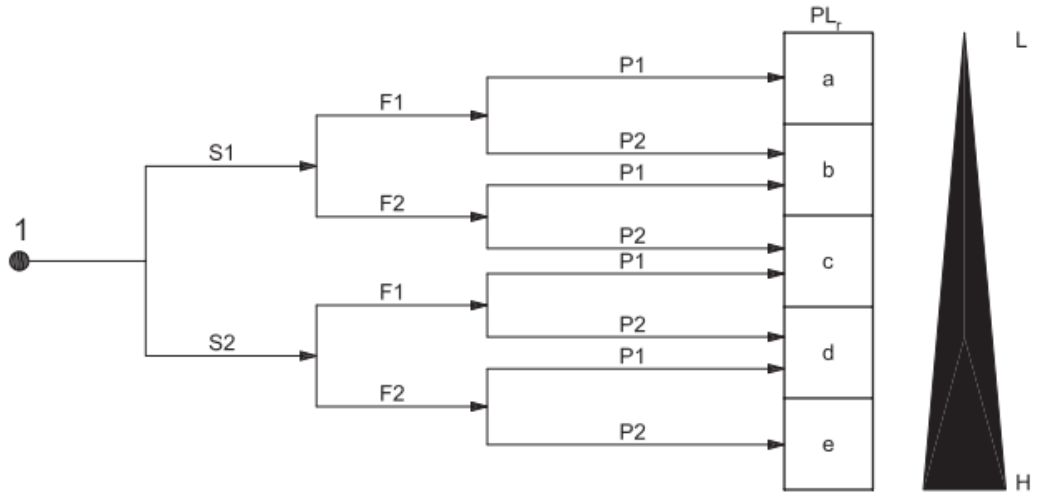
5.2 Suoritustasoihin perustuva määrittely

Suoritustasojen mukainen määrittely kerrotaan ohjausjärjestelmästandardin osassa SFS-EN ISO 13849-1:2015 ja järjestelmien kelpuutus osassa SFS-EN ISO 13849-2:2012. Suoritustasoihin perustuvaa määrittelyä voidaan tehdä kaikenlaisille järjestelmille, ja se ottaa huomioon myös hydrauliikkaa mutta hieman vähemmän ohjelmoitavaa elektroniikkaa. (Hietikko, Malm & Alanen 2009, 19.)

Suoritustaso kuvaa ohjausjärjestelmän kykyä toteuttaa turvatoiminto. Suoritustasoja ovat PL a, b, c, d ja e (Performance Level). Suoritustason määrittely on tehtävä jokaiselle ohjausjärjestelmän osalle tai niiden yhdistelmälle, joka toteuttaa turvatoimintoa. Ohjausjärjestelmästandardi jakaa ohjausjärjestelmät luokkiin B, 1, 2, 3 ja 4 perustuen ohjausjärjestelmän rakenteeseen ja luotettavuuteen. Luokalla voidaan vaikuttaa siihen, kuinka korkealle suoritustasolle voidaan päästä. (Siirilä & Tytykoski 2016, 560; SFS-EN ISO 13849-1:2015, 23.)

5.2.1 Vaadittavien suoritustasojen määrittely

Turvatoiminnoille, jotka valitaan osaksi ohjausjärjestelmää, on jokaiselle määriteltävä vaadittava suoritustaso PLr. Suoritustason määrittely lähtee liikkeelle turvatoiminnon riskien arvioinnista. Arvioinnissa käytetään riskimuuttujia S, F ja P. Jokainen muuttuja on syytä käydä läpi huolellisesti, että suoritustaso saadaan valittua tarpeeksi korkealle tasolle. Kuvion 6 mukaan edetään valittua muuttujaluokkaa, esimerkiksi S1, F1 ja P1 pitkin, ja päädytään turvatoiminnolta vaadittuun suoritustasoon, tässä tapauksessa tasoon PLr a. Kuvion 6 kolmio kuvastaa riskin osuuden pienentämistä kullakin suoritustasolla, L tarkoittaa pientä osuutta ja H vastaavasti suurta osuutta riskin pienentämisessä. (SFS-EN ISO 13849-1:2015, 55.)



Kuvio 6. Turvatoiminnolta vaadittavan suoritustason valintapuu. (SFS-EN ISO 13849-1:2015, 55.)

S-muuttuja luokitellaan joko S1- tai S2-tasoiseksi. S-muuttujalla arvioidaan karkeasti vamman vakavuutta, joka vaaratilanteesta voi aiheutua. Valintaperusteet ovat seuraavanlaiset:

- S1 valitaan, kun vaaratilanne voi aiheuttaa korkeintaan palautuvan vamman.
- S2 valitaan, kun vaaratilanne voi aiheuttaa palautumattoman tai kuolemaan johtavan vamman. (SFS-EN ISO 13849-1:2015, 55.)

Seuraavaksi edetään F-muuttujan tason valintaan ja sekin luokitellaan joko F1- tai F2-tasolle. F-muuttujalla arvioidaan vaaralle altistumisen taajuutta ja/tai kestoa. Valintaperusteet ovat seuraavanlaiset:

- F1 valitaan, kun vaaralle altistutaan harvoin tai toisinaan ja altistumisaika on lyhyt.
- F2 valitaan, kun vaaralle altistutaan toistuvasti tai jatkuvasti ja altistumisaika on pitkä. (SFS-EN ISO 13849-1:2015, 55.)

Viimeisenä luokitellaan P-muuttuja. P-muuttujalla arvioidaan mahdollisuutta välttää vaaratilannetta tai rajoittaa sen aiheuttamaa vahinkoa. P1- ja P2-tasot valitaan seuraavasti:

- P1 valitaan, kun vaaratilanne on mahdollista välttää tietyissä olosuhteissa.
- P2 valitaan, kun vaaratilannetta on mahdoton välttää. (SFS-EN ISO 13849-1:2015, 55.)

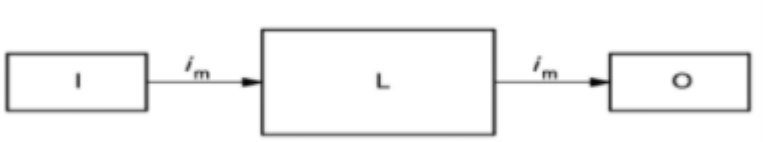
5.2.2 Ohjausjärjestelmien luokittelu

Ohjausjärjestelmästandardin esittämiä luokkia ovat B, 1, 2, 3 ja 4 (ks. liite 1) Jokaisella luokalla on tietyt perusvaatimukset niiden rakenteelle ja ominaisuuksille. Esimerkiksi B- ja 1-luokat eroavat muista luokista niin, että jo yksi vika voi johtaa turvatoiminnon menetykseen. Tästä syystä näissä luokissa on vaatimuksena ainoastaan vähentää vian todennäköisyyttä. Ohjausjärjestelmän paremmuus ei kuitenkaan ole kiinni luokasta, vaan sillä luodaan ainoastaan pohja ohjausjärjestelmälle. (Siirilä & Tytykoski 2016, 561.)

Luokat B ja 1

Luokissa B ja 1 vaatimukset ohjausjärjestelmän loogiselle rakenteelle ovat samanlaiset (ks. kuvio 7). Nämä luokat edustavat yksinkertaisinta ohjausjärjestelmän rakennetta turvatoiminnon toteutusta varten.

Rakenteen toimintaa voidaan kuvata seuraavalla tavalla:
Turvalaite, esimerkiksi valoverho, havaitsee valoverhon läpi kulkevan henkilön ja aiheuttaa tuloyksikön (I) signaalin logiikalle (L), joka ohjaa signaalin oikeaan lähtöyksikköön (O), esimerkiksi turvareleelle.



Kuvio 7. Ohjausjärjestelmän looginen rakenne luokissa B ja 1 (SFS-EN ISO 13849-1:2015, 42.)

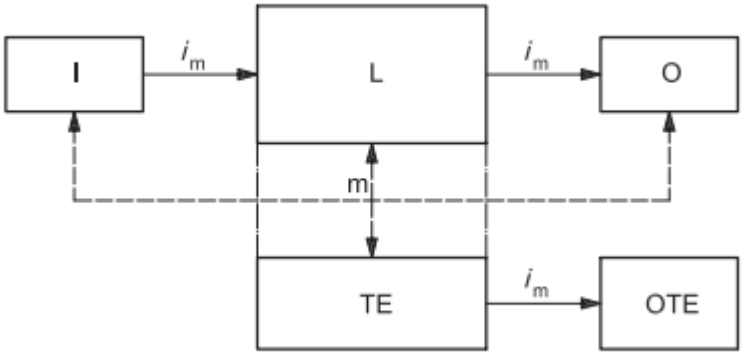
Kuten kuviosta 7 nähdään, kyseessä on 1-kanavainen rakenne ilman valvontaa ja signaali kulkee ainoastaan yhteen suuntaan (i_m), joten tietoa koneen luotettavasta pysähtymisestä ei järjestelmään tule koskaan. Tästä syystä yksikin vika voi aiheuttaa pysyvän vaaratilanteen tällä järjestelmän rakenteella. Järjestelmän turvallisuutta on parannettava toisin keinoin.

Luokassa B vaatimuksena on vian todennäköisyyden pienentäminen. Tämä voidaan toteuttaa pääosin komponenttien valinnalla. Kanavan vaarallisen keskimääräisen vikaantumisajan $MTTF_D$ on oltava vähintään tasolla pieni. Tällä luokalla päästään oikeilla komponenttivalinnoilla korkeintaan suoritustasoon PL b. (SFS-EN ISO 13849-1:2015, 41-42.)

Luokassa 1 vaatimuksena on vian todennäköisyyden pienentäminen B-luokkaan verrattuna. Tämä voidaan toteuttaa valitsemalla hyvin koeteltuja komponentteja ja ylimitoittamalla niitä. Kanavan vaarallisen keskimääräisen vikaantumisajan $MTTF_D$ on oltava vähintään tasolla korkea. Tällä luokalla päästään oikeilla komponenttivalinnoilla korkeintaan suoritustasoon PL c. (Siirilä & Tytykoski 2016, 561; SFS-EN ISO 13849-1:2015, 41-42.)

Luokka 2

Luokkaan 2 siirryttäessä rakenne säilyy käytännössä 1-kanavaisena, kuten B- ja 1-luokissa, mutta lisänä tulee turvatoiminnon tarkistus (ks. kuvio 8). Yksi vika voi edelleen aiheuttaa turvatoiminnon menetyksen, mutta vaaditaan säännöllisesti ajoitetun testauslaitteiston (TE) automaattisesti tekemä turvatoiminnon tarkastus. Tällä tavalla vika paljastuu hyvissä ajoin ja testauslaitteiston lähtösignaali (OTE) aktivoituu. Lähtösignaali käynnistää tarvittavan ohjaustoiminnon, joka riippuu vaadittavasta suoritustasosta PLr. Jos vikoja ei paljastu tarkastuksen aikana, sallitaan käynnistystoiminto normaalisti. Tarkastus voidaan ajoittaa käynnistyksen yhteydessä tehtäväksi. (SFS-EN ISO 13849-1:2015, 43-44.)



Kuvio 8. Ohjausjärjestelmän looginen rakenne luokassa 2 (SFS-EN ISO 13849-1:2015, 45.)

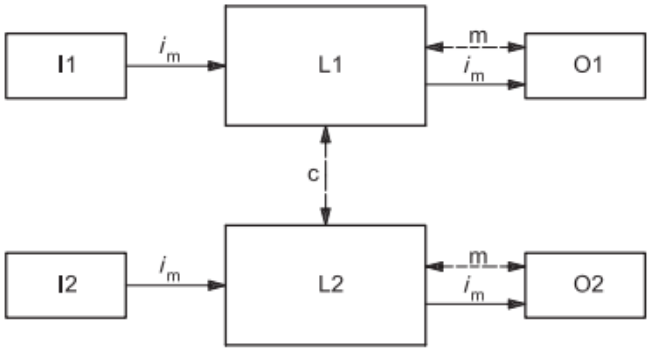
Ohjausjärjestelmän osien diagnostiikan keskimääräisen kattavuuden DC_{avg} on oltava vähintään tasolla matala. Kunkin kanavan vaarallisen keskimääräisen vikaantumisajan $MTTF_D$ on oltava vähintään tasolla pieni. Toimenpiteitä yhteisvikaantumisia CCF vastaan on käytettävä.

Luokalla 2 voidaan saavuttaa korkeintaan suoritustaso PL d, jos testauslaitteiston lähtösignaalin aiheuttama ohjaustoiminto aiheuttaa aina turvallisen tilan, joka poistuu vasta, kun vika on korjattu. Jos tämä toiminto ei ole käytännöllinen, on

ohjaustoiminnon mahdollisuuksien mukaan aiheutettava turvallinen tila. Tällöin päästään parhaimmillaan suoritustasoon PL c. Testauslaitteiston tekemä itsetarkistus ei saa kuitenkaan aiheuttaa vaaratilannetta esimerkiksi vasteajan kasvun takia. (SFS-EN ISO 13849-1:2015, 44.)

Luokat 3 ja 4

Luokkiin 3 ja 4 perustuvat järjestelmät ovat 2-kanavaisia eli redundanttisia (ks. kuvio 9). Redundanttisen järjestelmän hyvä puoli on se, että turvatoiminto voidaan toteuttaa vaikka yksi vika ilmeneekin. Luokkien 3 ja 4 erot ilmenevät pääosin valvonnan kattavuudessa. (Siirilä & Tytykoski 2016, 562.)



Kuvio 9. Ohjausjärjestelmän looginen rakenne luokissa 3 ja 4 (SFS-EN ISO 13849-1:2015, 46.)

Luokassa 3 ohjausjärjestelmän osien diagnostiikan keskimääräisen kattavuuden DC_{avg} on oltava vähintään tasolla matala. Kunkin kanavan vaarallisen keskimääräisen vikaantumisajan $MTTF_D$ on oltava vähintään tasolla pieni. Toimenpiteitä yhteisvikaantumisia CCF vastaan on käytettävä.

Turvallisuuteen liittyvät ohjausjärjestelmän osat on suunniteltava niin, että yksittäinen vika ei johda turvatoiminnon menetykseen. On kuitenkin mahdollista, että yksittäinen vika paljastuu vasta seuraavan vaateen yhteydessä tai ennen sitä.

