Joona Saarinen

Ohjausjärjestelmien turvaratkaisut ja niiden vaatimusten täyttymisen osoittaminen

Sähkötekniikan koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

Ohjausjärjestelmien turvaratkaisut ja niiden vaatimusten täyttymisen osoittaminen

Saarinen, Joona
Satakunnan ammattikorkeakoulu
Sähkötekniikan koulutusohjelma
Tammikuu 2015
Ohjaaja: Suvela, Timo
Sivumäärä: 67
Liitteitä: 9

Asiasanat: suoritustaso, ohjausjärjestelmä, koneturvallisuus

Tämän opinnäytetyön tarkoitus oli standardin SFS-EN ISO 13849-1 mukaan selvittää, millaisilla komponenttivalinnoilla ja ratkaisuilla Raumaster Paper Oy:n toimituksessa olevien laitteiden sähköiset ohjausjärjestelmät saadaan vastaamaan niiltä vaadittua turvallisuustasoa eli suoritustasoa. Työn tulokset auttavat sähkösuunnittelijoita sekä turvallisuuden kannalta oikeiden ratkaisujen tekemisessä että niiden perustelussa.

Työn alussa tarkastellaan ohjausjärjestelmän suoritustason määräytymistä yleisellä tasolla.

Työn tulokseksi saatiin, miten turvatoimintoa toteuttamassa olevien laitteiden ohjausjärjestelmät saadaan vastaamaan niiltä vaadittua turvallisuustasoa. Työssä lähdettiin siitä, että laitteita on yleensä monta, joten ei ole järkevää varata jokaiselle omaa turvalähtöä. Työssä tarkastellaan tästä syystä turvalogiikan ja standardi I/O moduuleiden yhdistämistä. Oven turvallistaminen otettiin myös tarkemman tarkastelun kohteeksi. Ohjausjärjestelmien turvaratkaisut osoitetaan vaatimukset täyttäviksi Sistema-ohjelmaa käyttäen. Työ pääsi tavoitteeseensa ja tuloksien todettiin auttavan suunnittelutyötä tilaajayrityksessä.

Safety solutions for control systems and proving they meet the standards

Joona, Saarinen
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Electrical Engineering
January 2014
Supervisor: Suvela, Timo
Number of pages: 67
Appendices: 9

Keywords: performance level, control system, safety of machinery

---

Purpose of this Bachelor's thesis was to find out how to design control systems to meet required performance level according to the standard SFS-EN ISO 13849-1. The results enable electrical designers to find right solutions and justify them. The thesis was commissioned by Raumaster Paper Oy.

In the beginning it is examinated how performance levels are determined in general. The results show how safety related control systems must be designed so that they meet the requirements. There are usually many devices and it does not make sense to allocate safety output for every device. Based on that, possibilities to use a safety plc and standard I/O modules together are studied. Safety doors were also examinated. The solutions were proved to meet the requirements by Sistema. In conclusion, all the solutions met the requirements successfully and they will be brought into use by the company.

SISÄLLYS

SYMBOLIT JA LYHENTEET

B_{10d}	Toimintajaksojen lukumäärä siihen asti kunnes 10 % komponenteista on vikaantunut vaarallisesti
Cat.	Luokka
CCF	Yhteisvikaantuminen
DC	Diagnostiikan kattavuus
DC_{avg}	Keskimääräinen diagnostiikan kattavuus
MTTF	Keskimääräinen vikaantumisaika
$MTTF_d$	Vaarallinen keskimääräinen vikaantumisaika
Nop	Keskimääräinen vuosittaisten toimintajaksojen lukumäärä
PFH_d	Vaarallinen keskimääräinen vikaantumisaika tuntia kohti
PL	Turvallisuuden suoritustaso
PL_{low}	Turvallisuuteen liittyvien ohjausjärjestelmän osien yhdistelmässä osa, jolla on matalin suoritustaso
PL_r	Vaadittava turvallisuustaso eli suoritustaso

1 JOHDANTO

Koneasetus velvoittaa, että ohjausjärjestelmät rakennetaan sellaisiksi, että ne estävät vaaratilanteiden syntymisen.

Nykyään koneissa käytetään paljon sähköisiä ohjausjärjestelmiä ja niiden osuus riskien pienentämisessä on monissakin sovelluksissa suuri. Siksi on tärkeää, että turvallisuuteen liittyvä ohjausjärjestelmä suunnitellaan ja rakennetaan voimassaolevia ohjausjärjestelmästandardeja noudattaen. Näin ohjausjärjestelmästä tulee varmasti määräävän konedirektiivin eli koneasetuksen mukainen. Ohjausjärjestelmän vaatimustenmukaisuuden osoittaminenkin helpottuu huomattavasti, kun se tehdään standardeja noudattaen.

Turvallisuuteen liittyviä ohjausjärjestelmiä on aikaisemmin suunniteltu konedirektiivin vaatimuksia vastaaviksi standardin SFS-EN 954-1 mukaan. Se on kuitenkin kumottu 30.11.2009, ja sen voimassaolo on päättynyt 31.12.2011. Tilalle on tullut standardi SFS-EN ISO 13849-1, jonka soveltamista käydään esimerkkien avulla tässä työssä läpi ja katsotaan, miten ohjausjärjestelmän vaatimustenmukaisuuden täyttyminen saadaan osoitettua siihen tarkoitettua ohjelmaa käyttäen.

Työn kappaleessa kolme käydään läpi turvallisuuteen liittyvät käsitteet ja turvallisuustason määräytyminen yleisellä tasolla. Luvusta neljä alkaen tarkastellaan varsinaista toimeksiantoa.

2 TILAAJAYRITYS

Raumaster Paper Oy, jolle opinnäytetyö tehtiin, on Raumaster Oy:n tytäryhtiö. Koko Raumaster konsernissa työntekijöitä on noin 300 ja vuonna 2013 liikevaihto oli 100 MEUR. Raumaster Paper irtautui tytäryhtiöksi Raumasterista vuonna 2003, ja henkilöstömäärä Raumaster Paperilla on noin 50. Raumaster Paperin osaamisalue on koko paperinkäsittelytekniikka ja logistiikka paperitehtaissa, konvertterilaitoksissa ja painotaloissa. (Raumaster Oy:n www-sivut 2014.)

3 TURVALLISUUTEEN LIITTYVÄ OHJAUSJÄRJESTELMÄ

Tässä luvussa käsitellään, mitkä tekijät vaikuttavat sähköisellä ohjausjärjestelmällä aikaan saatavaan riskien pienentämiseen. Kun ohjausjärjestelmälle vaaditaan tiettyä suoritustasoa tai turvallisuuden eheyden tasoa, niin se tarkoittaa sitä riskin pienentämisen määrää, joka ohjausjärjestelmältä vaaditaan.

Vaara-aluetta turvallistetaan standardin 12100 mukaan kolmessa vaiheessa:

Ensimmäisessä vaiheessa käytetään luontaisesti turvallisia suunnittelutoimenpiteitä eli koneen rakenneominaisuuksien sopivalla valinnalla poistetaan vaaroja tai pienennetään riskejä. Jos koneen riskitaso ei jää tässä vaiheessa siedettävälle tasolle, niin tarvitsee ryhtyä muihin suojausteknisiin toimenpiteisiin eli siirtyä toiseen vaiheeseen. (SFS-EN ISO 12100, 51.)

Toisessa vaiheessa käytetään sopivasti valittuja suojausteknisiä toimenpiteitä eli esimerkiksi suojuksia ja turvalaitteita ottaen huomioon tarkoitettu käyttö ja kohtuudella ennakoitavissa oleva väärinkäyttö. Riskit pitää saada siedettävälle tasolle. (SFS-EN ISO 12100, 51.)

Kolmannessa vaiheessa, jos toisesta vaiheesta jää jäännösriskejä, niin niistä ilmoitetaan käyttöohjeilla, merkinantolaitteilla, varoitusteksteillä yms. (SFS-EN ISO 12100, 32, 52).

3.1 Suoritustasot ja turvallisuuden eheyden tasot

Koneiden ohjausjärjestelmien avulla aikaan saatava riskien vähennys, voidaan kuvata ohjausjärjestelmästandardin SFS-EN ISO 13849-1 taulukon 1 suoritustasoilla (PL) ja kohdan 3.2.2 luokilla sekä standardin SFS-EN 62061 turvallisuuden eheyden tasoilla (SIL). Standardi SFS-EN ISO 13849-1 on perusstandardi koneiden ohjausjärjestelmien suunnitteluun ja arvioimiseen. Se kattaa muutkin kuin sähköiset osat, esim. hydrauliset. SFS-EN 62061 on taas lähinnä komponenttien valmistajien ja komponenteille ja järjestelmille tyyppitarkastuksia tekevien laitosten käyttämä standardi. Se kattaa vain sähköiset osat. Jos arvioitavassa järjestelmässä on esim. hydrauliikkaa ja ohjauselektroniikkaa niin kyseinen järjestelmä voidaan käsitellä näitä molempia standardeja käyttäen. (Siirilä 2008, 115; Siirilä 2009, 103.)

Taulukko 1. Suoritustasot (SFS-EN ISO 13849-1, 35)

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

Suoritustasot ja turvallisuuden eheyden tasot perustuvat kumpikin vaarallisen vikaantumisen todennäköisyyteen tuntia kohti. Taulukko 2 antaa niiden vastaavuuden keskenään. (Siirilä 2008, 129- 130; SFS-EN ISO 13849-1, 44.)

Taulukko 2. Suoritustasojen ja turvallisuuden eheyden tasojen vastaavuus (SFS-EN ISO 13849-1, 44)

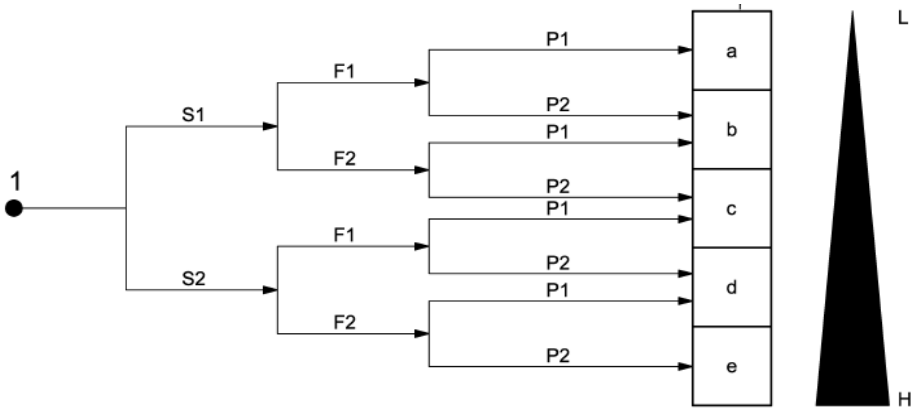
PL	**SIL** (IEC 61508-1, tiedoksi) tiheiden vaateiden tai jatkuvan toiminnan tapa
a	Ei vastaavuutta
b	1
c	1
d	2
e	3

3.2 Ohjausjärjestelmän suoritustaso

Kumotussa standardissa SFS-EN 954-1 turvapiirin rakenne on ollut ainoa turvaluokkaan vaikuttava tekijä. Tilalle tulleessa SFS-EN ISO 13849-1 standardissa pitää huomioida rakenteen lisäksi myös komponenttien vikaantumistodennäköisyys, diagnostiikan kattavuus ja yhteisvikaantumisen mahdollisuus. (Rantanen 2012, 30.)

3.2.1 Vaadittavan suoritustason (PL_r) määritys

Koneiden riskitason arvioimiseen on olemassa useita eri työkaluja. Vaadittavan suoritustason määrittämiseen turvatoiminnolle käytetään riskigraafia (kuva 1). Riskigraafia luetaan siten, että vasemmalla oleva piste 1 on lähtökohta, josta lähdetään arvioimaan turvatoiminnon osuutta riskin pienentämisessä. Riskigraafin oikealla puolella oleva kolmion kärki eli kirjain L kuvaa pientä riskiä ja kolmion kanta eli kirjain H kuvaa suurta riskiä. Ennen kuin päädytään pisteestä 1 kolmion tiettyyn kohtaan niin pitää arvioida, mitkä niiden välissä olevista muuttujista valitaan. Alla on ohjeita muuttujien S, F ja P valintaan. (SFS-EN ISO 13849-1, 98-100.)



Kuva 1. Riskigraafi vaadittavan suoritustason määrittämiseksi turvatoiminnolle (SFS-EN ISO 13849-1, 100)

Ohjeet kuvan 1 muuttujien S, F ja P valinnalle riskin suuruuden arvioinnissa:

Vahingon vakavuus, S1 tai S2

Turvatoiminnon vikaantumisen johdosta syntyvien vammojen vakavuuksista tarkastellaan vain lieviä eli tavallisesti palautuvia vammoja ja vakavia vammoja eli raajojen irtirepeytymisiä ja kuolemantapauksia. Muuttujien S1 ja S2 valinnassa olisi otettava huomioon tapaturmien tavanomaiset seuraukset ja paranemisprosessit. Esimerkiksi ruhjeet ja haavaumat ilman jälkitauteja voidaan määritellä S1:ksi ja irtileikkautumiset ja kuolemantapaukset S2:ksi. (SFS-EN ISO 13849-1, 98.)

Vaaralle altistumisen taajuus ja/tai kesto, F1 tai F2

Mitään yleispätevää aikaväliä muuttujien F1 ja F2 valinnalle ei voida määrittää. Seuraavilla asioilla voidaan kuitenkin helpottaa oikean valinnan tekemistä: F2 olisi valittava jos henkilö on toistuvasti tai jatkuvasti tarkasteltavalle vaara-alueelle altistuneena. Jos koneen käyttötavan vuoksi on siis toistuvasti ulotuttava työkappaleita siirrettäessä tai syötettäessä koneen vaarallisten liikkeiden vaikutusalueelle, olisi valittava F2,

muutoin valitaan F1. Jos ei mitään muita perusteluja ole ja taajuus on suurempi kuin kerran tunnissa, olisi valittava F2 (SFS-EN ISO 13849-1, 98).

Mahdollisuus välttää vaaraa, P1 tai P2

Muuttuja P1 voidaan valita, jos vaara on todellakin mahdollista välttää ennen sen johtamista tapaturmaan. Muuttaja P2 olisi valittava, jos vaaran välttäminen tuskin on mahdollista. (SFS-EN ISO 13849-1, 100.)

Standardin SFS-EN ISO 13849-1 kohdan A.2.3 mukaan ”Muita tärkeitä näkökohtia, jotka vaikuttavat muuttujan P valintaan, ovat esimerkiksi

- valvottu tai ilman valvontaa oleva käyttötoiminta
- ammattilaisten tai ammattitaidottomien käyttötoiminta
- mahdollisuudet välttää vaaraa (esim. pakenemalla)
- prosessiin liittyvät käytännön turvallisuuskokemukset.”

Muuttuja P2 tulisi valita, jos vaaran välttäminen on tuskin tai ei ole lainkaan mahdollista (SFS-EN ISO 13849-1, 100).

3.2.2 Ohjausjärjestelmän osien luokat

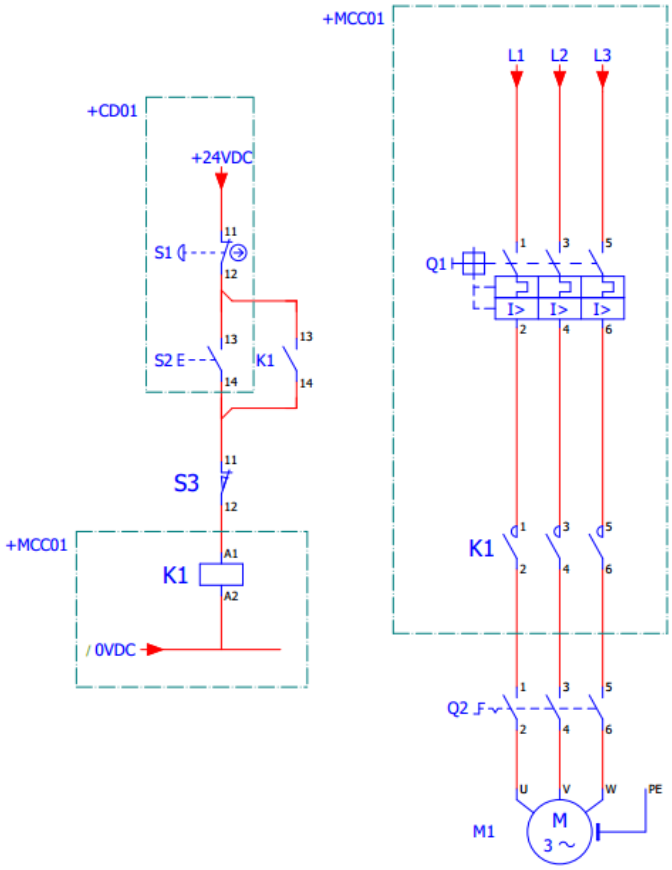
Luokkia on yhteensä viisi: B, 1, 2, 3, ja 4. Luokka B on perusluokka, jossa yksitäisen vian esiintyminen voi johtaa turvatoiminnon menettämiseen. Luokassa 1 vikakestoisuus on parempi eli käytetään luotettavampia komponentteja kuin luokassa B. Luokassa 1 lähdetään siitä, että vikoja ei esiinny, tai ne esiintyvät ainakin turvalliseen suuntaan. Luokissa 2, 3 ja 4 lähdetään taas siitä, että vikoja on, mutta ne tulevat havaituiksi kahdennuksien ja valvonnan avulla niin, että turvallisuus toteutuu, vaikka vika esiintyisi. (SFS-EN ISO 13849-1, 74; Siirilä 2009, 143.)

Joillekin vaara-alueille vaaditaan vaadittavan suoritustason lisäksi tietty luokka ohjausjärjestelmän osilta. Esimerkiksi jos vaara-alueella on robotti, niin sen lisäksi että ohjausjärjestelmän osien yhdistelmän on riitettävä suoritustasoon PL d, niiden on oltava myös Standardin SFS-EN ISO 13849-1 luokan 3 mukaisia. (SFS-EN ISO 10218-1, 24.)

Luokka B

Komponenttien valinnassa on huomioitava odotettavissa olevat käyttö- ja ympäristöolosuhteet. Luokan B rakenne (Kuva 2) on yksikanavainen ja komponenttien valinnassa on noudatettava turvallisuuden perusperiaatteita (Liite 1). Diagnostiikan kattavuus (DC_{avg}) on nolla, ja kanavan vaarallinen keskimääräinen vikaantumisaika on välillä 3-29 vuotta. Suurin saavutettavissa oleva suoritustaso on PL b. Vian esiintyminen saattaa johtaa turvatoiminnon menetykseen, sillä komponentteja ei valvota. (SFS-EN ISO 13849-1, 76; Suvela 2010, 17.)

Kuvan 2 luokan B ohjausjärjestelmässä vaarallinen vika syntyy, jos kontaktori K1 jää vetäneeseen tilaan esimerkiksi koskettimien kiinnihitsaantumisen seurauksena tai ohjauspiirissä ei saada pysäytykseen vaikuttavilla laitteilla katkosta aikaiseksi (Suvela 2010, 17).



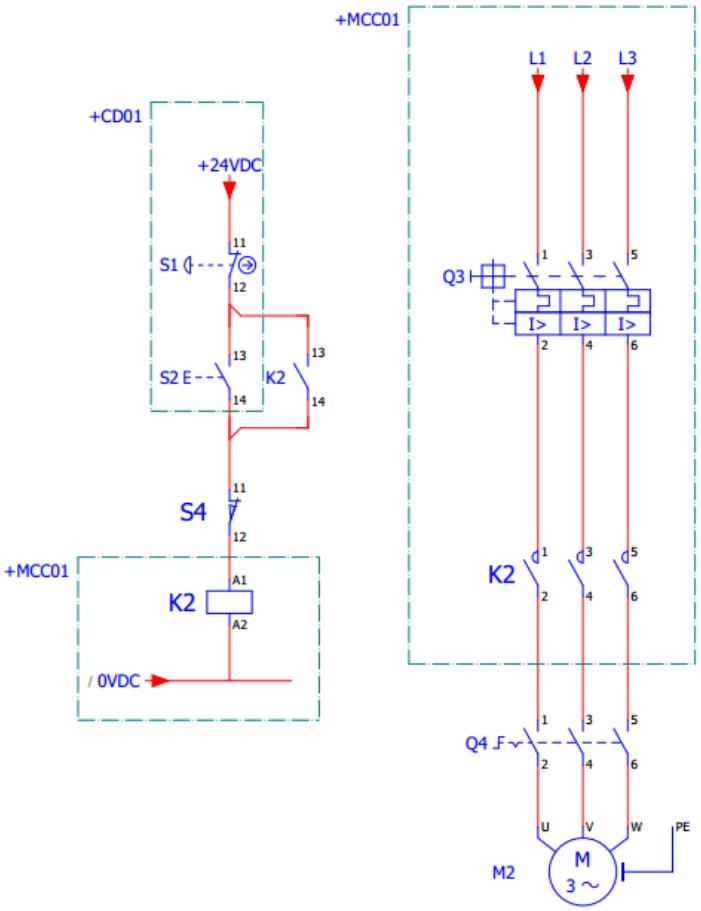
Kuva 2. Luokan B mukainen ohjausjärjestelmän rakenne

Luokka 1

Luokan 1 on täytettävä luokan B vaatimukset. Lisäksi ohjausjärjestelmän rakenne suunnitellaan ja rakennetaan käyttäen hyvin koeteltuja komponentteja (liite 2) ja noudatetaan hyvin koeteltuja turvallisuusperiaatteita (liite 3). Turvallisuussovelluksiin valmistettuja komponentteja ja komponentteja, joita on paljon käytetty ja joista on hyviä kokemuksia vastaavista sovelluksista, voidaan pitää hyvin koeteltuina. Diagnostiikan kattavuus (DC_{avg}) on nolla ja kanavan keskimääräinen vikaantumisaika on oltava korkea eli vähintään 30 vuotta. Vian esiintyminen voi kuitenkin johtaa turvatoiminnon menettämiseen, sillä komponentteja ei valvota. Vian esiintymisen todennäköisyys on pienempi kuin luokassa B. Suurin saavutettavissa oleva suoritustaso on PL c. (SFS-EN ISO 13849-1, 78; Suvela 2010, 18.)

