Mikko Vähäjylkkä

KONETURVALLISUUS OSANA SÄHKÖSUUNNITTELUA

Opinnäytetyö

CENTRIA AMMATTIKORKEAKOULU

Sähkötekniikka

Kesäkuu 2013

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Yksikkö Ylivieskan yksikkö	**Aika** Kesäkuu 2013	**Tekijä/tekijät** Mikko Vähäjylkkä
Koulutusohjelma Sähkötekniikan koulutusohjelma		
Työn nimi KONETURVALLISUUS OSANA SÄHKÖSUUNNITTELUA		
Työn ohjaaja Jari Halme		**Sivumäärä** 47 + 20
Työelämäohjaaja Ilkka Sikala		

Tämä insinöörityö toteutettiin Apex Automation Oy:lle, joka on Kokkolan seudun johtava energia- ja teollisuusalojen automaatio- ja sähkösuunnittelupalveluita tarjoava suunnittelutoimisto. Yritys on perustettu vuonna 1993, ja siitä on vuosien saatossa kehittynyt yksi alansa merkittävä toimija.

Työn aiheena oli selvittää koneiden sähkösuunnittelun kannalta olennaisia vaatimuksia koneen ohjausjärjestelmälle ja sähkölaitteistoille. Tavoitteena oli tuottaa mallipiirejä turvallisuuteen liittyvän ohjausjärjestelmän toteuttamiseksi, sekä laatia vaiheittainen ohjeistus turvapiirien todentamisesta Sistema-ohjelmistotyökalulla.

Opinnäytetyössä perehdyttiin ohjausjärjestelmiä käsitteleviin standardeihin, alan kirjallisuuteen ja Sistema-ohjelmistoon, joiden perusteella mallipiirit ja ohjelmiston käytön vaiheittainen ohjeistus laadittiin.

Insinöörityön kirjallisen osuuden tarkoitus on ohjeistaa yrityksen uusia sähkösuunnittelijoita turvallisuuteen liittyvän ohjausjärjestelmän suunnittelussa ja todentamisessa.

Asiasanat
Koneturvallisuus, Ohjausjärjestelmä, Sistema, Suoritustaso, Sähkösuunnittelu

ABSTRACT

CENTRIA UNIVERSITY OF APPLIED SCIENCES	Date June 2013	Author Mikko Vähäjylkkä
Degree programme Electrical engineering		
Name of thesis MACHINE SAFETY AS PART OF THE ELECTRICAL DESIGN PROCESS		
Instructor Jari Halme		**Pages** 47 + 20
Supervisor Ilkka Sikala		

This thesis was commissioned by Apex Automation Oy, which is a leading engineering office providing automation and electrical design services for industry and energy-related businesses operating in Kokkola area. The company was founded in 1993 and it has developed into one of the major operators over the years.

The subject of the thesis was to find out the requirements for machine control system and electrical equipment that are essential for electrical design. The aim was to provide models for the circuit diagrams in order to create a safety-related control system. In addition, the objective was to draw up step by step instructions for the verification of safety circuits using Sistema software.

The thesis deals focused on standards related to process control systems, field-specific literature and Sistema software on the basis of which the model circuits and the step-by-step instructions for using the software were created.

The written part of the thesis text is intended to instruct the company's new electrical designers in designing and verifying safety-related control systems.

Key words
Control system, Electrical design, Performance level , Safety of machinery, Sistema

KÄSITTEIDEN MÄÄRITTELY

B10d	Laitevalmistajan ilmoittama toimintakertojen määrä, jonka jälkeen 10% komponenteista vikaantuu vaarallisesti.
CCF	*Common Cause Failure*; yhteisvikaatuminen. Yhden alkusyyn aiheuttama vika, joka vaikuttaa useampaan komponenttiin.
DCavg	*Diagnostic Coverage average*; diagnostiikan kattavuuden keskiarvo, joka määrittelee ohjausjärjestelmän kyvyn havaita järjestelmän eri komponenteissa olevat viat.
EY	Euroopan yhteisö; nykyään osa Euroopan Unionia.
MTTFd	*Mean Time To dangerous Failure*; vaarallinen keskimääräinen vikaantumisaika vuosina. Odotettavissa oleva aika ohjausjärjestelmän komponentin tai kanavan vaarallisen vikaantumisen esiintymiseen.
PFH	*Probability of a dangerous random hardware Failure per Hour*; Vaarallisen keskimääräisen vikaantumisajan todennäköisyys tuntia kohden. Suoritustasot määrittävä arvo.
PL	*Performance level*; suoritustaso. Erillinen taso, jota käytetään määrittelemään turvallisuuteen liittyvän ohjausjärjestelmän osien kyky suorittaa turvatoiminto ennakoitavissa olosuhteissa.
PLr	*required Performance level*; Turvallisuuteen liittyvältä ohjausjärjestelmältä vaadittu suoritustaso, jolla on tarkoitus saavuttaa riskien arvioinnissa vaadittu riskin pienentäminen.
SIL	*Safety Integrity Level*; turvallisuuden eheyden taso. Standardien SFS-IEC 61508 ja SFS-EN 62061 määrittelemä turvallisuustaso.
STO	*Safe Torque Off*; Turvatoiminto, jolla voidaan estää koneen käynnistyminen odottamattomasti tai vahingossa.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO 1

2 APEX AUTOMATION OY 3

3 KONETURVALLISUUS 4
3.1 Koneiden sähkölaitteistot 4
3.2 Ohjausjärjestelmän toiminta 5
3.2.1 Koneen käynnistäminen 5
3.2.2 Koneen pysäyttäminen 6
3.2.3 Hätäpysäytys 8
3.2.4 Pysäytysvyöhykkeet 9
3.3 Riskien arviointi 11
3.4 Turvalaitteen valinta 13
3.5 Ohjausjärjestelmän luokittelu 16

4 TURVAPIIRIN SUUNNITTELU JA TODENTAMINEN 20
4.1 Turvapiirin suunnittelu 20
4.2 Turvapiirin valvontalaitteet 24
4.3 Vaarallisten liikkeiden pysäyttäminen 26
4.3.1 Suora moottorilähtö 26
4.3.2 Taajuusmuuttajalla ohjattu moottori 27
4.3.3 Turvataajuusmuuttajalla ohjattu moottori 28
4.3.4 Venttiiliohjaukset 29
4.4 Sistema-ohjelmistotyökalu 31
4.5 Turvapiirin todentaminen Sistema-ohjelmistotyökalulla 35
4.5.1 Valoverho 37
4.5.2 Turvarele 38
4.5.3 Turvakäyttöön hyväksytty rele 38
4.5.4 Taajuusmuuttaja 43

5 JOHTOPÄÄTÖKSET JA POHDINTA 45

LÄHTEET 46
LIITTEET

KUVIOT

KUVIO 1. Pysäytysluokat ja niiden ominaisuudet 7

KUVIO 2. Kahden turvavyöhykkeen välinen valvonta passivoitavalla valoverholla 10

KUVIO 3. Esimerkkejä turvalaitteiden käytöstä 15

KUVIO 4. Ohjausjärjestelmän luokat 17

KUVIO 5. Eri luokkien avulla saavutettavissa oleva suoritustaso 23

KUVIO 6. Suoran moottorilähdön turvapysäyttäminen kontaktoreilla 27

KUVIO 7. Taajuusmuuttajalla ohjatun moottorin pysäyttäminen turvatuloilla 29

KUVIO 8. Venttiilien turvatoiminnon toteutus 30

KUVIO 9. Turvatoiminnon toiminnallinen piirikaavio 32

KUVIO 10. Turvallisuuteen liittyvä lohkokaavio 32

KUVIO 11. Sistema-ohjelmiston hierarkia 33

KUVIO 12. Sistema-ohjelmiston riskigraafi 34

KUVIO 13. Todennettavan turvatoiminnon toiminnallinen piirikaavio 36

KUVIO 14. Suoritustason määrittäminen suoraan komponentille 37

KUVIO 15. Komponenttikirjastosta lisätty turvarele 38

KUVIO 16. Alajärjestelmän luokan valinta ja lisävaatimukset 39

KUVIO 17. Yhteisvikaantumisen välttämiseksi tehdyt toimet 41

KUVIO 18. Turvatoiminnon toimintakertojen määrän laskenta 42

KUVIO 19. B10d-arvon avulla laskettu MTTFd-arvo 42

KUVIO 20. Turvatoiminnon polku Sistema-ohjelmistossa 44

TAULUKOT

TAULUKKO 1. Riskin tason määrittäminen ja vaadittavat toimenpiteet 12

TAULUKKO 2. Ohjausjärjestelmän suoritustaso riskin suuruuden mukaan 13

TAULUKKO 3. Suoritustasojen määrittely 16

TAULUKKO 4. Suoritustason ja turvallisuuden eheyden tason vastaavuus 19

TAULUKKO 5. Diagnostiikan kattavuuden tasot 22

1 JOHDANTO

Suunniteltaessa sähköisesti ohjattavia koneita on otettava huomioon myös niiden ohjausjärjestelmän turvallisuusvaatimukset. Teollisuuden parissa työskentelevät sähkösuunnittelijat joutuvat tekemään koneiden sähkösuunnitelmia, vaikka heidän koulutuksessaan ei käsitellä koneturvallisuuteen liittyviä asioita juuri lainkaan. Suunnittelijoiden on perehdyttävä työssään koneturvallisuuden vaatimuksiin, jotta he osaisivat suunnitella koneet niiden mukaisesti. Uusille koneille asetettuja vaatimuksia käsitellään tuoreimmassa konedirektiivissä 2006/42/EY. Konedirektiivi tuli voimaan Suomen liittyessä EU:hun vuonna 1994. Se on tullut näkyvimmin yleiseen tietoisuuteen CE-merkinnän yhteydessä. Suomessa konedirektiiviä vastaa valtioneuvoston asetus 400/2008 eli niin sanottu koneasetus. Konedirektiivin perusperiaate on, että koneen valmistaja vastaa koneen turvallisuudesta. Konedirektiivin vaatimuksia täydennetään lukuisilla standardeilla.