Yksittäisen vian paljastuminen ei kuitenkaan tarkoita kaikkien vikojen olisi paljastuttava, tämä voi johtaa vikojen kerääntymiseen järjestelmään ja turvatoiminnon menettämiseen. Luokalla 3 voidaan päästä parhaimmillaan PL e tasoon. (SFS-EN ISO 13849-1:2015, 45.)

Luokassa 4 ohjausjärjestelmän osien diagnostiikan keskimääräisen kattavuuden DC_{avg} on oltava vähintään tasolla korkea. Kunkin kanavan vaarallisen keskimääräisen vikaantumisajan $MTTF_D$ täytyy olla vähintään tasolla korkea. Toimenpiteitä yhteisvikaantumisia CCF vastaan on käytettävä.

Turvallisuuteen liittyvät ohjausjärjestelmän osat on suunniteltava niin, että yksittäinen vika ei johda turvatoiminnon menetykseen. Yksittäisen vian paljastuminen täytyy tapahtua seuraavan vaateen yhteydessä tai ennen sitä. Jos vikojen paljastuminen ei ole mahdollista, niiden kerääntyminen järjestelmään ei saa aiheuttaa turvatoiminnon menettämistä. Luokalla 4 voidaan päästä parhaimmillaan PL e tasoon. (SFS-EN ISO 13849-1:2015, 46.)

5.2.3 Suoritustason määrittelyyn vaikuttavat tekijät

Suoritustaso täytyy arvioida jokaiselle valitulle turvatoiminnolle. Arviointi tehdään määrittelemällä turvatoiminnon

- jokaiselle komponentille vaarallinen keskimääräinen vikaantumisaika $MTTF_D$
- diagnostiikan kattavuus DC
- yhteisvikaantuminen CCF
- looginen rakenne
- käyttäytyminen vikatilanteessa
- turvallisuuteen liittyvä ohjelmisto
- systemaattinen vikaantuminen
- kyky toimia tulevissa ympäristöolosuhteissa. (SFS-EN ISO 13849-1:2015, 23.)

$MTTF_D$-määritys

Yksittäisen komponentin vaarallisen keskimääräisen vikaantumisajan saa selville yleensä valmistajan datalehdiltä. Tieto ilmoitetaan vuosina. Jos tietoa ei valmistajan puolesta ole saatavilla, voidaan käyttää standardin SFS-EN ISO 13849-1:2015 taulukkoa yleisimmistä MTTFd-arvoista (ks. liite 2), josta selviää eri tyyppisten komponenttien $MTTF_D$- tai B_{10D}-arvoja. B_{10D} kuvaa toimintajaksojen määrää, jolloin 10 % komponenteista on vikaantunut vaarallisesti. (SFS-EN ISO 13849-1:2015, 61.)

B_{10D}:n avulla voidaan laskea komponentin MTTFd-arvo kaavalla:

(1)

$MTTF_D = \frac{B_{10D}}{0{,}1 * n_{op}}$, missä

$MTTF_D$ on vuosina,

B_{10D} on valmistajalta saatu toimintajaksojen lukumäärän arvo,

N_{op} on keskimääräinen toimintajaksojen lukumäärä vuodessa, jonka voi laskea kaavalla:

(2)

$n_{op} = \frac{d_{op} * h_{op} * 3600\frac{s}{h}}{t_{cycle}}$, missä

d_{op} tarkoittaa komponentin arvioitua käyttöaikaa vuodessa (päivinä, d),

h_{op} tarkoittaa komponentin arvioitua käyttöaikaa päivässä (tunteina, h), ja

t_{cycle} yhden toimintajakson pituutta (sekunteina, s). (SFS-EN ISO 13849-1:2015, 62-63.)

Jos komponentille ei löydy edellä mainituillakaan tavoilla arvoja, käytetään $MTTF_D$:n arvona 10 vuotta. (SFS-EN ISO 13849-1:2015, 26.)

Kanavan (Tuloyksikkö-Logiikka-Lähtöyksikkö) vaarallisen vikaantumisen määrittely voidaan tehdä kanavan sisältävien komponenttien $MTTF_D$:n perusteella eli aikaisemmin mainitulla tavalla. Jos käytetään turvatoiminnossa yhden kanavan järjestelmää, esimerkiksi luokat B ja 1 (ks. luku 5.2.2), tehdään tarkastelu yhdelle kanavalle. Redundanttisia järjestelmiä käytettäessä, joka tarkoittaa useampaa kuin

yhtä kanavaa per turvatoiminto, tarkastelu täytyy tehdä jokaiselle kanavalle erikseen. (SFS-EN ISO 13849-1:2015, 25.)

Yhden kanavan MTTFd-arvon voi laskea seuraavalla tavalla:

(3)

$$MTTF_{D\,C} = \left[\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} \ldots \frac{1}{MTTF_{DN}}\right]^{-1}$$, missä

$MTTF_{D\,C}$ tarkoittaa yhden kanavan vaarallista keskimääräistä vikaantumisaikaa,

$MTTF_{D}$ tarkoittaa yhden komponentin MTTFd-arvoa.

(SFS-EN ISO 13849-1:2015, 67.)

Jos redundanttisten kanavien MTTFd-arvot ovat erisuuret, voidaan käyttää ”pahimman” kanavan arvoa (pienin arvo), tai yhtälöä:

(4)

$$MTTF_D = \frac{2}{3} * \left[MTTF_{D\,C1} + MTTF_{D\,C2} - \frac{1}{\frac{1}{MTTF_{D\,C1}} + \frac{1}{MTTF_{D\,C2}}}\right]$$, missä

$MTTF_{D\,C}$ tarkoittaa yhden kanavan MTTFd-arvoa

Kaavalla 4 saadaan MTTFd-arvo, jota voidaan käyttää redundanttisen järjestelmän arvona. Kaava perustuu oletukseen, että kanavat ovat toisistaan riippumattomia. MTTFd-arvon lopullinen merkitys turvallisuudelle saadaan selvitettyä taulukon 1 mukaan. (SFS-EN ISO 13849-1:2015, 68-69.)

Taulukko 1. MTTFd-arvon perusteella saatu kanavan merkitys turvallisuudelle (SFS-EN ISO 13849-1:2015, 25.)

	$MTTF_D$
Kunkin kanavan merkintä	**Kunkin kanavan vaihteluväli**
Pieni	3 vuotta ≤ $MTTF_D$ < 10 vuotta
Keskitaso	10 vuotta ≤ $MTTF_D$ < 30 vuotta
Suuri	30 vuotta ≤ $MTTF_D$ < 100 vuotta

Diagnostiikan kattavuuden arviointi

Diagnostiikan kattavuudella DC tarkoitetaan järjestelmän vikojen tai vikaantumistapojen paljastumista erilaisilla toimenpiteillä (ks. liite 3). Diagnostiikan kattavuudesta käytetään neljää tasoa (ks. taulukko 2), jotka vastaavat kukin tiettyä diagnostiikan kattavuuden vaihtelualuetta. (SFS-EN ISO 13849-1:2015, 7.)

Taulukko 2. Diagnostiikan kattavuuden merkitys turvallisuudelle (SFS-EN ISO 13849-1:2015, 26.)

Diagnostiikan kattavuus (DC)	
Merkintä	**Vaihtelualue**
Ei lainkaan	DC < 60 %
Matala	60 % ≤ DC < 90 %
Keskitaso	90 % ≤ DC < 99 %
Korkea	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 %.

Esimerkiksi tuloyksikön puolelta saavutetaan liitteen 3 mukaan 99 % diagnostiikan kattavuus toimenpiteen mielekkyyden tarkistuksella, joka tarkoittaa esim. sulkeutuvien ja avautuvien mekaanisesti yhdistettyjen koskettimien käyttämistä. (SFS-EN ISO 13849-1:2015, 70.)

Tällä kattavuudella päästäisiin jo korkeaan tasoon, mutta eri järjestelmän osilla, esim. logiikka ja lähtöyksikkö, saattaa olla eri diagnostiikan kattavuudet ja se vaikuttaa keskimääräiseen diagnostiikan kattavuuteen DC_{avg}. Keskimääräinen diagnostiikan kattavuus voidaan laskea yhtälöllä:

(5)

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

DC tarkoittaa järjestelmän osan diagnostiikan kattavuutta, ja

$MTTF_D$ sitä vastaavan järjestelmän osan keskimääräistä vaarallista vikaantumisaikaa (SFS-EN ISO 13849-1:2015, 72.)

Yhteisvikaantuminen

Yhteisvikaantumisella CCF tarkoitetaan esimerkiksi redundanttisen järjestelmän kummankin kanavan vikaantumista samaan aikaan, josta aiheutuu turvatoiminnon menetys. Yhteisvikaantumisen määrittely tehdään ohjausjärjestelmästandardissa olevan taulukon mukaan (ks. liite 4), joka sisältää toimenpiteitä yhteisvikaantumisen estämiseksi. Luokissa B ja 1 yhteisvikaantumista estävillä toimenpiteillä ei ole merkitystä. Pienin saavutettava pistemäärä on 65 luokissa 2-4 ja toimenpiteillä saavutettava maksimipistemäärä on 100 pistettä. (Siirilä & Tytykoski 2016, 568-569.)

Systemaattinen vikaantuminen

Systemaattisella vikaantumisella tarkoitetaan ennustettavissa olevaa vikaantumista tietyn syyn seurauksena. Kun järjestelmiä suunnitellaan samalla tavalla ja samoilla komponenteilla, on vikaantuminen ennustettavissa. Tästä syystä on hyvä jo suunnitteluvaiheessa sisäistää muutamia yksinkertaisia asioita, joilla systemaattista vikaantumista voidaan ehkäistä. (SFS-EN ISO 13849-1:2015, 10.)

Systemaattista vikaantumista voidaan hallita mm. seuraavilla toimenpiteillä:

- Lepovirtaperiaatteella, turvallisuuteen liittyvät osat erotetaan energiasta tehonsyötön katketessa.
- Edellä mainittua periaatetta voidaan käyttää myös jännitekatkon sattuessa
- Fyysisen ympäristön fysikaalisten tekijöiden hallinnalla.
- Ohjausjärjestelmän osiin, jotka sisältävät ohjelmistoja, on käytettävä virheellisten ohjelmajaksojen paljastamiseksi ohjelman suorituksen valvontaa.
- Tietoliikenteestä aiheutuvien virheiden hallinnalla. (SFS-EN ISO 13849-1:2015, 75-76.)

Lisäksi sovelletaan yhtä tai useampaa alla lueteltua toimenpidettä suoritustasosta riippuen:

- keskenään erilaisten laitteiden käyttö
- kanavien testausten automaattinen ajoittaminen
- koskettimien pakkotoiminen avautuminen
- koskettimien välinen mekaaninen liitäntä
- komponenttien ylimitoitus valmistajan tietojen mukaan. (SFS-EN ISO 13849-1:2015, 75-76.)

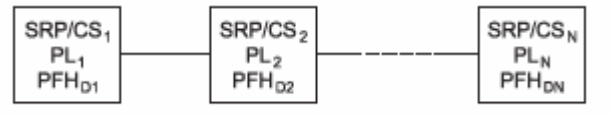
5.2.4 Suoritustason määrittely

Suoritustason määrittelyyn on standardissa kehitetty yksinkertainen tapa, joka on esitelty taulukossa 3. Kahdessa aikaisemmassa luvussa esiteltyjen ohjausjärjestelmänluokitteluiden ja suoritustasoon vaikuttavien tekijöiden valinnan jälkeen voidaan taulukon 3 perusteella määritellä suoritustaso. (SFS-EN ISO 13849-1:2015, 27.)

Taulukko 3. Yksinkertainen menetelmä suoritustason PL määrittämiseksi (SFS-EN ISO 13849-1:2015, 28.)

Luokka	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**nolla**	**nolla**	**matala**	**keskitaso**	**matala**	**keskitaso**	**korkea**
Kunkin kanavan $MTTF_D$							
Matala	a	Ei kata	a	b	b	c	Ei kata
Keskitaso	b	Ei kata	b	c	c	d	Ei kata
Korkea	Ei kata	c	c	d	d	d	e

Kuviossa 10 on nähtävissä ohjausjärjestelmän osia, joista muodostetaan ohjausjärjestelmä. Jokaisella osalla on oma PFHd-arvo ja niiden summana saadaan kaavan 6 mukaan koko järjestelmän PFHd-arvo. Taulukon 4 mukaan voidaan lopuksi valita PFHd-arvon mukaan määräytyvä suoritustaso PL. (SFS-EN ISO 13849-1:2015, 49.)



Kuvio 10. Ohjausjärjestelmän osia (SFS-EN ISO 13849-1:2015, 49.)

$$PFHD = PFHD_1 + PFHD_2 + .. + PFHD_n \quad (6)$$

Taulukko 4. PL-tasoja vastaavat PFHd-arvot (SFS-EN ISO 13849-1:2015, 19.)

PL	Vaarallisen keskimääräisen vikaantumisajan todennäköisyys tuntia kohden (PFHD) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

Laskennallinen osuus vaikuttaa suoritustasoon, koska suoritustaso määritellään PFHd-arvon perusteella. Laskettu PL taso ei kuitenkaan toteudu ellei luvussa 5.2.3 esiteltyjä yhteisvikaantumisen CCF alinta pistemäärää 65 pistettä ole täytetty ja toimenpiteitä systemaattista vikaantumista vastaan ei ole käytetty. (SFS-EN ISO 13849-1:2015, 49.)

Suoritustason määrittelyyn kokonaisuutena vaikuttaa siis komponenttien perusteella saadut arvot, järjestelmän rakenne ja tiettyjen toimenpiteiden käyttö.

Esimerkki yksinkertaisesta määrittelystä:

Oletetaan että turvatoimintona on moottorin pysähtyminen henkilön avatessa vaara-alueelle johtavan turvaoven. Tuloyksikköön sisältyy turvaovi, jonka lukon sisällä on

kaksi asemantuntokytkintä valvomassa oven avautumista. Turvalogiikka valvoo oven lukon asemantuntokytkimiä sekä lähtöyksikön turvareleen takaisinkytkentää. Lähtöyksikkö koostuu turvareleestä, josta on käytetty kahta kosketinta. Koskettimien avautuessa, moottori pysähtyy ja turvalogiikka saa tiedon koskettimen avautumisesta takaisinkytkennän avulla.