Hyviksi koettuja turvallisuusperiaatteita ovat muun muassa vikaantumisen tapahtuminen aina samalla tavalla. Esimerkkinä on avautuvien koskettimien käyttö, eli tällöin leikkaavan liikkeen seurauksena tapahtuva signaalijohtimen katkeaminen saa aikaan koneen pysähtymiskäskyn. Lisäksi komponenttien ylimitoittaminen ja vioista aiheutuvien seurausten välttäminen tai niiden vähentäminen esim. maadoittamalla kuuluvat hyvin koeteltuihin turvallisuusperiaatteisiin (Liite 3). (SFS-EN ISO 13849- 2, 90; Suvela 2010, 18.)

Kuvassa 3 yksi vika voi aiheuttaa turvatoiminnon menetyksen. Esimerkiksi vika ohjauspiirissä olevissa pysäytyksen hoitavissa laitteissa tai kontaktorin K2 kiinnihitsaantuminen. Kontaktorin kiinnihitsaantuminen on kuitenkin luokassa 1 epätodennäköisempää kuin luokassa B, sillä se on ylimitoitettu luokassa 1 siten, että koskettimien läpi kulkeva virta on alle puolet niiden nimellisvirrasta. Lisäksi komponentin kytkentätaajuuden tulee olla alle puolet mitoitusarvosta ja odotettavissa olevien kytkentätoimintojen tulisi olla enintään 10 % laitteen sähköisestä kestävyydestä eli B_{10}-arvosta. (Suvela 2010, 18; SFS-EN ISO 13849-2, 90.)

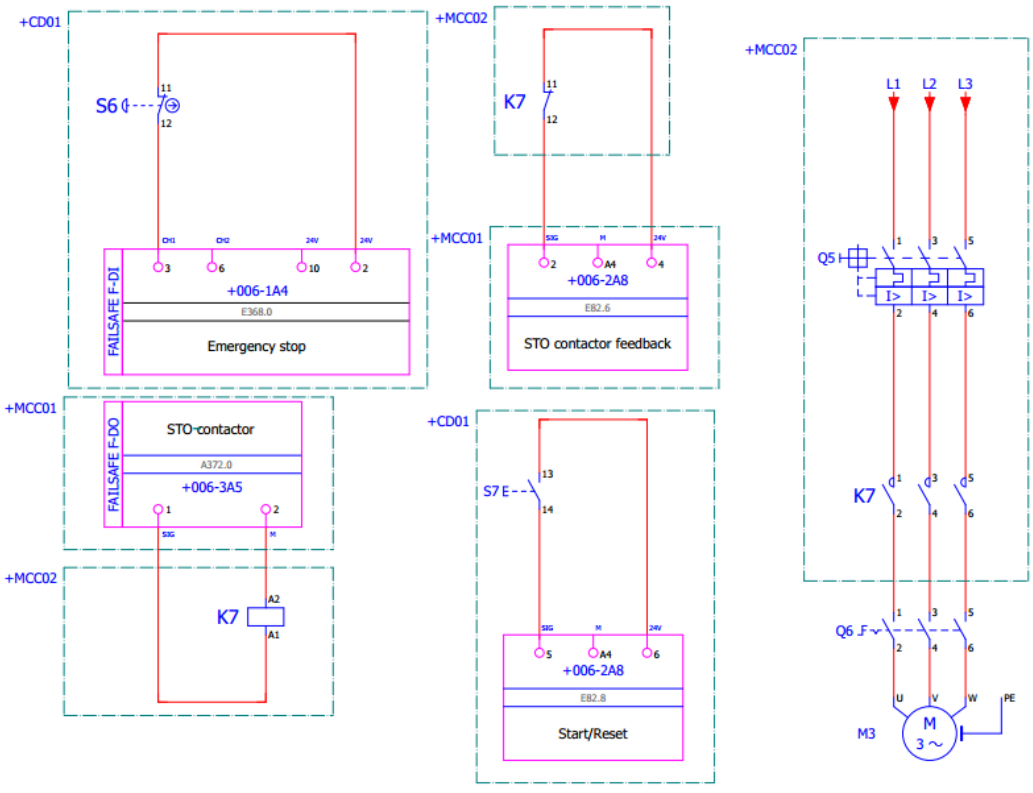


Kuva 3. Luokan 1 mukainen ohjausjärjestelmän rakenne

Luokka 2

Luokassa 2 on noudatettava luokan B periaatteita ja sen lisäksi hyvin koeteltuja turvallisuusperiaatteita (Liite 3). Ohjausjärjestelmän on tarkastettava turvatoiminnon kunto koneen käynnistyksen yhteydessä ja ennen minkään vaaratilanteen alkamista sekä tarpeen mukaan koneen toiminnan aikana. Testaustaajuuden on oltava 100 kertaa suurempi kuin turvatoiminnon tarvitsemisen taajuus. Kun vika havaitaan, on ohjausjärjestelmän estettävä koneen käynnistyminen tai pysäytettävä jo käynnissä oleva kone. Vaarallisen keskimääräisen vikaantumisajan on oltava vähintään 3 vuotta ja keskimääräisen diagnostiikan kattavuuden vähintään 60 % (Liitteessä 4 on esimerkkejä diagnostiikan kattavuuksista). (SFS-EN ISO 13849-1, 80; Siirilä 2009, 144.)

Turvalogiikka testaa kontaktorin K7 kunnon sekä käynnistysten yhteydessä että ajoittain koneen käytön aikana. Lisäksi Hätäseispainikkeen (S6) oikosulkua valvotaan turvalogiikan testipulsseilla (kuva 4). (Suvela 2010, 21.)



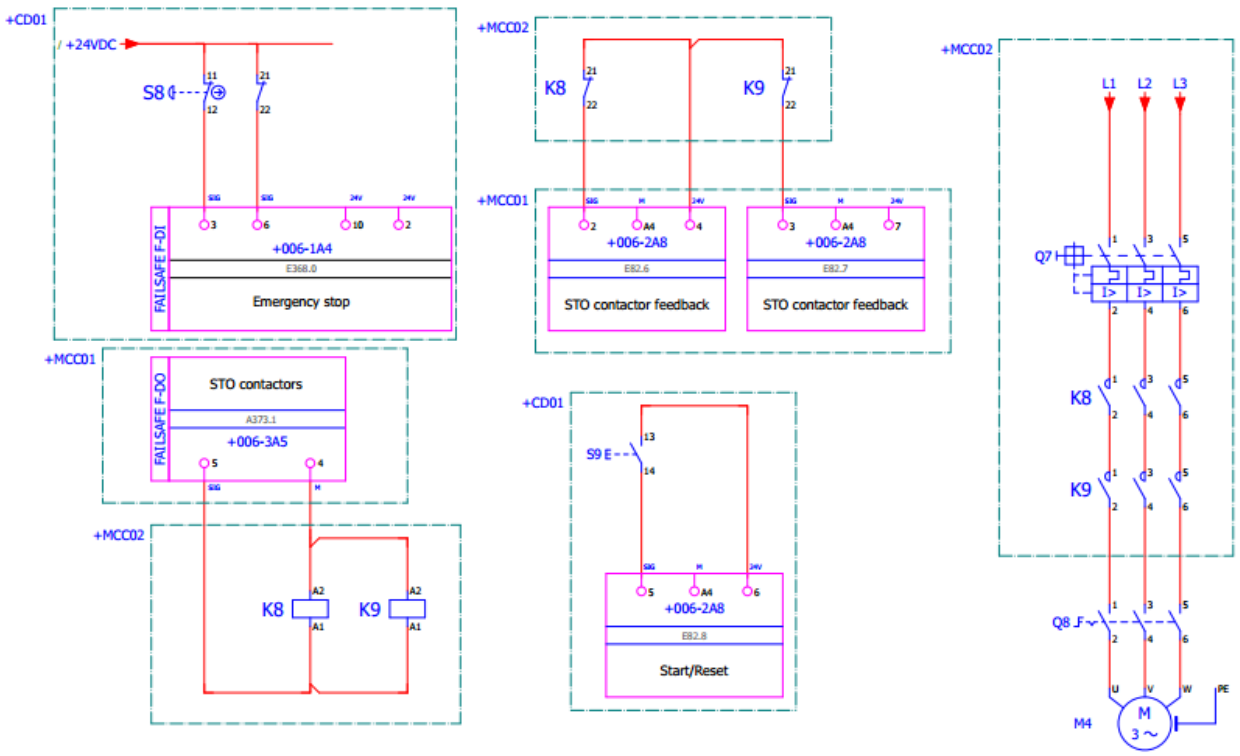
Kuva 4. Luokan 2 mukainen ohjausjärjestelmä

Luokka 3

Luokassa 3 on sovellettava myös luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita. Yksittäinen vika ei saa johtaa turvatoiminnon menettämiseen. Vikoja ei välttämättä havaita, joten vikojen kerääntyminen saattaa johtaa turvatoiminnon menettämiseen. (SFS-EN ISO 13849-1, 82.)

Luokan 3 rakenne hoidetaan komponenttien kahdennuksella. Jokaisen kanavan vaarallisten vikaantumisten välisen keskimääräisen ajan on oltava vähintään 3 vuotta. Diagnostiikan keskimääräisen kattavuuden on oltava vähintään 60 %. Lisäksi yhteisvikojen todennäköisyyden on oltava pieni. Liitteessä 3 on lueteltu toimenpiteitä yhteisvikaantumisen välttämiseksi. (Siirilä 2009, 144.)

Kontaktoreja K8 ja K9 valvotaan käynnistyksen yhteydessä. Hätäpysäytyksen tulopiirejä ei valvota, joten oikosulku hätäseispainikkeen (S8) jännitteen ja tulojen välillä aiheuttaa turvatoiminnon menetyksen (kuva 5). (Suvela 2010, 25.)

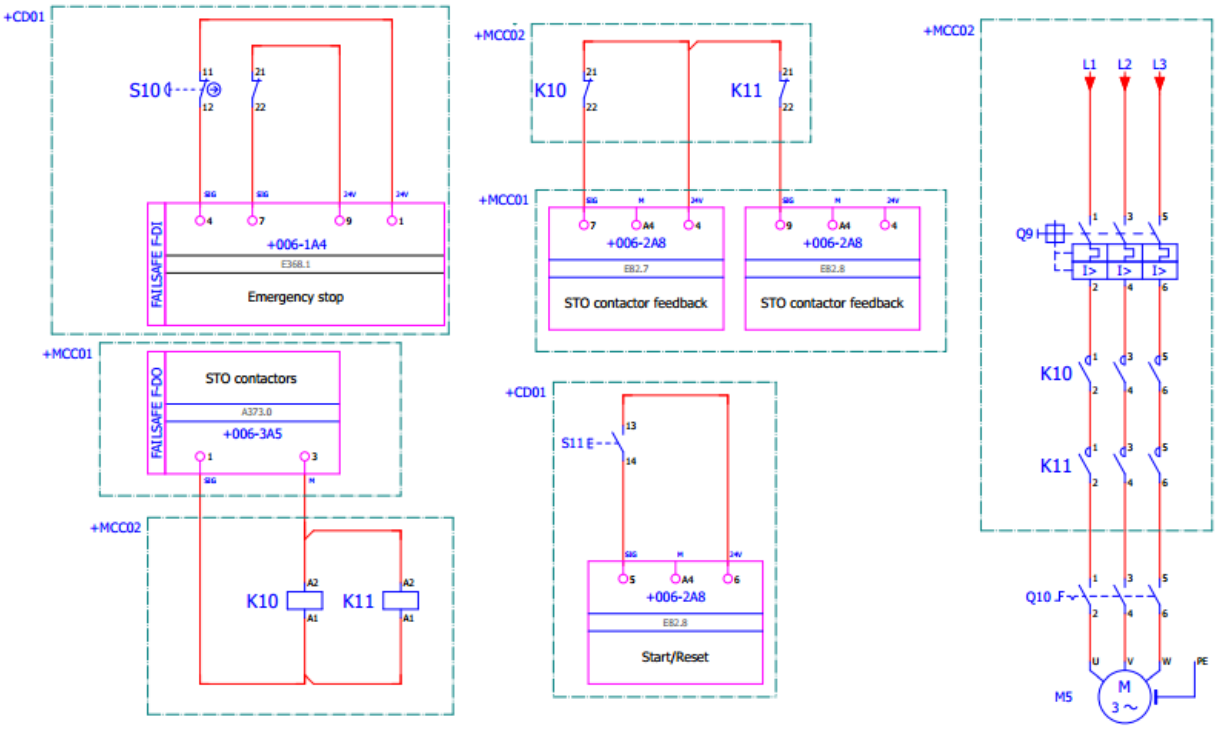


Kuva 5. Luokan 3 mukainen ohjausjärjestelmä

Luokka 4

Luokassa 4 on sovellettava luokan B vaatimuksia sekä käytettävä hyvin koeteltuja turvallisuusperiaatteita (Liite 3). Luokan 4 erona luokkaan 3 on, että yksittäinen vika missään turvallisuuteen liittyvässä osassa ei johda turvatoiminnon menettämiseen. Tämä tarkoittaa sitä, että kaikkien vikojen on paljastuttava. Vaaditaan siis, että jokaisen kanavan vaarallisen keskimääräisen vikaantumisen välisen ajan on oltava 30 vuotta eli korkea ja keskimääräisen diagnostiikan kattavuuden on oltava 99 % eli korkea. (SFS-EN ISO 13849-1, 84; Siirilä 2009, 144.)

Kontaktoreja K10 ja K11 valvotaan käynnistyksen yhteydessä takaisinkytkennällä logiikkaan. Hätäpysäytyspainikkeen avautuvat koskettimet kytketään molemmat omiin turvalogiikan tuloihin. Turvalogiikan testipulsseilla valvotaan tulopiirien oikosulkua (kuva 6). (Suvela 2010, 28.)



Kuva 6. Luokan 4 mukainen ohjausjärjestelmä

3.2.3 Keskimääräinen vaarallinen vikaantumisaika $MTTF_d$

MTTFd-arvo on yksi standardin SFS-EN ISO 13849-1 tärkeistä tekijöistä. Se kertoo vaarallisen keskimääräisen vikaantumisajan järjestelmän eri komponenteissa. Jos vaarallisten vikojen osuutta ei tarkasti tiedetä, niin yleisesti arvioidaan, että puolet vioista ovat vaarallisia. Kanavan keskimääräinen vikaantumisaika määritellään käyttäen kolmea eri tasoa: taso 1 on 3-10 vuotta (matala), taso 2 on 10-30 vuotta (keskimääräinen), taso 3 on 30-100 vuotta (korkea). (Hietikko, Malm ja Alanen 2009, 21.)

Kun vaarallista vikaantumisaikaa määritellään, niin ensisijaisesti käytetään valmistajan antamia komponenttitietoja. Ne ovat muita vaihtoehtoja tarkemmat, sillä ne koskevat valmistajan itsensä valmistamia ja mahdollisesti testaamia komponentteja (Sundquist 2010, 11). Valmistaja ilmoittaa yleensä komponentin B_{10d}-arvon, jonka avulla voidaan laskea $MTTF_d$-arvo.

Jos ei valmistajalla ole antaa komponenttitietoja, on hyvä tietää, että standardin SFS-EN ISO 13849-1 liitteessä C on karkeita likiarvoja $MTTF_d$-arvoista, mutta niitä tulee välttää käyttämästä ilman tarkempaa arviointia komponentin ominaisuuksista ja soveltuvuudesta tarkasteltavaan turvatoimintoon. (Sundquist 2010, 11.)

Jos ei mitään tietoa ole saatavilla komponentin vikaantumisajasta, niin voidaan valita komponentin $MTTF_d$-arvoksi 10 vuotta vain yksinkertaisissa järjestelmissä, joissa turvatoiminnoille ei ole asetettu korkeita suoritustasovaatimuksia. (Sundquist 2010, 11.)

Komponentin $MTTF_d$ -arvon laskeminen B_{10d} -arvon avulla

”Komponentin valmistajan olisi määritettävä keskimääräinen toimintajaksojen lukumäärä, johon mennessä 10 % komponenteista vikaantuu vaarallisesti (B_{10d})” (SFS-EN ISO 13849-1, 110).

$MTTF_d$-arvo voidaan laskea yhtälöllä 1 muuttujien B_{10d} ja n_{op} avulla seuraavasti:

$$\mathrm{MTTF_d} = \frac{\mathrm{B_{10d}}}{0{,}1 \times \mathrm{n_{op}}} \quad (1)$$

jossa

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 s/h}{t_{jakso}} \quad (2)$$

jossa

”n_{op} =toimintajaksojen määrä vuodessa
h_{op} = keskimääräinen toiminta-aika, tuntia päivässä
d_{op} = keskimääräinen toiminta-aika, päivää vuodessa
t_{jakso} = komponentin kahden peräkkäisen toimintajakson alkamisajankohdan välinen keskimääräinen aikaväli, sekuntia/toimintajakso” (SFS-EN ISO 13849-1, 110.)

Kanavaan sarjaan kytketyt komponentit:

Yleinen yhtälö (3) kanavan keskimääräisen vikaantumisajan laskemiseen, kun siinä on useampi sarjaankytketty komponentti, on seuraavanlainen:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \quad (3)$$

jossa

$MTTF_d$ on koko kanavan vaarallisen vikaantumisen keskimääräinen arvo
$MTTF_{di}$ on kunkin kanavan arvo, jotka ovat toteuttamassa turvatoimintoa (SFS-EN ISO 13849-1, 120.)

Redundanttiset eli rinnakkaiset kanavat:

Jos kahdella rinnakkaisella kanavalla on eri $MTTF_d$-arvo, niin kanavista olisi valittava joko alhaisemman vikaantumisajan omaava kanava tai tehtävä kanaville symmetrisointi yhtälön 4 avulla. Tämän jälkeen molemmilla kanavilla on sama $MTTF_d$-arvo. (SFS-EN ISO 13849-1, 76.)

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTD_{dC2}}}\right] \quad (4)$$

jossa

$MTTF_{dC1}$ ja $MTTF_{dC2}$ ovat kahden erilaisen kanavan vaarallisen vikaantumisen keskimääräiset ajat (SFS-EN ISO13849-1, 122).

3.2.4 Diagnostiikan kattavuus DC

Jotta vaatimus turvallisuudesta vioista huolimatta olisi mahdollista toteuttaa, ohjausjärjestelmän on pystyttävä havaitsemaan järjestelmän eri komponenteissa olevat viat. Vian tultua havaituksi järjestelmän on toteutettava vian varalle suunniteltu toiminto, yleensä pysäytettävä kone. (Siirilä 2009, 159.)

Liitteessä 4 on esimerkkejä diagnostiikan kattavuuden arvioimiseksi (SFS-EN ISO 13849-1, 124-126).

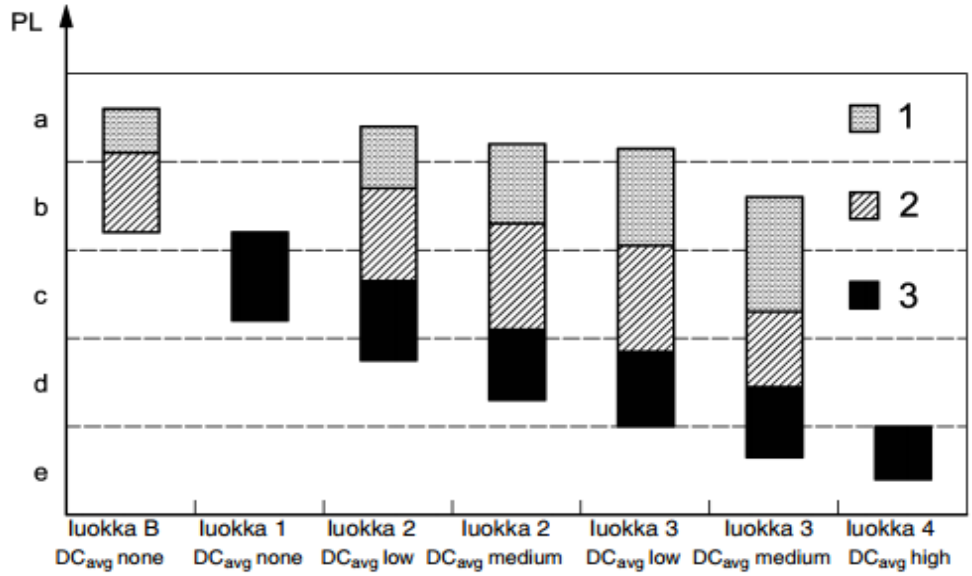
3.2.5 Yhteisvikaantuminen CCF

Yhteisvikaantumisella tarkoitetaan vikaantumista, joka vaikuttaa yhden alkusyyn seurauksena yhtä aikaa useampaan kuin yhteen komponenttiin tai osakokonaisuuteen. Turvallisuusjärjestelmän on luokassa 2-4 selviydyttävä näistäkin tilanteista, kun samasta syystä aiheutuu useita vikoja eli järjestelmän kahdennetuissa rakenteissa sattuu molemmissa osarakenteissa vika samaan aikaan. Liitteessä 5 on lueteltu yhteisvikaantumisen estämiseksi tehtäviä toimenpiteitä. (Siirilä 2009, 155; SFS-EN ISO 13849-1, 130.)

Kun liitteen 5 taulukosta saatava yhteispistemäärä turvajärjestelmälle on vähintään 65, järjestelmän katsotaan täyttävän riittävän hyvin yhteisvikaantumisen välttämiseksi tehdyt toimenpiteet.

3.2.6 Turvatoiminnolla saavutettu suoritustaso

Kun turvallisuuteen vaikuttavan alajärjestelmän luokka, $MTTF_{d,}$ ja DC_{avg} (pl. luokat B ja 1) ovat tiedossa sekä yhteisvikaantumisen eli CCF:n välttämisen arvioinnissa saatu vähintään 65 pistettä (pl. luokat B ja 1), niin kuviosta 1 voidaan katsoa turvallisuuteen vaikuttavan alajärjestelmän suoritustaso.



Kuvio 1. Suoritustason määräytyminen (SFS-EN ISO 13849-1, 52)

Esimerkki kuvion 1 käytöstä: jos alajärjestelmä kuuluu luokkaan kolme, keskimääräinen diagnostiikan kattavuus kanavien komponenteille on keskimääräinen ja vaarallinen vikaantumisaika on korkea (30-100 vuotta) eli numero kolme kuvion oikeassa reunassa, niin päästään suoritustasoon PL d ja joissakin erikoistapauksissa voidaan päästä suoritustasoon PL e.

Turvallisuuteen liittyvän ohjausjärjestelmän osien eli alajärjestelmien yhdistelmälle voidaan arvioida suoritustaso taulukon 3 avulla (SFS-EN ISO 13849-1, 90).