Koneiden ohjausjärjestelmille asetettujen vaatimusten tunteminen vaatii syvällistä perehtymistä aihetta käsitteleviin standardeihin ja alan kirjallisuuteen. Myös suunnittelijan ammattitaidon ylläpito on tärkeää, koska vanhoja standardeja korvataan uusilla, jolloin niiden sisältökin muuttuu. Esimerkiksi vuoden 2013 aikana vahvistetaan käyttöön uusi koneiden toimintaan kytkettyjä suojuksia käsittelevä standardi EN ISO 14119, joka korvaa vielä voimassa olevan standardin EN 1088. Uudesta standardista on odotettavissa suomeksi käännetty versio vuoden 2013 aikana.

Tämän opinnäytetyön tarkoituksena on selvittää koneiden sähkölaitteistoja ja ohjausjärjestelmiä käsittelevien standardien vaatimuksia standardien SFS-EN 60204 ja SFS-EN ISO 13849-1 pohjalta. Työssä keskitytään erityisesti standardin SFS-EN ISO 13849-1 määrittelemiin yleisiin suunnitteluperiaatteisiin.

Käsittelen työssäni koneen riskien arvioinnilla määritettyä riskin suuruutta ja sen vaikutusta koneen ohjausjärjestelmältä vaadittuun suoritustasoon. Tarkoituksena on selvittää, mitkä asiat vaikuttavat ohjausjärjestelmän suoritustasoon ja millaisilla suunnitteluratkaisuilla nämä suoritustasot voidaan saavuttaa. Saavutettu suoritustaso voidaan selvittää laskennallisesti Sistema-ohjelmistotyökalun avulla. Pyrin työssäni selvittämään ohjelmiston käytön ja laatimaan vaiheittaisen ohjeistuksen turvapiirin todentamisesta ohjelmistolla.

Opinnäytetyö on tehty Apex Automation Oy:n toimeksiantona. Työn kirjallisen osuuden tarkoitus on ohjeistaa koneiden sähkösuunnittelua ja turvapiirien todennuslaskentaa aloittavia uusia suunnittelijoita työssään.

2 APEX AUTOMATION OY

Apex Automation Oy on Kokkolan seudun johtava energia- ja teollisuusalojen automaatio- ja sähkösuunnittelupalveluita tarjoava suunnittelutoimisto. Yritys on perustettu vuonna 1993, ja se on vuosi vuodelta jatkanut tasaista kasvuaan yhdeksi alansa merkittäväksi toimijaksi. Yritys työllistää tällä hetkellä noin 50 työntekijää, ja viimeisen päättyneen tilikauden liikevaihto oli lähes 3,7 miljoonaa euroa. Apex Automation Oy tarjoaa asiakkailleen suunnittelupalveluita ja automaation kokonaisratkaisuja ”avaimet käteen” -periaatteella tai pienempinä kokonaisuuksina. (Apex Automation Oy 2011.)

Yrityksen keskeisimpiin asiakkaisiin kuuluvat energiantuotanto- ja jakeluyhtiöt sekä niiden järjestelmätoimittajat, prosessiteollisuus, teollisuuden laite- ja järjestelmätoimittajat sekä liike- ja julkisrakentaminen. (Apex Automation Oy 2011.)

Apex Automation Oy:n keskeisimpiä palveluita ovat teollisuuden ja rakennusten sähkösuunnittelupalvelut, kenttälaite- ja virtapiirisuunnittelu, logiikoiden ja prosessiautomaatiojärjestelmien ohjelmointi sekä sähkö- ja automaatiokeskusten valmistus. Lisäksi yritys tarjoaa sähkö- ja koneturvallisuuspalveluita, kaukokäyttöjärjestelmiä, PC-valvomoita sekä koulutus- ja konsultointipalveluita. (Apex Automation Oy 2011.)

3 KONETURVALLISUUS

Koneturvallisuutta käsittelevissä standardeissa SFS-EN 60204-1, SFS-EN ISO 13849-1, SFS-EN ISO 13849-2 ja SFS-EN 62 061 määritellään vaatimuksia automaattisten koneiden turvallisuudelle. Standardissa SFS-EN 60204-1 määritellään yleiset vaatimukset koneiden sähkölaitteistolle, ja standardeissa SFS-EN ISO 13849-1 ja SFS-EN 62061 on asetettu vaatimuksia niiden ohjausjärjestelmille. Tämä luku käsittelee standardien olennaisimpia asioita. Keskityn erityisesti ohjausjärjestelmää käsitteleviin standardeihin, koska koneita suunnittelevien henkilöiden on tärkeää tuntea niiden sisältöä.

3.1 Koneen sähkölaitteistot

Standardi SFS-EN 60204-1 määrittelee yleisiä vaatimuksia ja suosituksia koneiden sähkölaitteistolle. Näillä ohjeistuksilla pyritään parantamaan koneiden turvallisuutta ja yhdenmukaistamaan niiden ohjausta ja toimintaa. Tässä kappaleessa esitellään lyhyesti tärkeimpiä standardissa käsiteltyjä asioita, jotka on syytä huomioida koneen sähkösuunnittelussa.

Koneen sähkönlaadun on täytettävä standardin asettamat vaatimukset. Koneen jännitteelle alttiit osat ja johtavat rakenneosat pitää maadoittaa. Sähkölaitteiden aiheuttamia sähkömagneettisia häiriöitä rajoitetaan suodattimilla ja kaapeleiden suojaamisella, jotta ne eivät aiheuta koneen virhetoimintoja. Koneen tai koneiden jokaisessa sähkönsyötössä on oltava lukittava syötönerotuskytkin, jolla voidaan tarvittaessa erottaa koneen sähkölaitteisto syöttöverkosta. Odottamattoman käynnistyksen estämiseksi pitää olla kytkinlaitteet, ja ne on merkittävä siten, että niiden tarkoitus on helposti tunnistettavissa. Sähkölaitteisto tulee suojata niin, että henki-

löille ei voi aiheutua sähköiskua suorasta tai epäsuorasta kosketuksesta. Sähkölaitteet on suojattava myös ylivirralta, ylikuormitukselta, ylilämpenemiseltä ja sähkönlaadun muutoksilta. Koneen on kestettävä sen ympäristön aiheuttamat rasitukset. Jos koneessa käytetään vaihtovirralla toteutettua ohjauspiiriä, on käytettävä ohjausjännitemuuntajaa. Koneen sähkölaitteiston kunto on tarkistettava mittaamalla ennen koneen käyttöönottoa. (SFS-EN 60204-1 2006.)

3.2 Ohjausjärjestelmän toiminta

Automaattisten koneiden turvallisuus perustuu suurelta osin ohjausjärjestelmän suorittamiin turvatoimintoihin. Ohjausjärjestelmä koostuu koneen hallintalaitteista, ohjauspiireistä, tehonohjauselimistä ja ohjelmistosta. Ohjausjärjestelmän täytyy sisältää kaikki turvallisuuden kannalta tarpeelliset turvatoiminnot. Koneen turvatoimintoihin kuuluvat turvalaitteen aikaansaama pysäytystoiminto, turvapiirin kuittaus, koneen käynnistys ja uudelleenkäynnistys, paikallinen ohjaus, turvalaitteen passivointi, koneen pakko- ja sallintakäyttö sekä koneen odottamattoman käynnistyksen estäminen. Koneen turvatoiminnot on suunniteltu takaamaan koneen turvallinen käyttö kaikissa olosuhteissa. (Siirilä & Kerttula 2007, 130; Siirilä 2009, 59-60.)

3.2.1 Koneen käynnistäminen

Koneen käynnistämisen ehtona on, että kaikki turvatoiminnot ja suojaukset ovat kunnossa. Tämän ehdon lisäksi koneessa on oltava erillinen käynnistyksen hallintaelin, josta varsinainen käynnistyskäsky annetaan. Kone ei saa käynnistyä silloin, kun siihen kytketään sähkö, paineilma tai muu energiansyöttö, eikä silloin, kun koneen ajotavan valintakytkimen asentoa muutetaan tai kun turvalaite kuitataan

kuittauspainikkeesta. Joissakin tapauksissa voidaan käyttää automaattisesti kuittaantuvaa turvalaitetta, jolloin kone voi suorittaa seuraavan työvaiheen loppuun automaattisesti. Automaattikuittaukseen vaaditaan kuitenkin tiukkoja lisäehtoja, esimerkiksi käyttäjän jatkuvaa hallintaelimeen vaikuttamista liikkeiden aikana. (Siirilä 2009 261-262 & SFS-EN 60204-1 2006, 152.)