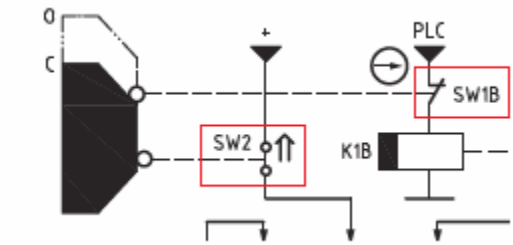
Tuloyksikkö:
Oletetaan, että tuloyksikön turva-oven B10d-arvo on 20 000 000 toimintajaksoa asematuntokytkimelle tyypillisten arvojen mukaan (ks. liite 2). MTTFd-arvo voidaan laskea luvussa 5.2.3 esitetyllä kaavalla 1:

$$MTTF_D = \frac{B_{10D}}{0{,}1 * n_{op}}$$

Oletetaan toimintajaksojen keskimääräisen määrän n_{op} olevan 8760 toimintajaksoa vuodessa, joka on reilusti yläkanttiin, sillä porttia avattaisiin tällöin tunnin välein vuoden jokaisena päivänä. MTTFd-arvoksi saadaan:

$$MTTF_D = \frac{20\,000\,000}{0{,}1 * 8760} = 22831\ vuotta$$

Luvussa 5.2.3 olevan taulukon 1 mukaan MTTFd:n maksimiarvo on 100 vuotta, joten luku tasoitetaan siihen. Turvaoven MTTFd-arvon merkitys turvallisuudelle voidaan asettaa siis tasolle suuri. Turvaoven avautumisen tunnistavat asematuntokytkimet on toteutettu avautuvilla ja sulkeutuvilla koskettimilla (ks. kuvio 11). Diagnostiikan kattavuus DC arvioidaan siten olevan 99 % mielekkyyden tarkistamisen vuoksi (ks. liite 3). Tällä diagnostiikan kattavuudella päästään taulukon 2 mukaan tasolle korkea.



Kuvio 11. Asematuntokytkimien toteutus sulkeutuvilla ja avautuvilla koskettimilla (SFS-EN ISO 13849-1:2015, 84.)

Taulukon 3 mukaan, tuloyksikkö yltää siis luokan 4 ohjausjärjestelmään MTTFd:n ja DC:n ollessa korkea. Tällä ohjausjärjestelmän osalla päästään siten suoritustasolle PL e.

Logiikka:

Turvalogiikan osalta tarkkaa MTTFd-arvoa ei ole saatavilla, joten oletetaan sen yltävän vähintään PL d tasolle ja luokan oletetaan olevan vähintään 3. Tämä on turvalogiikoiden tyypillinen suoritustaso ja luokka. Lisäksi tulo- ja lähtöyksiköiden puolelta tulee 2-kanavaiset johdotukset, joten logiikalla on käytettävissä redundanttista dataa luokan 3 vahvistamiseksi.

Lähtöyksikkö:

Lähtöyksikön turvareleen datalehdeltä saadaan MTTFd-arvo 100 vuotta. MTTFd turvareleen osalta luokitellaan siis tasolle suuri. Diagnostiikan kattavuus arvioidaan suoran valvonnan mukaisesti 99 %:iin. Tällöin se pääsee tasolle korkea. Lopulliseksi suoritustasoksi lähtöyksikön osalta muodostuu PL e ja luokka 4.

Ohjausjärjestelmän kokonaissuoritustaso:

Ohjausjärjestelmän kokonaissuoritustason selvittämiseksi olisi ensin laskettava järjestelmän keskimääräinen diagnostiikan kattavuus DCavg ja MTTFd:n kokonaisarvo niiltä osin kuin se on mahdollista, eli tässä tapauksessa tulo- ja lähtöyksikön mukaan. Alaindeksit I ja O kuvaavat kaavoissa tulo- ja lähtöyksikön arvoja.

Keskimääräisen diagnostiikan kattavuuden laskenta kaavan 5 mukaan:

$$DC_{avg} = \frac{\frac{DC_I}{MTTF_{DI}} + \frac{DC_O}{MTTF_{DO}}}{\frac{1}{MTTF_{DI}} + \frac{1}{MTTF_{DO}}}$$

$$DC_{avg} = \frac{\frac{99\%}{100} + \frac{99\%}{100}}{\frac{1}{100} + \frac{1}{100}} = 99\%$$

Laskukaava antaa saman prosenttimäärän diagnostiikan keskimääräiseksi kattavuudeksi kuin tulo- ja lähtöyksikkö yksistään, sillä MTTFd- ja DC-arvot ovat niillä yhtä suuret.

MTTFd:n laskeminen tulo- ja lähtöyksikön osalta kaavalla 3:

$$MTTF_{D\,C} = \left[\frac{1}{MTTF_{DI}} + \frac{1}{MTTF_{DO}}\right]^{-1}$$

$$MTTF_{D\,C} = \left[\frac{1}{100\ vuotta} + \frac{1}{100\ vuotta}\right]^{-1} = 50\ vuotta$$

MTTFd-arvo laskee siis koko ohjausjärjestelmän osalta puoleen alkuperäisestä 100 vuodesta. MTTFd:n korkealle tasolle se kuitenkin riittää, joten vaikutusta lopputulokseen ei ole. Voidaan edetä siis yksiköiden saavuttamien suoritustasojen mukaan.

Ohjausjärjestelmien osien suoritustasot ja luokat muodostuivat seuraavanlaisiksi:

- Tuloyksikkö: PL e, luokka 4
- Logiikka: PL d, luokka 3
- Lähtöyksikkö: PL e, luokka 4

Seuraavaksi katsotaan suoritustasoja vastaavat PFHd-arvot taulukosta 4 ja sijoitetaan ne kaavaan 6 ja nimetään tekijät seuraavalla tavalla laskemista varten: tuloyksikkö ($PFHd_I$), logiikka ($PFHd_L$) ja lähtöyksikkö ($PFHd_O$)

$$PFHD = PFHD_I + PFHD_L + PFHD_O$$

Sijoitetaan kaavaan 6 ohjausjärjestelmien osien arvot taulukon 4 mukaisesti valittuna:

$$PFHD = 1 * 10^{-8} + 1 * 10^{-7} + 1 * 10^{-8} = 1{,}2 * 10^{-7}$$

Lopulliseksi PFHd-arvoksi saadaan $1{,}2 * 10^{-7}$. Tämä arvo sijoittuu taulukon 4 mukaisesti PL d tasolle määritetylle välille $10^{-7} to\ 10^{-6}$. Koko ohjausjärjestelmän suoritustasoksi muodostuu siten PL d. Ohjausjärjestelmän osien luokkien ollessa suurempaa kuin luokkaa 2, täytyy yhteisvikaantumisen estämiseksi käyttää toimenpiteitä, joilla saadaan vähintään 65 pistettä liitteen 4 ja luvun 5.2.3 mukaisesti. Lisäksi systemaattisen vikaantumisen estämiseksi on hyvä käyttää luvussa 5.2.3 esiteltyjä toimenpiteitä.

5.3 Eheystasoihin perustuva määrittely

Turvallisuuden eheystasot määritellään kansainvälisen IEC standardisoimisjärjestön ohjausjärjestelmiin liittyvässä standardissa IEC 62061 ja tasoja ovat SIL 1-4 (Safety Integrity Level). SIL 1 on alin ja SIL 4 korkein taso. SIL 4 tasoa ei käytetä normaalisti koneturvallisuuden sovelluksissa, joten sitä ei esitellä EN 62061 standardissa. SIL 4 tasoon otetaan kantaa turvallisuuteen liittyvien järjestelmien toiminnallisen turvallisuuden standardissa SFS-EN 61508-1. IEC 62061 standardi on hyväksytty CENELEC:n toimesta vuonna 2004 eurooppalaiseksi EN 62061 standardiksi. Eheystasoihin perustuvaa määrittelyä käytetään yleensä paljon elektronisia ohjelmoitavia järjestelmiä sisältävissä sovelluksissa. Hydrauliikka kyseinen määrittelytapa ei käsittele. (Hietikko, Malm & Alanen 2009, 19.) Turvallisuuden

eheystasoilla kuvataan turvallisuuteen liittyvän järjestelmän kykyä toteuttaa turvatoiminto. (Siirilä & Tytykoski 2016, 563.)

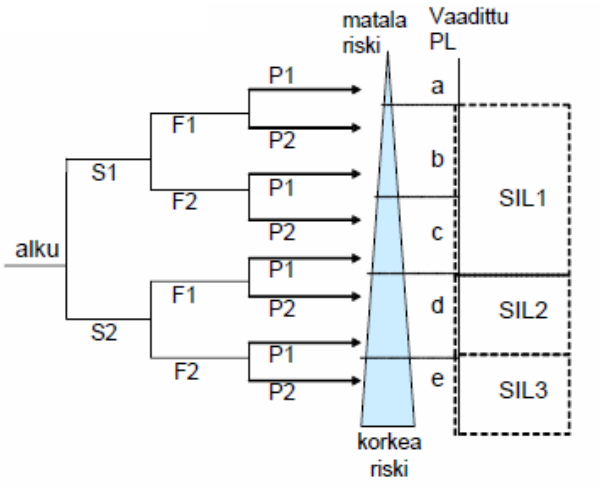
5.3.1 Vaaditun eheystason asettaminen ohjausjärjestelmälle

Eheystasojen (SIL) asettaminen lähtee liikkeelle vaarojen tunnistamisesta ja niiden riskien suuruuden arvioinnista. Riskien suuruuden arviointia varten on olemassa joukko muuttujia, joiden avulla voidaan arvioida ohjaustoiminnolta vaadittu SIL taso. Jokainen muuttuja on syytä arvioida pahimman tilanteen mukaan, jotta turvallisuuden eheystasoa ei asetettaisi virheellisesti alempaan tasoon. (SFS-EN 62061:2005, 140.)

Muuttujia riskin suuruuden arviointiin ovat:

- Se, Severity. Tarkoittaa vaarasta mahdollisesti aiheutuvan vahingon vakavuutta.
- Fr, Frequency. Tarkoittaa vaaralle altistumisen taajuutta ja kestoa, eli kuinka usein ja kuinka kauan kerrallaan.
- Pr, Propability. Tarkoittaa vaarallisen tapahtuman esiintymistodennäköisyyttä.
- Av, Avoidance. Tarkoittaa mahdollisuutta välttää tai rajoittaa vahinkoa. (SFS-EN 62061:2005, 136-138.)

Eheystasot voidaan määritellä myös suoritustasoihin liittyvän määrittelyn avulla kuvion 12 mukaisesti. Määrittely on esitelty tarkemmin luvussa 5.2.1.



Kuvio 12. Vaaditun SIL-tason karkea määrittely (Hietikko, Malm & Alanen 2009, 20.)

Vahingon vakavuus

Vahingon aiheuttaman vamman vakavuuden luokat on luokiteltu neljään eri luokkaan taulukon 5 mukaisesti. Painavat liikkuvat osat sekä liikutettavat kuormat voivat aiheuttaa vakaviakin vammoja, joten vaara-alueella mahdollisesti aiheutuvia vammoja on syytä arvioida hiukan yläkanttiin. (SFS-EN 62061:2005, 138.)

Taulukko 5. Vahingon vakavuuden (Se) arviointi (SFS-EN 62061:2005, 138.)

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

Vaaralle altistumisen taajuus ja kesto

Vaaralle altistumisen arvioinnissa on otettava huomioon millainen on vaaravyöhykkeelle pääsyn tarve ja luonne. Huoltotilanteessa vaaralle altistumisen kesto lisääntyy selvästi mutta määräaikaiset huollot voivat tapahtua esimerkiksi

kerran vuodessa, joten riski ei ole suuri. Vikatilanteet normaalikäytön aikana saattavat aiheuttaa kuitenkin vaara-alueella käyntiä useamminkin. Huomioimalla näitä asioita, voidaan arviointia tehdä luotettavasti. (SFS-EN 62061:2005, 140.)

Vaaralle altistuminen on pisteytetty taulukon 6 mukaisesti. Altistumisen taajuuden arvioinnin jälkeen arvioidaan kuinka kauan vaaralle altistutaan kerralla. Pisteytys valitaan niin, että alle 10 minuutin kestävä altistuminen voidaan laskea alempaan pisteytykseen, kuin taajuuden perusteella aluksi on valittu. Yli 10 minuuttia kestävälle altistukselle valitaan suoraan taajuuden mukaan pisteytys. Altistumisen kesto vaikuttaa pisteytykseen kaikissa muissa kohdissa paitsi enintään kerran tunnissa altistumisen rivillä. (SFS-EN 62061:2005, 140.)

Taulukko 6. Vaaralle altistumisen (Fr) arviointi (SFS-EN 62061:2005, 140.)

Altistumisen taajuus ja kesto (Fr)	
Altistumisen taajuus	Kesto > 10 minuuttia
≤ 1 tunti	5
> 1 tunti...≤ 1 päivä	5
> 1 päivä...≤ 2 viikkoa	4
> 2 viikkoa...≤ 1 vuosi	3
> 1 vuosi	2

Vaarallisen tapahtuman esiintymistodennäköisyys

Tällaisen tapahtuman esiintymistodennäköisyyttä on syytä arvioida ilman siihen liittyvien Fr ja Av muuttujien huomioimista. Arvioinnissa otetaan huomioon mm. koneen käyttötavat ja inhimillisten tekijöiden vaikutus. Koneen normaalin toiminnan aikana ei välttämättä ole kovin todennäköistä joutua vaaraan, mutta kunnossapidolliset syyt voivat esimerkiksi lisätä riskiä joutua tapaturmaan. Myös työntekijöiden väsymys, stressi tai kokemattomuus on otettava huomioon arvioinnissa. Taulukon 7 mukaan voidaan arvioida Pr-taso, missä on otettu huomioon edellä mainitut seikat. (SFS-EN 62061:2005, 141-142.)

Taulukko 7. Vaarallisen tapahtuman (Pr) esiintymistodennäköisyyden arviointi (SFS-EN 62061:2005, 142.)

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

Vahingon välttämisen tai rajoittamisen todennäköisyys

Vahingon välttämisen tai rajoittamisen arviointiin käytetään muuttujaa Av. Soveltuva Av-taso valitaan taulukon 8 mukaisesti huomioimalla tekijöitä, joiden avulla on mahdollista välttää vaaraa. Vaaratilanne voi syntyä äkillisesti tietyssä kohtaa aluetta tai tila voi esimerkiksi loppua kesken, jolloin väistämismahdollisuutta ei ole. Kuumia putkia sekä paljaita sähköosia saattaa esiintyä vaara-alueella ja nekin on syytä ottaa huomioon tarkastelussa. (SFS-EN 62061:2005, 142.)