Taulukkoa 3 luetaan siten, että katsotaan, mikä on turvajärjestelmän alajärjestelmä, jolla on matalin suoritustaso eli PL_{low}. Tämän jälkeen katsotaan em. alajärjestelmien lukumäärä, minkä jälkeen luetaan kyseisen vaakarivin perästä suoritustaso PL tarkasteltavalle turvajärjestelmälle. (SFS-EN ISO 13849-1, 92.)

Taulukkoon 3 liittyy yksi huomio: ”Taulukkoon lasketut arvot perustuvat luotettavuusarvioihin kunkin suoritustason keskipisteessä” (SFS-EN ISO 13849-1, 92). Taulukko 3 ei siis pidä paikkaansa esim. Sistema-laskelmassa, jossa on esimerkiksi paljon PL d-

suoritustason alajärjestelmiä, mutta kaikilla pieni PFH_d- arvo eli keskimääräisen vaarallisen vikaantumisen todennäköisyys tuntia kohden. Tällöin ollaan suoritustason yläarajalla eikä muutama saman tasoinen sarjaan kytketty PL d -suoritustason omaava alajärjestelmä laske kokonaissuoritustasoa PL c:hen. (Rantanen, henkilökohtainen tiedonanto 25.8.2014; SFS-EN ISO 13849-1, 92.)

Taulukko 3. Sarjaankytkettyjen ohjausjärjestelmän osien suoritustaso (SFS-EN ISO 13849-1, 92)

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

4 TYÖN TOTEUTUS

Työ aloitettiin tutustumalla Tapio Siirilän koneturvallisuuskirjoihin sekä voimassa oleviin koneturvallisuuden standardeihin. Työn alkuvaiheessa tutustuttiin erityisesti Tapio Siirilän koneturvallisuuskirjaan Ohjausjärjestelmät ja turvalaitteet, joka perustuu Konedirektiivin 2006/42/EY eli niin kutsutun koneasetuksen liitteen 1 vaatimuksiin. Nimenomaan tuossa liitteessä 1 annetaan vaatimuksia koneiden ohjausjärjestelmille ja turvalaitteille. Työssä sovellettiin koneturvallisuusmateriaaleissa esitettyjä turvallisuuden ohjausjärjestelmiä ja tukea tähän saatiin SICKin ja Siemensin turvakonsulteilta. Lisäksi työssä käytetyn Sistema-ohjelman käyttöön saatiin apua SICKiltä. Eplan-ohjelmalla kuvien luomisessa hyödynnettiin Raumaster Paper Oy:n olemassa olevia sähkökuvia ja automaatiopäällikön Eplan-osaamista.

4.1 Työssä tarkasteltavat turvatoiminnot ja -laitteet

Työssä tarkemman tarkastelun kohteeksi otettiin vaara-alueelle johtavan oven turvallistamisratkaisut. Lisäksi työssä käsiteltäviä ohjausjärjestelmiin liittyviä turvalaitteita ja turvallistettavia laitteita ovat

– valoverho
– taajuusmuuttaja
– oikosulkumoottori
– hydrauliikka
– hätäseispainike

4.2 Ovi

Automaattisen koneen perusominaisuutena on, että se tekee töitä ilman jatkuvaa ihmisen läsnäoloa tai ohjausta. Tällaisessa koneessa käytetään koneen rakenteita, kiinteitä suojuksia ja turvalaitteita suojaamaan, ettei normaalin automaattisen käyttötoiminnan aikana ihminen pääsisi ulottumaan koneen vaarallisiin liikkeisiin. (Siirilä 2008, 49.)

Koneiden tavallisin suojalaite on koneen toimintaan kytketty ovi. Oven avaamisen on saatava aikaan koneen pysähtyminen, ennen kuin vaarakohtaan voidaan ehtiä. Tarvittaessa ovessa voidaan käyttää lukintaa, joka estää oven avaamisen vaarallisten liikkeiden ollessa käynnissä. Lukintaa käytetään sekä tarpeettomien hankalien pysäytysten estämiseen että turvallisuusmielessä. (Siirilä 2008, 150.)

Lisäksi oven turvalaitteiden pitää olla sellaisia, että niiden helppo mitätöiminen ei ole mahdollista (Siirilä 2008, 376).

4.2.1 Oven valvonta

Jotta verkko-oven turvallisuudessa päästäisiin korkeaan suoritustasoon (PL d tai e), pitää käyttää ovirajakytkimien kahdennusta eli on käytettävä kahta eri komponenttia. Tällöin komponentti ei ole pelkästään sähköisesti kahdennettu (kahdennetut koskettimet), vaan myös mekaanisesti kahdennettu. Siitä seuraa, että esimerkiksi ovilukon (kuva 7) ohjauskappaleen kielen katkeaminen tai vääntyminen ei johda turvatoiminnon menettämiseen, kun samassa ovessa on lisäksi toinen, mielellään eri teknologialla toimiva rajakytkin. (Rantanen henkilökohtainen tiedonanto 10.10.2014.)

Kuva 7. I200 ovilukko (SICK Oy:n www-sivut)

Jos vaara-alue on sellainen, ettei tarvitse päästä kuin suoritustasoon PL c, niin periaatteessa riittää yksi rajakytkin, jossa on pakkoavautuvat koskettimet. Mutta, jos asennettava rajakytkin on tavallinen lukollinen ovirajakytkin ilman mitään yksilöllisiä koodauksia (esim. lukollinen ovirajakytkin, joka on mahdollista ohittaa erillisellä irtokielellä), niin tällöin tulee helposti kysymykseen se, että helpon ohittamisen estämiseksi ei ole tehty toimenpiteitä. Tästä syystä on hyvä lisätä yhden jo vaadittavaan PL c suoritustasoon yltävän rajakytkimen rinnalle helppoa ohittamista vaikeuttamaan toinen rajakytkin. (Rantanen henkilökohtainen tiedonanto 10.10.2014; Siirilä 2013, 17.)

4.2.2 Oven lukitus

Oven lukitusta voidaan käyttää vaara-alueen toimintaan liittyvänä asiana tai sitten turvatoimintona. SICK Oy:n I200 E lukollinen ovirajakytkin on tarkoitettu tuotantopysäytykseen ja oven valvontaan. Kyseisessä rajakytkimessä on lukitus sitä varten, ettei ovea ”riuhtaistaisi” auki sellaisessa kohtaa, jossa koneiden ei haluta pysähtyvän. Lukko myös aukeaa, jos siitä häviää sähköt eli lukituksen kiinni pysymistä ei varmisteta jousivoimalla. Kyseisen lukollisen rajakytkimen käyttäminen edellyttää, että jos ovi saadaan auki vaikka sähkökatkon aikana, niin vaara-alueella olevien liikkeiden täytyy olla pysähtyneenä, ennen kuin niiden vaikutusalueelle ehditään. Se edellyttää yleensä koneisiin liitettyjen jarrujen käyttämistä. (Rantanen henkilökohtainen tiedonanto 10.10.2014.)

SICK Oy:n I200M lukinnalla varustettu ovirajakytkin on taas tarkoitettu turvatoiminnoksi eli lukko ei aukea sähkökatkon aikanakaan, sillä jousivoima pitää lukon kiinni. Lukko pysyy lukossa niin kauan, kun se sähköllä ohjataan auki. Kyseisen lukollisen ovirajakytkimen käyttäminen vaatii, että varmistetaan vaara-alueella olevien vaarallisten liikkeiden pysähtyneenä oleminen, ennen turvalogiikan suorittamaa lukituksen avaamista. Vaarallisten liikkeiden pysähtyneenä oleminen voidaan varmistaa koneen toimintaan kytkettyjen pyörimisantureiden avulla. (Rantanen henkilökohtainen tiedonanto 10.10.2014.)

Oven ulkopuolella on hyvä olla ohjauspaneeli, jossa on avauspyyntönappi ja kuittausnappi sellaisessa kohdassa, että joka puolelle vaara-aluetta on hyvä näkyvyys. Tarvittaessa näkyvyys vaara-alueelle varmistetaan peileillä tai kamerajärjestelmillä. Useamman kuittausnapin käyttö tarvittaessa on myös hyvä ratkaisu. (Siirilä 2013, 28.)

Avauspyyntönapin ideana on, että logiikka pysäyttää koneet sopivaan kohtaan ennen kuin se avaa oven lukituksen vaara-alueelle pääsemiseksi. Kuittausnapilla taas varmistetaan, että logiikka ei käynnistä vaara-alueen toimintoja ennen kuin kuittausnappia painava henkilö toteaa, että vaara-alueella ei ole henkilöitä.

Jos ihminen mahtuu kokonaan aidassa olevan lukitun ja suljetun oven sisäpuolelle, niin lukinta pitää voida avata sisäpuolelta erillisellä niin kutsutulla ulospääsyvapautuksella (Siirilä 2013, 27).

4.3 Saranoitu ovi

Saranatappeihin yhdistetyn rajakytkimen (kuva 8) ja magneettisen rajakytkimen, jossa on koodattu ohjauskappale (kuva 9), huijaaminen on huomattavasti hankalampaa kuin viputyyppisen (kuva 10), jonka koskettimet voidaan sitoa kiinni toimimattomaksi tai induktiivisen (kuva 11) rajakytkimen, jota voidaan huijata erillisellä metallipalalla. Saranatappiin yhdistetyn rajakytkimen etuna on, että sen ohittaminen on erittäin hankalaa ja asennus menee varmemmin kerralla oikein. (Siirilä 2008, 362; Siirilä 2013, 33.)

Kuva 8. I10R rajakytkin (SICK Oy:n www-sivut)

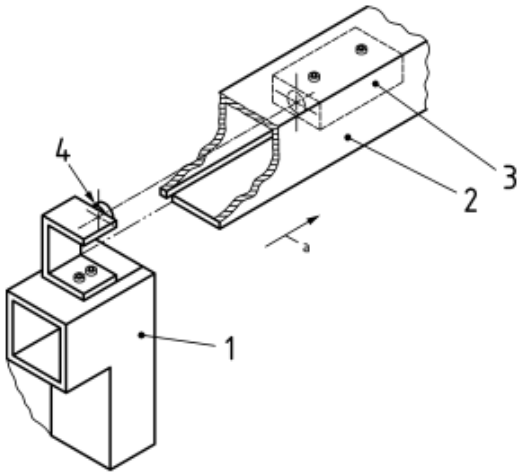
Kuva 9. RE1 rajakytkin (SICK Oy:n www-sivut)

Kuva 10. I110R rajakytkin (SICK Oy:n www-sivut)

Kuva 11. IN4000 rajakytkin (SICK Oy:n www-sivut)

4.4 Liukuovi

Liukuvan oven turvallistaminen voidaan tehdä käyttäen pelkkää lukollista ovirajakytkintä huomioiden, että se tehdään helpon ohittamisen estävästi, jos vaatimuksena on luokan 1 suoritustaso PL c. Kun vaaditaan vähintään luokan 3 PL d-suoritustasoa, käytetään ovilukon ja sähkömekaanisen tai kosketuksettoman ovirajan yhdistelmää. Rajakytkinten helppo ohittaminen saadaan estettyä käyttäen lukollisen ovirajan parina magneettista rajakytkintä, jossa on koodattu vastakappale (kuva 9). Näin magneettikytkintä ei voida huijata erillisellä irtomagneetilla. Yhtenä vaihtoehtona on myös käyttää erillistä suojaa (kuva 12), jolloin rajakytkimen mahdollinen ”käpälöiminen” on huomattavasti hankalampaa. (Siirilä 2009, 363-364; SFS-EN ISO 14119, 52.)



Kuva 12. Rajakytkimen suojaus

Kuvan 12 numeroidut osat ovat:
1: liukuva suojus
2: rajakytkimen suojus
a: sulkeutumissuunta
3: rajakytkin
4: rajakytkimeen vaikuttaja (SFS-EN ISO 14119, 52)

4.5 Turvallisuuteen liittyvä ohjausjärjestelmä

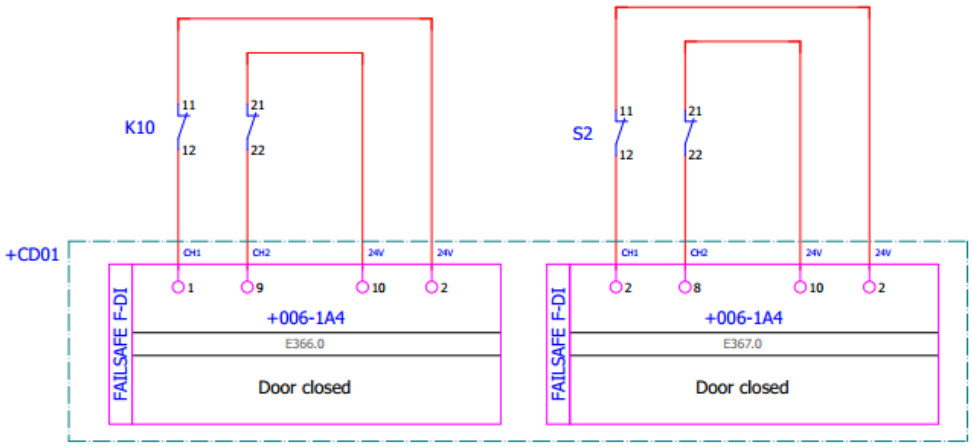
Raumaster Paper Oy:n toimituksessa olevilla laitteiden muodostamilla vaara-alueilla on riskinarviointien mukaan, joko PL c tai d suoritustason tarve ohjausjärjestelmälle asetetussa riskien pienentämisen osuudessa. Niinpä käsitellään tässä luvussa esimerkkejä käyttäen, millaisia komponentteja ja turvapiirejä ehdotetaan em. vaara-alueiden riskien pienentämiseen. Luvussa 5 varmistetaan vaaditun riskien pienennyksen toteutuminen Sistema-ohjelmaa käyttäen.

Tarkasteltavalle vaara-alueelle pääsee kulkemaan ovista ja valoverhoilla valvotuista aukoista. Vaara-alueella on suoraan kontaktoreilla käytettyjä moottoreita ja taajuusmuuttajakäyttöjä. Lisäksi alueella on hydraulisia toimilaitteita.
Alueeseen vaikuttaa myös hätäseispainike. Kyseinen alue halutaan tarkastella suoritustasolla PL c ja d. Ohjauksen ”älynä” käytetään Siemens S7 -turvalogiikkaa.

4.5.1 Ovirajat vaara-alueille PL c ja d

Tehtävänannossa sanottiin, että ovirajojen osalta PL c ja d -suoritustasoille etsitään yhtenäinen ratkaisu. Niinpä käytetään kahta erilaista turvahyväksyttyä rajakytkintä.

Kuvassa 13 on rajakytkimien sähköinen ja mekaaninen kahdennus, sillä käytössä on kaksi eri komponenttia. Oikosulut paljastuvat myös, koska turvalogiikka testaa tulopiirejä testipulsseilla. K10 koskettimet ovat lukollisen ovirajakytkimen oven aukiolon ilmoittamiseen ja S2 on lukollisen ovirajakytkimen pariksi valittu toinen turvahyväksytty oven aukiolon tunnistava rajakytkin.



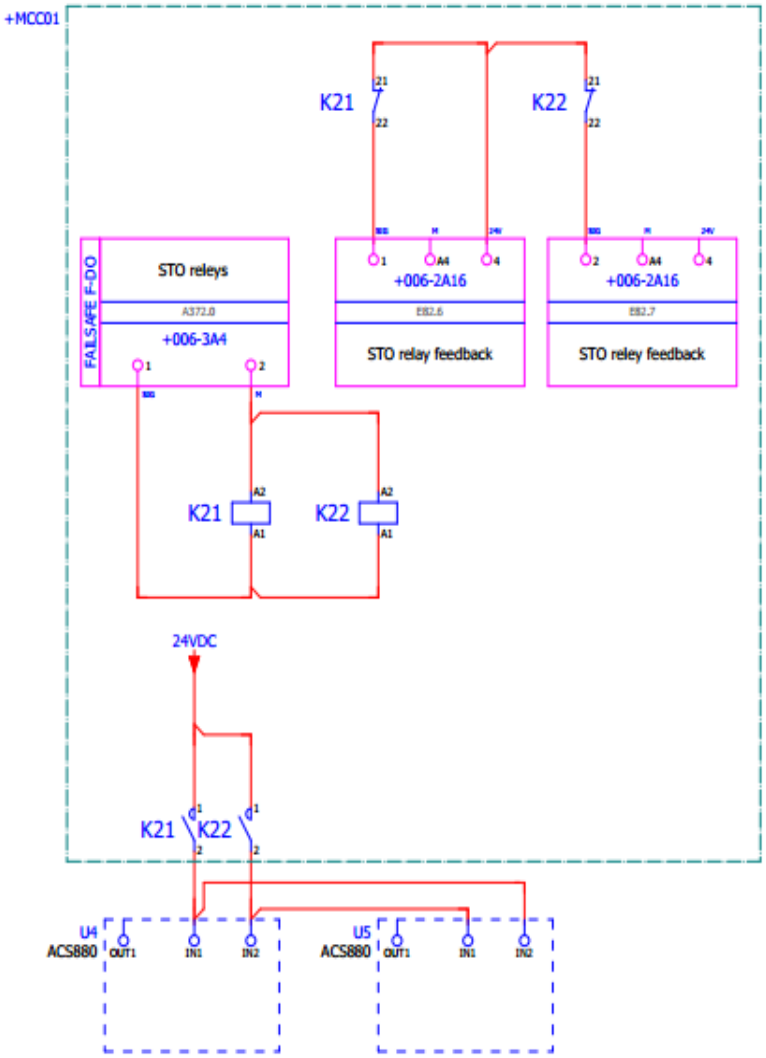
Kuva 13. Ovirajojen kahdennettu rakenne automaattisella tulopiirien valvonnalla

4.5.2 Taajuusmuuttaja vaara-alueille PL c ja d

Taajuusmuutajan STO- eli Safety torque off -toimintoa käytetään odottamattoman käynnistyksen estämisen lisäksi pysähtymiseen liittyviin toimintoihin, jotka mahdollistavat koneen turvallisen käytön ja huollon, vaikkei verkon jännitesyöttöä taajuusmuuttajaan katkaista. Kun Safety torque off -toiminto aktivoituu, niin taajuusmuuttaja ei tuota enää pyörivää magneettikenttää ja näin ollen moottori ei pysty tuottamaan momenttia akseliinsa. (ABB industrial drives.)

Tarkastelun kohteeksi valittiin ABB ACS 880 -taajuusmuuttaja. STO-tuloja ohjataan kahdella turvalogiikan lähdöillä ohjatulla releellä, joista otetaan takaisinkytkennät standardilogiikan tulokorteille (kuva 14). Näin voidaan tehdä, kun käytetään dynaamista periaatetta, eli kun releet päästää, niiden apukoskettimien pitää muuttaa tilaa tietyssä määritellyssä aikaikkunassa. (Rantanen henkilökohtainen tiedonanto 10.10.2014.)

ABB määrittelee ACS 880 -taajuusmuuttajan STO-tuloille suoritustason PL e ja käytetyllä releohjauksella se ei huonone, kun releet ovat luotettavat ja ympäristöönsä sopivat. Taajuusmuuttajat U4 ja U5 voidaan ketjuttaa kuvan 14 mukaisesti. Ketjuun voidaan lisätä enemmänkin taajuusmuuttajia. (ABB industrial drives.)

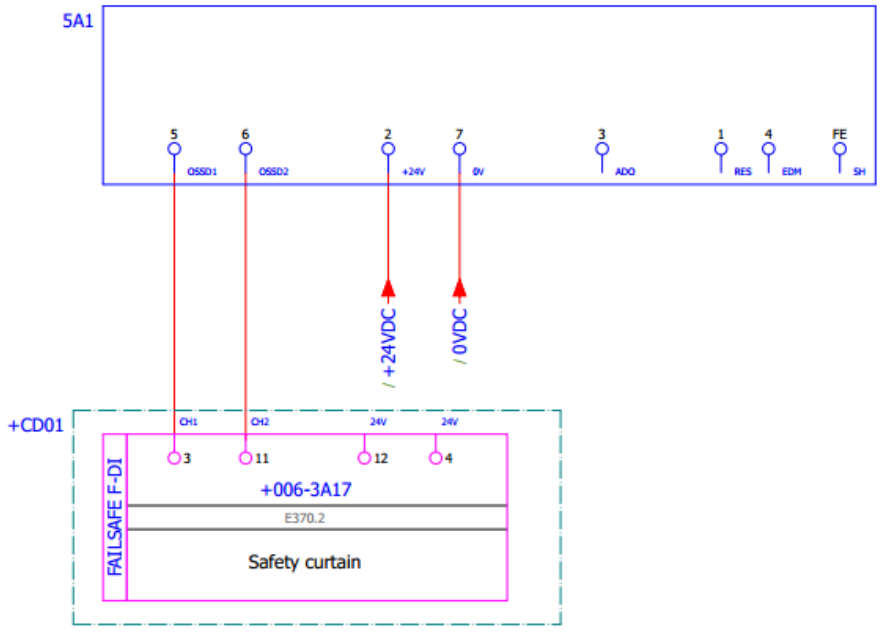


Kuva 14. Taajuusmuuttajan STO-tulojen ohjaus

4.5.3 Valoverho vaara-alueille PL c ja d

Valoverho on siitä erityisen kätevä, että se toimii ja havaitsee ihmisen riippumatta ihmisen ajattelemattomuudesta tai muuten virheellisestä toiminnasta. Valoverho on myös luotettava, koska se on turvaluokiteltu komponentti ja sen toiminta perustuu lähettimen ja vastaanottimen välisen valonsäteen katkeamiseen. (Siirilä 2008, 151.)
SICK Oy:ltä löytyy valoverho C2000, jolle valmistaja antaa suoritustason PL d. Se on luokan 2 turvalaite, joka käy hyvin PL c vaara-alueelle.

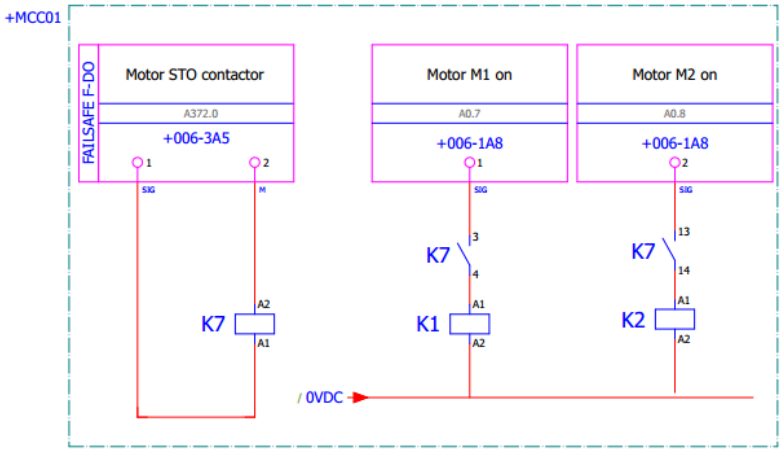
PL d vaara-alueelle valitaan SICKiltä C4000 valoverho (kuva 15), joka yltää suoritustasoon PL e ollen luokan 4 turvalaite kahdennetuilla turvatuloilla.