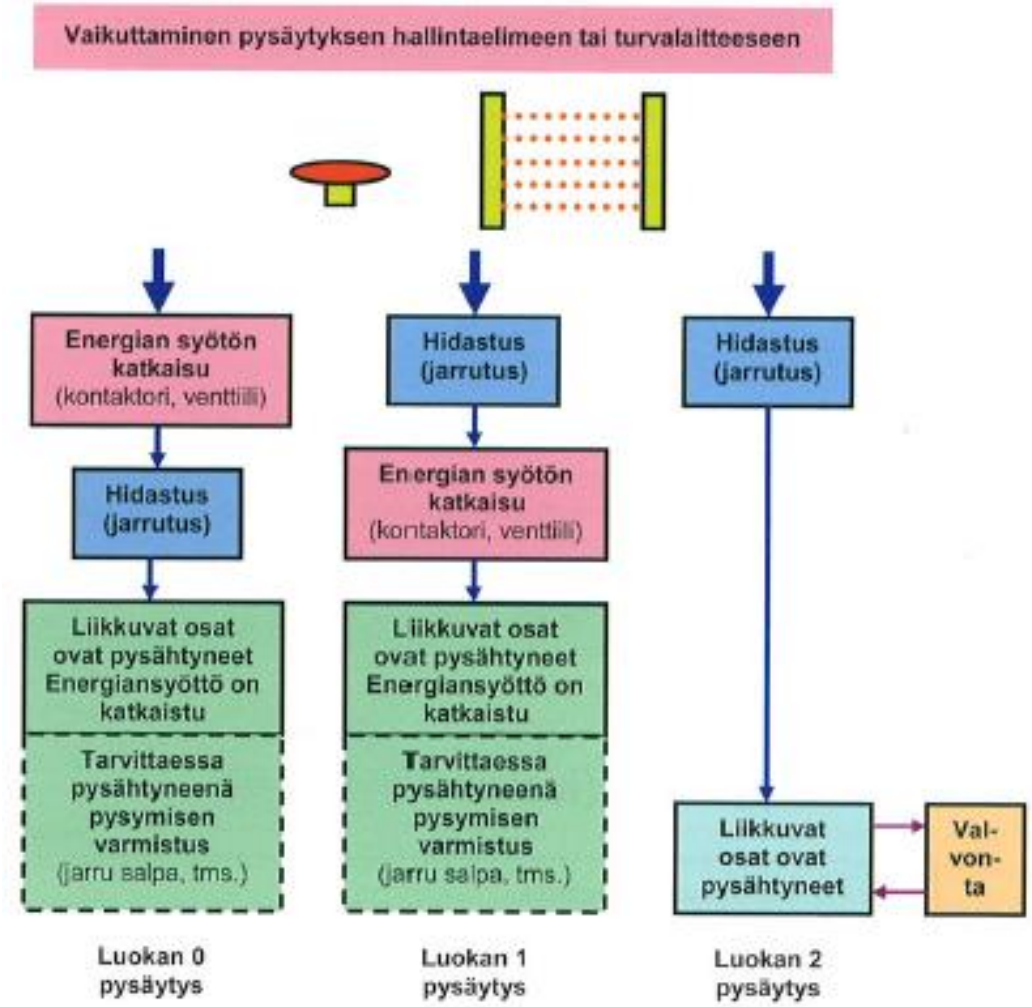
3.2.2 Koneen pysäyttäminen

Myös koneen pysäyttämiselle on oltava erityinen hallintaelin, joka saa aikaan koneen normaalin hallitun tuotantopysäytyksen. Normaalissa pysäytyksessä energiansyöttöjä ei katkaista, vaan kone pysäytetään ohjelmallisesti, ja ohjelma jää odottamaan seuraavaa käskyä. Tämä pysäytystapa ei ole riittävä turvallisuusmielessä, koska kone voi käynnistyä odottamattomasti häiriön, vian tai erehdyksen sattuessa. Siksi koneissa käytetään turvalaitteita, jotka saavat aikaan turvapysäytyksen. Turvapysäytyksessä kaikki energiansyötöt katkaistaan ja kone pysäytetään mahdollisimman nopeasti. Koneen pysäyttäminen voidaan toteuttaa kolmella eri tavalla, joita kutsutaan pysäytysluokiksi. (Siirilä & Kerttula 2007, 132.)

Luokan 2 pysäytys on normaali tuotantopysäytys, jossa energiaa voidaan käyttää laitteen nopeaan ja hallittuun hidastukseen. Energiansyöttö jää päälle, vaikka liikkeet on pysäytetty. Jos tätä pysäytysluokkaa käytetään silloin, kun henkilö on vaarallisella alueella, koneen pysähtyneenä pysymistä on luotettavasti valvottava. (Siirilä & Kerttula 2007, 133.)

Luokan 1 pysäytys on turvapysäytys, jossa energiaa voidaan käyttää laitteen nopeaan ja hallittuun hidastukseen. Kun liikkeet on pysäytetty, laitteiden energiansyöttö katkaistaan. (Siirilä & Kerttula 2007, 133.)

Luokan 0 pysäytys on turvapysäytys, jossa energian syöttö katkaistaan välittömästi pysäytyskäskyn jälkeen. Koneen nopea hidastaminen ja pysäyttäminen hoidetaan tarvittaessa jousivoimalla toimivia jarruja käyttäen. (Siirilä & Kerttula 2007, 133.)



KUVIO 1. Pysäytysluokat ja niiden ominaisuudet (Siirilä 2009, 277.)

Turvalaitteen aikaansaaman turvatoiminnon on saatettava kone turvalliseen tilaan niin nopeasti kuin on tarpeen. Koneen pysähtymisajan täytyy olla niin lyhyt, että turvalaitteeseen vaikuttanut ihminen ei ehdi koskettaa koneen liikkuvia osia ennen niiden pysähtymistä. Jos pysähtymiseen kuluva aika on pitkä, on suojaukseen

käytettävä lukittavaa suojusta, joka aukeaa vasta, kun liikkeet ovat pysähtyneet. (Siirilä & Kerttula 2007, 134-135.)

Konedirektiivin mukaan kone tai konelinja on voitava erottaa kaikesta energiansyötöstä lukittavalla syötönerotuskytkimellä. Energiansyötöllä tarkoitetaan sähkön lisäksi myös paineilmaa ja hydrauliikan painetta. Suuressa järjestelmässä yksi syötönerotuskytkin tai sulkuventtiili ei riitä, vaan yksittäinen kone on voitava erottaa energiansyötöstä käsikäyttöisellä syötönerotuskytkimellä tai sulkuventtiilillä huoltoa ja kunnossapitoa varten. (Siirilä 2009, 297.)

3.2.3 Hätäpysäytys

Hätäpysäytystoiminto vaaditaan kaikissa koneissa lukuun ottamatta käsikäyttöisiä ja kannateltavia koneita. Hätäpysäytys ei ole varsinainen ensisijainen turvatoiminto, vaan sitä käytetään vain, jos jotakin odottamatonta tapahtuu tai koneen normaali pysäytystoiminto vikaantuu. Sellaisissa tilanteissa tuotannon keskeytyminen ja laitteen vaikea uudelleenkäynnistys ovat pieniä ongelmia vahingon välttämiseen verrattuna. Hätäpysäytyksen on ohitettava kaikki muut toiminnot ja saatava aikaan luokan 0 tai 1 pysäytys koneen turvallisuusvaatimusten mukaan. Hätäpysäytyskäskyn on jäätävä voimaan valvontalaitteen kuittaukseen asti hätäpysäyttimeen vaikuttamisen jälkeen. Hätäpysäytyspiirin kuittaus ei saa käynnistää konetta, vaan se on käynnistettävä erillisestä hallintalaitteesta. (Siirilä 2009, 280-284; Siirilä & Kerttula 2007, 135-137.)

Tavallisin hätäpysäytyslaite on sienimäinen hätäpysäytyspainike. Painikkeiden lisäksi markkinoilla on turvaköysirajoja, jotka voidaan sijoittaa esimerkiksi konelinjaston läheisyyteen siten, että koneen käyttäjillä on riittävän lyhyt matka nopeaa

hätäpysäytystä varten. Jos konetta voidaan ohjata useasta paikasta, on jokainen ohjauspaikka varustettava hätäpysäytyslaitteella.

3.2.4 Pysäytysvyöhykkeet

Konelinja tai koneyhdistelmä koostuu useista yhdessä toimimaan suunnitelluista yksittäisistä koneista. Tällaisten järjestelmien turvatoimintojen suunnittelu ja toteuttaminen on haastavaa, koska turvatoiminnon on koskettava varsinaisen koneen lisäksi myös muita linjaston koneita, jos niiden toiminnan jatkuminen voi aiheuttaa vaaratilanteita. Selkein ratkaisu turvatoiminnon toteuttamiseksi konelinjassa on pysäyttää koko konelinjasto ruuhkien ja virhetoimintojen välttämiseksi. Tämä ei kuitenkaan ole aina järkevää tuotannon ja toiminnan joustavuuden kannalta, koska luokan 0 tai 1 pysäyttäminen koko linjastolle on turhaa, jos pysäyttämistarve liittyy vain yhteen koneen osaan. Tästä syystä konelinjastossa on tarvittaessa oltava useita turvavyöhykkeitä. (Siirilä & Kerttula 2007, 133.)

Turvavyöhykkeisiin jaetulla konelinjalla voidaan tuotantoa jatkaa muilla koneilla, vaikka yhteen linjan osaan olisi tullut häiriö. Muut linjan koneet voivat jatkaa tuotantoa niin kauan, kuin tuotetta riittää tai sillä on tilaa siirtyä eteenpäin. Sen jälkeen näiden koneiden pitää pysähtyä pysäytysluokan 2 tilaan. Häiriön poistuttua yksittäisestä koneesta konelinjasto jatkaa toimintaansa automaattisesti. Turvavyöhykkeitä käytettäessä vyöhykkeet on erotettava toisistaan turvalaitteilla tai suojuksilla. Pääsy turvavyöhykkeeltä toiselle ei saa olla mahdollista ilman, että turvalaite havaitsee sen ja saattaa koneen turvalliseen tilaan. (Siirilä & Kerttula 2007, 133.)

Konelinjoissa, joissa tuote liikkuu turvavyöhykkeiden välillä, on tarpeen käyttää turvalaitteen passivointia. Passivoinnilla tarkoitetaan turvatoiminnon väliaikaista automaattista poistamista esimerkiksi silloin, kun valmistettava tuote siirtyy turva-

vyöhykkeeltä toiselle. Passivointi täytyy toteuttaa siten, että turvatoiminto on poiskytkettynä vain sen hetken, kun tuote on turvalaitteen havaitsemisalueella. Kun tuote on siirtynyt havaitsemisalueelta, turvatoiminto palautuu automaattisesti ja turvavyöhykkeiden välinen valvonta jatkuu normaalisti. (Siirilä & Kerttula 2007, 142-143.)

KUVIO 2. Kahden turvavyöhykkeen välinen valvonta passivoitavalla valoverholla (Sundcon Oy)

Turvavyöhykkeisiin jakaminen vaikuttaa myös riskien pienenemiseen, koska koneen käyttäjän on helpompi hallita konelinjastoa pienempinä turvavyöhykkeinä. Jos yksittäisen koneen turvapiiri laukeaa, sen kuittaaminen on turvallisempaa, koska kuittauspaikalta voidaan nähdä koko kuitattava turva-alue. Jos koko konelinja olisi yksi iso turva-alue, kuittaus menettäisi merkityksensä, koska koneenkäyttäjä ei voi nähdä kuittauspaikalta koko kuitattavaa turva-aluetta. (Siirilä & Kerttula 2007, 133.)