Taulukko 8. Vahingon välttämisen tai rajoittamisen mahdollisuuden (Av) arviointi (SFS-EN 62061:2005, 144.)

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

SIL-tason valinta

Muuttujien huolellisen valinnan jälkeen vaara-alue voidaan sanoa hyvin kartoitetuksi. Muutoksia saattaa suurella todennäköisyydellä ilmaantua suunnittelun edetessä ja kaikki muutokset olisi syytä ottaa uudelleen tarkastelun kohteeksi. Lopuksi lasketaan yhteen arvioidut Fr, Pr ja Av muuttujat ja näistä arvoista muodostuu kaavan 7 mukaan luokka (Cl). (SFS-EN 62061:2005, 136.)

(7)

$$Cl = Fr + Pr + Av$$

Yhteenlaskun tuloksena saadun arvon perusteella katsotaan mihin luokka-asteikkoon se taulukon 9 mukaan sopii. Esimerkiksi, jos tulokseksi saataisiin 10, valittaisiin keskimmäinen 8-10 luokan sarake. Sen jälkeen arvioidun vahingon vakavuuden (Se) arvon perusteella saadaan SIL-taso, jota ohjausjärjestelmällä lähdetään tavoittelemaan. Harmaalla olevat (OM) merkinnät tarkoittavat, että suositellaan käytettäväksi muita turvallisuustoimenpiteitä kuin sähköisiä, eli käytännössä suojia ja esteitä. (SFS-EN 62061:2005, 144.)

Taulukko 9. Taulukko SIL-tason asettamista varten (SFS-EN 62061:2005, 144.)

Vahingoon 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 2s	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

5.3.2 SIL-tason määrittely

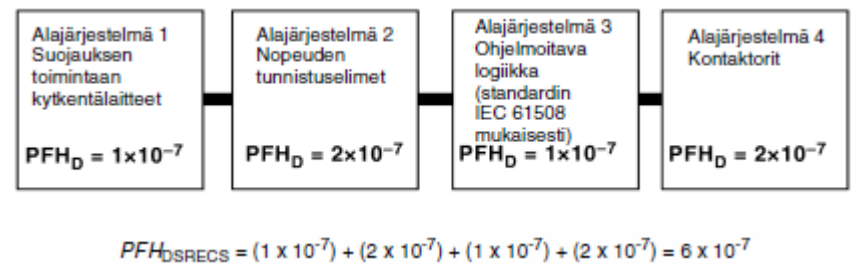
Järjestelmän eheystason SIL määrittely tehdään laskemalla vaarallisen vikaantumisen todennäköisyys tuntia kohden (PFHd) avulla, kuten suoritustasojen määrittelyssä. Tästä syystä suoritustasoon voidaan suhteuttaa myös eheystasoihin (ks. taulukko 10).

Taulukko 10. Suoritustasojen (PL) ja eheystasojen (SIL) suhde (SFS-EN ISO 13849-1:2015, 24.)

PL	SIL (IEC 61508–1, tiedoksi) tiheiden vaateiden tai jatkuvan toiminnan tapa
a	Ei vastaavuutta
b	1
c	1
d	2
e	3

Myös laitevalmistaja antaa turvalaitteille SIL tason, jolle laite parhaimmillaan yltää. Laitteen SIL-tason perusteella voidaan valita PFHd-arvo (ks. taulukko 11). Kuviossa 13 on esimerkkinä ohjausjärjestelmä jaettuna alajärjestelmiin, joille on annettu PFHd-arvoja. PFHd-arvojen mukaan voidaan kaavalla 6 laskea koko järjestelmän vikaantumisaika tuntia kohden:

$$PFHD = PFHD_1 + PFHD_2 + .. + PFHD_n$$



Kuvio 13. Ohjausjärjestelmän osia ja PFHd:n laskuesimerkki (SFS-EN 62061:2005, 158.)

Taulukko 11. Turvallisuuden eheyden tasoja vastaavat PFHd-arvot (SFS-EN 62061:2005, 48.)

Turvallisuuden eheyden taso	Vaarallisen vikaantumisen todennäköisyys PFH_D
3	≥ 10^{-8}...< 10^{-7}
2	≥ 10^{-7}...< 10^{-6}
1	≥ 10^{-6}...< 10^{-5}

Lopuksi tarkastetaan onko ohjausjärjestelmällä määritelty SIL-taso vähintään samantasoinen kuin luvun 5.3.1 mukaan asetettu vaadittu SIL-taso. Turvallisuuden eheystasojen määrittelyn esittely on tehty tässä työssä hieman lyhyemmällä tavalla suoritustasojen laajempaa määrittelyä myötäillen.

6 Turvallisten järjestelmien suunnittelu

Turvallisuuteen liittyvien järjestelmien suunnittelussa on otettava huomioon erilaisia asioita suunnittelijaryhmistä loppukäyttäjiin saakka. Esittelen tässä luvussa lyhyesti ko. järjestelmien suunnittelun kannalta tärkeitä asioita.

6.1 Vaatimustenmäärittely

Turvallisten järjestelmien suunnittelu edellyttää hyvin tehtyä vaatimustenmäärittelyä. Huolimattomasti tehdyn vaatimustenmäärittelyn takia aiheutuu paljon vaaratilanteita, ja siksi se on tärkeä ja huolellisuutta vaativa vaihe suunnittelussa (Ohjelmallinen turvallisuus 2014, 3).

Vaatimustenmäärittely lähtee liikkeelle vaatimusten keräämisestä. Esimerkiksi koneen loppukäyttäjä voi esittää vaatimuksia turvallisuuden tasosta ja vaatimuksia esitetään myös jatkuvasti suunnitteluprosessin aikana. Vaatimuksia on yleensä esitetty koneesta tehdyssä riskinarvioinnissa. Riskinarviointi ottaa kantaa esimerkiksi jokaiseen suunnittelun kohteena olevan koneen vaarakohtaan. Riskinarviointi elää suunnittelun edetessä ja saatetaan huomata uusia vaarakohtia. Tärkeää on suunnittelijana analysoida kerättyjä vaatimuksia ja tapauskohtaisesti tutkia, ovatko vaatimukset asianmukaisia (Ohjelmallinen turvallisuus 2014, 16).

Suunnittelua varten on tärkeää tarkentaa vaatimuksia konekohtaisiksi, jotta esimerkiksi tässä opinnäytetyössä esiteltyä turvallisuusmäärittelyä voidaan tehdä. Toteutetut vaatimukset täytyy myös todentaa ja kelpuuttaa. Todennus tarkoittaa sitä, että vastaako vaaditut toimet toteutusta. Vaatimuksena oleva toiminto täytyy siis olla myös oikeasti tehtynä vaatimuksen mukaan. Kelpuutus on viimeinen vaihe suunnitteluprosessissa. Kelpuutus tehdään, kun kerättyjä vaatimuksia vastaava laitteisto ja toiminnot on jo toteutettu. Kelpuutuksella otetaan kantaa tehtyjen asioiden oikeellisuuteen. Esimerkiksi ohjausjärjestelmänstandardi 13849-2:2012 kertoo, miten ohjausjärjestelmät kelpuutetaan (Ohjelmallinen turvallisuus 2014, 16-24).

Vaatimustenmäärittelyssä on yleensä käytetty joko suoritustasoja (PLr) tai turvallisuuden eheystasoja (SIL) kuvaamaan vaadittua tasoa, johon sekä ohjelman, että laitteistojen on pystyttävä. Aikaisemmin mainitsemani riskiarvioinnin eläminen tarkoittaa sitä, että vaadittava suoritustaso saattaa muuttua jossain kohtaa konetta. Tällöin täytyy tarkastaa, yltääkö jo suunniteltu ohjausjärjestelmä tähän tasoon ja mahdollisesti tehdä muutoksia tason saavuttamiseksi.

6.2 Dokumentointi

Turvallisuuteen liittyvien järjestelmien dokumentointi on erittäin tärkeää siitä syystä, että tiedetään, miten turvatoiminnot toimivat. Selkeys on yksi tärkein prioriteetti lähdettäessä dokumentoimaan näitä järjestelmiä, sillä niiden on oltava kaikille ymmärrettävässä muodossa. Yhtä tärkeänä asiana pidetään dokumentaation revisiointia. Revisioinnin myötä tiedetään, mitä milloinkin on tehty ja onko asia varmasti päivitetty jokaiseen muutokseen liittyvään dokumenttiin (Ohjelmallinen turvallisuus 2014, 13).

Tärkeimpiä dokumentoitavia asioita turvallisuuteen liittyvien järjestelmien suunnittelussa Siirilän ja Tytykosken mukaan ovat:

- kaikki ohjausjärjestelmällä toteutettavat turvatoiminnot
- ohjausjärjestelmän tarkat alku- ja loppukohdat kunkin turvatoiminnon osalta
- kyseisen ohjausjärjestelmän käyttökelpoisuus toimintaympäristöön
- turvatoiminnon tarkoitus ja ominaisuudet
- suoritustaso PL tai eheystaso SIL, jonka turvatoiminto kykenee toteuttamaan
- turvatoiminnon luokittelu (B, 1, 2, 3, 4)
- MTTFd-, DC- ja CCF-muuttujien arvot sekä näihin liittyvien toimenpiteiden esittely (ks. luku 5.2.4)
- järjestelmän oletettu toiminta-aika
- käytettyjen teknologioiden maininta, kuten sähkö, hydrauliikka, ohjelmoitava elektroniikka
- tarkasteluissa olleiden vikojen esittely ja poissuljettujen vikojen perustelut

- toimenpiteet turvatoimintojen mitätöintiä vastaan. Mitätöinti tarkoittaa turvatoiminnon tietoista ohitusta. (Siirilä & Tytykoski 2016, 573.)

Turvadokumentaatiota tehtäessä kannattaa miettiä samalla myös mihin muuhun suunnitteluun dokumenttia käytetään. Esimerkiksi ohjelmistosuunnittelija voi haluta nähdä tästä dokumentista tiettyjä asioita turvaohjelman tekoa varten. Myös suoritustasojen laskenta esimerkiksi Sistema-ohjelmistotyökalulla on tehokkaampaa, jos dokumentaatio on tehty Sistemaa hiukan silmällä pitäen. Turvapiirien testauksen kannalta on myös suotavaa, että se voitaisiin tehdä helposti turvadokumentaation avulla (Ohjelmallinen turvallisuus 2014, 21).

7 Turvadokumentointimallin suunnittelu

Protaconin tarvitseman turvadokumentoinnin päätarkoituksena oli kehittää turvatoimintojen toteutuksesta mallidokumentaatio, jota voi soveltaa eri projekteihin. Ongelmana on tähän asti ollut se, että tiedonsiirto laitteistosuunnittelun (HW) ja ohjelmistosuunnittelun (SW) välillä ei ole ollut ohjausjärjestelmien turvatoimintoihin liittyen niin optimaalista, kuin se olisi voinut olla. Turvallisuuteen liittyvien ohjausjärjestelmien dokumentointimallin tulisi olla selkeä ja sen avulla tulisi löytää reitti, jota signaali etenee aina toimilaitteelle saakka. Esittelen tässä luvussa apunani käyttämät käytännön suunnittelun työkalut ja tiedonlähteet, joiden avulla saatiin selvitettyä, mikä on Protaconille hyödyllisin tapa esittää turvadokumentaatio jatkossa.

7.1 Turvapiirien suoritustasojen laskenta Sistemalla

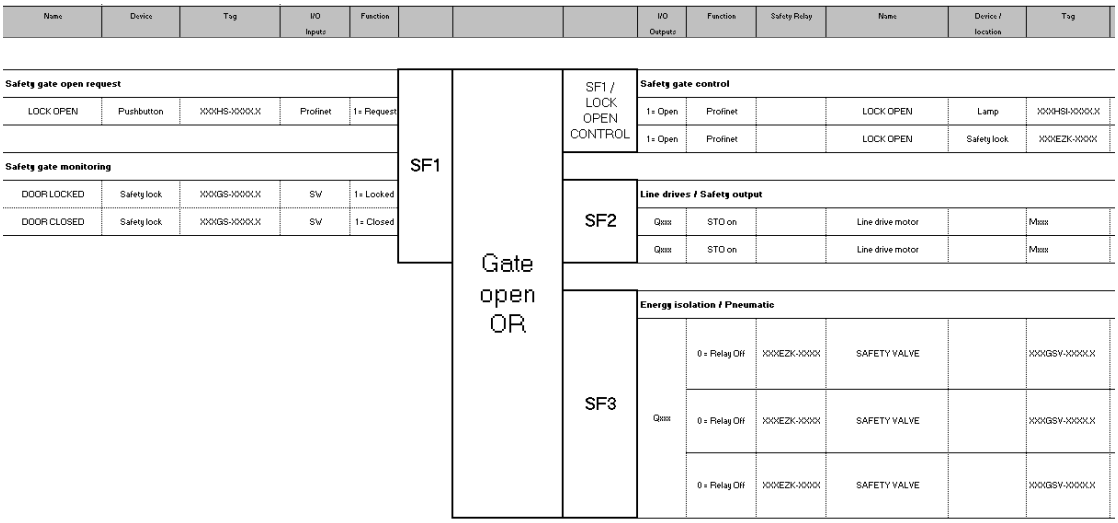
Turvadokumentaation suunnitteluprosessi aloitettiin tekemällä erääseen Protaconilla meneillään olevaan projektiin turvatoimintojen suoritustasojen laskentaa Sistema ohjelmistotyökalulla. Sistema on saksalaisen työsuojeluun erikoistuneen tutkimuslaitoksen IFA:n tarjoama ilmainen ohjelmistotyökalu. Sisteman avuksi tarvitaan yleensä suunnittelun kohteesta konekohtaiset riskianalyysit ja turvalohkokaaviot joka koneen, tai esimerkiksi turva-alueen osalta.

Sistemalla työskentely alkoi lataamalla IFA:n verkkosivuilta ohjelman viimeisimmän version. Tärkeää on valita viimeisin versio ohjelmasta, sillä ohjelma käyttää standardeja ISO 13849-1:2015 ja 13849-2:2012, joita päivitetään aika ajoin. Kuviossa 14 nähdään kuvakaappaus Sisteman versiosta ja käytettävistä standardeista. Nämä standardien versiot olivat opinnäytetyön kirjoitushetkellä viimeisimmät julkaisut ja näin voitiin varmistaa, että määrittelyt ja laskenta on tehty ajankohtaisten standardien mukaisesti.