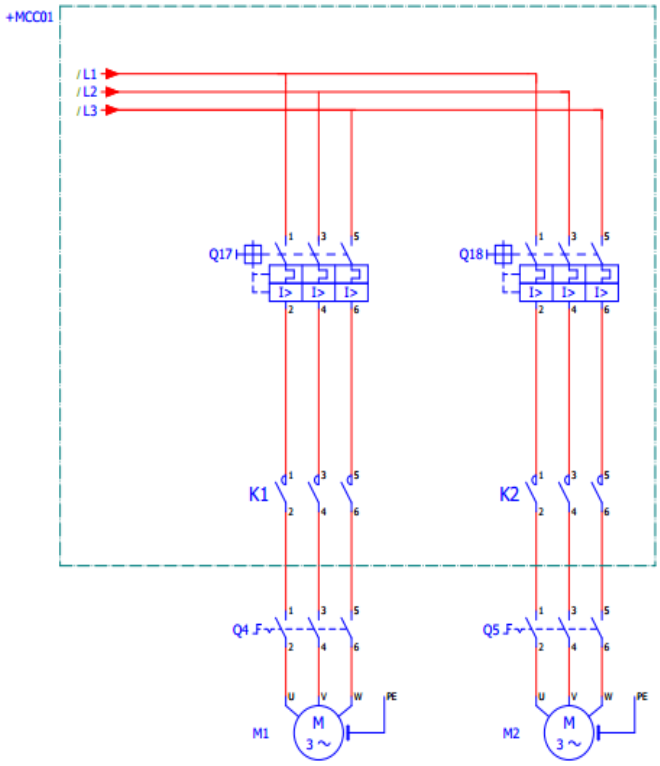
Kuva 15. Valoverho kahdennetuilla turvatuloilla

4.5.4 Oikosulkumoottori vaara-alueelle PL c

Vaara-alueella on yleensä useita suoria moottorilähtöjä ja jokaista ei tarvitse välttämättä ohjata omalla turvalogiikan lähdöllä, jos niiden määrässä halutaan säästää. Yksi ratkaisu on ohjata yhtä tai tarvittaessa useampaa kontaktoria turvalogiikan lähdöllä tai lähdöillä ja käyttää kyseisen tai kyseisten kontaktorin koskettimia katkaisemaan normi- eli stardardilogiikan korttien ohjaamilta kontaktoreilta sähköt (kuva 16). Useampiakin moottoreita voidaan kytkeä saman hätäseiskontaktorin koskettimien perään. Kontaktorien luotettavalla ylimitoituksella varmistetaan kontaktorien koskettimien epätodennäköisempi kiinnihitsaantuminen moottorien päävirtapiireissä (kuva 17).



Kuva 16. Hätäseiskontaktori K7 virtapiiressä

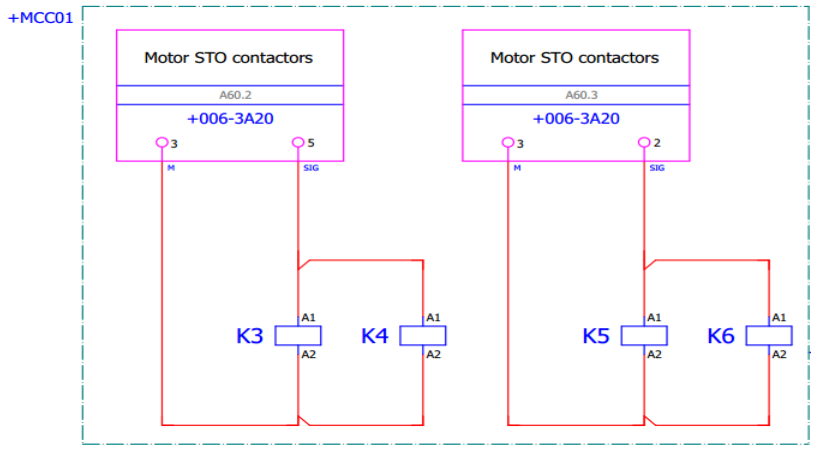


Kuva 17. PL c oikosulkumoottorien päävirtapiirit

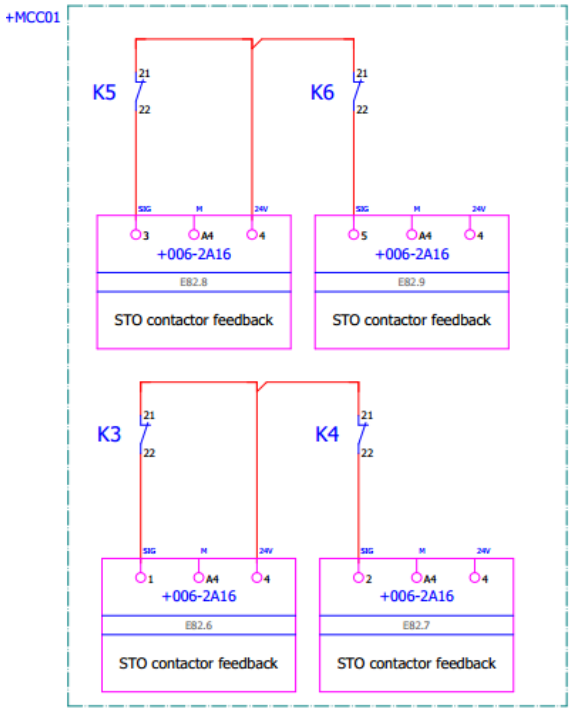
4.5.5 Oikosulkumoottori vaara-alueelle PL d

Samoin kuin oikosulkumoottoreissa kohdassa 4.5.4, turvalogiikan lähtöjen määrässä halutaan säästää. Niinpä ainakin yksi ratkaisu on käyttää turvalogiikan ohjaamaa turvapoweria, jonka perään voidaan kytkeä standardilogiikan lähtöjä ja näin kytkeä niiden perään suorat moottoriohjaukset (kuva 18). Siemensin ET 200 S turvapoweri yltää suoritustasoon PL d, joten valitaan se käytettäväksi.

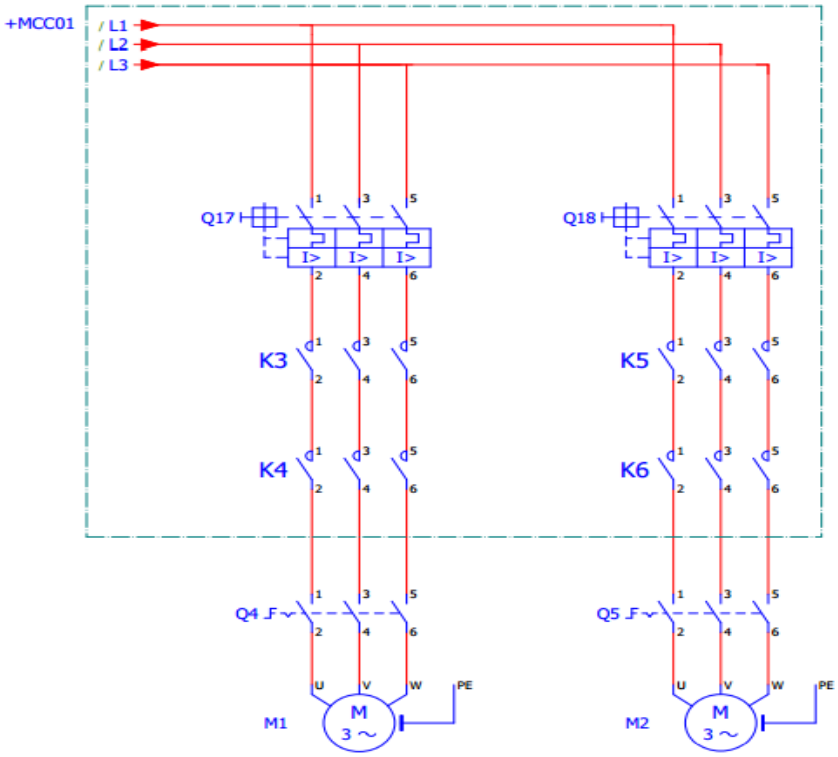
Kontaktorien takaisinkytkentätieto voidaan tuoda standardilogiikan tulokortille (kuva 19) samoin periaattein kuin kohdan 4.5.2 taajuusmuuttajaohjauksessa. Kahden kontaktorin koskettimet tulee aina yhteen suoraan moottorilähtöön (kuva 20).



Kuva 18. Turvapowerin ohjaamat standilogiikan lähdöt ohjaavat moottoripiirien kontaktoreita



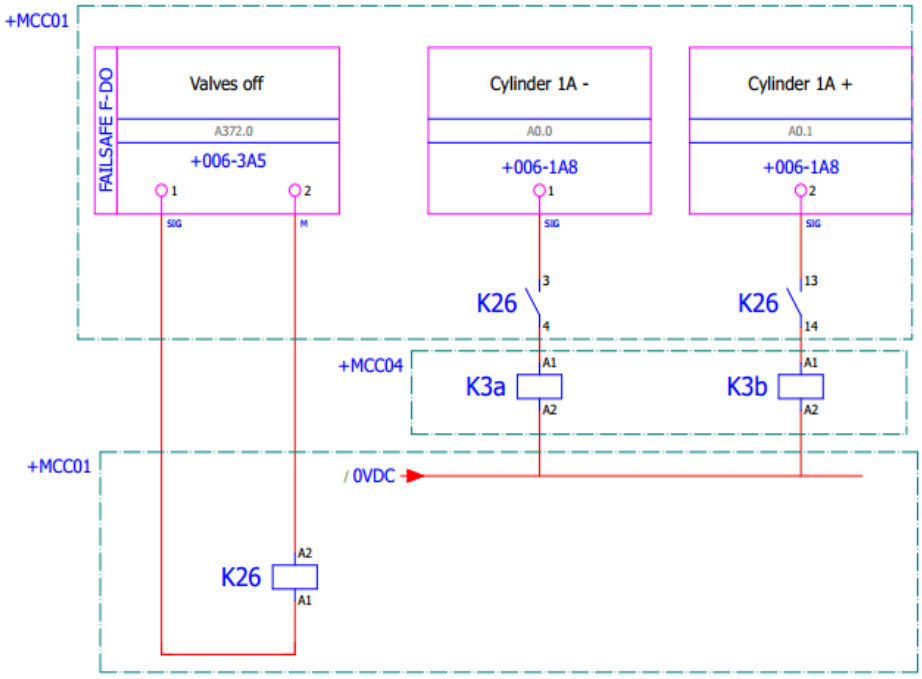
Kuva 19. Takaisinkytkentä standardilogiikan tulokorteille



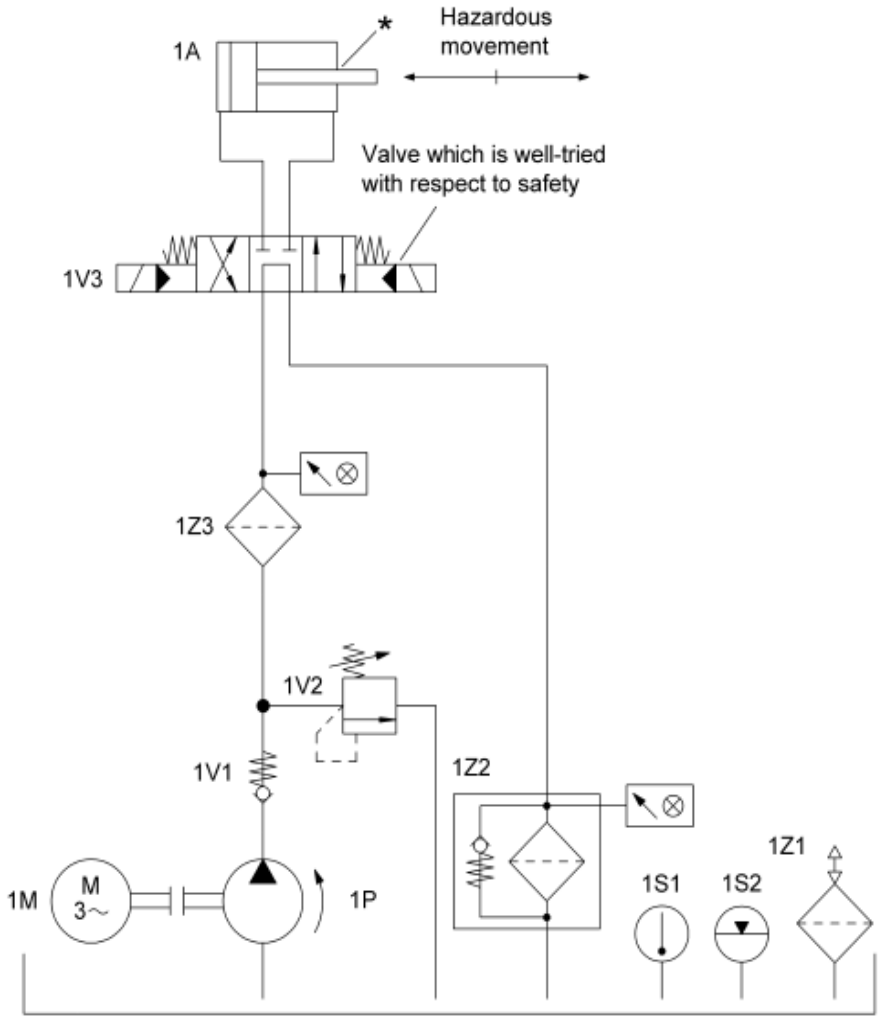
Kuva 20. Moottorien päävirtapiirit suoritustasoon PL d

4.5.6 Hydrauliikka vaara-alueelle PL c

Hydrauliikan tarkastelussa on sama tarve kuin kohdan 4.5.4 oikosulkumoottorien tarkastelussa. Kun on useampi hydraulinen toimilaite, voidaan ottaa turvalogiikan ohjaaman hätäseiskontaktorin sulkeutuvat koskettimet suuntaventtiilien kelojen ohjauspiireihin. Kuvassa 21 on liitetty hätäseiskontaktori K26:n koskettimet kelojen ohjauspiireihin. Toiminta perustuu siihen, että kun suuntaventtiilin molemmilta keloilta katkaistaan sähkö, niin suuntaventtiilin asento muuttuu lukituksi keskiasennoksi, eikä se päästä enää virtausta männän eikä varren puolelle. Kuvassa 22 painesuodatin 1Z3 lisää suuntaventtiilin 1V3 luotettavuutta. Sylinterin 1A männän varressa oleva tähti kuvastaa jonkinlaista lian torjujaa. (Hauke 2008, 148.)



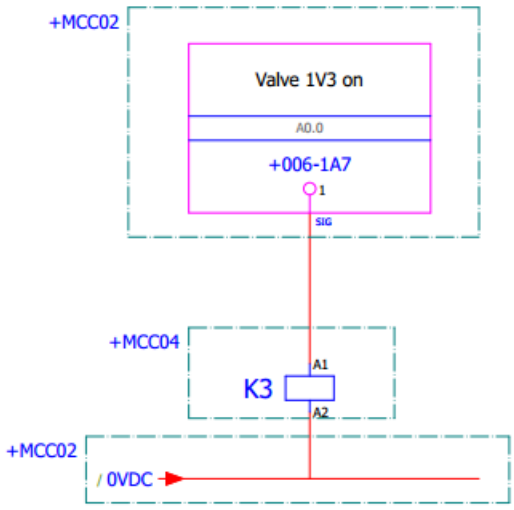
Kuva 21. Hätäseiskontaktori K26:n koskettimet suuntaventtiilin kelojen ohjauspiireissä



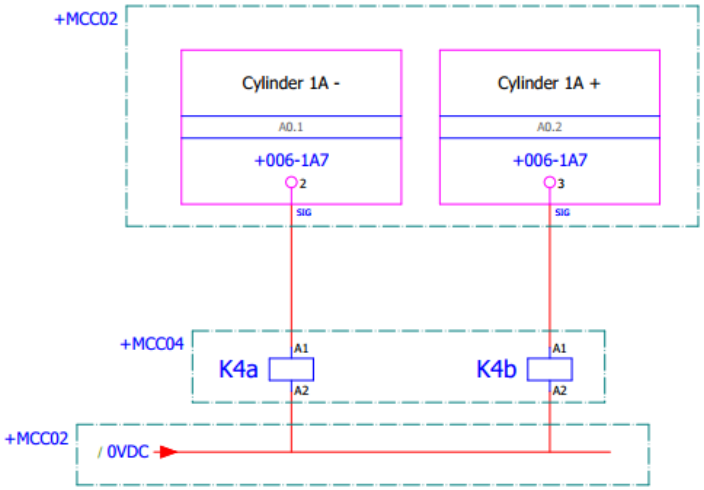
Kuva 22. Hydrauliikan pääkaavio suoritustasoon PL c (Hauke 2008, 147)

4.5.7 Hydrauliikka vaara-alueelle PL d

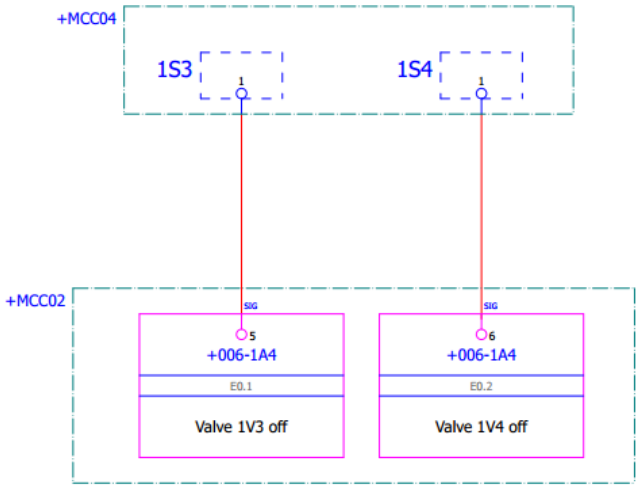
Hydrauliikan kohdalla tulee sama asia kysymykseen kuin kohdan 4.5.5 oikosulkumoottoreiden kohdalla, eli hydraulisia toimilaitteita on yleensä monta ja jokaiselle ei haluta varata omaa lähtöä turvalogiikan kortilta. Niinpä ohjataan turvalogiikan ja turvapowerin kautta logiikan standardilähtöjä ja niillä suuntaventtiilien 1V3 ja 1V4 keloja (kuva 23 ja 24). Suuntaventtiilien karojen asentoa valvovilta elimiltä 1S3 ja 1S4 otetaan digitaalinen takaisinkytkentä logiikan standardituloihin (kuva 25) dynaamista periaatetta käyttäen. Tällä periaatteella voidaan käyttää useampia hydraulisia toimilaiteita turvalogiikan lähtöjä säästäen. Kuvassa 26 on hydrauliikan pääkaavio tälle toteutukselle.



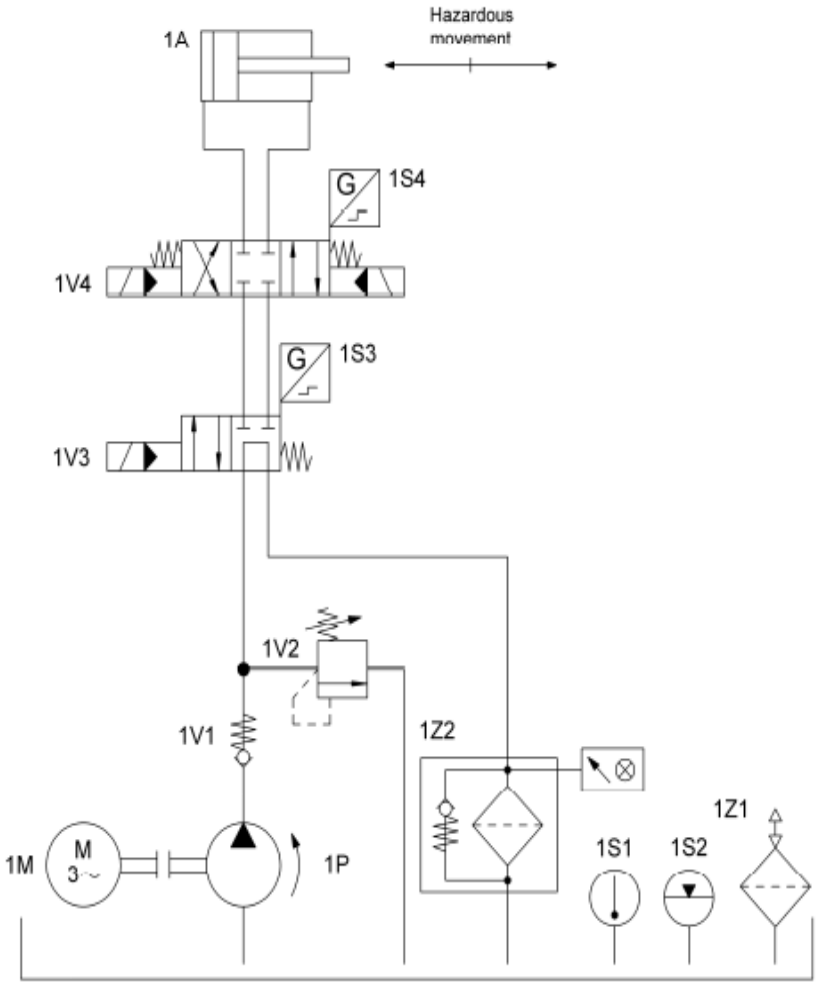
Kuva 23. Suuntaventtiilin 1V3 kelan ohjaus



Kuva 24. Suuntaventtiilin 1V4 kelojen ohjaus



Kuva 25. Suuntaventtiilien karoja valvovat elimet 1S3 ja1S4



Kuva 26. Hydrauliikan pääkaavio suoritustasoon PL d (Hauke 2008, 257)

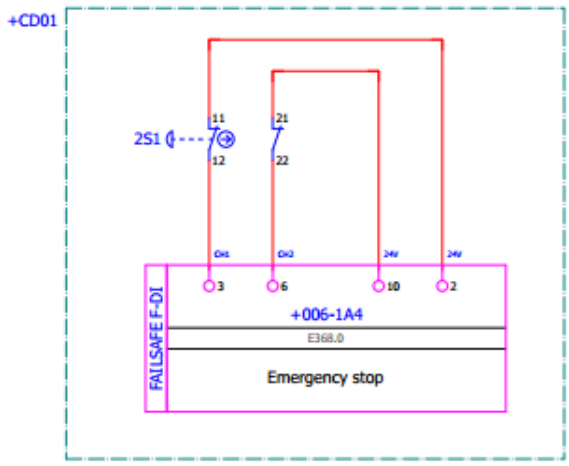
4.5.8 Hätäseispainike vaara-alueille PL c ja d

Koneasetus 400/2008 mukaan: ”koneessa on oltava yksi tai useampia hätäpysäytyslaitteita, joiden avulla todellinen tai uhkaava vaara voidaan torjua.”