Suurissakin järjestelmissä hätäpysäytys on toteutettava ensisijaisesti siten, että hätäpysäytyskäsky vaikuttaa koko konelinjan koneisiin. Tästä voidaan kuitenkin

poiketa, jos järjestelmä suunnitellaan siten, että pysäytysvyöhykkeet ja niiden hallintaelimet on helppo erottaa toisistaan. Lisäksi on huolehdittava siitä, että eri vyöhykkeisiin kuuluvat koneet erotetaan selvästi toisistaan turvalaitteilla tai suojuksilla, ja siitä, että vyöhykkeiden rajapinnoissa ei ole mitään vaaroja. (Siirilä & Kerttula 2007, 135.)

3.3 Riskien arviointi

Koneen valmistajan velvollisuus on varmistaa, että koneen suunnittelun yhteydessä tehdään riskien arviointi, koska kone on suunniteltava ja rakennettava niin, että riskien arvioinnin tulokset otetaan huomioon. Riskien arviointiin kuuluu määrittää koneen käytön raja-arvot, joihin sisältyvät koneen normaali käyttö ja ennakoitavissa oleva väärinkäyttö. Arvioinnissa on tunnistettava koneen aiheuttamat vaarat ja arvioitava riskien suuruus. Riskien suuruuden ja mahdollisten terveyshaittojen tai vammojen perusteella on arvioitava, onko riskejä pienennettävä konedirektiivin vaatimusten täyttämiseksi. Jos riskejä on pienennettävä, konetta täytyy muuttaa tai turvalaitteita lisätä. (Siirilä 2009, 39.)

Riskien arviointiin on useita eri menetelmiä, mutta varsinaista standardisoitua menetelmää ei ole olemassa. Yleisesti kaikissa menetelmissä arvioidaan vahinkojen vakavuutta ja todennäköisyyttä. Arvioinnissa olisi huomioitava ihmisen erehtyväisyys, ja tahallinen riskin ottaminen ja se, joutuvatko koneen käyttäjä tai muut työntekijät olemaan vaaravyöhykkeellä. Myös ohjausjärjestelmän vikaantuminen ja siitä aiheutuvat seuraukset on huomioitava. Erityisesti automaattisissa koneissa, joissa on liikkuvia osia ja joiden parissa ihmiset työskentelevät, riskien suuruus kasvaa. Tällöin ohjausjärjestelmän ja muiden suojalaitteiden on estettävä koneen joutuminen sellaiseen tilaan, josta voisi aiheutua vaaraa ympäristölle. (Siirilä 2009, 43-45.)

Riskien arvioinnin perusteella päätetään, millä keinoilla koneen riskejä pienennetään. Jos konetta ei voi suojata kiinteillä suojilla niin, että niiden avulla riskit saataisiin riittävän pieneksi, on riskejä pienennettävä ohjausjärjestelmällä. Ohjausjärjestelmän merkitys turvallisuudelle on sitä suurempi, mitä suurempi osa riskeistä vähennetään sen avulla. Riskien arvioinnilla ohjausjärjestelmälle määritellään suoritustaso, joka sen on täytettävä. (Siirilä 2009, 57.)

Riskien arvioinnin yleisessä menetelmässä vahingon vakavuus jaetaan asteikolle 1…100. Asteen 1 vahingon vakavuudesta esimerkkinä voisi olla pieni nipistys, haava tai mustelma, kun taas asteen 100 vahingon vakavuus voisi olla kuolema tai hyvin vakava vammautuminen. Muut mahdolliset vahingot jaotellaan vakavuuden mukaan näiden arvojen välille. Vahingon todennäköisyys pisteytetään asteikolle 0,1…1. Asteen 1 vahingon toteutuminen on käytännössä varmaa, kun taas asteen 0,1 toteutuminen on äärimmäisen epätodennäköistä. (Siirilä 2009, 40,43,45.)

Riskin suuruus lasketaan kertomalla vahingon vakavuuden arvioitu arvo sen todennäköisyyden arvioidulla arvolla. Laskennalla saadaan riskille lukuarvo, joka kuvaa riskin suuruutta (TAULUKKO 1). Tämä tarkoittaa sitä, että suuriakin vahinkoja aiheuttavan koneen riski saadaan pieneksi, jos todennäköisyys vahingolle saadaan pieneksi. Toisaalta voidaan ajatella, että pienenkin vahingon aiheuttavan koneen riski kasvaa suureksi, jos vahingon todennäköisyys on suuri. (Siirilä 2009, 52.)

TAULUKKO 1. Riskin tason määrittäminen ja vaadittavat toimenpiteet (mukaillen Siirilä 2007, 47)

RISKIN TASO	LUKUARVO	VAADITTAVAT TOIMENPITEET
Sietämätön	**49…100**	Riskiä on pienennettävä
Merkittävä	**29…48**	Riskiä on pienennettävä
Kohtalainen	**16…28**	Riskiä on pienennettävä
Siedettävä	**6…15**	Seuranta ja myöhemmin tehtävä uudelleen arviointi
Vähäinen	**0,1…5**	Toimenpiteitä ei tarvita

Riskin tasojen mukaan on määritelty taulukko, joka kertoo vaadittavan ohjausjärjestelmän suoritustason, jos riskiä ei voida vähentää muilla toimenpiteillä (TAULUKKO 2).

TAULUKKO 2. Ohjausjärjestelmä suoritustaso riskin suuruuden mukaan (mukaillen Siirilä 2009, 58)

RISKIN TASO	VAADITTU SUORITUSTASO (PL)	VAADITTU EHEYSTASO (SIL)
Sietämätön	**e**	**3**
Merkittävä	**d**	**2**
Kohtalainen	**c**	**1**
Siedettävä	**b**	**1**
Vähäinen	**a**	

Esimerkkinä riskien arvioinnista voidaan kuvitella kone, jonka aiheuttama suurin vahinko voisi olla käden leikkautuminen irti. Vahinko on aika vakava, mutta ei kuitenkaan verrattavissa kuolemaan, joten sen suuruus olisi arviolta 80. Kone on kuitenkin hyvin suojattu, ja vaara-alueelle pääsyä valvotaan turvalaitteilla, joten todennäköisyys vahingolle olisi epätodennäköinen eli 0,2. Tämä laskenta aiheuttaisi lukuarvon 16 eli kohtalaisen riskin. Tässä tapauksessa ohjausjärjestelmän tulisi täyttää suoritustaso c.

3.4 Turvalaitteen valinta

Jos riskien arvioinnissa havaittua riskiä ei ole mahdollista pienentää kiinteillä suojuksilla, on käytettävä turvalaitetta. Turvalaitteen tehtävä on varmistaa, että koneen liikkuviin osiin päästään koskettamaan vain niiden ollessa pysähtyneinä, ja estää odottamaton liike henkilön ollessa vaarakohdassa. Havaitsemisvyöhykkeen on oltava aukoton, sillä vaaravyöhykkeelle ei saa päästä ilman turvalaitteen havahtumista. Oikean turvalaitteen valinta käyttökohteeseen on tärkeää, koska huonosti valittu laite tai huonosti toteutettu turvapiiri voi haitata merkittävästi koneen

käyttöä. Tällöin vaarana on tahallinen turvalaitteen ohittaminen koneen käytön helpottamiseksi. Tämä puolestaan aiheuttaa vaaratilanteita, koska turvapiiri ei turvalaitteen ohittamisen jälkeen ole toiminnassa. (Siirilä 2009, 348,354.)

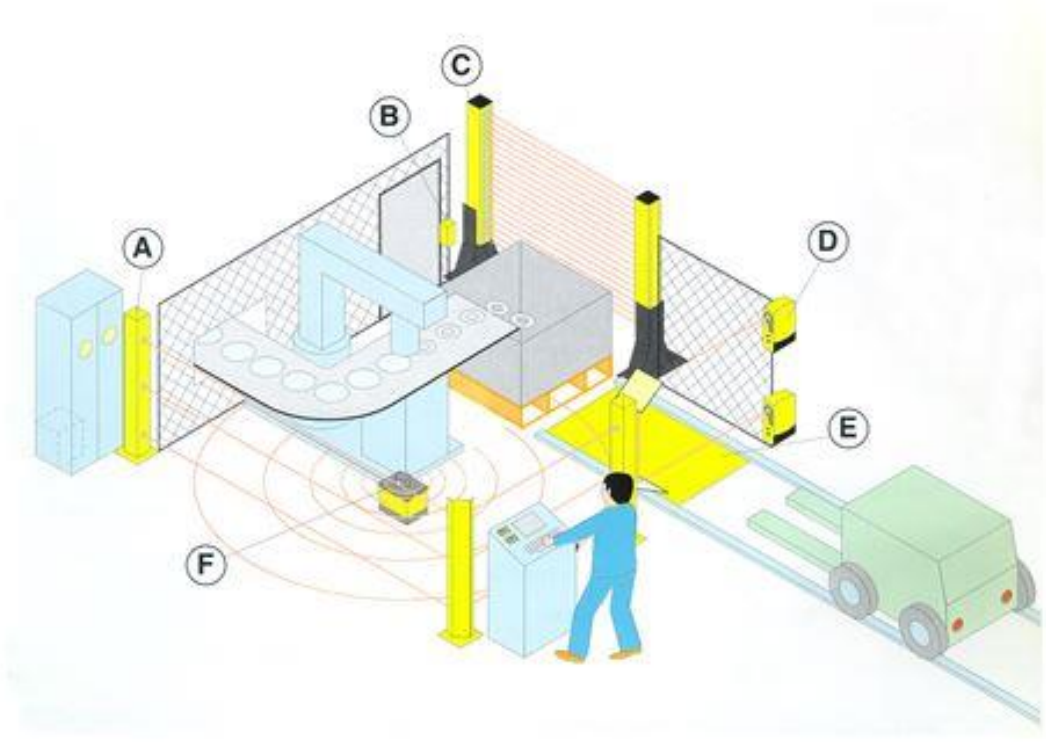
Markkinoilla on turvalaitteita, joilla voidaan tehdä aluevalvontaa ja kulunvalvontaa, tai käyttäjä voidaan sitoa tiettyyn paikkaan koneen käytön ajaksi. Aluevalvontaan käytettäviä turvalaitteita ovat laserskannerit ja tuntomatot. Käytettäessä kyseisiä turvalaitteita henkilöstä saadaan havainto koko ajan hänen ollessaan vaaravyöhykkeellä. Jos turvalaite havaitsee henkilön vaaravyöhykkeellä, turvapiiriä ei voi kuitata toimintakuntoon eikä kone käynnistyä. Aluevalvontaan käytettävien turvalaitteiden valvonta-alueeseen ei saa jäädä aukkopaikkoja, joissa ihmisen olisi mahdollista olla vaaravyöhykkeellä. Tuntomattojen ja laserskannereiden käyttö on perusteltua, jos vaaravyöhykettä ei ole mahdollista suojata esimerkiksi aidoilla tai vyöhykkeelle on huono näkyvyys koneen ohjauspaikalta. (Siirilä 2009, 398.)