Kuvio 14. Kuvakaappaus Sisteman aloitusnäkymästä

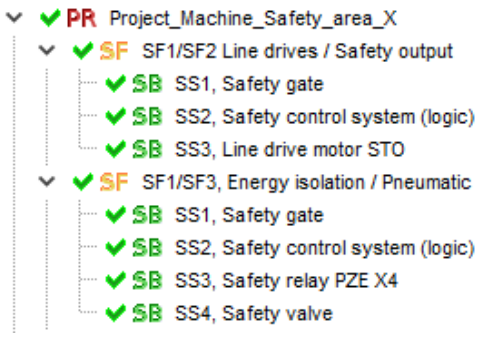
Aluksi täytyi opiskella hieman Sistema-ohjelman toimintaa ja miettiä, miten lohkokaavion data voitaisiin siirtää järkevästi siihen. Alkuperäisen, yrityksen käytössä olleen turvalohkokaavion pohja (ks. kuvio 15) oli aikaisemman Protaconin projektin lohkokaavioiden perusteella tehty ja toteutus oli toimiva myös Sisteman kannalta.

Aikaisemmassa dokumentointitavassa on käytetty dokumentointiin liittyviä tärkeimpiä osia (ks. luku 6.2). Turva-alueen kaikki turvatoiminnot, eli SF1/SF2 ja SF1/SF3 on esitelty kyseisen turva-alueen lohkokaaviossa. Myös signaalin alku- ja loppukohdat on esitelty tässä dokumentaatiossa tarkasti, joten dokumenttiin liittyviin piirikaavioihin päästiin helposti käsiksi ”Tag”- ja ”I/O inputs”- sekä ”I/O outputs”-sarakkeiden perusteella. Turvatoiminnon tarkoitus on kerrottu lyhyehkösti ”Gate Open”-tyylisesti, se tarkoittaa oven aukaisusta aiheutunutta turvatoiminnon aktivoitumista. Tarkempi kuvaus on tehty riskinarvioinnissa.



Kuvio 15. Kuvakaappaus alkuperäisestä turvalohkokaaviosta

Kuviossa 16 nähdään ensimmäinen projektipuu, jonka laadin Sistemaan kuvion 15 turvalohkokaavion pohjalta. Sisteman projektipuussa project (PR)-kohtaan on tehty turva-alue, jonka turvatoimintojen suoritustasoja ryhdytään laskemaan. Seuraavana tulee safety function (SF), joka tarkoittaa yhtä turvatoimintoa. SF:n alla on subsystems (SB) eli alajärjestelmät, jotka turvatoiminto sisältää. Alajärjestelmä kuvaa ohjausjärjestelmän osaa, eli komponentteja tässä tapauksessa. Erilaiset ohjausjärjestelmien rakenteet on esitelty luvussa 5.2.2.



Kuvio 16. Kuvakaappaus Sisteman projektipuusta

Esittelen seuraavaksi kuvioihin 15 ja 16 liittyvän esimerkin turvatoimintojen SF1/SF2 ja SF1/SF3 toiminnasta:

Esimerkki 1.

SF1/SF2 tapauksessa (ks. kuviot 15 ja 16) tarkoitetaan turvatoimintoa, joka poistaa vääntömomentin linjakäyttömoottorilta taajuusmuuttajan STO-toiminnolla. Ensimmäisenä tulee SS1 eli turvaportin antama signaali, kun turvaportti on auki. Seuraavaksi signaali etenee turvalogiikalle SS2. Turvalogiikalta signaali ohjataan linjakäyttöjen taajuusmuuttajien STO-request lähtöön, jolloin moottorin akselin pyörimisnopeus alkaa hidastua ja lopulta pysähtyy.

Esimerkki 2.

SF1/SF3 on turvatoiminto (ks. kuviot 15 ja 16), joka poistaa järjestelmän paineilmat tarvittavilta laitteilta turvaventtiilin avulla. Turvaportin antama signaali SS1 etenee turvalogiikalle profinetin välityksellä. Turvalogiikka SS2 katkaisee signaalin turvareleen kelalta. Turvareleen SS3 koskettimet aukeavat ja turvaventtiili SS4 reagoi jännitteen katkeamiseen päästämällä paineilmat pois järjestelmästä. Esimerkki päättyy.

Kuvioissa 17 ja 18 on kuvakaappaukset Sistemaan luomistani alajärjestelmistä kutakin turvatoimintoa kohden. Kuviossa 17 nähdään, että jokainen turvatoiminnon SF1/SF2-alajärjestelmä (SB) on yltänyt korkeimpaan tasoon PL e. Turvatoiminnon SF1/SF3 (ks. kuvio 18) osalta turvaventtiili SS4 on heikoin lenkki suoritustasollaan PL d, ja tällä on vaikutusta koko turvatoiminnon suoritustasoon.

Status	Name	Ref. des.:	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔SB	SS1, Safety gate		e	n.a.	4,1E-8	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔SB	SS2, Safety control system (logic)		e	n.a.	3,2E-8	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔SB	SS3, Line drive motor STO		e	n.a.	1E-9	*not relevant*	*not relevant*	*not relevant*	3	fulfilled

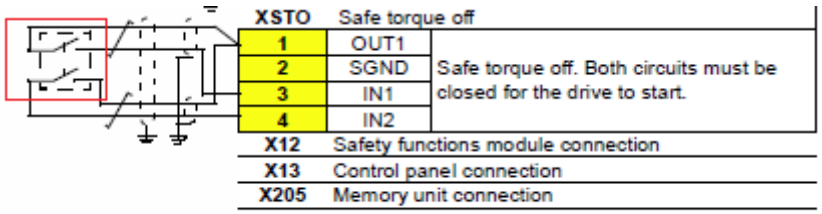
Kuvio 17. Alajärjestelmien suoritustasot SF1/SF2

Status	Name	Ref. des.:	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category
✔ SB	SS1, Safety gate		e	n.a.	4,1E-8	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	SS2, Safety control system (logic)		e	n.a.	3,2E-8	*not relevant*	*not relevant*	*not relevant*	3	fulfilled
✔ SB	SS3, Safety relay PZE X4		e	n.a.	3,2E-8	*not relevant*	*not relevant*	*not relevant*	4	fulfilled
✔ SB	SS4, Safety valve		d	n.a.	3,2E-7	*not relevant*	*not relevant*	*not relevant*	3	fulfilled

Kuvio 18. Alajärjestelmien suoritustasot SF1/SF3

Kuvioissa 17 ja 18 näkyviä suoritustasoja ei ole tarvinnut laskea Sistemassa yhtä monimutkaisesti kuin standardi 13849-1:2015 esittää, sillä suoritustasot ja luokat on saatu laitteiden valmistajien datalehdistä sekä Sistemaan ladattavista valmistajakohtaisista kirjastoista.

Alajärjestelmiä tehdessä kannattaa ottaa huomioon valmistajan valmiiksi datalehdissä ja manuaaleissa antamat järjestelmän kytkentätavat. Turvapiirejä suunniteltaessa turvapiirit kannattaa toteuttaa komponentin valmistajan manuaaleista löytyvien kytkentätapojen mukaisesti. Tällöin valmistaja on vastuussa siitä, että kytkentätapa on standardien mukainen. Kuviossa 19 on esimerkki ABB:n taajuusmuuttajan STO kortille liitynnästä. Kuviossa näkyy punaisen neliön sisällä turvaohjauspiirin, esimerkiksi turvareleen koskettimet. Jos valmistaja ei anna tällaista kytkentäohjetta, on lisättävä turvarele erillisenä alajärjestelmänä Sistemaan. Käytännössä se tarkoittaisi, että kuviossa 16 näkyvään SF1/SF2-turvatoiminnon ketjuun lisättäisiin SS2:n ja SS3:n väliin käytetty turvarele ja sen vikaantumistiedot.



Kuvio 19. ABB ACS880-taajuusmuuttajan STO-liitäntä (Hardware manual ACS880-01 drives 2017, 111)

Tällä tavalla valmistajan tietoja hyödyntämällä voidaan ohittaa yksityiskohtainen manuaalinen tietojen lisäys Sistemaan. Käytännössä tarvitsee vain katsoa, minkä suoritustason ja luokan valmistaja on ilmoittanut (ks. kuvio 20).

Safety data (SIL, PL)

The safety data for the Safe torque off function is given below.

Note: The safety data is calculated for redundant use, and does not apply if both STO channels are not used.

Frame size	SIL/ SIL CL	SC	PL	SFF (%)	PFH (T_1 = 20 a) (1/h)	PFD_{avg} (T_1 = 2 a)	PFD_{avg} (T_1 = 5 a)	$MTTF_D$ (a)	DC (%)	Cat.	HFT	CCF	Life-time (a)
U_N = 230 V													
R1	3	3	e	>99	2.84E-09	2.37E-05	5.91E-05	10530	≥90	3	1	80	20
R2	3	3	e	>99	2.84E-09	2.37E-05	5.91E-05	10529	≥90	3	1	80	20
R3	3	3	e	>99	2.84E-09	2.37E-05	5.91E-05	10489	≥90	3	1	80	20
R4	3	3	e	>99	2.89E-09	2.41E-05	6.02E-05	10442	≥90	3	1	80	20
R5	3	3	e	>99	2.89E-09	2.41E-05	6.02E-05	10240	≥90	3	1	80	20

Kuvio 20. Valmistajan antamat turvallisuustiedot (Hardware manual ACS880-01 drives 2017, 246)

Dokumentointiin liittyvät vaatimuksia on luvun 6.2 mukaisesti täytetty Sistemalla työskennellessä, sillä ohjelma perustuu standardeihin. Näin ollen turvatoimintojen suoritustasot PL on oikeilla menetelmillä määritelty sekä ohjausjärjestelmän luokka on valittava ohjelman oikean toiminnan kannalta (ks. kuvio 17 ja 18). Loput arvot $MTTF_D$, DC, CCF ja oletettu toiminta-aika on mainittu valmistajan datalehdillä, joten Sistemassa pelkkä viittaus datalehteen riittää dokumentaatioksi näiden osalta.

Kummankin turvatoiminnon osalta nähdään myös turvatoiminnolta vaadittu taso PLr ja PL, jotka on laskettu yksinkertaisesti PFHd-arvojen yhteenlaskuna Sistemassa. Kuvioissa 17 ja 18 näkyvät PFHd-tasot, joiden perusteella lopullinen suoritustaso PL (ks. kuvio 21) saadaan laskettua ohjelmassa. SF1/SF3-turvatoiminnon osalta PL-taso laskee d-tasoon, koska PFHd:n arvo yhteenlaskun seurauksena kasvaa suuremmaksi ja lopullinen PFHd-arvo asettuu taulukon 4 mukaisesti PL d tasolle määritetylle välille $10^{-7} to\ 10^{-6}$.

Vaatimukset näiden turvatoimintojen osalta on asetettu PLr a tasolle, eli sen mukaan

oletetaan, että riski joutua tapaturmaan on erittäin pieni ja tapaturma aiheuttaisi korkeintaan palautuvan vamman. Todellisuudessa PLr taso ei ole näin alhainen kyseisellä koneen osalla ja tästä syystä turvatoiminnotkin on suunniteltu niin, että suoritustaso yltää luotettavammalle tasolle. Syy matalan PLr-tason asettamiselle oli tässä vaiheessa koneen riskiarvioinnin tulkinnasta aiheutuvissa ongelmissa.

Status	Name	Type	PLr	PL
✔ SF	SF1/SF2 Line drives / Safety output	Safety-related stop functi...	a	e
✔ SF	SF1/SF3, Energy isolation / Pneumatic	Safety-related stop functi...	a	d

Kuvio 21. Turvatoimintojen PLr- ja PL-tasot

7.2 Turvalohkokaaviomallin luominen

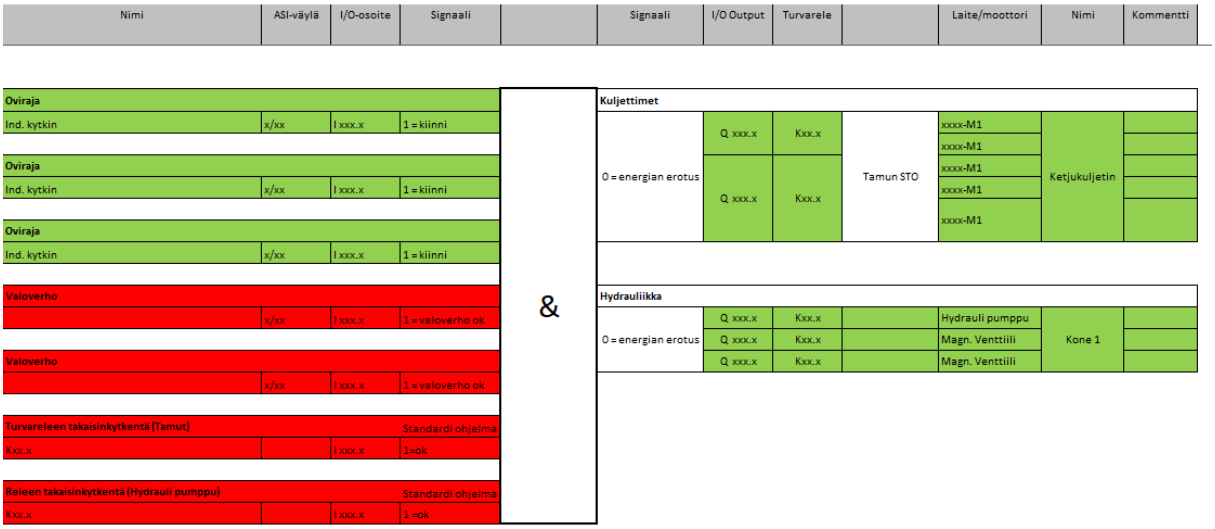
Sistemalla työskentelyn jälkeen aloin tutkia, että onko jo aikaisemmin käytetty turvalohkokaavion pohja (ks. kuvio 15) sopiva jatkossakin mallipohjana käytettäväksi. Peruskomponentit ko. turvalohkokaaviossa olivat kunnossa. Hyviä puolia olivat mm. turvatoimintojen erittely ja tarvittavien tietojen esimerkiksi I/O-osoitteiden ja tunnuksien näkyminen. Lohkokaaviosta on mielestäni näistä syistä helppo seurata turvatoiminnon aiheuttaman signaalin polkua, joka on tärkeä asia dokumentoinnin selkeyttä ajatellen.