Hätäpysäytin ei ole turvalaite: koneen rakenteella, suojuksilla ja turvalaitteilla (esim. valoverho) huolehditaan ensisijaisesti siitä, että kone ei vaaranna kenenkään turvallisuutta (Rantanen 2012, 6).

Hätäpysäytys on turvatoiminto: sitä käytetään hätätilanteessa tai uhkaavassa tilanteessa koneen vaarallisten liikkeiden pysäyttämiseen, kun henkilön terveys tai turvallisuus on uhattuna (Rantanen 2012, 6).

Hätäseispainikkeen avautuvat koskettimet kytketään molemmat omaan turvalogiikan tulokanavaan (Kuva 27). Tulopiirien oikosulkua valvotaan turvalogiikan testipulsseilla. Näin kaikki viat tulevat havaituiksi.



Kuva 27. Hätäseispainikkeen koskettimien kahdennettu rakenne tulopiirien valvonnalla

5 TURVATASOJEN LASKEMINEN SISTEMA-OHJELMALLA

Varmistetaan vielä luvun 4.5 ohjausjärjestelmän osien suoritustasojen riittävyys vaara-alueilla PL d ja c. Käytetään suoritustasojen laskennassa Sistema-ohjelmaa, josta saadaan kirjallinen raportti vaatimusten täyttymisestä. Sistemaan voidaan ladata valmiita komponenttikirjastoja, joista voi tarvittavan komponentin lisätä suoraan laskelmaan. ”Älykkäämmät” komponentit löytyvät suoraan komponenttikirjastosta alajärjestelmänä, eli SB-tunnuksella. Valmistaja määrittää ”älykkäämmille” komponenteille suoraan luokan ja suoritustason, ja vastaa myös niiden täyttymisestä.

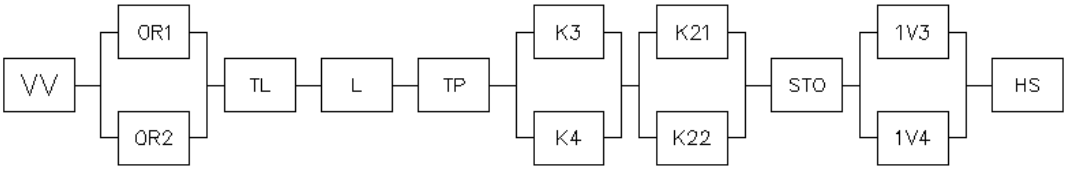
Sistema-ohjelmistotyökalu on Saksassa (IFA) kehitetty tietokoneavusteinen suunnittelumenetelmä, joka perustuu kaikilta osin ISO 13849 standardiin.
Työkalu tekee automaattisesti luotettavuuslaskelmat ilmoitettujen komponenttien ja arvojen perusteella. (Sundcon Oy:n www-sivut.)

Sundcon Oy:n www-sivuilla on lueteltu joitakin etuja ohjelman käytöstä:
– ”yhdenmukaisten käsitteiden käyttö vähentää väärinkäsityksiä ja karkeita virheitä, jotka voisivat olla etenkin toiminnallisen turvallisuuden ja luotettavuuden varmistamisen kannalta katastrofaalisia
– dokumenttien hallinta helpottuu, mikä on ensiarvoista toiminnallisen turvallisuuden käytönaikaiseen varmistamiseen ja muutostöihin
– vaatimustenmukaisuuden varmistaminen helpottuu niin asiakkaan kuin viranomaistenkin suuntaan”.

5.1 Vaara-alue PLd

Ennen kuin turvallisuuteen liittyvät komponentit lisätään Sistema–laskelmaan, on hyvä piirtää lohkokaavio laskettavan turvatoiminnon ohjausjärjestelmän osista (kuvio 2). Kuvio 2 on suunniteltu PL d luokan vaaraa-alueeseen.

Käyttökelpoinen tapa on ajatella eri ohjausjärjestelmän alajärjestelmät sarjaan toteuttamaan turvatoimintoa. Jokainen yksittäinen sarjaankytketty lohko on alajärjestelmä ja kaksi rinnakkain olevaa lohkoa muodostavat yhdessä alajärjestelmän. Kuvioon on lisätty vain yhtenä jokainen erityyppinen alajärjestelmä.



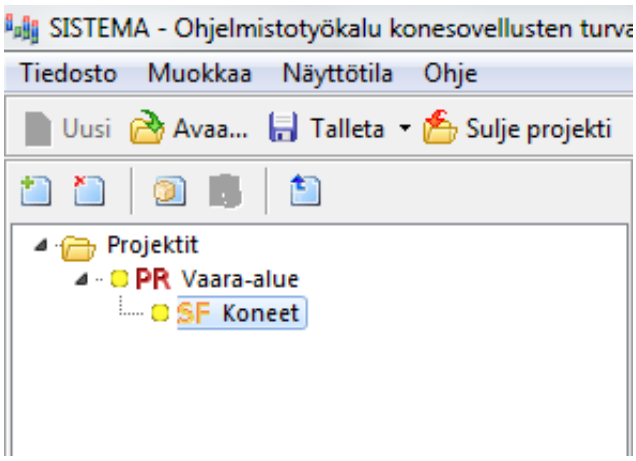
Kuvio 2. Turvallisuuteen liittyvä lohkokaavio

Kuvion 2 eri alajärjestelmät ovat:

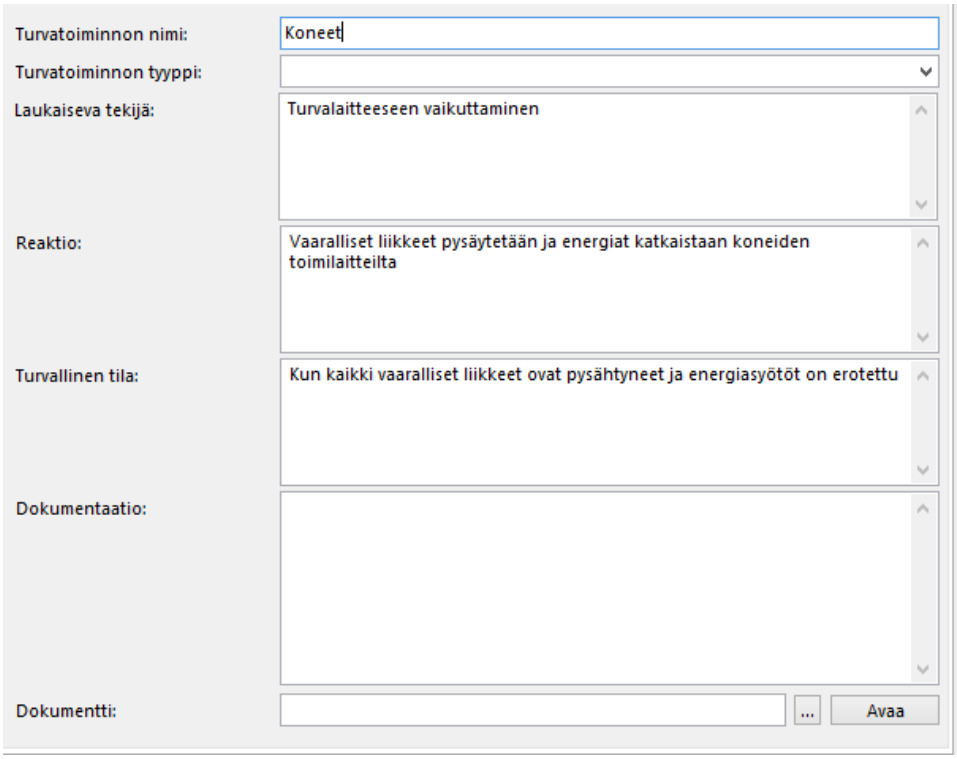
VV= valoverho
OR1, OR2 = oven turvarajakytkimet
TL= turvalogiikan komponentit
L= standardilogiikan lähtökortti
TP= turvapoweri
K3,K4= oikosulkumoottorin kontaktorit
K21,K22= taajuusmuuttajan STO-tulojen releet
STO= safety Torque Off
1V3,1V4= suuntaventtiilit
HS= hätäseispainike

5.1.1 Projektin ja turvatoiminnon luominen Sistemaan

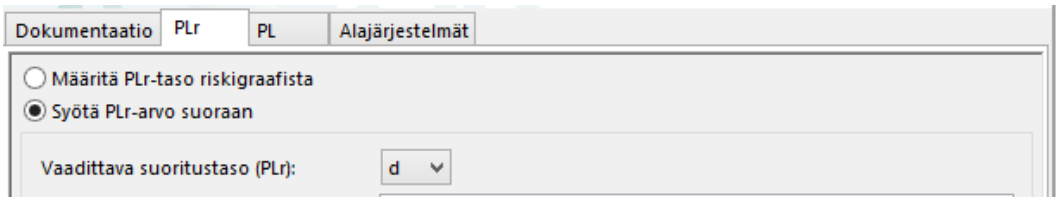
Tarkastellaan ensiksi luokan PL d vaara-aluetta. Tarkastelun kohteena olevat piirikaaviot löytyvät liitteestä 6. Aloitetaan Sistema-laskelma perustamalla uusi projekti Vaara-alue ja luomalla sen alle uusi turvatoiminto Koneet (kuva 28) määritellään turvatoiminnolle asetetut turvallisuuteen liittyvät tiedot (kuva 29). Tämän jälkeen asetetaan turvatoiminnolta vaadittu suoritustaso PL_r (kuva 30). Tässä se voidaan tehdä suoraan, sillä se on jo aiemmin erikseen määritelty. Sen voisi tehdä myös käyttäen Sistemassa ja kohdassa 3.2.1 olevaa riskigraafia.



Kuva 28. Uuden projektin ja turvatoiminnon luominen



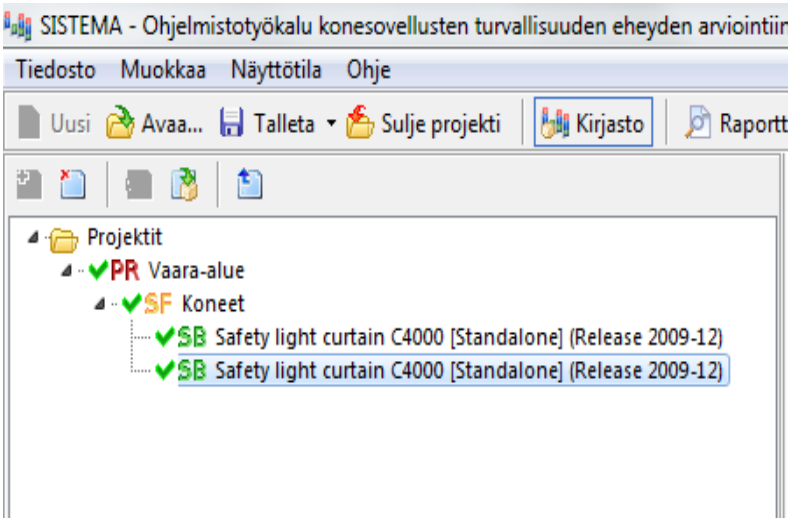
Kuva 29. Turvatoiminnon tietojen nimeäminen



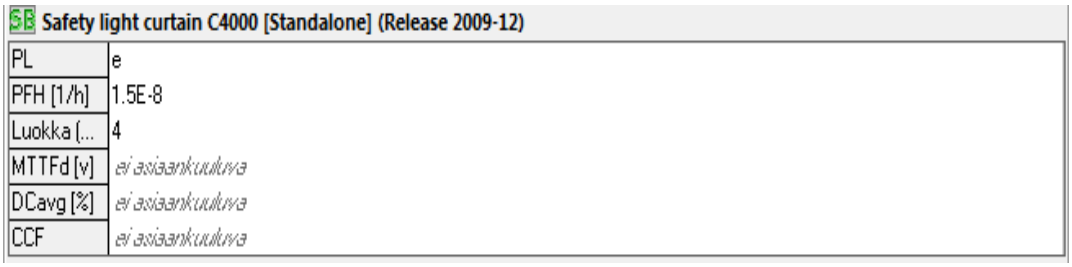
Kuva 30. PLr-arvon määrittämien

5.1.2 Valoverhot

Vaara-alueelle johtaa kaksi valoverhoilla valvottua aukkoa. Lisätään SICKin komponenttikirjastosta C4000 valoverhot (kuva 31), joille on määritelty luokan 4 suoritustaso PL e (kuva 32), suoraan laskelmaan omiksi alajärjestelmiksi.



Kuva 31. Valoverhojen lisääminen kirjastosta



Kuva 32. Valoverhojen luokka ja suoritustaso

5.1.3 Ovet

Vaara-alueelle voidaan kulkea yhteensä kolmen oven kautta. Yksi ovista on saranoitu ovi ja kaksi on liukuovia. Lisätään laskelmaan jokainen verkko-ovi omaksi alajärjestelmäksi.

Aloitetaan lisäämällä alajärjestelmä Ovi. Valitaan kohdasta PL: Määritä PL/PFH Luokan, MTTFd- ja Dcavg-arvojen avulla (kuva 33). Valitaan luokaksi neljä ja klikataan valinnat aktiiviseksi luokan vaatimusten täyttymisestä (kuva 34). Rajakytkinten tulopiirit on kytketty logiikan testipulssien valvontaan, näin vikoja ei pääse kertymään. Ko. alajärjestelmästä tulee kahdennettu ja sen alle ilmestyy kaksi kanavaa.

Saranoidun oven valvontaan valitaan lukinnalla varustettu ovirajakytkin ja saranaan asennettava ovirajakytkin SICKiltä, jotka lisätään komponenttikirjastosta lohkoina (BL) kanaviin 1 ja 2 (kuva 35), jolloin järjestelmä on sekä sähköisesti että mekaanisesti kahdennettu.

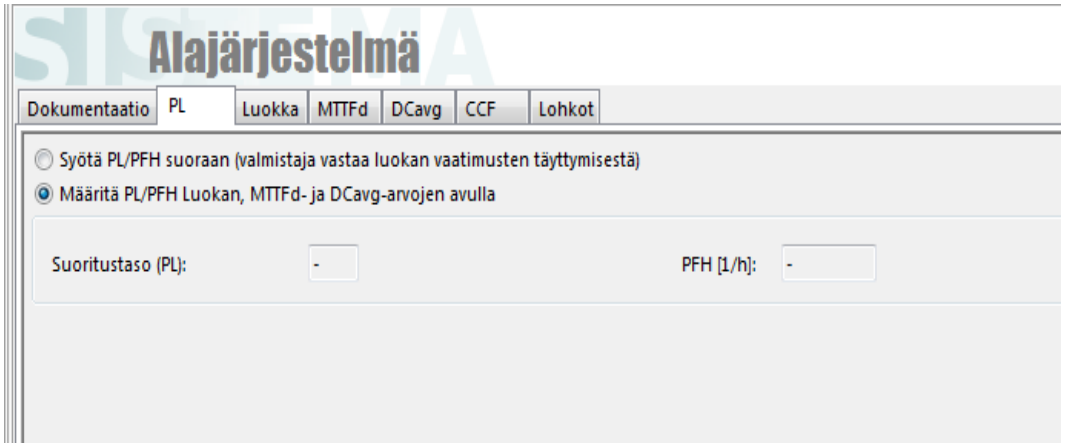
$MTTF_d$-valikosta valitaan ”Määritä $MTTF_d$-arvo lohkojen avulla” (kuva 36), jolloin Sistema laskee automaattisesti näille redundanttisille kanaville yhteisen $MTTF_d$-arvon, sillä valmistaja on sen molemmille rajakytkimille jo erikseen määritellyt.

DC-arvo voidaan määrittää molemmille lohkoille käyttämällä sovellettavia toimenpiteitä sen arvioimiseksi (kuva 37), kirjasto-painiketta painamalla pääsee valitsemaan DC-arvoja. DC-arvo voidaan myös ilmoittaa suoraan, jos se on tiedossa. Mutta kun arviointi tehdään sovellettavien toimenpiteiden avulla, asiaan saadaan samalla myös jonkinlainen perustelu loppuraporttiin tulevaksi. DC-arvoksi saadaan 99 % (kuva 38). Molemmilla ovirajakytkimillä on sama DC-arvo, sillä ne on molemmat kytketty samanlailla turvalogiikan tulokanaviin, joten toiselle lohkolle voidaan tehdä myös sama toimenpide.

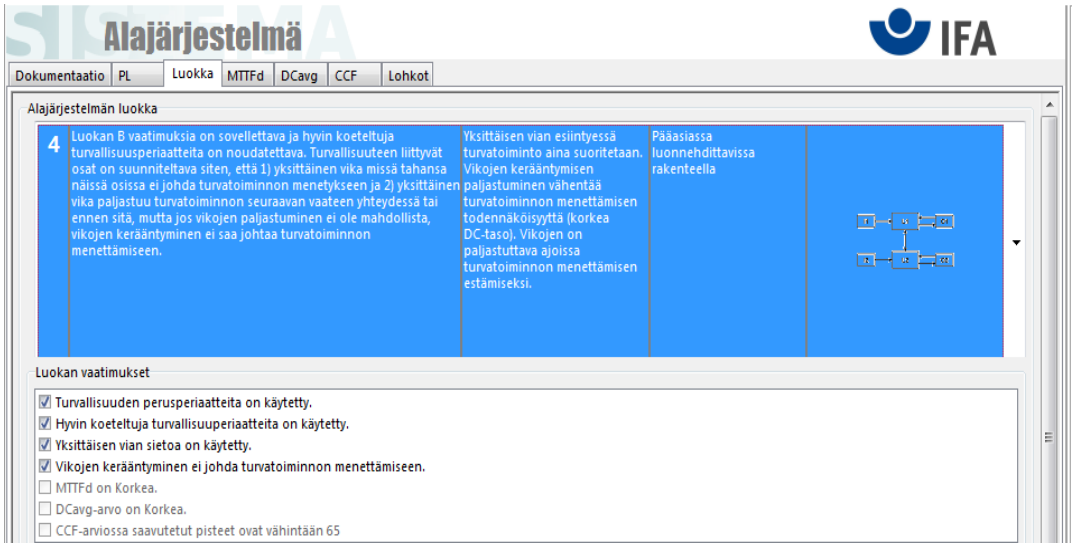
Vielä pitää määritellä tehdyt toimenpiteet yhteisvikaantumisen eli CCF:än estämiseksi. Sitä päästään arvioimaan valikosta CCF klikkaamalla valintaa: ”Valitse so-

vellettavat toimenpiteet CCF:än arvioimiseksi”. Tämän jälkeen kirjastopainiketta klikkaamalla päästään hakemaan em. sovellettavat toimenpiteet (kuva 39). yhteispistemääräksi saadaan 75 eli vaadittava 65 pistettä täyttyy kirkkaasti (kuva 40).

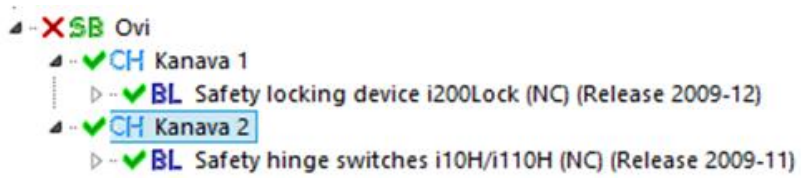
Kun edellä olevat kohdat on määritelty, niin Ovi on lisätty onnistuneesti laskelmaan. Lisätään liukuovi 1 ja 2 laskelmaan muuten samalla tavalla, mutta valitaan niihin saranaan kytkettävän ovirajakytkimen sijasta i10R-rajakytkin.