Kulunvalvontaan perustuvia turvalaitteita ovat erilaiset valosähköiset laitteet, kuten valoverhot ja valopuomit. Kulunvalvontaan tarkoitetuilla turvalaitteilla turvatoiminto saavutetaan, kun henkilö katkaisee valosähköisen turvalaitteen tuottaman valonsäteen. Turvalaite ei voi havaita henkilöä vaaravyöhykkeellä, kun hän ei ole enää laitteen havaitsemisalueella. Tässä tapauksessa turvapiirin kuittaaminen ja koneen käynnistäminen vahingossa ovat mahdollisia henkilön ollessa vaaravyöhykkeellä. Kulun valvontaan perustuvien turvalaitteiden valinta on perusteltua, jos kone on suojattu aidoilla, koneen alueelle on hyvä näkyvyys ohjauspaikalta, vaaravyöhykkeellä täytyy käydä suhteellisen useasti tai koneen valmistama tuote siirretään valoverholla valvotusta aukosta aidan ulkopuolelle. (Siirilä 2009, 398.)

Kone voidaan suojata myös kiinteillä suojuksilla kokonaan, mutta huoltoa ja kunnossapitoa varten vaaravyöhykkeellä on toisinaan käytävä. Kiinteään suojukseen on mahdollista tehdä avattava suojus, jonka kautta kulku vaaravyöhykkeelle voidaan järjestää. On kuitenkin huomioitava, että avattavassa suojuksessa on oltava turvalaite, joka sallii koneen käyttämisen vain silloin, kun se on suljettu. Jos suojus

avataan kesken koneen toiminnan, liikkeet on pysäytettävä. Avattava suojus voidaan myös varustaa lukinnalla, jos ihminen voi ehtiä sen kautta vaarallisiin liikkuviin osiin ennen niiden pysähtymistä. (Siirilä 2009, 388 – 389.)

Koneen käyttäjän joutuminen vaaravyöhykkeelle voidaan estää myös käyttämällä turvalaitteena pakkokäyttöisiä hallintalaitteita. Ne sijaitsevat vaaravyöhykkeen ulkopuolella, ja käyttäjän on vaikutettava niihin koko ajan koneen liikkeiden aikana. Tällaiset turvalaitteet suojaavat vain koneen käyttäjän, joten kone on mahdollista käynnistää toisen ihmisen ollessa vaarakohdassa. Pakkokäyttöisen hallintalaitteen käyttäminen turvalaitteena on perusteltua silloin, kun koneen täytyy olla jatkuvasti ihmisen valvonnassa tai sen liikkeitä ei tarvitse suorittaa jatkuvasti. (Siirilä 2009, 398.)



A. Valopuomi
B. Oven kytkentä koneiden toimintaan
C. Valoverho
D. Valopuomi
E. Tuntomatto
F. Laserskanneri

KUVIO 3. Esimerkki turvalaitteiden käytöstä (Siirilä 2013)

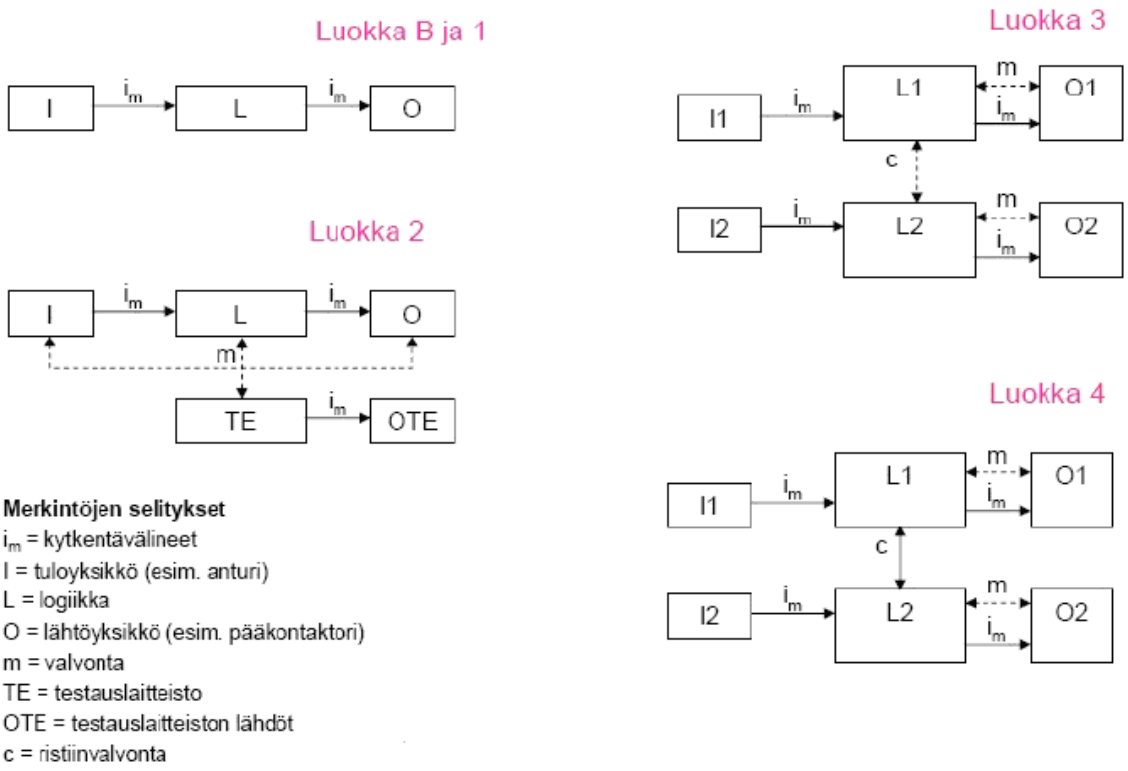
3.5 Ohjausjärjestelmän luokittelu

Koneen ohjausjärjestelmää käsitellään standardeissa SFS-EN ISO 13849-1 (osa 1, Yleiset suunnitteluperiaatteet), SFS-EN ISO 13849-2 (osa 2, Kelpuutus) ja SFS-EN 62061(Toiminnallinen turvallisuus). Standardi SFS-EN ISO 13849-1 jakaa ohjausjärjestelmän nimettyihin rakenteisiin eli luokkiin ja suoritustasoihin, kun taas standardi SFS-EN 62061 määrittelee ohjausjärjestelmälle turvallisuuden eheyden tasot. Esittelen tässä kappaleessa tarkemmin standardin SFS-EN ISO 13849-1 mukaisen jaottelun, koska sen käyttö on perusteltua koneiden turvallisuutta käsiteltäessä. Käsittelen lyhyesti myös turvallisuuden eheyden tasojen mukaisen jaottelun, koska laitevalmistajat voivat ilmoittaa tuotteidensa turvaluokituksen turvallisuuden eheyden tasoilla.

Ohjausjärjestelmästandardissa SFS-EN ISO 13849-1 esitetään turvallisuuden arviointiin yksinkertaistettu menetelmä, jossa arviointi perustuu nimettyihin rakenteisiin eli luokkiin ja suoritustasoihin eli PL -tasoihin (a, b, c, d, e), jotka määritellään vaarallisen vikaantumisen todennäköisyytenä tuntia kohti (TAULUKKO 3). Suoritustasoilla määritellään turvallisuuteen liittyvän ohjausjärjestelmän kyky suorittaa turvatoiminto. Luokat (B, 1, 2, 3, 4) kuvaavat ohjausjärjestelmän rakennetta, eli miten ohjausjärjestelmän turvallisuus on varmistettu vikatilanteissa.

TAULUKKO 3. Suoritustasojen määrittely (mukaillen ISO 13849-1, 34)

Suoritustaso (PL)	Keskimääräinen vaarallisen vian todennäköisyys tunnissa PFH [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	$\geq 10^{-8} < 10^{-7}$



KUVIO 4. Ohjausjärjestelmän luokat (Sundquist 2010, 9)

Luokassa B komponenttien määrän tulee olla mahdollisimman pieni turvallisuuteen liittyvässä järjestelmässä. Komponenttien on kestettävä odotettavissa olevat käyttö- ja ympäristöolosuhteet. Rakenteessa on noudatettava yleisiä turvallisuuden perusperiaatteita. Vaarallisten vikaantumisten välisen keskimääräisen aika eli MTTFd-arvon on oltava 3…29 vuotta. (Siirilä 2009, 143.)

Luokassa 1 on käytettävä luokan B vaatimusten lisäksi hyvin koeteltuja turvallisuusperiaatteita ja komponentteja siten, että viat ovat epätodennäköisiä ja tapahtuvat turvalliseen suuntaan. Hyvin koetellut komponentit on tarpeen ylimitoittaa ja niiden mekaanisesta pakkotoimisuudesta on huolehdittava. MTTFd-arvon on oltava 30…100 vuotta. (Siirilä 2009, 143-144.)

Luokassa 2 vaatimuksena on luokkien B ja 1 yleisten turvallisuuden perusperiaatteiden ja hyvin koeteltujen turvallisuusperiaatteiden lisäksi se, että koneen ohjaus-

järjestelmä tarkistaa turvatoimintojen toimivuuden tietyin väliajoin. Vian havaitsemisen jälkeen kone on pysäytettävä tai sen käynnistäminen estettävä. Diagnostiikan keskimääräinen kattavuuden pitää olla 60…98%. Yhteisvikojen todennäköisyyden eli CCF-arvon on oltava pieni. MTTFd-arvon täytyy olla 3…100 vuotta. (Siirilä 2009, 144.)