Opinnäytetyöni kannalta alkoi hyvään aikaan eräs turvapiirien tarkistukseen ja dokumentointiin liittyvä projekti. Yhtenä osana tätä projektia oli tuottaa siis turva-alueiden dokumentaatio. Päätimme projektin vetäjän kanssa, että toteutan turvadokumentaation mallin luomisen tämän projektin yhteydessä.

7.2.1 Ensimmäinen versio lohkokaaviomallista

Aloitin työnteon tutustumalla projektin lähtötietoihin, joista löytyi kyseisen linjaston riskinarviointidokumentti ja layoutkuva. Tein layoutista suuntaa antavan esimerkin

kohteena olevien turva-alueiden hahmottamiseksi (ks. liite 5). Riskinarvioinnista selvisi mm. koneesta aiheutuvat mahdolliset vaarat, vaadittavat toimenpiteet riskien pienentämiseksi sekä ohjausjärjestelmältä vaadittu suoritustaso PLr. Riskinarviointidokumentti oli jaettu osiin linjastolla sijaitsevien koneiden perusteella, joten turva-alueet, joilla oli enemmän koneita, oli jaettu useampaan osaan. Riskinarvioinnin perusteella pystyin luomaan aikaisemman mallin mukaiset turvalohkokaaviot joka turva-alueesta ja jakamaan turva-alueilla sijaitsevat koneet ja laitteet oikeille turva-alueille. Kuviossa 22 nähdään ensimmäinen esimerkki turva-alueesta lohkokaavion muodossa.



Kuvio 22. Turvalohkokaavion ensimmäinen versio

Turvalohkokaavion ensimmäisessä versiossa on käytetty samaa tyyliä, kuin Protaconin aikaisemmassa dokumentointitavassa (ks. kuvio 15). Tuloyksikönpuolelle, eli vasemmalle puolelle AND-porttia (&), on lisätty kaikki turva-alueeseen vaikuttavat turvalaitteiden tilatiedot. Oikealla puolella on lähdöt, jotka täytyy pysäyttää tulojen kääntyessä nollaksi (0). Värejä lisättiin tähän malliin projektiin liittyvistä syistä. Syy saman mallin käyttämiseen oli se, että tarvitsin kommentteja ja palautetta siitä, mikä nykyisessä versiossa on huonoa ja mikä hyvää.

Dokumenttia käytetään Protaconilla turvaohjelman suunnittelussa ja mahdollisesti piirien testauksessa apuna, joten tarvitsin kommentteja kokeneemmilta kollegoilta.

Kävin keskustelua laitteisto- ja ohjelmistopuolen kollegoiden kanssa luodusta turvalohkokaavion mallista ja seuraavia seikkoja tuli ilmi:

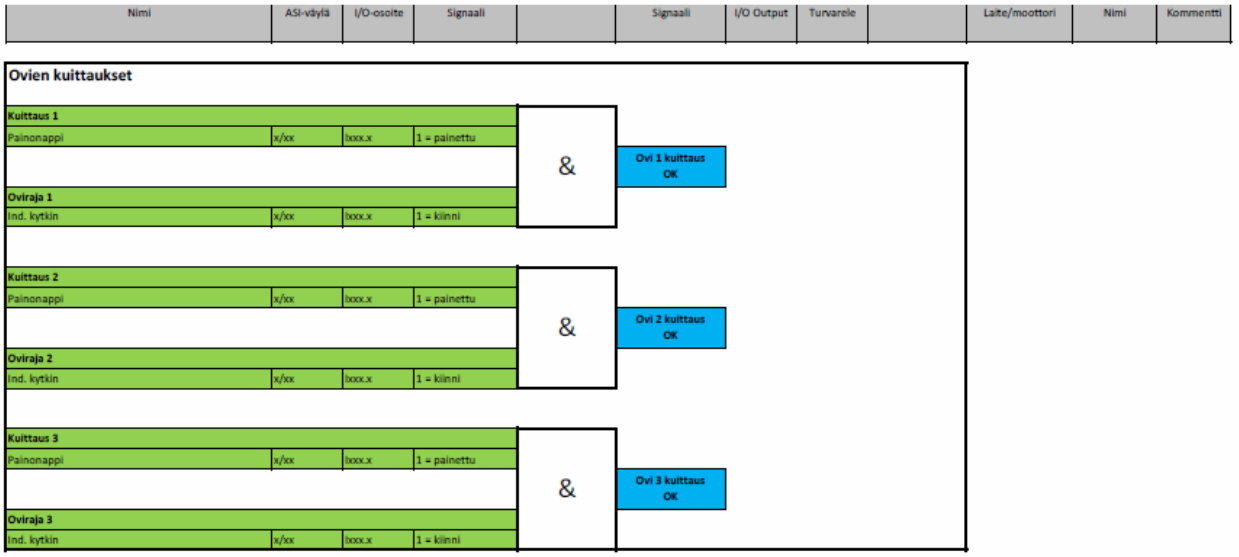
- Miten kerrotaan ohjelmistosuunnittelijalle usean turva-alueen vaikutus pysäytettävään laitteeseen tai koneeseen?
- Pitää saada turvaohjelman suunnittelijalle välitettyä tieto, mitkä kaikki tulot pysäyttävät tietyn lähdön.
- Ohjelmistosuunnittelija ajattelee asiaa ohjelmablokkien muodossa ja ei esitä yhdessä blokissa kaikkia turva-alueen tuloja ja lähtöjä. Ehdotuksena oli mieluummin useamman tiivistetyn blokin tekeminen tuloista turva-alueittain.
- Pysäytettävien lähtöjen keräys vaikuttavan turva-alueen dokumenttiin. Tällä estettäisiin lähtöjen näkyminen monessa paikassa ja aiheutuisi vähemmän toistoa suunnittelussa.
- Kommentteja ja huomautuksia enemmän dokumenttiin.

Palautteen ansiosta sain käsityksen siitä, millaisen mallin Protacon haluaisi käyttöönsä turvadokumentaatiosta. Ensimmäinen versio turvadokumentin mallista oli omasta mielestäni riittävän hyvä, sillä olin työskennellyt suurimman osan ajasta lähinnä Sisteman parissa. Olin kuitenkin ehtinyt jo tehdä kaikkien kymmenen turva-alueen kaaviot jo valmiiksi ensimmäisen version mukaan, joten itsekin huomasin toistoa lähtöjen listaamisessa turva-alueiden dokumentteihin.

7.2.2 Uudistettu lohkokaaviomalli

Lopullinen turvadokumentin mallin työstäminen aloitettiin muuttamalla ensimmäistä versiota kommentit ja dokumentoinnin perusasiat huomioiden. Käytännössä alkuperäisiä tuloja ja lähtöjä ei tarvinnut muutella paljon, sillä turvalohkokaavion peruselementit eli tulo- ja lähtötiedot olivat jo kasassa. Ainoat lisäykset tuloihin olivat kuittauspainikkeet. Suurinta muutosta lähdettiin tekemään dokumentin järjestyksen ja toiminnallisuuden kannalta. Toiminnallisuuden tarkastus tarkoittaa tässä

turvapiirien kannalta oikeaa toimintaa eli sitä toimivatko tässä luvussa esittellyt lohkot oikein myös loogisessa mielessä.



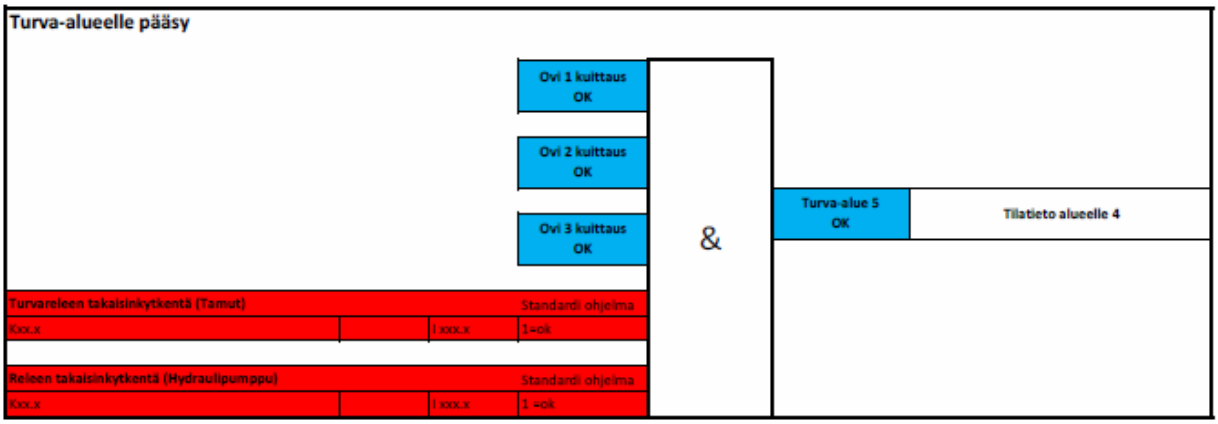
Kuvio 23. Uudistettu turvalohkokaavion malli, ovien kuittaukset

Turvalohkokaavion uudistettu malli vaati hiukan tarkempaa miettimistä kuittausten ja ovien toiminnan kannalta (ks. kuvio 23). Lohkokaaviota lähdettiin toteuttamaan yksinkertaisilla yksittäisistä turvapiirien palasista tiivistetyistä OK-tiedoista. OK-tiedot on koottu niiden ovien tai valoverhojen tulotiedoista, joista on pääsy sisälle turva-alueella. Ovien vieressä on myös kuittauspainikkeet, joilla voidaan kuitata turva-alue tyhjäksi henkilöistä alueelta poistumisen jälkeen.

Toiminta on nyt kuvattu niin, että esimerkiksi oven 1 aukaisu kääntää ”Ovi 1 kuittaus OK”-tiedon nollaksi (0). Oven aukaisun jälkeen kyseisen avatun oven kuittaus 1 vaihtaa tilansa turvaohjelmassa myös nollaksi (0). Kun turva-alue on varmistettu tyhjäksi henkilöistä ja ovi on kiinni (1), kuittauspainikkeen painaminen asettaa kuittauksen tilan ykköseksi (1). Kun oven ja kuittauspainikkeen tilat ovat kummatkin ykkösiä (1), ”Ovi 1 kuittaus OK”-tieto vaihtuu jälleen ykköseksi (1). Tässä on esitelty ohjelmistosuunnittelijalle tarpeeksi tarkasti kyseinen toiminto. Turvaohjelmassa

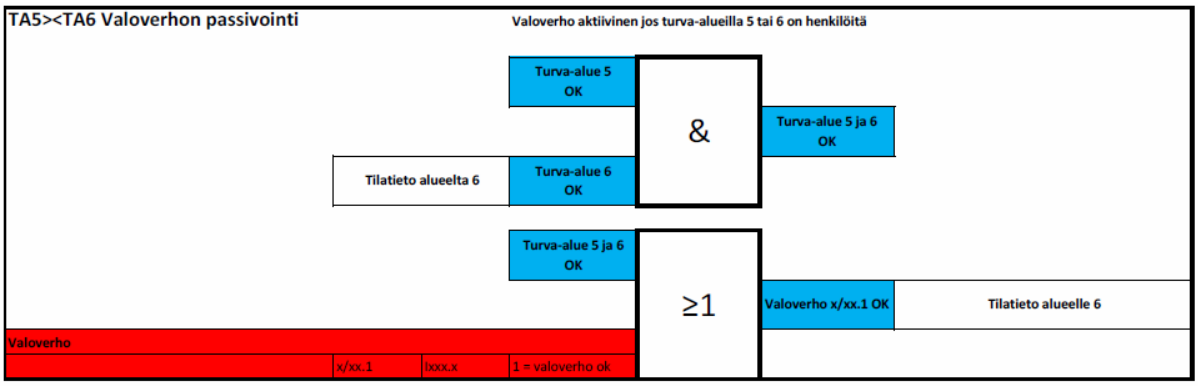
kuittauksia ei tehdä aivan samalla tavalla, sillä on olemassa valmiita valmistajan laatimia ohjelmablokkeja turvaovien ja valoverhojen ohjelmointia varten.

Tällainen rakenne on hyvä, jos sisäänpääsyaukkoja tai ovia tulee lisää, jolloin ei tarvitse kuin yhteen dokumenttiin lisätä uusi tulo. Uutta ovea lisätessä täytyy myös I/O testata, joten testausmielessäkin tämä rakenne on yksinkertainen. Testauksessa riittää vain tarkastus OK-tietoon saakka, sillä loppuosa ohjelmasta on säilynyt ennallaan.



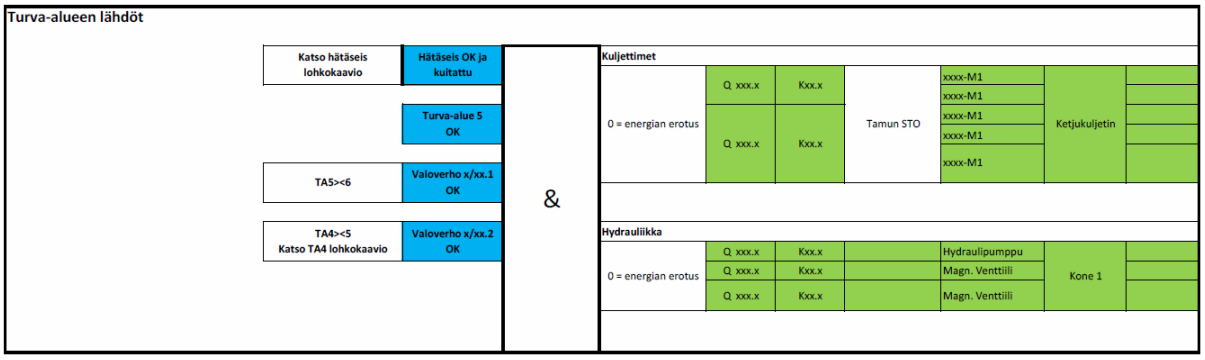
Kuvio 24. Uudistettu turvalohkokaavion malli, turva-alueelle pääsy

Kuvion 24 ”Turva-alueelle pääsy”-blokki tiivistää kuviossa 23 luodut ”Ovi x kuittaus OK”-tiedot. Lisänä on vielä käytetty kyseiseen alueeseen liittyvien kuljettimien ja koneiden takaisinkytkennästä tulevaa pysäytystietoa. Taajuusmuuttajan ja hydrauliikkapumpun pysäytystieto on saatu saman turvareleen koskettimilta, joka pysäyttää kyseiset laitteet oven aukaisun tai valoverhon laukaisun yhteydessä. Kuittauspainikkeen painaminen palauttaa turvareleen ja ”Ovi x Kuittaus OK”-tiedon takaisin normaaliin tilaan, jonka jälkeen ”Turva-alue 5 OK”-tieto vaihtuu myös jälleen ykköseksi (1). Taajuusmuuttajien ohjaamat moottorit, ja hydrauliikkapumput eivät kuitenkaan saa heti kuittauksen jälkeen lähteä käyntiin uudestaan, vaan turvaohjelmassa määritellään tarkemmin että käynnistyskäsky vaaditaan vielä erikseen. Tilatieto turva-alueen tilasta viedään myös turva-alueelle 4.