Kuva 33. Suoritustason määrittäminen luokan, MTTFd- ja Dcavg-arvojen avulla

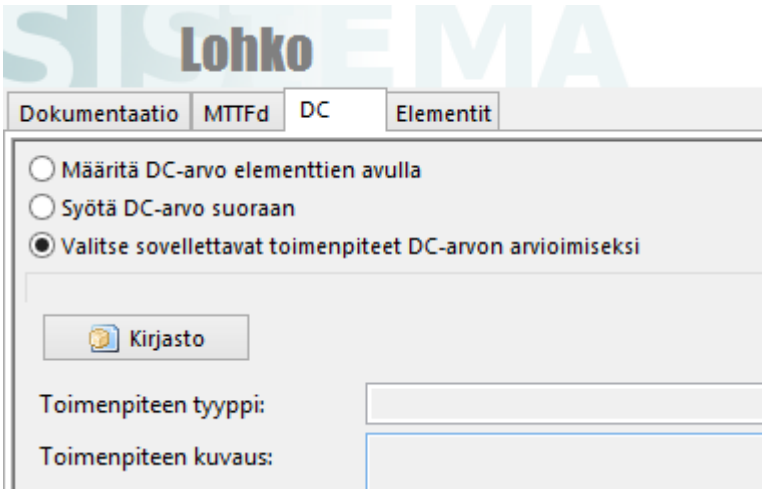


Kuva 34. Luokan valitseminen

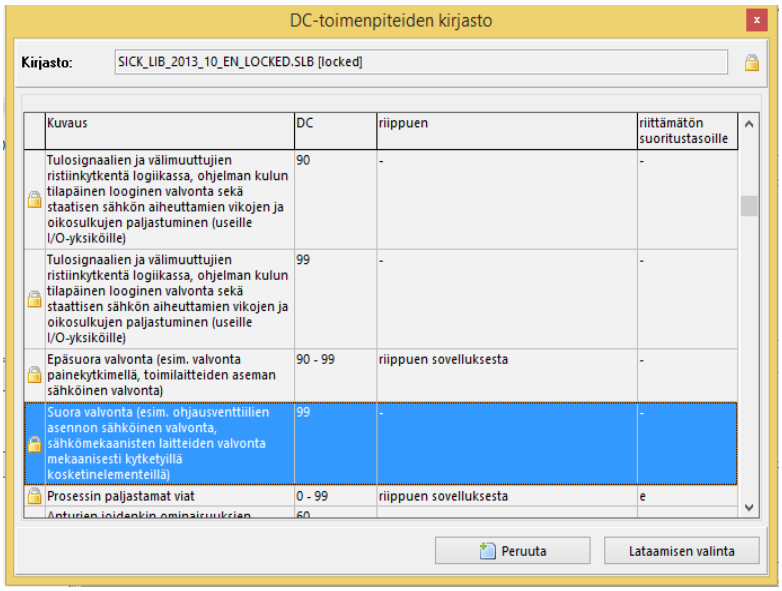


Kuva 35. Ovirajakytkimien kahdennettu rakenne

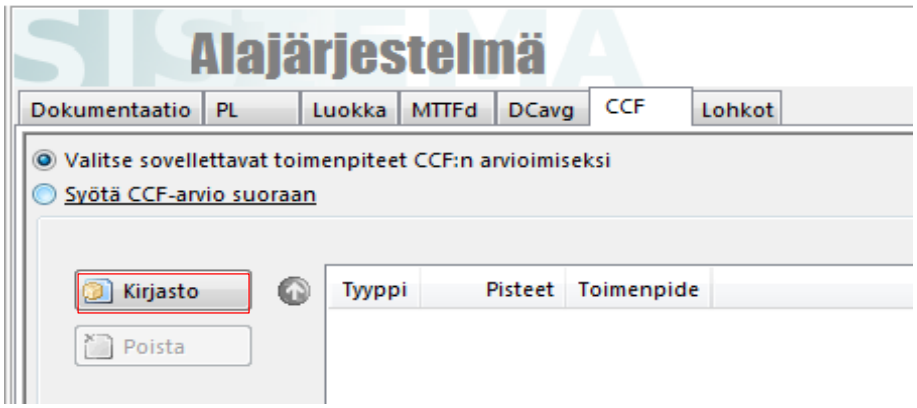
Kuva 36. Oven $MTTF_d$-arvon määrittäminen lohkojen avulla



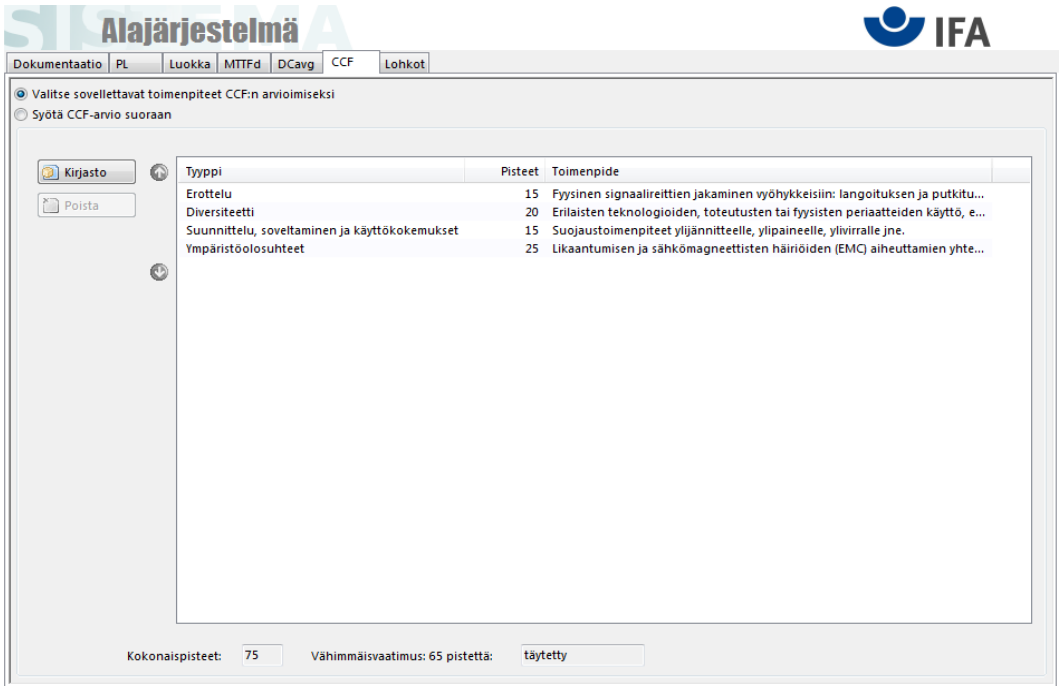
Kuva 37. DC-arvon arvioiminen



Kuva 38. DC-arvon valitseminen



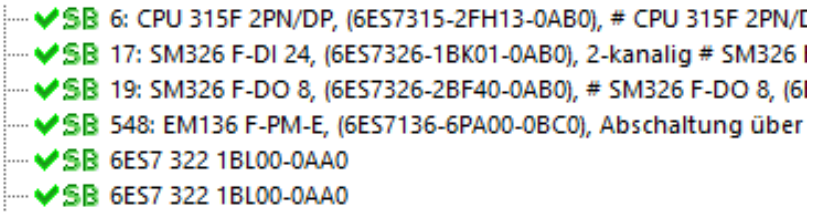
Kuva 39. Yhteisvikaantumisen arvioiminen kirjastoa apuna käyttäen



Kuva 40. Yhteisvikaantumisen estämiseksi tehdyt toimenpiteet

5.1.4 Turvalogiikka, turvapoweri ja standardilähtökortit

Turvalogiikan CPU-yksikkö ja tulo- ja lähtökortit sekä turvapoweri saadaan lisättyä laskelmaan suoraa Siemensin komponenttikirjastosta. Valmistaja on määritellyt niille myös suoraan suoritustason PL ja PFH-arvon. Standardilogiikan lähtökorteille löytyi suoritustasoja Siemensin luettelosta ja niille Siemens ilmoittaa suoraa suoritustason PL d, jos niitä käytetään turvapowerin ohjaamana. Muuta ei tarvitse tehdä kuin lisätä kyseiset komponentit alajärjestelmiksi laskelmaan (Kuva 41) ja lisätä standardilähtökorteille valmistajan ilmoittama arvo.



Kuva 41. Logiikkaohjaukseen liittyvät komponentit

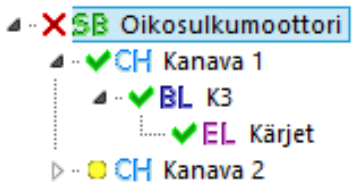
5.1.5 Oikosulkumoottori

Oikosulkumoottori lisätään omaksi alajärjestelmäksi. Luokaksi valitaan neljä, jolloin järjestelmästä tulee kaksikanavainen ja kahdennettu. Nimetään järjestelmän toisen kanavan lohko (BL) K3:ksi ja annetaan lohkon elementille (EL) nimi Kärjet (kuva 42). Valitaan elementille Kärjet teknologiaksi sähkömekaaninen (kuva 43). $MTTF_d$-välilehdellä valitaan: ”komponenttien tyypilliset arvot (hyvät insinöörikäytännöt-menetelmä)” (kuva 44). Sen alta löytyy lista, jossa on kohta: ”kontaktorit nimelliskuormituksella (mekaaninen kuormitus)” (kuva 45). Kun kontaktorit nimelliskuormituksella $B10_d$ -arvo on valittu, niin $MTTF_d$-välilehdellä voidaan laskea $MTTF_d$-arvo Nop-arvolla.

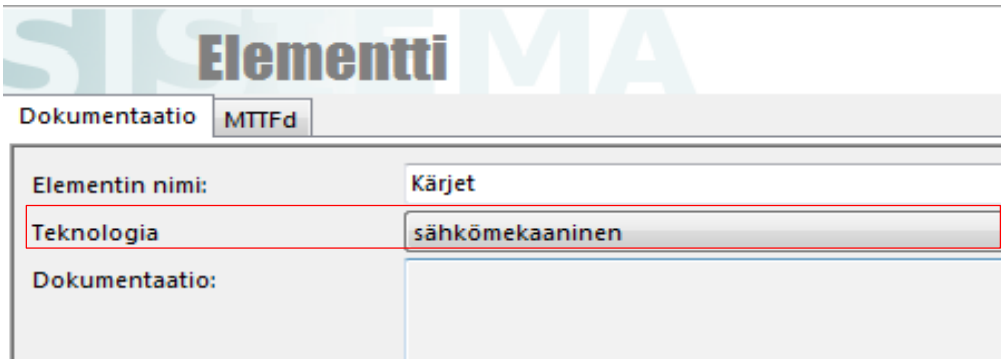
Ilmoitetaan, että moottori käy 365 päivää vuodessa ja 24 tuntia vuorokaudessa ja turvatoiminnon toimintojen välinen aika on yksi tunti eli 3 600 s (kuva 46). Kun edelliset

kohdat on valittu, kontaktorin $MTTF_d$-arvo on saatu laskettua, ja se on tässä sovelluksessa korkea.

Diagnostiikan kattavuus saadaan arvioitua alajärjestelmän DC_{avg}-välilehdeltä klikkaamalla valintaa: ”määritä DC_{avg}-arvo lohkoista ja tämän jälkeen valitaan lohkon DC-välilehdestä: ”valitse sovellettavat toimenpiteet DC-arvon arvioimiseksi”, minkä jälkeen kirjastopainikkeesta avautuu lista, josta valitaan: Dynaaminen periaate, joka tarkoittaa sitä, että kun rele ohjataan päälle tai pois niin releen takaisinkytkentätiedon on tultava tietyssä määritetyssä aikaikkunassa turvalogiikan CPU:lle releen ohjaamisesta. Tällä määrittelyllä lohkon K3 diagnostiikan kattavuus on 99 %. Kun lohko K3 on määritelty, niin kopioidaan se kanavaa 2 ja vaihdetaan nimeksi K4. Vielä pitää arvioida soveltuvat toimenpiteet yhteisvikojen välttämiseksi ja saada siitä vähintään 65 pistettä. kopioidaan määritelty oikosulkumoottori vielä toiseen kertaa laskelmaan, sillä tarkastellaan kohdan 4.5.5 tapausta.

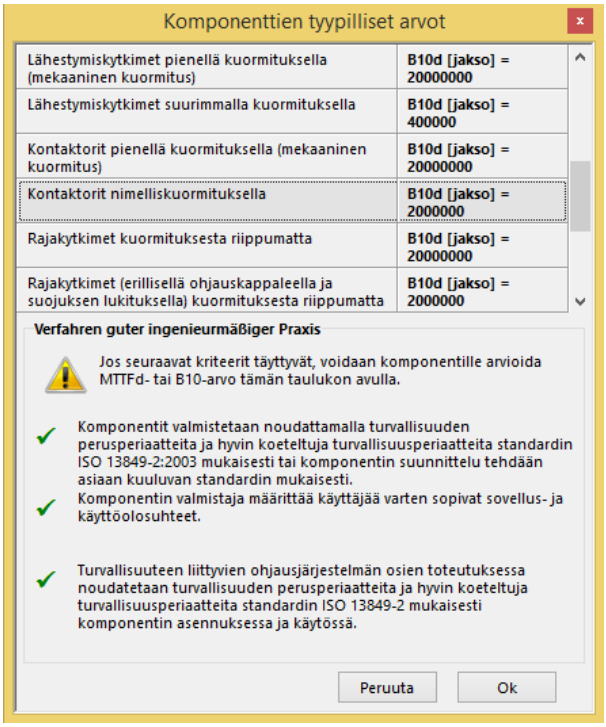


Kuva 42. Oikosulkumoottorin osien nimeäminen

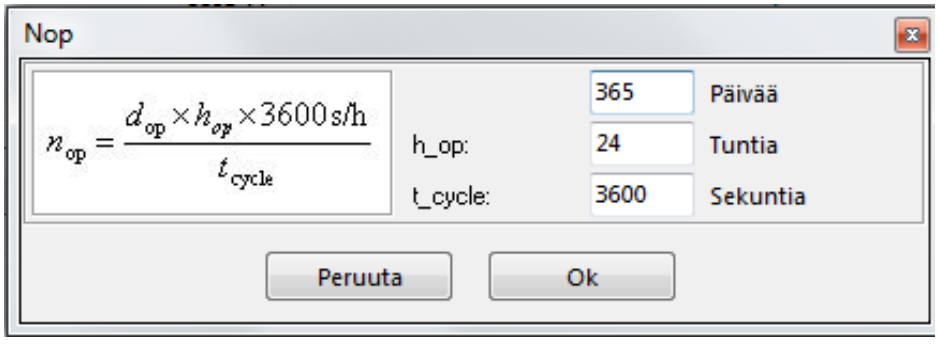


Kuva 43. Teknologian valitseminen elementille

Kuva 44. Komponenttien tyypilliset arvot



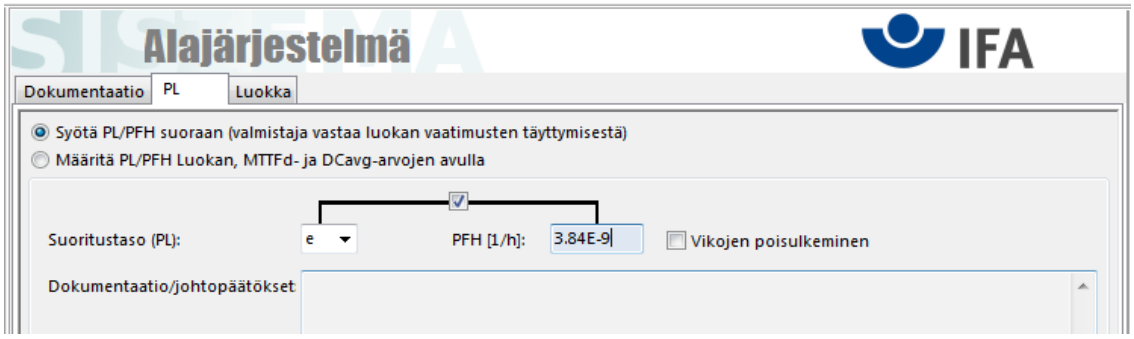
Kuva 45. Kontaktorille $B10_d$-arvon valitseminen



Kuva 46. N_{op}-arvon laskeminen

5.1.6 Taajuusmuuttaja

Lisätään laskelmaan kohdan 4.5.2 taajuusmuuttajakäytöt. Taajuusmuuttajien STO-tuloja ohjaavat releet syötetään laskelmaan muuten samoin kuin kohdan 5.1.5 kontaktorit. Annetaan releiden muodostamalla alajärjestelmälle tässä esimerkiksi nimeksi STO-releet. Tämän jälkeen lisätään taajuusmuuttaja laskelmaan nimellä ACS 880 ja syötetään sille suoraan valmistajan ilmoittamat PL- ja PFH-arvo (Kuva 47). Tällöin valmistaja vastaa taajuusmuuttajan luokan täyttymisestä.



Kuva 47. Taajuusmuuttajan lisääminen Sistema-laskelmaan

5.1.7 Hydrauliikka

Lisätään kohdan 4.5.7 hydrauliikan turvallisuuteen liittyvä ohjausjärjestelmä laskelmaan nimellä Hydrauliikka. Annetaan ko. alajärjestelmälle luokaksi 4 ja lisätään molempiin alajärjestelmän alle ilmestyviin kanaviin suuntaventtiilit. Kanavaan 1 suuntaventtiili 1V3 ja kanavaan 2 suuntaventtiili 1V4. Annetaan suuntaventtiilien elementeille nimeksi Kara. Elementtiä klikkaamalla päästään valitsemaan suuntaventtiilin teknologia, valitaan hydraulinen. Komponenttien tyypilliset arvot kohdasta valitaan ”hydrauliset komponentit”, joille on määritelty suoraa $MTTF_d$-arvo 150 vuotta. DC-arvoiksi voidaan valita DC-kirjastosta molemmille kohta ”suora valvonta”, joka antaa

Diagnostiikan kattavuudeksi 99 %. Tämän jälkeen arvioidaan vielä sovelletut toimenpiteet yhteisvikaantumisen välttämiseksi ja näin hydrauliikkaohjaus on lisätty laskelmaan.

5.1.8 Hätäseispainike

Valitaan jokin SFS-EN 60947-5-5 standardin mukaan valmistettu hätäpysäytyspainike Kyseisen standardin mukaan valmistetuille hätäpysäytyslaitteille sallitaan mekaanisten vikojen poissulkeminen, jos otetaan huomioon suuri käyttökertojen määrä. (SFS-EN ISO 13849-2, D.8.) Eli Sistemassa voidaan valita em. standardia noudattavalle hätäpysäytyspainikkeelle suoritustaso PL e ja PFH-arvoksi nolla.(Hauke 2012, 5.)

5.2 Turvatoiminnon suoritustaso

Vaadittu suoritustaso PL_r on d ja suoritustaso, johon päästään on myös PL d (kuva 48). Liitteessä 8 on lyhyt Sisteman antama raportti turvatoiminnolle asetettujen vaatimusten täyttymisestä.

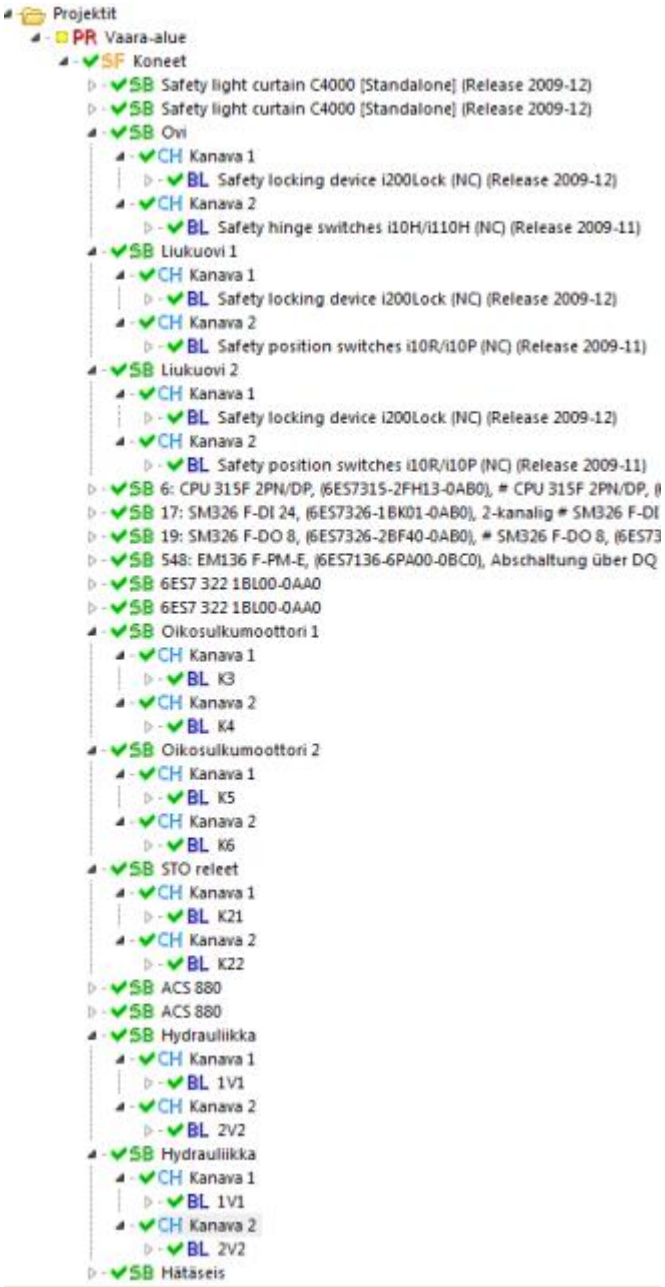
Koneet

PLr	d
PL	d
PFH [1/h]	8,72E-7

Kuva 48. Vaadittu ja saavutettu suoritustaso

5.3 Laskelman rakenne

Kuvassa 49 näkyy laskelmaan vaikuttavat alajärjestelmät ja niiden lohkot

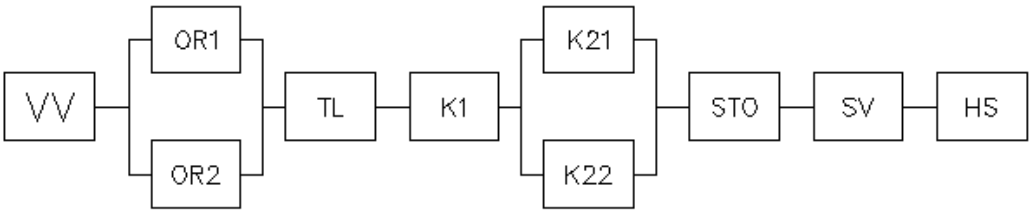


Kuva 49. Laskelmaan vaikuttavat alajärjestelmät ja niiden lohkot

5.4 Vaara-alue PL c

Lasketaan sama vaara-alue samoine laitteineen kuin kohdan 5.1 laskelmassa, mutta nyt vaara-alueen ohjausjärjestelmältä vaaditaan suoritustaso PL c. Esitetään turvallisuuteen liittyvä ohjausjärjestelmä lohkokaaviona ja lähdetään sen pohjalta tekemään Sistema-laskelmaa. Niin kuin nähdään, lohkokaavio yksinkertaistuu hieman kohdan 5.1 lohkokaaviosta. Lohkokaaviossa on esitetty kaikki vaara-alueella olevien turvatoimintojen- ja laitteiden komponentit vain yhteen kertaan.

Tässä luvussa esitetään esimerkkilaskut vain laitteista, joiden ohjausta muutetaan tähän luokkaan riittäväksi. Liitteessä 7 on tähän luokkaan erikseen suunnitellut piirikaaviot.



Kuvio 3. Turvallisuuteen liittyvä lohkokaavio

Kuvion 3 eri alajärjestemät ovat:
VV= valoverho
OR1,OR2= oven turvarajakytkimet
TL= turvalogiikan komponentit
K1= oikosulkumoottorin kontaktori
K21,K22= taajuusmuuttajan STO-tulojen releet
STO= Safety Torque Off
SV= suuntaventtiili
HS= hätäseispainike

5.4.1 Valoverho

Valitaan PL d suoritustason omaavat C2000 valoverhot SICKin komponenttikirjastosta.