Luokassa 3 on noudatettava luokkien B ja 1 yleisiä turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita. Yksittäisen vian sattuessa ohjausjärjestelmän on pystyttävä suorittamaan turvatoiminto. Järjestelmän täytyy myös havaita useimmat viat. Vikasietoisuus saavutetaan käyttämällä piirin kahdennusta. Diagnostiikan keskimääräisen kattavuuden on oltava 60…98% ja yhteisvikojen todennäköisyyden pieni. MTTFd-arvon pitää olla 3…100 vuotta. (Siirilä 2009, 144.)

Luokassa 4 on noudatettava luokkien B ja 1 turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita ja luokan 3 vaatimusta yksittäisestä viasta. Järjestelmän täytyy havaita kaikki viat. Vaatimukset voidaan toteuttaa piirien kahdennuksilla ja jatkuvalla automaattisella vikaantumisen valvonnalla. Diagnostiikan keskimääräisen kattavuuden on oltava 99…100%, Yhteisvikojen todennäköisyyden pitää olla pieni ja MTTFd-arvon 3…100 vuotta. (Siirilä 2009, 144.)

Turvatoiminnon suoritustason määrittämiseen tarvitaan luokan lisäksi tiedot laitteiden vaarallisen vikaantumisen todennäköisyydestä (MTTFd-arvo), turvapiirin diagnostiikan kattavuuden keskiarvo (DCavg-arvo) sekä tiedot turvapiirin yhteisvikaantumisen todennäköisyydestä (CCF-arvo). Laitevalmistaja on yleensä määrittänyt laitteelleen MTTFd-arvon. Jos valmistaja ei ole ilmoittanut sitä, on suunnittelussa mahdollista käyttää standardissa SFS-EN ISO 13849-1 liitteessä C taulukoituja yleisiä arvoja laitteille (LIITE 1). Samassa standardissa liitteessä E on taulukoitu turvapiireille diagnostiikan kattavuuden arvoja erilaisia ratkaisuja käytettäessä (LIITE 2). Liitteessä F puolestaan esitellään toimenpiteitä turvapiirissä olevien laitteiden yhteisvikaantumisen välttämiseksi (LIITE 3).

Standardissa SFS-EN 62061 ohjausjärjestelmän kykyä selvitä vikatilanteessa turvatoiminnoista kuvataan turvallisuuden eheyden tasoilla (SIL 1, 2, 3). Standardi SFS-EN 62061 on erityisesti komponenttien valmistajien ja tyyppitarkastuksia tekevien laitosten käyttämä standardi. Standardia käytetään pääasiassa prosessiteollisuuden turvallisuuden tarkasteluissa. Standardin päätarkoitus on, että kone toimii turvallisuusvaatimusten mukaisesti ja ei-toivotuilta toiminnoilta vältytään. Standardi SFS-EN 62061 on tehty laajemman ohjausjärjestelmää käsittelevän standardin SFS-IEC 61508 pohjalta, ja siinä esitellään myös turvallisuuden eheyden taso SIL 4. Koneissa turvallisuuden eheyden ylin arvo on käytännössä SIL 3. Tasoa SIL 4 käytetään vain sovelluksissa, joiden aiheuttamat seuraukset voivat olla katastrofaaliset, kuten ydinvoimaloissa. Koneiden ei oleteta saavan toiminnallaan aikaan katastrofaalisia seurauksia, joten taso SIL 3 on riittävä. (Siirilä 2009, 103, 143, 195.)

On siis olemassa kaksi standardia, jotka molemmat esittävät oman tapansa ohjausjärjestelmän turvallisuuden tasojen arviointiin. Tämän takia standardissa SFS-EN ISO 13849-1 esitetään taulukko suoritustasojen ja turvallisuuden eheyden tasojen vertaamiseksi keskenään.

TAULUKKO 4. Suoritustason ja turvallisuuden eheyden tason vastaavuus (ISO 13849-1, 44)

SUORITUSTASO (PL)	TURVALLISUUDEN EHEYDEN TASO (SIL)
a	Ei vastaavuutta
b	1
c	1
d	2
e	3

4 TURVAPIIRIN SUUNNITTELU JA TODENTAMINEN

Turvapiirin suunnittelun lähtökohtana on riskienarvioinnista saatu suoritustaso PLr, joka ohjausjärjestelmän tulee täyttää. Suoritustason jälkeen arvioidaan toteutettavalle ohjausjärjestelmälle luokka, jolla on mahdollista saavuttaa vaadittu suoritustaso. Lisäksi on arvioitava, kuinka korkeaan keskimääräiseen vaaralliseen vikaantumisaikaan on päästävä, kuinka yhteisvikaantuminen on huomioitava järjestelmässä ja kuinka korkea diagnostiikan kattavuuden tulee olla. Järjestelmän rakenteella ja komponenttivalinnoilla on suuri merkitys siihen, mihin suoritustasoon voidaan päästä.

Suunnittelun aikana on todennettava, että turvapiiri täyttää sille asetetun suoritustason. Käytän standardiin SFS-EN ISO 13849-1 perustuvaa Sistema-ohjelmistotyökalua todentamislaskentaan.

4.1 Turvapiirin suunnittelu

Kappaleessa ohjausjärjestelmän suunnittelu luokissa 1…4 määriteltiin, että niissä on käytettävä turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita. Lisäksi luokassa 1 oli käytettävä hyvin koeteltuja komponentteja siten, että viat ovat epätodennäköisiä ja tapahtuvat turvalliseen suuntaan. Hyvin koetelluilla komponenteilla tarkoitetaan sitä, että niitä on käytetty pitkään vastaavissa turvallisuuteen liittyvissä piireissä ja niiden toiminnasta on saatu hyviä kokemuksia. (Siirilä & Kerttula 2007, 162.) Turvallisuuden perusperiaatteilla tarkoitetaan asioita, joita käsittelin aiemmin kappaleessa Koneen sähkölaitteistot.

Hyvin koeteltujen turvallisuusperiaatteiden mukaan valvontatoiminnoissa on käytettävä laitteita, joissa on mekaanisesti yhteen kytketyt koskettimet, jotta esimerkiksi kärkien kiinnihitsautuminen havaitaan. Turvallisuuteen liittyvässä ohjausjärjestelmässä käytetään suojattuja kaapeleita, joiden suojavaippa on kytketty maadoitukseen, jotta voidaan välttää kaapelivikoja. Laitteet ja liittimet sijoitetaan niin, etteivät ne vahingossa pääse koskettamaan toisiaan. Piirien komponentit ylimitoitetaan niin, että koskettimissa käytetään vain puolta niiden nimellisvirrasta. Komponentit valitaan siten, että niiden kytkentälukumäärä on kymmenen kertaa vähemmän kuin laitteille ilmoitettu mekaaninen ja sähköinen elinikä. Turvaratkaisut pyritään toteuttamaan mahdollisimman pienellä komponenttimäärällä. Turvallisuustoimintoihin liittyvät komponentit ja kaapeloinnit pidetään erillään muista toiminnoista. (Siirilä & Kerttula 2007, 163.)

Komponenttivalinnoilla on suuri merkitys siihen, kuinka korkea suoritustaso voidaan saavuttaa. Laitevalmistaja ilmoittaa laitteen datalehdessä sille suoraan suoritustason, jonka se täyttää, tai MTTFd-arvon keskimääräiselle vaaralliselle vikaantumiselle. Jotkut valmistajat eivät anna suoraan MTTFd-arvoa vaan antavat B10d-arvon, joka ilmoittaa toimintakertojen määrän, jonka jälkeen 10 % komponenteista vikaantuu vaarallisesti. Yleisesti datalehdissä on saatavilla komponenttien mekaaninen ja sähköinen kestävyys. Mekaanisen kestävyyden arvoa voidaan käyttää B10d-arvona silloin, kun laiteessa käytetty kuorma on alle puolet sen nimellistehosta. Muutoin on käytettävä sähköisen kestävyyden arvoa. Joskus voi tulla vastaan komponentteja, joille valmistaja ei ole ilmoittanut mitään edellä mainituista arvoista. Näissä tapauksissa voidaan käyttää komponenteille arvioituja yleisiä MTTFd- tai B10d-arvoja, joita on määritelty yleisille komponenteille standardissa SFS-EN ISO 13849-1 (LIITE 1).

Diagnostiikan kattavuuteen arvon (DCavg) määrittää suurelta osin turvapiirin valvontalaite. Diagnostiikalla tarkoitetaan ohjausjärjestelmän kykyä havaita järjestelmän eri komponenteissa olevat viat. Jos niitä havaitaan, ohjausjärjestelmän on saatettava kone turvalliseen tilaan. Oikein suunnitellussa ohjausjärjestelmässä tapahtuva johtimen irtoaminen tai katkeaminen aiheuttaa koneen pysähtymisen tai

käynnistyksen estämisen. Näin turvallinen tila saavutetaan eikä viasta aiheudu vaaratilannetta. Turvapiirin valvontalaitteissa diagnostiikka hoidetaan yleisesti erillistä takaisinkytkentäpiiriä käyttäen, ja sillä varmistetaan järjestelmän ohjaamien komponenttien toiminta. Lisäksi kehittyneissä laitteissa valvotaan myös turvalaitetta, jolloin saadaan tieto esimerkiksi rikkoontuneesta anturista tai katkenneesta johdosta. Standardin SFS-EN ISO 13849-1 liitteessä E esitellään diagnostiikan kattavuuden arvoja erilaisia valvontaratkaisuja käytettäessä (LIITE 2). (Siirilä & Kerttula 2007, 169.)