Kuvio 25. Uudistettu turvalohkokaavion malli, valoverhon passivointi.

Valoverho oli lohkokaavion ensimmäisessä versiossa (ks. kuvio 22) samassa blokissa, kuin alueelle johtavat ovet. Todellisuudessa valoverhot sijaitsevat kahden turva-alueen rajalla ketjukuljettimen kohdalla liitteen 5 mukaisesti. Jos ohjelma olisi suoraan tehty aikaisemman version tavalla, kuljettimella kulkeva kuorma olisi aina pysäyttänyt ympäröivät alueet. Alueiden välissä oleville valoverhoille tehtiin siis omat blokit turva-alueittain (ks. kuvio 25), joka sallii kuorman kulkemisen valoverhon läpi ilman alueiden pysähtymistä. Jos turva-alueelle kuitenkin mennään sisälle, kyseinen alue pysähtyy ja alueiden välinen valoverho muuttuu aktiiviseksi. Tällä tavalla saadaan pysäytettyä seuraava turva-alue, jos esimerkiksi ihminen yrittäisi mennä toisen valoverhon läpi seuraavalle alueelle.



Kuvio 26. Uudistettu turvalohkokaavion malli, lähdöt.

Lopuksi edellä esitellyistä blokeista kerättiin tiivistettyjä OK-tietoja näkyvään turva-alueen lähdöt (ks. kuvio 26) nimiseen blokkiin kuljettimien ja laitteiden pysäyttämiseksi. Tietoja kerättiin hätäseiskaaviosta ja ympäröivistä turva-alueista sen mukaan, miten niiden oli tarkoitus vaikuttaa alueen lähtöihin. Lähdöt saatiin kopioimalla ne ensimmäisestä turvalohkokaavion mallista.

7.2.3 Yhteenveto

Lopputuloksena saatiin yksinkertainen esimerkki turvallisuuteen liittyvien järjestelmien dokumentoinnista. Turvapiirin osien pilkkominen pienempiin osiin dokumentissa helpottaa lukemista ja ymmärtämistä. Dokumentointiin liittyviä perusasioita (ks. luku 6.2) on käytetty tässä dokumentointitavassa soveltuvin osin. Kaikki turva-alueen ohjausjärjestelmällä toteutetut turvatoiminnot on esitetty lohkokaaviossa, jäljitettävyys I/O ja ASi-väylä osoitteen perusteella sekä releiden ja moottorien tunnuksien mukaan on mahdollista. Tiivistämällä tietoja yksittäisiksi OK-tiedoiksi, saatiin dokumenteista helpommin jäljitettäviä ja yksinkertaisempia ohjelmistosuunnittelijan käyttöön. Toiminnallisiin testauksiin lohkokaaviot sopivat nyt myös paremmin. Lisäksi tarkentavaa kommentointia voidaan tehdä ymmärtämisen helpottamiseksi, mutta tämän työn dokumenteista ne on poistettu projektien tietosuojan vuoksi.

Koko turva-alueen 5 turvalohkokaavio on nähtävissä liitteissä 6 ja 7. Havainnoinnin helpottamiseksi lisäsin liitteeksi myös turva-alueen 6 lohkokaavion (ks. liite 8), joka sijaitsee tässä esitellyn turva-alueen 5 vieressä.

8 Pohdinta

Opinnäytetyön tavoitteena oli kehittää Protaconille soveltuva toimintatapa ja malli, jolla turvatoimintojen dokumentointi projekteissa toteutetaan, sekä perehtyä samalla koneturvallisuuteen. Työn tuloksena saatiin kehitettyä dokumentointitapa ja malli, joka soveltuu toimeksiantajan käyttöön projektista riippumatta. Malli täyttää myös ohjausjärjestelmästandardissa ISO 13849-1:2015 esitellyn turvallisuuteen

liittyvän lohkokaavion piirteet. Työn tulosta voidaan hyödyntää kaikissa turvallisuuteen liittyvien piirien dokumentoinnissa. Jatkokehitysmahdollisuuksia on rajattomasti ja käytännössä nykyinen dokumentointimalli on tehty tämän hetkisten suunnittelijoiden toiveiden mukaiseksi.

Opinnäytetyön eteneminen oli mielestäni järjestelmällistä alun vaikeuksien jälkeen, sillä aluksi perehdyin koneturvallisuuteen itsenäisesti ja teorian opiskelua auttoi myöhemmin projektit, joissa pääsin tekemään koneturvallisuuteen liittyvää määrittelyä. On ollut mukava huomata, että alun karkeasta ja suuresta tietomäärän opiskelusta on projektien myötä saanut selville, mitkä ovat tärkeimmät asiat koneturvallisuuteen liittyvissä määrittelyissä. Kollegoiden näkemykset auttoivat myös loppuvaiheessa keskittymään enemmän oikeisiin asioihin työn kannalta. Käytännön työt opinnäytetyöhön liittyen ovat olleet myös erityisen mielenkiintoisia ja hyvää kokemusta uralleni. Ammatillista kehitystä on tapahtunut paljon, niin piirikaavioiden lukemisessa, kuin koneturvallisuuden tärkeyden ymmärtämisessä.

Opinnäytetyöstä haastavan teki koneturvallisuuden laaja aihealue sekä se, että kokemusta aiheesta minulla ei ollut juuri ollenkaan. Alussa oli vaikeuksia tietää, mistä lähteä etenemään ja mikä on oikea polku opinnäytetyöni konkreettista tavoitetta ajatellen. Pääsin kuitenkin kiinni aiheeseen koneturvallisuuteen perehtyvän kirjallisuuden avulla ja se auttoi ymmärtämään, mitkä standardit ovat työni taustalla. Työssä esiteltyjen kahden eri turvallisuusmäärittelyn osalta päädyin siihen, että esittelen laajemmin suoritustasoihin liittyvän määrittelyn. Eheystasoihin liittyvää määrittelyä jätin hieman vähemmälle tarkastelulle, sillä sen voi tehdä karkeasti suoritustasojen määrittelyyn liittyen.

Koneturvallisuuden aihe ja sen syvempi opiskelu opinnäytetyön toteutusta varten on monipuolistanut osaamistani työelämässä sekä luonut minulle enemmän mahdollisuuksia pärjätä työmarkkinoilla tulevaisuudessa. Uskon että turvallisuudesta ei jatkossakaan aleta tinkimään ja että turvallisuus tulee parantumaan automaation lisääntymisen seurauksena. Silloin vaaditaan yhä enemmän osaamista koneturvallisuuden saralla sekä jatkuvaa ammatillista kehitystä tekniikan mukana

pysymisessä. Näistä syistä tekemäni opinnäytetyöni on mielestäni loistava johdatus uralleni koneturvallisuuden parissa.

Lähteet

Hardware manual ACS880-01 drives. 2017. ABB Group. Viitattu 12.10.2017. https://search-ext.abb.com/library/Download.aspx?DocumentID=3AUA0000078093&LanguageCode=en&DocumentPartId=1&Action=Launch

Hietikko, M. Malm, T. & Alanen, J. 2009. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen. Viitattu 13.10.2017. http://www.vtt.fi/Documents/2009_T2485.pdf

Konedirektiivin 2006/42/EY soveltamisopas. 2010. Euroopan komissio. Yritys- ja teollisuustoiminta. 2.p. Viitattu 4.7.2017. https://ec.europa.eu/docsroom/documents/9202/attachments/1/translations/fi/renditions/pdf

Me olemme Protacon. 2017. Ladattava esite Protaconin verkkosivuilla. Viitattu 27.10.2017 https://www.protacon.com/me-olemme-protacon/

Ohjelmallinen turvallisuus. 2014. SARLIN. Viitattu 13.7.2017. Protaconin tietokanta.

Profinet. N.d. Siemensin verkkosivut. Viitattu 17.10.2017. http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/automaatiotekniikka/teollinen_tiedonsiirto_esim_profinet/profinet.htm

SFS 5974. 2011. Opastusta standardien ISO 13849-1 ja IEC 62061 soveltamiseksi koneen turvallisuuteen liittyvien ohjausjärjestelmien suunnittelussa. Suomen Standardisoimisliitto SFS. Viitattu 10.7.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

SFS-EN ISO 13849-1:2015. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 3.p. Suomen Standardisoimisliitto SFS. Viitattu 17.10.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

SFS-EN ISO 13850:2015 Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet. 3.p. Suomen Standardisoimisliitto SFS. Viitattu 5.7.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

SFS-EN ISO 14119:2013. Koneturvallisuus. Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta. Suomen Standardisoimisliitto SFS. Viitattu 4.7.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

SFS-EN 60204-1:2006. Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset. 3.p. Suomen Standardisoimisliitto SFS. Viitattu 5.7.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

SFS-EN 62061:2005. Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Suomen Standardisoimisliitto SFS. Viitattu 13.7.2017. Protacon Technologies Oy:n SFS Online lisenssillä.

Siirilä, T. 2014. Turvalaitteiden passivoinnin turvallinen toteuttaminen. Viitattu 6.7.2017. http://www.metsta.fi/www/koneturvallisuuden_teemasivut/artikkelit/2014_nro_012.pdf

Siirilä, T. & Tytykoski, K. 2016. Koneturvallisuuden käsikirja. Helsinki: Inspecta

Liitteet

Liite 1. Taulukko luokkien yhteenvedosta (SFS-EN ISO 13849-1:2015, 47-48.)

Luokka	Yhteenveto vaatimuksista	Järjestelmän käyttäytyminen	Turvallisuuden saavuttamiseksi käytettävä periaate	Kunkin kanavan $MTTF_D$	DC_{avg}	Yhteisvikaantuminen, CCF
B (ks. 6.2.3)	Turvallisuuteen liittyvät ohjausjärjestelmän osat ja/tai niihin liittyvät turvalaitteet sekä niiden komponentit on suunniteltava, rakennettava, valittava, kokoonpantava ja yhdistettävä asiaan kuuluvien standardien mukaisesti siten, että ne voivat kestää odotettavissa olevat vaikutukset. Turvallisuuden perusperiaatteita on noudatettava.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen.	Pääsiassa luonnehdittavissa komponenttien valinnalla.	Matala ... Keskitaso	Ei lainkaan	Ei merkitystä
1 (ks. 6.2.4)	Luokan B vaatimuksia on sovellettava. Hyvin koeteltuja komponentteja ja periaatteita on sovellettava.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen, mutta vian esiintymistodennäköisyys on pienempi kuin luokassa B.	Pääsiassa luonnehdittavissa komponenttien valinnalla.	Korkea	Ei lainkaan	Ei merkitystä
2 (ks. 6.2.5)	Luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita on sovellettava. Koneen ohjausjärjestelmän on tarkistettava turvatoiminto sopivin väliajoin. (ks.4.5.4)	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen tarkistusten välisenä aikana. Turvatoiminnon menetys paljastetaan tarkistuksella.	Pääsiassa luonnehdittavissa rakenteella.	Matala ... Korkea	Matala ... Keskitaso	Ks. liite F
3 (ks. 6.2.6)	Luokan B vaatimuksia ja hyvin koeteltuja periaatteita on sovellettava. Turvallisuuteen liittyvät osat on suunniteltava siten, että — yksittäinen vika missä tahansa näissä osissa ei johda turvatoiminnon menettämiseen ja — jos on kohtuudella mahdollista, yksittäinen vika paljastuu.	Yksittäisen vian esiintyessä turvatoiminto suoritetaan aina. Muutamat viat paljastuvat mutta eivät kaikki. Paljastumattomien vikojen kerääntyminen voi johtaa turvatoiminnon menettämiseen.	Pääsiassa luonnehdittavissa rakenteella.	Matala ... Korkea	Matala ... Keskitaso	Ks. liite F
4 (ks. 6.2.7)	Luokan B vaatimuksia ja hyvin koeteltuja periaatteita on sovellettava. Turvallisuuteen liittyvät osat on suunniteltava siten, että — yksittäinen vika missä tahansa näissä osissa ei johda turvatoiminnon menettämiseen — yksittäinen vika paljastuu turvatoiminnon seuraavan vaateen yhteydessä tai ennen sitä, mutta jos tämä vikojen paljastuminen ei ole mahdollista, vikojen kerääntyminen ei saa johtaa turvatoiminnon menettämiseen.	Yksittäisen vian esiintyessä turvatoiminto suoritetaan aina. Vikojen kerääntymisen paljastuminen vähentää turvatoiminnon menettämisen todennäköisyyttä (DC on korkea). Viat paljastuvat ajoissa turvatoiminnon menettämisen estämiseksi.	Pääsiassa luonnehdittavissa rakenteella.	Korkea	Korkea, vikojen kerääntyminen otetaan huomioon	Ks. liite F

Liite 2. Yleisiä komponenttien MTTFd ja B10D –arvoja (SFS-EN 13849-1:2015, 60-61.)