5.4.2 Oikosulkumoottorit

Lisätään kohdan 4.5.4 mukaiset oikosulkumoottorit laskelmaan yksikanavaisena eli Oikosulkumoottoreille määritellään luokka 1. Samaan kanavaan lisätään kaikki hätäpysäytykseen osallistuvat kontaktorit (kuva 50). Tässä sovelluksessa moottoreita on kaksi, joiden kontaktorit ovat K1 ja K2. Varsinainen hätäseiskontaktori on turvalogiikan ohjaama K7. Määritellään kontaktorin luotettavuus samoin kuin luvussa 5.1.5 paitsi kontaktori K7, jolle valitaan B_{10d}-arvoksi ”kontaktorit pienellä kuormituksella”, sillä se toimii ohjausvirtapiirissä ja näin sen koskettimiin ei kohdistu suurta sähkövirran aiheuttamaa lämpörasitusta. Sistema ilmoittaa Oikosulkumoottorien pääsevän luokkaan PL c.

Kuva 50. Oikosulkumoottorien pysäytykseen osallistuvat lohkot

5.4.3 Hydrauliikka

Hydraulisylinterin ohjauksessa voidaan käyttää yhtä luotettavaa suuntaventtiiliä luvun 4.5.6 mukaisesti. Annetaan alajärjestelmän Hydrauliikka lohkolle nimeksi Suuntaventtiili ja lohkon elementille nimeksi Kara. Valitaan elementin teknologiaksi hydraulinen (kuva 51). $MTTF_d$-välilehdeltä valitaan ”komponenttien tyypilliset arvot” -painikkeen alta listalta Hydrauliset komponentit, joille on suoraa määritelty $MTTF_d$-arvoksi 150 vuotta (kuva 52). Näin kaikki tarvittavat määritykset on tehty kun DC- ja CCF- arvoja ei huomioida luokan 1 rakenteessa. Sistema ilmoittaa, että hydrauliikalla päästään näillä määrityksillä luokan 1 suoritustasoon PL c.

Kuva 51. Suuntaventtiilille teknologian valitseminen

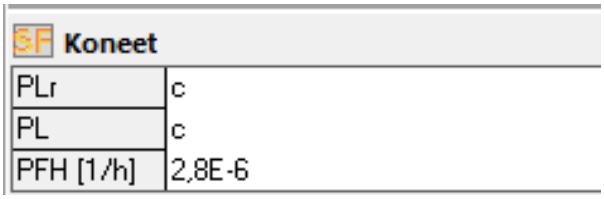
Kuva 52. Hydraulisten komponenttien $MTTF_d$-arvo

5.5 Turvatoiminnon suoritustaso

Kun kohdan 5.1 PL d suoritustason laskelma on muutettu vastaamaan PL c -suoritustason vaara-aluetta, niin Sistema näyttää, ettei edellä olevilla ratkaisuilla saada turvatoimintoa Koneet vastaamaan vaadittua suoritustasoa PL c vaan jäädään PL b:hen (kuva 53). Pitää siis tehdä jotakin järjestelmän luotettavuuden parantamiseksi.

Tehdään sellainen juttu, että parannetaan oikosulkumoottorien luotettavuus kohdan 5.1.5 tasolle. Eli tehdään oikosulkumoottorien ohjauksesta kaksi kanavainen. Em. toimenpiteen jälkeen saavutetaan vaadittu suoritustaso on PL c (Kuva 54). Liitteessä 9 on lyhyt Sisteman antama raportti turvatoiminnolle asetettujen vaatimusten täyttymisestä.

Kuva 53. Vaadittu ja saavutettu suoritustaso



Kuva 54. Luotettavuuden parantamisen jälkeen vaadittu ja saavutettu suoritustaso

5.6 Laskelman rakenne

Kuvassa 55 näkyy laskelmaan vaikuttavat alajärjestelmät ja niiden lohkot

Kuva 55. Laskelmaan vaikuttavat alajärjestelmät ja niiden lohkot

6 JOHTOPÄÄTÖKSET

Työn tavoitteena oli löytää ratkaisut sähköisten ohjausjärjestelmien toteuttamiseen erikseen tarkasteltaville laitteille. Ratkaisuja ja ratkaisuille tuotettuja mallilaskelmia on tarkoitus hyödyntää tilaajayrityksessä jatkossa.

Työhön ryhtyessäni tuli vastaan runsas tietotulva koneturvallisuusasiaa. Aluksi oli siksi tärkeää kerätä vain työhön liittyvät lähteet yhteen lähdekriittisyyttä missään vaiheessa unohtamatta. Muutaman kerran harhailin huonoissa tai väärissä tietoläteissä, mutta otin niistä opiksi. Hyviä lähteitä työssä alkuun pääsemiseksi sain työni ohjaajalta.

Sistema-laskelmien läpikäyminen kuvien ja kirjallisen selostuksen avulla oli hieman kankeaa ja aikaa vievää. Vastaavissa tapauksissa olisi varmasti monin kerroin parempi tapa videon avulla laskelmien läpikäyminen.

Sen lisäksi että opin tarkastelemaan koneiden ohjausjärjestelmiä turvallisuuden kannalta, opin paljon koneturvallisuudesta yleisesti ja sen tärkeydestä. Työstä teki mielenkiintoisen ja motivoivan se, että huomasi koko ajan kehittyvänsä työn edetessä, ja sai olla eri alojen asiantuntijoiden kanssa tekemisissä. Asiantuntijat auttoivat osaltaan työn etenemisessä ja heiltä sainkin arvokasta tietoa työn eteenpäin viemiseksi. Työssä sain myös tutustua nykyaikaisiin tietokoneohjelmiin, joita suunnittelijat työssään käyttävät. Tämä toi myös osaltaan ammatillista kasvua.

Työ oli erittäin mielenkiintoinen mahdollisuus tutustua aikaisemmin itselleni verrattain tuntemattomaan koneturvallisuuteen. Toivon, että saisin tulevaisuudessa työskennellä vielä koneturvallisuuden parissa.

LÄHTEET

ABB industrial drive. ACS 880, single drive –taajuusmuuttajat 0,55-250 kW. Tuoteluettelo.Viitattu9.12.2014. http://www.auser.fi/data/attachments/ACS880%20esite%202014.pdf

Hauke M. 2008. BGIA Report 2/2008e. Berlin: DGUV. Viitatu 24.11.2014. http://www.dguv.de/medien/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf

Hauke, M. 2012, The SISTEMA Cookbook 4. Berlin: DGUV. Viitattu 24.11.2014. http://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook4_en.pdf

Hietikko M, Malm T ja Alanen J 2009. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen. Viitattu 14.12.2014. http://www.vtt.fi/inf/pdf/tiedotteet/2009/T2485.pdf

ISO/TR 14121-2:2012. Koneturvallisuus. Riskin arviointi. Osa 2: käytännön opastusta ja esimerkkejä menetelmistä. Suomen standardoimisliitto SFS. Helsinki: SFS. Viitattu 24.11. http://www.sfs.fi

Koneasetus.2008. A12.6.2008/400.Viitattu9.12.2014. http://www.finlex.fi/fi/laki/ajantasa/2008/20080400

Rantanen, P. 2012. Koneen hätäpysäytysjärjestelmä, vaatimustenmukaisuuden osoittaminen. Esimerkkitapaus SFS-EN ISO 13849-1 mukaisesti. Oppimateriaali. Saatavilla Samkin Moodlessa.

Rantanen, P. 2014. Tuotepäällikkö, SICK Oy. Turku. Henkilökohtainen tiedonanto 25.8.2014.

Rantanen, P. 2014. Tuotepäällikkö, SICK Oy. Turku. Henkilökohtainen tiedonanto 10.10.2014.

Raumaster Oy:n www-sivut. 2014. Viitattu 23.6. http://www.raumaster.fi

SFS-EN ISO 10218-1. Robots and robotic devices. Safety requirements for industrial robots. Part 1: Robots (ISO 120218-1:2011). 2011. Finnish Standards Association SFS. Helsinki: SFS. Viitattu 24.11.2014. http://www.sfs.fi/

SFS-EN ISO 12100. Safety of machinery. General principles for design. Risk assessment and risk reduction (ISO 12100:2010). 2010. Finnish Standards Association SFS. Helsinki: SFS. Viitattu 24.11.2014. http://www.sfs.fi/

SFS-EN ISO 13849-1. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design (ISO 13849-1:2006). 2008. Finnish Standards Association SFS. Helsinki: SFS

SFS-EN ISO 13849-2. Safety of machinery. Safety-related parts of control system. Part 2: Validation (ISO 13849-2:2012). 2012. Finnish Standards Association SFS. Helsinki: SFS. Viitattu 24.11.2014. http://www.sfs.fi/

SFS-EN ISO 14119. Safety of machinery. Interlocking devices associated with guards. Principles for design and selection. (ISO 14119:2013). 2013. Finnish Standards Association SFS. Helsinki: SFS. Viitattu 24.11.2014. http://www.sfs.fi/

SICK Oy:n www-sivut. 2014. Viitattu 7.9.2014. http://www.sick.com/fi

Siirilä, T. 2008. Koneturvallisuus, EU:n direktiivien ja standardien soveltaminen käytännössä. Keuruu: Otavan Kirjapaino Oy.

Siirilä, T. 2009. Koneturvallisuus, Ohjausjärjestelmät ja turvalaitteet. Keuruu: Otavan Kirjapaino Oy.

Siirilä,T.2013. Suojusten kytkentä koneen toimintaan: Metsta, 27-28, 33. Viitattu 24.11.2014.http://www.metsta.fi/www/koneturvallisuuden_teemasivut/artikkelit/2013_nro_011.pdf

Sundcon Oy:n www-sivut. 2014. Viittattu 18.11.2014. http://www.sundcon.fi/
Sundquist, M. Ohjelmatyökalun Sistema käyttö koneiden turvatoimintojen suunnittelussa. Metsta, 11. Viitattu 24.11.2014. http://www.metsta.fi/www/koneturvallisuuden_teemasivut/artikkelit/2010_nro_004.pdf

Suvela,T. 2010. Luentoaineisto: SFS-EN ISO 13849-1 koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa: yleiset suunnitteluperiaatteet. Saavilla Samkin Moodlessa.

Taulukko D.1 Turvallisuuden perusperiaatteet

Turvallisuuden perusperiaate	Huomautuksia
Sopivien materiaalien ja soveltuvien valmistustapojen käyttö	Valitaan materiaali, valmistustavat ja käsittelymenetelmät suhteessa esim. kuormitukseen, kestävyyteen, joustavuuteen, kitkaan, kulumiseen, korroosioon, lämpötilaan, johtavuuteen ja eristelujuuteen.
Oikea mitoitus ja muotoilu	Otettava huomioon esim. kuormitus, jännitys, väsyminen, pinnankarheus, toleranssit ja valmistus.
Komponenttien ja/tai järjestelmän oikea valinta, yhdistely, järjestelyt, kokoonpano ja asennus	Sovelletaan valmistajan antamia käyttöön soveltamista koskevia ohjeita esim. tuoteluettelo, asennusohjeet, määrittelyt, ja noudatetaan hyvää insinöörikäytäntöä.
Oikeanlainen suojamaadoitus	Ohjauspiirin yksi puoli, kunkin sähkömagneettisen laitteen ohjauskelan tai muun sähkölaitteen yksi liitin yhdistetään suojamaadoituspiiriin (IEC 60204-1:2005 kohta 9.4.3.1).
Eristyksen valvonta	Käytetään eristyksen valvontalaitetta, joka joko ilmoittaa maasulusta tai erottaa virtapiirin automaattisesti maasulun tapahduttua (IEC 602041:2005 kohta 6.3.3).

(*jatkuu*)

Taulukko D.1 (*päättyy*)

Turvallisuuden perusperiaate	Huomautuksia
Energiattomaksi tekemisen soveltaminen	Turvallinen tila saavutetaan kytkemällä kaikki asianomaiset laitteet jännitteettömiksi esim. käyttämällä tuloissa avautuvia koskettimia (painikkeet ja asemantuntokytkimet) ja käyttämällä releissä sulkeutuvia koskettimia (ks. myös ISO 12100:2010 kohta 6.2.11.3). Joissain sovelluksissa voi esiintyä poikkeuksia, esim. kun sähkön syötön katkeaminen aiheuttaa lisävaaran. Järjestelmän turvallisen tilan saavuttamiseen voidaan tarvita aikaviivetoimintoja (ks. IEC 60204-1:2005, kohta 9.2.2).
Jännitepiikkien vaimennus	Käytetään vaimennuskomponentteja (RC-piiri, diodi, varistori) kytkettynä rinnakkain kuorman kanssa, mutta ei rinnakkain koskettimien kanssa. HUOM. Diodi pidentää POIS-kytkennän aikaa.
Vasteajan lyhentäminen	Minimoidaan tehonsyötön kytkentäkomponenttien viive.
Yhteensopivuus	Käytetään komponentteja, jotka ovat yhteensopivia käytettävän jännitteen ja virran kanssa.
Ympäristöolosuhteiden sieto	Laite suunnitellaan siten, että se kykenee toimimaan kaikissa odotettavissa olevissa ympäristöissä ja missä tahansa ennakoitavissa olevissa epäsuotuisissa olosuhteissa, esim. lämpötila, kosteus, tärinä ja sähkömagneettinen häiriö (EMI, ks. kohta 10).
Tuloihin liitettävien laitteiden kiinnityksen varmistus	Varmistetaan tuloihin liitettävien laitteiden, esim. toimintaankytkennän kytkimien, asemantuntokytkimien, rajakytkimien ja lähestymiskytkimien kiinnitys siten, että niiden asema, kohdistus ja kytkentätoleranssi säilyvät kaikissa ennakoiduissa olosuhteissa, esim. tärinä, tavanomainen kuluminen, vieraiden esineiden sisäänpääsy ja lämpötila. Katso ISO 14119:1998 kohta 5.
Odottamattomalta käynnistymiseltä suojautuminen	Estetään odottamaton käynnistyminen esimerkiksi tehonsyötön palautumisen jälkeen (ks. standardit ISO 12100:2010 kohta 6.2.11.4, ISO 14118 ja IEC 60204-1).
Ohjauspiirin suojaaminen	Ohjauspiiri suojataan standardin IEC 60204:-1:2005 kohtien 7.2 ja 9.1.1 mukaisesti.
Sarjamuotoinen kytkentä redundanttisia signaaleja muodostavalle kosketinpiirille	Molempien koskettimien kiinnihitsautumisen aiheuttaman yhteisvikaantumisen välttämiseksi niiden kytkeminen päälle ja pois päältä ei saa tapahtua samanaikaisesti, vaan toisen koskettimen on aina kytkeydyttävä ilman virtaa.

Taulukko D.3 Hyvin koetellut komponentit

Hyvin koeteltu komponentti	Lisäehdot käsitteelle "hyvin koeteltu"	Standardi
Pakko-ohjattu (pakkoavautuva) kytkin, esim. — painike — asemantuntokytkin — ohjauskappaleella vaikutettava valintakytkin, esim. toimintatavan valintaan	–	IEC 60947-5-1:2003, liite K
Hätäpysäytyslaite	–	ISO 13850 IEC 60947-5-5
Sulake	–	IEC 60269-1
Katkaisija	–	IEC 60947-2
Katkaisijat, erottimet	–	IEC 60947-3
Vikavirtasuojakatkaisija/RCD (jäännösvirran tunnistin)	–	IEC 60947-2:2006, liite B

(*jatkuu*)

Taulukko D.3 (*jatkuu*)

Hyvin koeteltu komponentti	Lisäehdot käsitteelle "hyvin koeteltu"	Standardi
Pääkontaktori	Komponentti on hyvin koeteltu vain jos a) muut vaikutukset otetaan huomioon, esim. tärinä b) vikaantuminen vältetään sopivien menetelmien, esim. ylimitoittamisen avulla (ks. taulukko D.2) c) tehonsyöttöä kuormaan rajoitetaan ylikuumenemissuojauksen avulla ja d) piirit on suojattu suojalaitteella ylikuormituksen estämiseksi. HUOM. Vikojen poissulkeminen ei ole mahdollista.	IEC 60947-4-1
Ohjaus- ja suojakytkinlaitteet tai välineet	–	IEC 60947-6-2
Apukontaktori (esim. relekontaktori)	Komponentti on hyvin koeteltu vain jos a) muut vaikutukset otetaan huomioon, esim. tärinä b) toiminta tapahtuu pakkotoimisesti c) vikaantuminen vältetään sopivien menetelmien, esim. ylimitoittamisen avulla (ks. taulukko D.2) d) koskettimissa kulkeva virta rajoitetaan sulakkeella tai katkaisijalla koskettimien kiinnihitsautumisen välttämiseksi ja e) valvontaan käytettävät koskettimet ovat mekaanisesti pakko-ohjattuja. HUOM. Vikojen poissulkeminen ei ole mahdollista.	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001 liite F
Rele	Komponentti on hyvin koeteltu vain jos a) muut vaikutukset otetaan huomioon, esim. tärinä b) toimintaankytkentä tapahtuu pakkotoimisesti c) vikaantuminen vältetään soveltuvien menetelmien, esim. ylimitoittamisen avulla (ks. taulukko D.2) ja d) koskettimissa kulkeva virta rajoitetaan sulakkeella tai katkaisijalla koskettimien kiinnihitsautuminen välttämiseksi. HUOM. Vikojen poissulkeminen ei ole mahdollista.	IEC 61810-1 IEC 61810-2
Muuntaja	–	IEC 61558
Kaapeli	Koteloinnin ulkopuolella oleva kaapelointi olisi suojattava mekaaniselta vaurioitumiselta (mukaan lukien esim. tärinä tai taipuminen).	IEC 60204-1:2005, kohta 12

(*jatkuu*)

Taulukko D.2 Hyvin koetellut turvallisuusperiaatteet

Hyvin koeteltu turvallisuusperiaate	Huomautus
Koskettimet ovat mekaanisesti pakkotoimisia	Käytetään mekaanisesti pakkotoimisia koskettimia, esim. valvontatoiminnoissa luokkien 2, 3 ja 4 järjestelmissä (ks. EN 50205, IEC 60947-4-1:2001, liite F, IEC 60947-5-1:2003 + A1:2009, liite L).
Kaapelivikojen välttäminen	Käytetään kahden vierekkäisen johtimen välisen oikosulun välttämiseksi joko — kaapelia, jossa on suojavaippa ja jonka jokainen johdin on kytketty suojamaadoituspiiriin, tai — litteissä kaapeleissa yhtä maadoitettua johdinta jokaisen signaalijohtimen välissä.
Erotusetäisyys	Käytetään riittävää etäisyyttä liittimien, komponenttien ja johdotuksen välillä tarkoittamattomien kosketusten välttämiseksi.
Energian rajoittaminen	Käytetään kondensaattoria rajallisen energiamäärän syöttämiseksi, esim. ajastinsovelluksessa.

(*jatkuu*)

Taulukko D.2 (*päättyy*)

Hyvin koeteltu turvallisuusperiaate	Huomautus
Sähköisten muuttujien rajoittaminen	Vaaralliseen tilan välttämiseksi rajoitetaan jännitettä, virtaa, energiaa tai taajuutta liikkeen rajoittamiseksi, esim. vääntömomentin rajoittamiseksi, pakkokäyttöisen ohjaimen aikaan saaman liikkeen matkan ja/tai ajan rajoittamiseksi tai nopeuden vähentämiseksi.
Määrittelemättömien tilojen välttäminen	Ohjausjärjestelmässä on vältettävä määrittelemättömiä tiloja. Ohjausjärjestelmä suunnitellaan ja rakennetaan siten, että sen tila, esim. lähdöt, voidaan ennakoida tavanomaisen käytön aikana ja kaikissa odotettavissa olevissa käyttöolosuhteissa.
Pakkotoimisuus	Ohjaus suoraan mekaanisen voiman vaikutuksella ilman joustavia elementtejä, esim. ilman jousta ohjauskappaleen ja koskettimien välissä (ks. ISO 14119:1998 kohta 5.1 ja ISO 12100:2010 kohta 6.2.5).
Vikaantumistavan suuntaaminen	Aina kun mahdollista, laitteen ja/tai piirin olisi vikaannuttava turvalliseen tilaan tai olosuhteeseen.
Vikaantumisen suuntaaminen	Tietyllä tavalla vikaantuessa suuntautuvia komponentteja tai järjestelmiä olisi käytettävä silloin kun se käytännöllistä (ks. ISO 12100:2010, kohta 6.2.12.3).
Ylimitoittaminen	Turvapiireissä käytettävien komponenttien kuormitusta pienennetään esim. seuraavilla keinoilla: — kytkettyjen koskettimien läpi kulkevan virran olisi oltava alle puolet niiden nimellisvirrasta — komponenttien kytkentätaajuuden olisi oltava alle puolet niiden mitoitusarvosta — odotettavissa olevien kytkentätoimintojen määrän olisi oltava enintään 10 % laitteen sähköisestä kestävyydestä. HUOM. Kuormituksen pienentäminen voi riippua suunnitteluperusteista.
Minimoidaan vikaantumisen mahdollisuus	Turvallisuuteen liittyvät toiminnot erotetaan muista toiminnoista.
Tasapaino monimutkaisuuden ja/tai yksinkertaisuuden välillä	Seuraavien tekijöiden välillä olisi saavutettava tasapaino — monimutkaisuus pyrittäessä parempaan ohjaukseen — yksinkertaistaminen pyrittäessä parempaan luotettavuuteen.