TAULUKKO 5. Diagnostiikan kattavuuden tasot (mukaillen ISO 13849-1, 48)

DIAGNOSTIIKAN KATTAVUUSTASO	VAIHTELUALUE %
Olematon	…60
Matala	60…89
Keskimääräinen	90…98
Korkea	98…

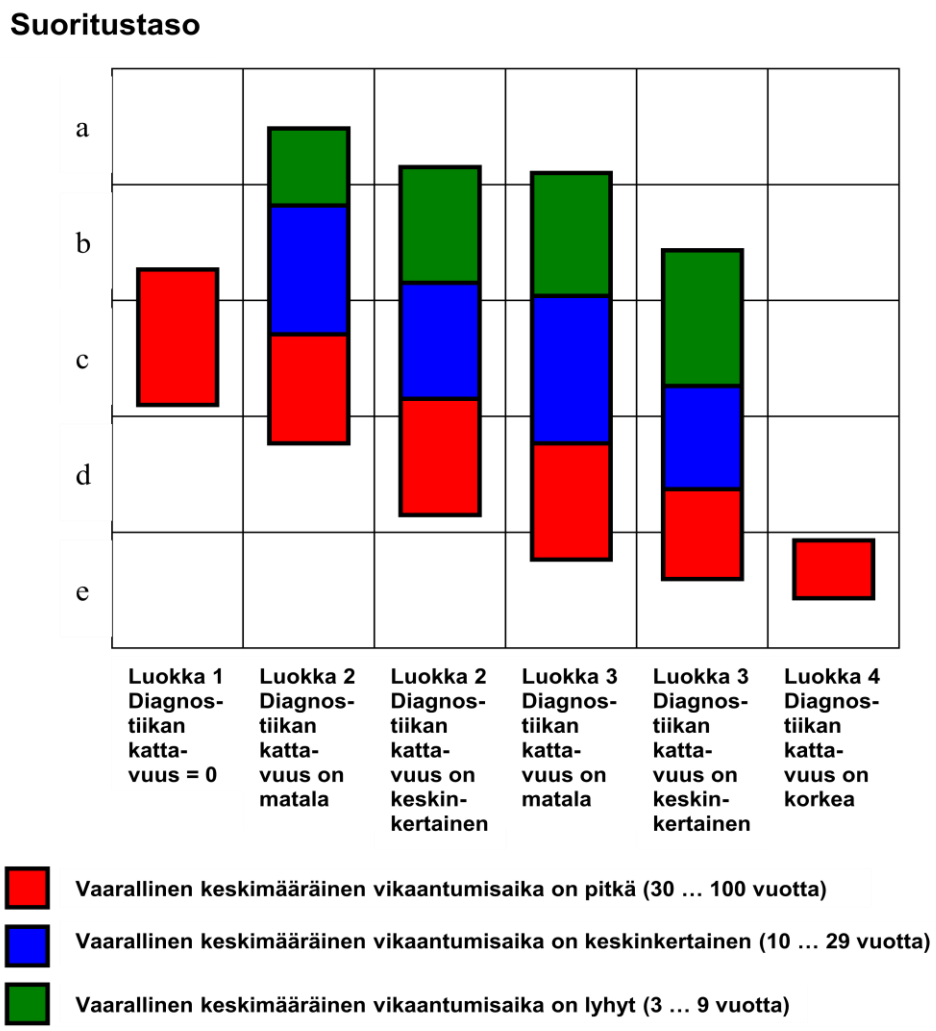
Yhteisvikaantuminen (CCF) tarkoittaa sitä, että yhdestä viasta seuraa vika useampaan laitteeseen. Ohjausjärjestelmän on selvittävä tällaisistakin tilanteista niin, että koneen turvallisuus säilyy. Järjestelmän suunnittelussa on käytettävä standardin SFS-EN ISO 13849-1 liitteen F taulukon mukaisia keinoja yhteisvikaantumisen välttämiseksi (LIITE 3). Yhteisvikaantumisen välttämiseen käytetyistä menetelmistä voi maksimissaan saada 100 pistettä. Järjestelmän on saavutettava vähintään 65 pisteen verran näistä toimenpiteistä, jotta se täyttää yhteisvikaantumisen todennäköisyyden vaatimukset. (Siirilä 2009, 155-158.)

Yhteisvikaantumisen vaaraa voidaan vähentää seuraavilla keinoilla:

- turvallisuuteen liittyvien signaali- ja sähkökaapeleiden suojaaminen tai niiden riittävä erottaminen toisistaan
- erilaisten tekniikoiden (elektroninen komponentti, sähkömagneettinen rele) käyttäminen turvapiirissä
- vika-analyysin tulosten huomioon ottaminen

- laitteiden suojaaminen ylivirralta, ylijännitteeltä ja ylipaineelta
- hyvin koeteltujen komponenttien valinta
- yhteisvikaantumisen vaarojen ymmärtäminen (suunnittelijat ja kunnossapitäjät)
- laitteiden likaantumisen ja sähkömagneettisten häiriöiden estäminen (SFS-EN ISO 13849-1, 132.)

Kaikki kappaleessa Turvapiirin suunnittelu esitellyt asiat vaikuttavat osaltaan siihen, mihin suoritustasoon suunnitellulla järjestelmällä on mahdollista päästä. Lopullinen suoritustaso määräytyy siitä, miten nämä asiat ovat tasapainossa keskenään (KUVIO 4).



KUVIO 5. Eri luokkien avulla saavutettavissa oleva suoritustaso (Siirilä 2009, 167)

Kuviosta 4 voidaan havaita, että luokan 1 yksikanavaisella rakenteella voidaan melkein saavuttaa suoritustaso c, kun vaarallinen vikaantumisaika on pitkä. Toisaalta luokan 3 kahdennetulla ja valvotulla rakenteella saavutetaan vain sama suoritustaso c, kun vaarallinen vikaantumisaika on keskinkertainen ja diagnostiikan kattavuus on 90…98 %.

4.2 Turvapiirin valvontalaitteet

Kaikki turvatoiminnon aikaansaavat komponentit kuuluvat turvapiiriin. Se on ketju, joka alkaa turvalaitteesta ja päättyy esimerkiksi energiansyötön katkaiseviin kontaktoreihin. Turvapiirissä on aina valvontalaite, joka tutkii turvalaitteelta tulevaa signaalia ja toteuttaa sen perusteella turvatoiminnon. Valvontalaitteina voidaan käyttää ohjelmoitavaa logiikkaa, turvarelettä tai ohjelmoitavaa turvalogiikkaa. Jokaisella komponentilla on käyttötarkoituksesta riippuen omat hyvät puolensa.

Ohjelmoitava logiikka on yleinen automaattisten koneiden ohjauslaite. Sitä voidaan käyttää myös turvapiirien valvontaan, mutta sillä ei saada aikaan niin hyvää diagnostiikan kattavuutta kuin turvapiirien valvontaan valmistetuilla laitteilla. Ohjelmoitavan logiikan ohjelmalla on mahdollista tehdä aikaperusteista valvontaa, mutta sillä saavutetaan vain matala diagnostiikan kattavuus. Ohjelmoitavaa logiikkaa on kuitenkin hyödyllistä käyttää esimerkiksi vanhan koneen saneerauksen yhteydessä niissä tapauksissa, joissa sähkökeskuksissa ei ole riittävästi tilaa uusille valvontalaitteille ja ohjelmoitava logiikka on keskuksessa jo entuudestaan. Ohjelmoitavaa logiikkaa käytettäessä turvapiireistä voi tulla monimutkaisia, koska muita komponentteja tarvitaan turvapiiriin enemmän. Monimutkaisuus ja suuri komponenttien määrä voivat aiheuttaa sekaannusta, ja piirillä on suurempi todennäköisyys vikaantua.

Turvarele on turvapiirien valvontaan suunniteltu laite, jolla voidaan valvoa pieniä ja yksinkertaisia turvapiirejä. Turvarele sisältää kaksi erillistä relettä, joita ohjataan samalla ohjaussignaalilla. Erillisten releiden koskettimet on kytketty sarjaan, ja ne ovat pakkotoimisia luotettavamman turvatoiminnon aikaansaamiseksi. Pakkotoimisuudella tarkoitetaan koskettimien mekaanista yhteen kytkentää, jolloin kaikki koskettimet vaihtavat tilansa samanaikaisesti. Turvareleellä aikaansaatava hyvä suoritustaso sekä korkea diagnostiikan kattavuus saavutetaan kahdennetuilla piireillä ja kattavalla valvonnalla. Turvarele kykenee itse testaamaan valvottavan turvalaitteen piiriä ja takaisinkytkennän avulla ohjattavia toimilaitteita. Jos turvarele havaitsee turvalaitteen tilan muutoksen tai piirissä olevan vian, se katkaisee jännitesyötöt ohjattavilta toimilaitteilta, ja koneen turvallinen tila saavutetaan. Turvarele on mahdollista kuitata takaisin toimintaan automaatti- tai käsikuittauksella, jos vika piirissä on poistunut ja turvalaite muuttanut tilan takaisin. Turvareleen valinta valvontalaitteeksi on perusteltua silloin, kun turvapiirissä on yhdestä kahteen valvottua turvalaitetta ja kummallakin niistä saadaan aikaan sama turvallinen tila, esimerkiksi kaikkien liikkeiden pysäyttäminen.

Turvalogiikka on yleisin valvontalaite konelinjoissa tai suurissa koneissa, joissa turvalaitteiden määrä on suurempi ja ohjausjärjestelmältä vaaditaan monentasoisia turvatoimintoja. Turvalogiikan etuina turvareleeseen verrattuna ovat suurempi turvatulojen ja -lähtöjen määrä. Lisäksi turvalogiikalla on mahdollista tehdä useita eritasoisia turvapysäytyksiä. Esimerkiksi hätäpysäytyspainikkeeseen vaikutettaessa kaikki koneen liikkeet pysähtyvät, kun taas valoverhoon vaikuttaminen pysäyttää vain yhden kuljettimen. Turvalogiikalla on mahdollista päästä korkeaan diagnostiikan kattavuuteen kattavan valvonnan avulla. Suurin ero turvalogiikan ja turvareleen välillä on se, että turvarele voidaan ottaa käyttöön pelkillä kytkennöillä, mutta turvalogiikan toiminta täytyy määrittää ohjelmallisesti. Useimmat ohjelmoitavat logiikat voidaan kytkeä osaksi turvaväylää, jolloin on mahdollista muodostaa suuriakin turvakokonaisuuksia.