	Standardin ISO 13849-2:2012 mukaiset turvallisuuden perusperiaatteet ja hyvin koetellut turvallisuusperiaatteet	Asiaankuuluvat standardit	Tyypilliset arvot: $MTTF_D$ (vuotta) B_{10D} (toimintajaksoa)
Mekaaniset komponentit	Taulukot A.1 ja A.2	—	$MTTF_D = 150$
Hydrauliset komponentit, joiden vuosittainen toimintajaksojen lukumäärä (n_{op}) ≥ 1 000 000 toimintajaksoa vuodessa	Taulukot C.1 ja C.2	ISO 4413	$MTTF_D = 150$
Hydrauliset komponentit, joiden toimintajaksojen lukumäärä on 1000000 > n_{op} ≥ 500 000 toimintajaksoa vuodessa	Taulukot C.1 ja C.2	ISO 4413	$MTTF_D = 300$
Hydrauliset komponentit, joiden toimintajaksojen lukumäärä on 500 000 > n_{op} ≥ 250 000 toimintajaksoa vuodessa	Taulukot C.1 ja C.2	ISO 4413	$MTTF_D = 600$
Hydrauliset komponentit, joiden toimintajaksojen lukumäärä on 250 000 vuodessa > n_{op}	Taulukot C.1 ja C.2	ISO 4413	$MTTF_D = 1\,200$
Pneumaattiset komponentit	Taulukot B.1 ja B.2	ISO 4414	$B_{10D} = 20\,000\,000$
Releet ja apukontaktorit pienellä kuormituksella	Taulukot D.1 ja D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 20\,000\,000$
Releet ja apukontaktorit nimelliskuormituksella	Taulukot D.1 ja D.2	EN 50205 IEC 61810 IEC 60947	$B_{10D} = 400\,000$
Lähestymiskytkimet pienellä kuormituksella	Taulukot D.1 ja D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Lähestymiskytkimet nimelliskuormituksella	Taulukot D.1 ja D.2	IEC 60947 ISO 14119	$B_{10D} = 400\,000$
Kontaktorit pienellä kuormituksella	Taulukot D.1 ja D.2	IEC 60947	$B_{10D} = 20\,000\,000$
Kontaktorit nimelliskuormituksella	Taulukot D.1 ja D.2	IEC 60947	$B_{10D} = 1\,300\,000$ (ks. huomautus 1)
Asemantuntokytkin [a]	Taulukot D.1 ja D.2	IEC 60947 ISO 14119	$B_{10D} = 20\,000\,000$
Asemantuntokytkimet (erillisellä vaikutuselimellä, suojuksen lukinnalla) [a]	Taulukot D.1 ja D.2	IEC 60947 ISO 14119	$B_{10D} = 2\,000\,000$
Hätäpysäytyslaitteet [a]	Taulukot D.1 ja D.2	IEC 60947 ISO 13850	$B_{10D} = 100\,000$
Painikkeet (esim. sallintakytkimet) [a]	Taulukot D.1 ja D.2	IEC 60947	$B_{10D} = 100\,000$

Suureen B_{10D} määritelmä ja käyttö: ks. kohta C.4.

HUOM. 1 Suureen B_{10D} arvioidaan olevan kaksi kertaa B_{10} (50 % vaarallisia vikaantumisia), ellei muuta tietoa (esim. tuotestandardi) ole saatavilla.

HUOM. 2 "Nimelliskuormitus" tai "pieni kuormitus" olisi otettava huomioon standardissa ISO 13849-2 kuvattavien turvallisuusperiaatteiden noudattamisessa, kuten nimellisvirta-arvon ylimitoitus. "Pieni kuormitus" tarkoittaa esimerkiksi 20 % nimelliskuormituksesta.

HUOM. 3 Standardien IEC 60947–5–5 ja ISO 13850 mukaiset hätäpysäytyslaitteet ja standardin IEC 60947–5–8 mukaiset sallintakytkimet voidaan arvioida luokan 1 tai kategorian 3/4 alajärjestelmäksi riippuen sähköisten lähtökoskettimien lukumäärästä ja seuraavan turvallisuuteen liittyvän ohjausjärjestelmän osan vikojen paljastamiskyvystä. Kukin kosketinelementti (mukaan lukien mekaaninen toiminto) voidaan katsoa yhdeksi kanavaksi, jolla on vastaava B_{10D} -arvo. Standardin IEC 60947–5–8 mukaisissa sallintakytkimissä tämä tarkoittaa painamalla tai vapauttamalla toimivaa avautumistoimintoa. Joissakin tapauksissa on mahdollista, että koneen valmistaja voi soveltaa standardin ISO 13849-2, taulukon D.8 mukaista vikojen poissulkemista ottamalla huomioon kyseessä olevan sovelluskohteen ja laitteen ympäristöolosuhteet.

[a] Jos vian poissulkeminen pakkotoimiselle avautumiselle on mahdollista.

Liite 3. Esimerkkejä diagnostiikan kattavuudesta (SFS-EN ISO 13849-1:2015, 70-71.)

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...99 % riippuen sovelluksesta
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99 %
Vikojen paljastuminen prosessin kautta	0...99 % 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 %
Logiikka	
Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta)	90...99 % riippuen sovelluksesta
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 toteutetaan 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 prosessin kautta	0...99 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle PL_r e.
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 toimilaitteiden valvonnalla joko logiikan tai testauslaitteen avulla	99 %
Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta)	90...99 % riippuen sovelluksesta
Vikojen paljastuminen prosessin kautta	0...99 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle PL_r e.
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99 %

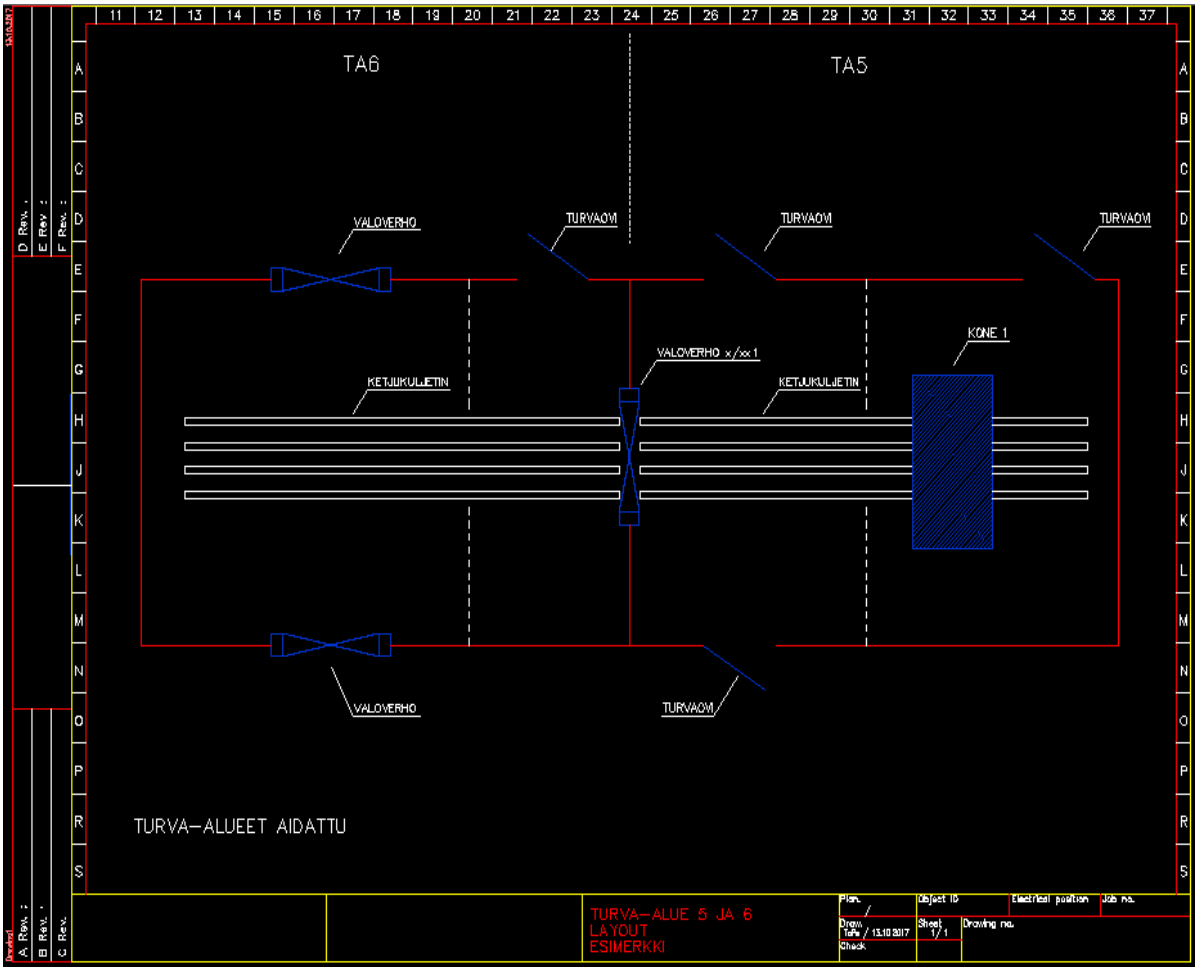
Liite 4. Yhteisvikaantumisen pisteyttäminen (SFS-EN ISO 13849-1:2015, 73-74.)

Nro.	Yhteisvikaantumista estävä toimenpide	Pisteet
1	**Erottelu/erottaminen**	
	Signaalireittien fyysinen erottaminen, esimerkiksi: — johdotuksen/putkituksen erilleen sijoittaminen — oikosulkujen ja avointen piirien paljastaminen dynaamisella testauksella — jokaisen kanavan signaalireittien erillinen suojaaminen — riittävät ilma- ja pintavälit painetuissa piirilevyissä.	**15**
2	**Erilaisuus (diversiteetti)**	
	Erilaisten teknologioiden, toteutustapojen tai fyysisten periaatteiden käyttö, esimerkiksi: — ensimmäinen kanava toteutetaan elektronisesti tai ohjelmoitavalla elektroniikalla ja toinen kanava sähkömekaanisesti kiinteästi langoitettuna — turvatoimintojen eri kanavien erilainen käynnistystapa (esim. asema, paine, lämpötila) ja/tai — muuttujien digitaalinen ja analoginen mittaaminen (esim. etäisyys, paine tai lämpötila) ja/tai eri valmistajien komponentit.	**20**
3	**Suunnittelu, soveltaminen ja kokemukset**	
3.1	Suojaustoimenpiteet ylijännitteelle, ylipaineelle, ylivirralle, liian korkealle lämpötilalle jne.	**15**
3.2	Käytetyt komponentit ovat hyvin koeteltuja	**5**
4	**Arviointi ja analyysit**	
	Turvallisuuteen liittyvien ohjausjärjestelmän osien jokaiselle osalle on tehty vika- ja vaikutusanalyysi ja sen tulokset on otettu huomioon suunnittelussa yhteisvikaantumisen estämiseksi.	**5**
5	**Pätevyys ja koulutus**	
	Suunnittelijat koulutetaan ymmärtämään yhteisvikaantumisten syyt ja seuraukset.	**5**
6	**Ympäristöolosuhteet**	
6.1	Likaantumisen ja sähkömagneettisten häiriöiden (EMC) estäminen sähköisissä/elektronisissa järjestelmissä yhteisvikaantumisten estämiseksi soveltuvien standardien mukaisesti (esim. IEC 61326–3–1). Pneumaattiset- ja hydrauliset järjestelmät: väliaineen suodatus, likaisen imuilman estäminen ja paineilman kuivatus, esim. komponentin valmistajan esittämien väliaineen puhtausvaatimusten mukaisesti. HUOM. Yhdistetyt sähköiset ja hydrauliset tai pneumaattiset järjestelmät: olisi otettava huomioon molemmat edellä mainittavat näkökohdat.	**25**
6.2	Muut vaikutukset Kaikkien asiaan liittyvien ympäristövaikutusten välttämiseksi on otettava huomioon sietokyky, esim. lämpötila, iskut, tärinä, kosteus (asiaankuuluvien standardien erittelyn mukaisesti).	**10**
	Yhteensä	**[mahdolliset maksimipisteet 100]**

Kokonaispisteet	Toimenpiteet yhteisvikaantumisen välttämiseksi [a]
65 tai enemmän	Täyttää vaatimukset
vähemmän kuin 65	Ei täytä vaatimuksia ⇒ valitaan lisätoimenpiteitä

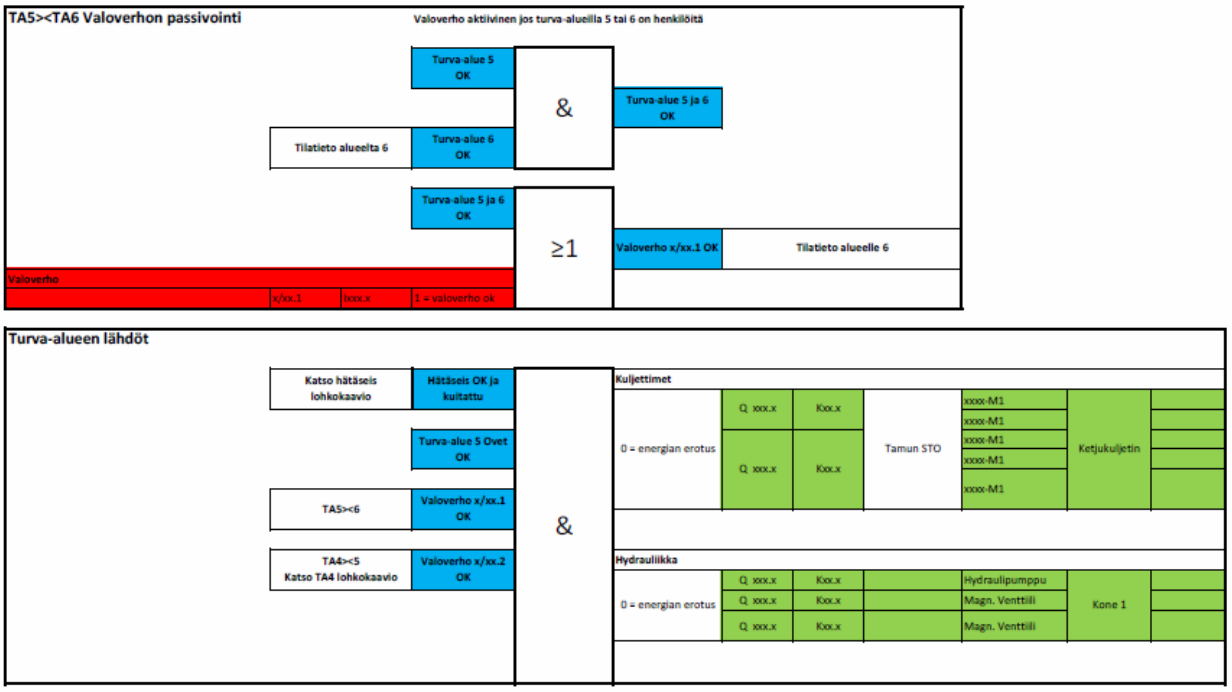
[a] Jos teknologiset toimenpiteet eivät ole asiaan kuuluvia, tähän sarakkeeseen liittyviä pisteitä voidaan tarkastella kokonaisvaltaisessa laskelmassa.

Liite 5. Turva-alue 5 ja 6 esimerkki layout



Liite 6. Uusi dokumentointimalli, turva-alue 5

Liite 7. Uusi dokumentointimalli, turva-alue 5



Liite 8. Uusi dokumentointimalli, turva-alue 6