Taulukko E.1 Esimerkkejä diagnostiikan kattavuudesta

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

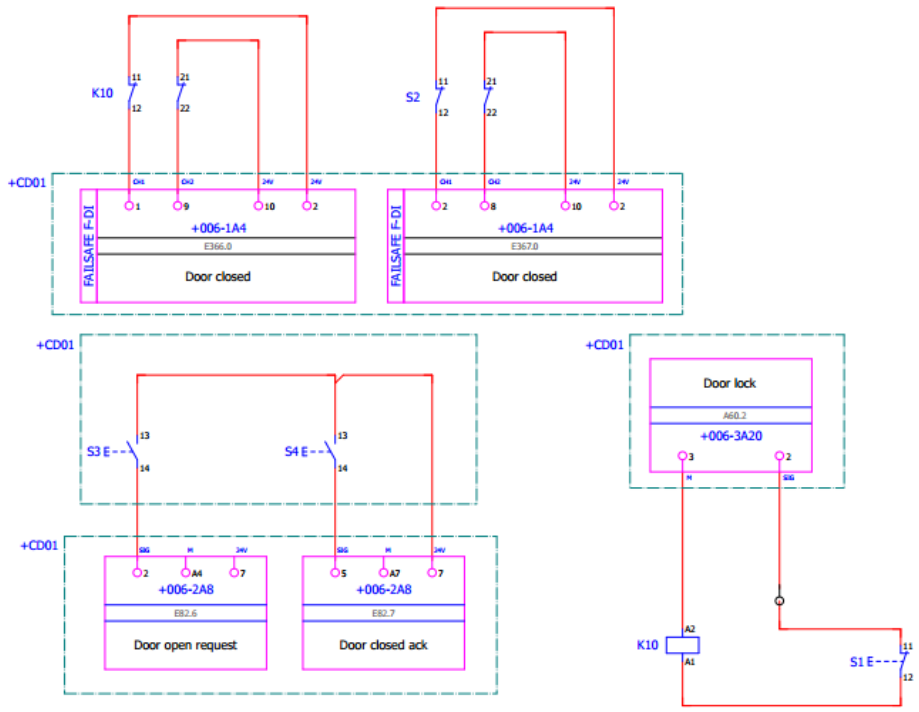
Taulukko E.1 (jatkuu)

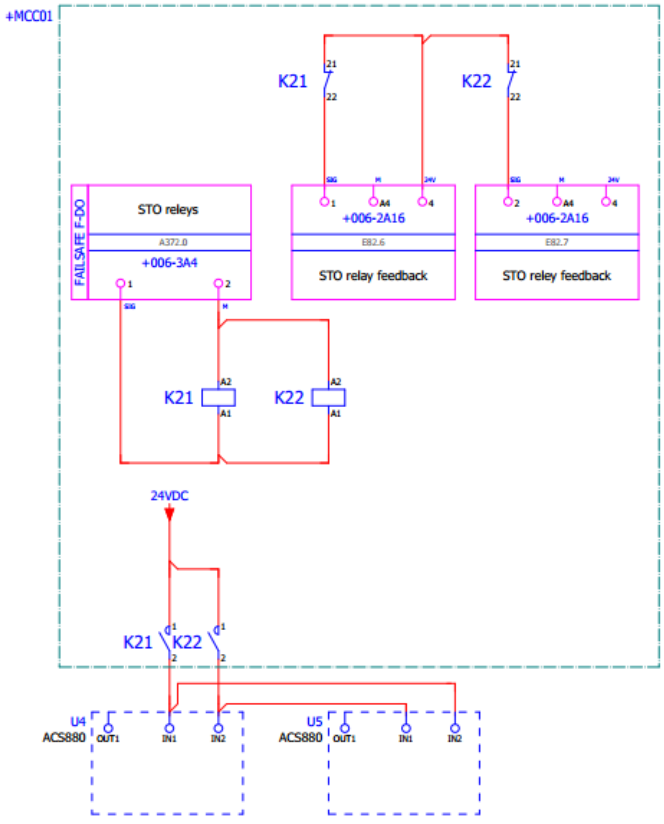
Toimenpide	**Diagnostiikan kattavuus (DC)**
Logiikka	
Epäsuora valvonta (esim. painekytkimen suorittama valvonta, toimilaitteiden aseman sähköinen valvonta)	90...99 % sovelluksesta riippuen
Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti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

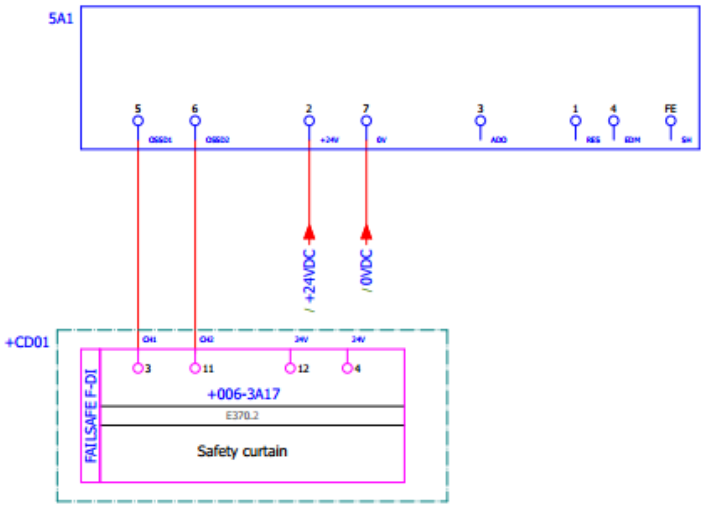
Taulukko E.1 (jatkuu)

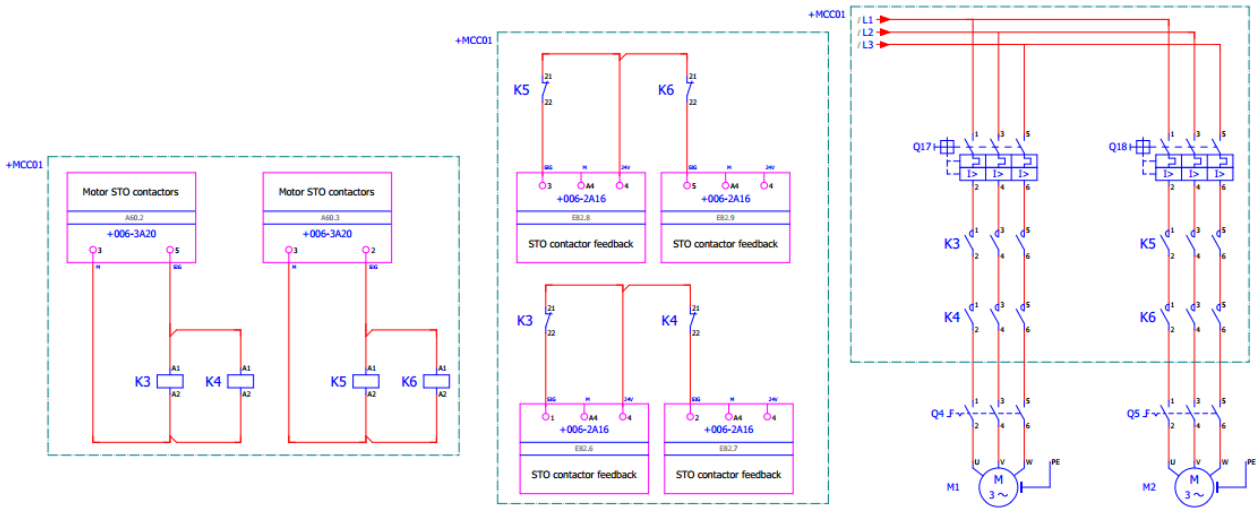
Toimenpide	**Diagnostiikan kattavuus (DC)**
Lähtöyksikkö	
Yhden kanavan lähtöjen valvonta ilman dynaamista testausta	0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan signaalia
Lähtöjen ristiinvalvonta ilman dynaamista testausta	0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan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

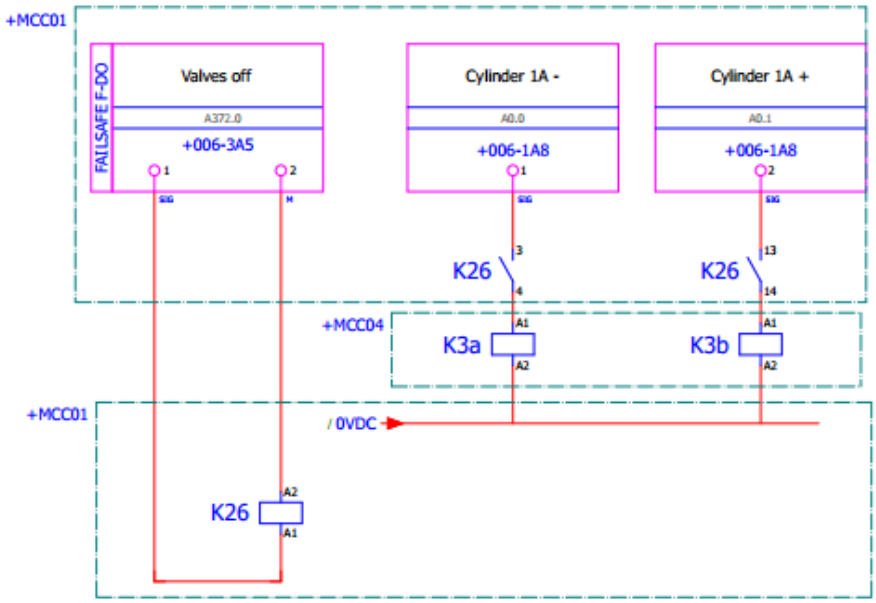
Nro	Kohde	Ohjauspiirin pisteet	Saavutettavissa olevat suurimmat pisteet
1	**Erottelu/Erottaminen**		
	Signaalireittien fyysinen erottaminen	15	15
2	**Erilaisuus (diversiteetti)**		
	Erilaisten teknologioiden, toteutustapojen tai fyysisten periaatteiden käyttö	20	20
3	**Suunnittelu, soveltaminen ja käyttökokemukset**		
3.1	Suojaustoimenpiteet ylijännitteelle, ylipaineelle, ylivirralle jne.	Ei lainkaan	15
3.2	Käytetyt komponentit ovat hyvin koeteltuja	5	5
4	**Arviointi ja analyysit**		
	Onko vika- ja vaikutusanalyysin tulokset otettu huomioon toteutuksessa yhteisvikaantumisten estämiseksi?	5	5
5	**Pätevyys ja koulutus**		
	Onko suunnittelu- ja ylläpitohenkilöstö koulutettu ymmärtämään yhteisvikaantumisten syyt ja seuraukset?	Ei lainkaan	5
6	**Ympäristöolosuhteet**		
6.1	Likaantumisen estäminen ja sähkömagneettinen yhteensopivuus yhteisvikaantumisten estämiseksi soveltuvien standardien mukaisesti	25	25
6.2	**Muut vaikutukset** Onko kaikkien asiaankuuluvien ympäristövaikutusten sietokyky otettu huomioon kuten lämpötila, iskut, tärinä, kosteus (asiaankuuluvien standardien erittelyn mukaisesti?	10	10
	Yhteensä	80	Max. 100

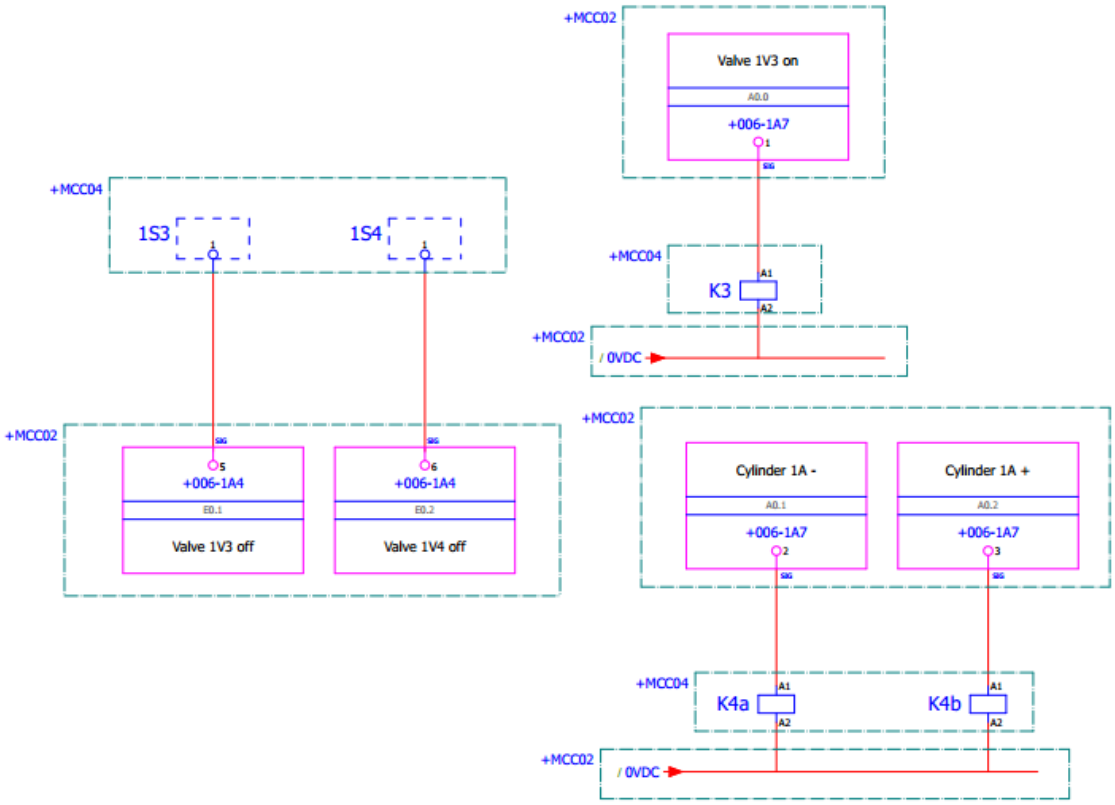

K10
S2
+CD01
FAILSAFE F-DI
+006-1A4
E366.0
Door closed
E367.0
Door closed
S3 E
S4 E
+006-2A8
E82.6
Door open request
E82.7
Door closed ack
Door lock
A60.2
+006-3A20
K10
S1 E

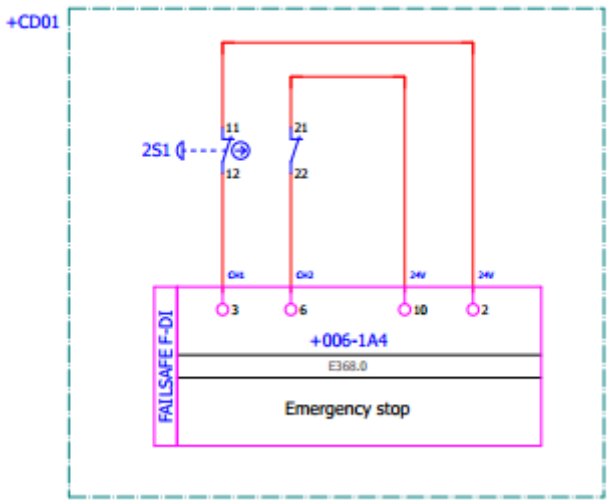

+MCC01
K21
K22
FAILSAFE F-DO
STO releys
A372.0
+006-3A4
+006-2A16
E82.6
STO relay feedback
E82.7
STO releay feedback
24VDC
U4
ACS880
U5
ACS880
OUT1
IN1
IN2

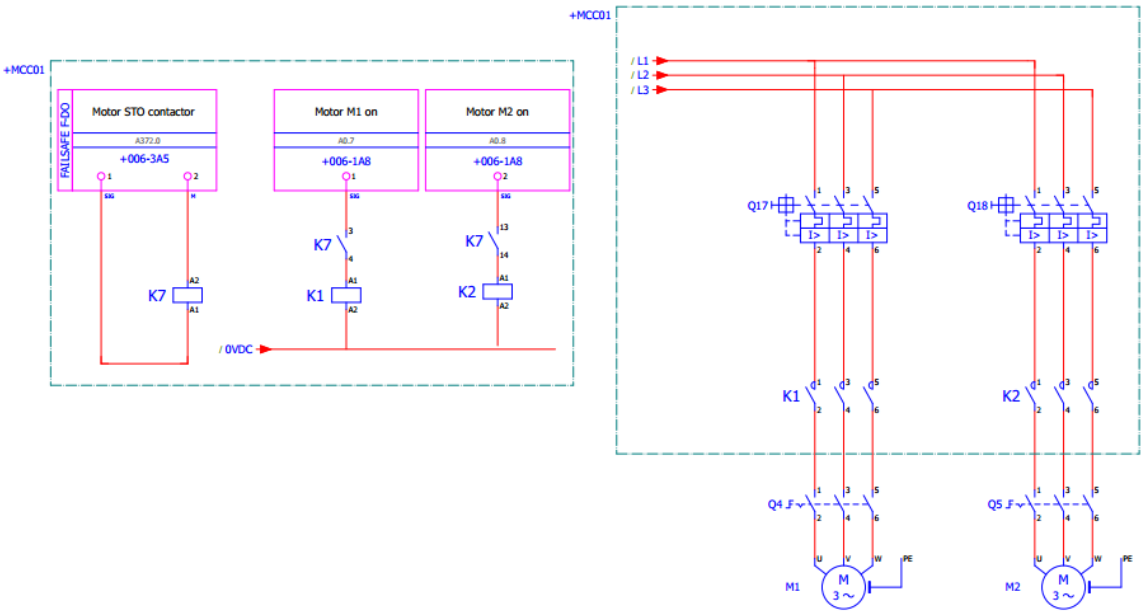

5A1
5
6
2
7
3
1
4
FE
+24VDC
0VDC
+CD01
3
11
12
4
+006-3A17
E370.2
Safety curtain
FAILSAFE F-DI

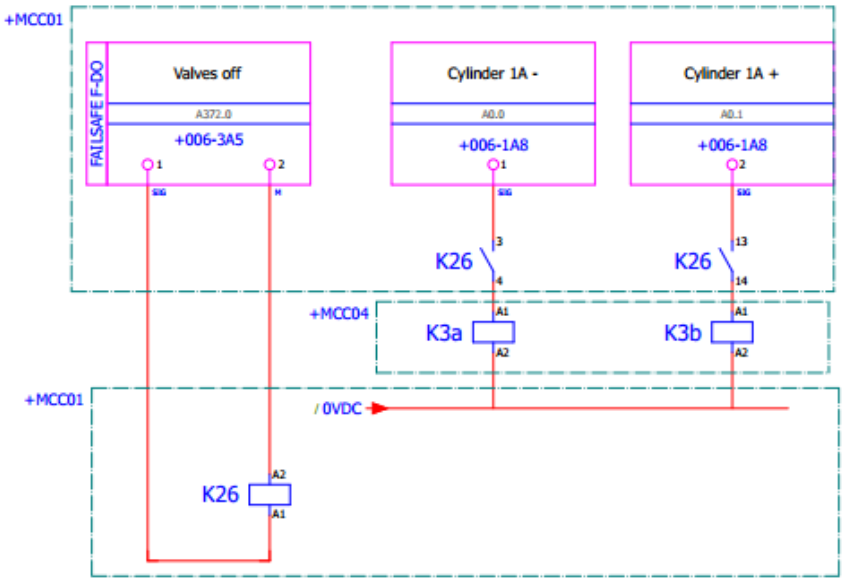

+MCC01
Motor STO contactors
A60.2
+006-3A20
Motor STO contactors
A60.3
+006-3A20
K3
K4
K5
K6
+MCC01
K5
K6
+006-2A16
EB2.8
STO contactor feedback
+006-2A16
EB2.9
STO contactor feedback
K3
K4
+006-2A16
EB2.6
STO contactor feedback
+006-2A16
EB2.7
STO contactor feedback
+MCC01
L1
L2
L3
Q17
Q18
K3
K4
K5
K6
Q4
Q5
M1
M2
PE


+MCC01
FAILSAFE F-DO
Valves off
A372.0
+006-3A5
1
2
Cylinder 1A -
A0.0
+006-1A8
1
Cylinder 1A +
A0.1
+006-1A8
2
3
K26
4
13
K26
14
+MCC04
A1
K3a
A2
A1
K3b
A2
+MCC01
/ 0VDC
A2
K26
A1


+MCC02
Valve 1V3 on
A0.0
+006-1A7
1
+MCC04
1S3
1
1S4
1
+MCC04
K3
A1
A2
+MCC02
/ 0VDC
+MCC02
5
+006-1A4
E0.1
Valve 1V3 off
6
+006-1A4
E0.2
Valve 1V4 off
+MCC02
Cylinder 1A -
A0.1
+006-1A7
2
Cylinder 1A +
A0.2
+006-1A7
3
+MCC04
K4a
A1
A2
K4b
A1
A2
+MCC02
/ 0VDC


+CD01
2S1
11
12
21
22
DI1
DI2
24V
24V
3
6
10
2
FAILSAFE F-DI
+006-1A4
E368.0
Emergency stop


+MCC01
FAILSAFE F-DO
Motor STO contactor
A372.0
+006-3A5
Motor M1 on
A0.7
+006-1A8
Motor M2 on
A0.8
+006-1A8
K7
K7
K1
K2
/ 0VDC
+MCC01
/ L1
/ L2
/ L3
Q17
Q18
K1
K2
Q4
Q5
M1
M2
M
3 ~
PE


+MCC01
FAILSAFE F-DO
Valves off
A372.0
+006-3A5
Cylinder 1A -
A0.0
+006-1A8
Cylinder 1A +
A0.1
+006-1A8
K26
K26
+MCC04
K3a
K3b
+MCC01
/ 0VDC
K26

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Vaara-alue

Tiedoston päiväys: 24.11.2014 Raportin päiväys: 24.11.2014 Tarkistussumma: 09d76fb3749d2307e5c149553f8e9602

PR Projektin nimi: Vaara-alue

Tekijä:	Joona
Vaarallinen kohta/kone:	
Dokumentaatio:	
Dokumentti:	
Tiedoston nimi:	F:\Opinnäytetyö 2014\Vaara-alue oppariin.ssm
Ohjelmistonversio:	1.1.6
Standardin versio:	ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008
Tarkistussumma:	09d76fb3749d2307e5c149553f8e9602
Asetukset:	☑ Käytä DC:n väliarvoja PFH:n laskentaan (tarkempi). ☐ Nosta MTTFd-arvon yläraja 100 vuodesta 2500 vuoteen luokassa 4
Tila:	vihreä
Huomautus:	Tähän projektiin (tai siihen kuuluviin peruselementteihin) ei ole merkitty yhtään varoitusta.

Tähän kuuluvat turvatoiminnot

SF Nimi: Koneet

Vaadittu: PLr d | Saavutettu: PL d | PFH [1/h]: 8,72E-7 | Tila: vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Vaara-alue

Tiedoston päiväys: 22.11.2014 Raportin päiväys: 24.11.2014 Tarkistussumma: b62131c0e4fb87dc4a6706ce039cdb65

PR Projektin nimi: Vaara-alue

Tekijä:	Joona
Vaarallinen kohta/kone:	
Dokumentaatio:	
Dokumentti:	
Tiedoston nimi:	C:\Users\Joona\Google Drive\Vaara-alue oppariin.ssm
Ohjelmiston versio:	1.1.6
Standardin versio:	ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008
Tarkistussumma:	b62131c0e4fb87dc4a6706ce039cdb65
Asetukset:	☑ Käytä DC:n väliarvoja PFH:n laskentaan (tarkempi). ☐ Nosta MTTFd-arvon yläraja 100 vuodesta 2500 vuoteen luokassa 4
Tila:	vihreä
Huomautus:	Tähän projektiin (tai siihen kuuluviin peruselementteihin) ei ole merkitty yhtään varoitusta.

Tähänkuuluvatturvatoiminnot

SF Nimi:Koneet

Vaadittu: PLr c | Saavutettu: PL c | PFH [1/h]: 2,8E-6 | Tila: vihreä