4.3 Vaarallisten liikkeiden pysäyttäminen

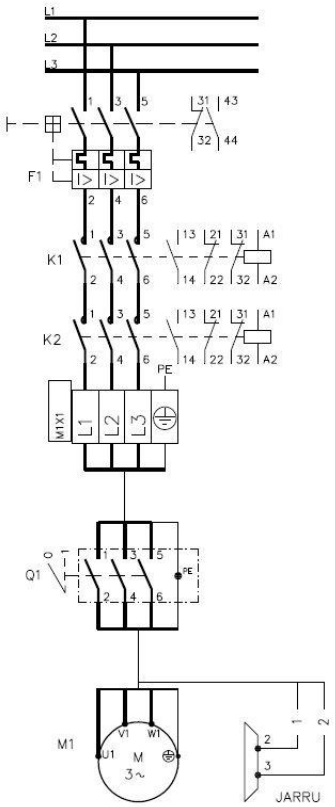
Kappaleessa Koneen pysäyttäminen todettiin, että koneen ohjausjärjestelmän suorittamassa turvapysäytyksessä koneen vaaralliset liikkeet on pysäytettävä niin nopeasti kuin mahdollista. Sähköisesti ohjattavissa koneissa tämä tarkoittaa sähkönsyötön katkaisemista toimilaitteilta, jotka saavat aikaan liikkeitä. Liikkeitä tuotetaan tavallisesti moottoreilla, paineilmalla tai hydrauliikalla. Moottoreita käytettäessä voidaan valita suora moottorilähtö tai taajuusmuuttajalla ohjattuja moottori. Hydrauliikkaa tai paineilmaa käytettäessä konetta ohjataan venttiileillä. Esittelen tässä kappaleessa liitteenä olevien yksinkertaisten mallipiirikaavioiden avulla vaihtoehtoja turvatoiminnon toteuttamiseen.

4.3.1 Suora moottorilähtö

Mallipiirissä 1 (LIITE 4) on kuvattu turvatoiminto, jossa on kaksi sarjaan kytkettyä turvarelettä. Ensimmäinen valvoo hätäpysäytyspainiketta ja toinen kosketuksetonta ovirajaa. Hätäpysäytintä painamalla tai turvaovi avaamalla saavutetaan sama turvatoiminto, eli suoralla käytöllä ohjattavan moottorin pysähtyminen kontaktoreiden avulla.

Suoralla käytöllä ohjattavan moottorin turvapysäyttäminen toteutetaan kontaktoreilla moottorin päävirtapiirissä (KUVIO 6). Jos vaadittuun suoritustasoon pääseminen vaatii piirin kahdentamista, joudutaan moottorin syöttöjännite katkaisemaan kahdella turvapiirin ohjaamalla kontaktorilla. Niiden koskettimien kiinnihitsautumisen valvonta toteutetaan avautuvilla koskettimilla, jotka kytketään turvareleiden takaisinkytkentäpiireihin. Liikkeiden nopeaan pysäyttämiseen käytetään jarrua, joka pysäyttää moottorin jousivoimalla sähkönsyötön katketessa. Kun moottori

halutaan käynnistää, sähkönsyöttö palautuu moottorille ja jarru aukeaa. Tällaisella turvapiirillä voidaan saavuttaa suoritustaso d (LIITE 4).



KUVIO 6. Suoran moottorilähdön turvapysäyttäminen kontaktoreilla

4.3.2 Taajuusmuuttajalla ohjattu moottori

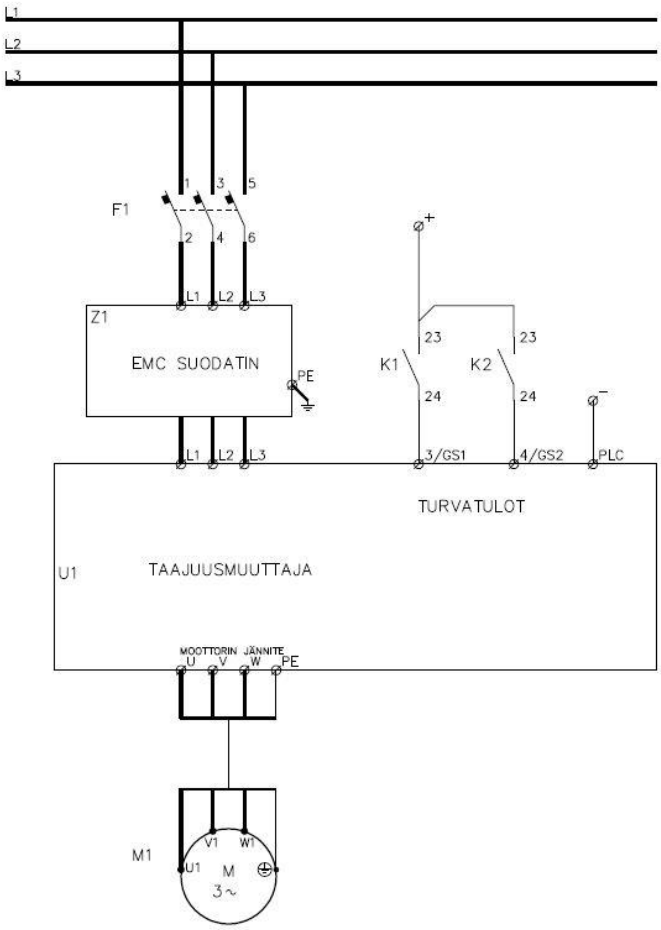
Taajuusmuuttajalla ohjattu moottori on yleinen ratkaisu koneissa, joissa tarvitaan momentin tai nopeuden säätöä. Myös taajuusmuuttajalla ohjatun moottorin pysäyttäminen voidaan hoitaa katkaisemalla päävirtapiiri kontaktoreilla. Mallipiirissä 2 (LIITE 5) on esitetty turvalogiikalla toteutettu turvapiiri. Turvalogiikka valvoo hätäpysäytyspainiketta ja ovirajaa. Turvaovi on lisäksi varustettu lukolla, jota ohjataan turvalogiikalla. Hätäpysäytyspainiketta painamalla tai turvaovi avaamalla saavutetaan koneen turvallinen tila, jolloin taajuusmuuttajalla ohjattu moottori pysähtyy. Kontaktorien koskettimien kiinnihitsautumisen valvonta hoidetaan turvalogiikan takaisinkytkentäpiirillä, ja oven lukinnan lukitustieto saadaan omana piirinään tur-

valogiikkaan. Moottorin nopeaa pysäyttämistä varten voidaan käyttää sähköllä avattavaa jarrua. Liitteen 5 mukaisella turvapiirillä voidaan saavuttaa suoritustaso d.

4.3.3 Turvataajuusmuuttajalla ohjattu moottori

Taajuusmuuttajan jatkuva sähkönsyötön katkaiseminen rasittaa taajuusmuuttajaa ja voi lyhentää sen käyttöikää. Tämän takia uudempiin taajuusmuuttajiin on kehitetty sisäinen turvatoiminto Safe Torque Off (STO), jonka avulla taajuusmuuttajalla ohjattu moottori saadaan pysäytettyä ohjauspiirin avulla. Taajuusmuuttajassa on turvatulot, joihin kytketään jännite silloin, kun turvapiiri sallii koneen liikkeet. Turvapiiri on kahdennettu, eli kumpaankin turvatuloon on syötettävä ohjausjännite, jotta taajuusmuuttaja voi ohjata moottoria. Turvatulojen käytön etuna on komponenttien määrän pieneneminen turvapiirissä, koska sähkönsyöttöä katkaisevia kontaktoreita ei tarvita.

Mallipiirissä 3 (LIITE 6) esitetään turvapiiri, joka on toteutettu turvalogiikalla. Se valvoo hätäpysäytyspainiketta ja valoverhoa. Hätäpysäytintä painettaessa tai valoverhon havahtuessa aikaansaadaan turvatoiminto, jolloin turvataajuusmuuttajalla ohjattu moottori pysäytetään releiden koskettimien katkaiseman ohjausjännitteen avulla. Releiden avautuvat koskettimet sekä turvataajuusmuuttajan takaisinkytkentätieto on kytketty turvalogiikan takaisinkytkentäpiiriin, jotta turvalogiikka voi havaita laitteissa ilmenevät viat. Käytettäessä turvataajuusmuuttajaa voidaan myös jarrun ohjaus toteuttaa taajuusmuuttajalla, koska turvapysäytyksessäkin taajuusmuuttajan sähkönsyöttö säilyy ja se voi ohjata releen avulla moottorin jarrua.

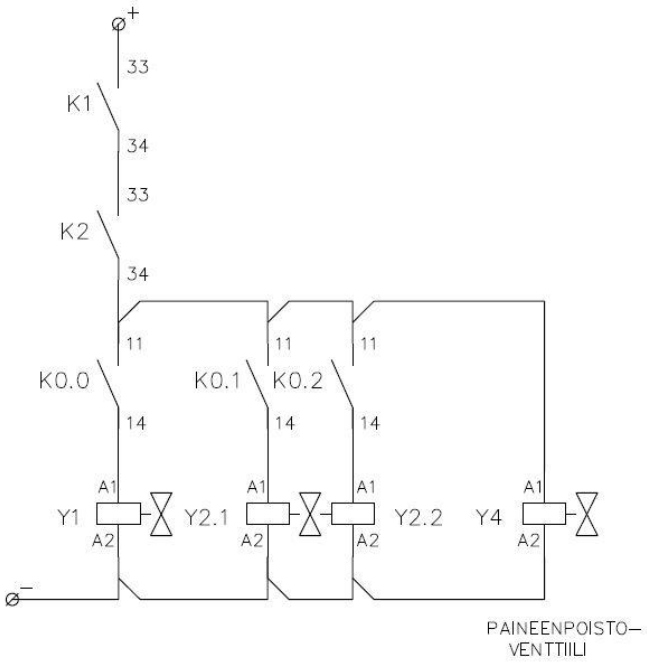


KUVIO 7. Taajuusmuuttajalla ohjatun moottorin pysäyttäminen turvatuloilla

4.3.4 Venttiiliohjaukset

Käytettäessä hydrauliikkaa ja paineilmaa koneen liikkeiden tuottamiseen on muistettava myös vaarallisten liikkeiden pysäyttäminen. Mallikuvassa 3 (LIITE 6) on esitetty turvataajuusmuuttajalla ohjatun moottorin lisäksi myös paineilmaventtiileiden ohjauksia. Turvatoiminnon tapahtuessa turvatoiminnon aikaansaavien releiden koskettimet aukeavat, joten paineilmaventtiilien sähkönsyöttö katkeaa. Tämä aiheuttaa sen, että jousella palautuva venttiili Y1 sulkeutuu, mutta kaksisuuntainen venttiili Y2 jää siihen tilaan, jossa se sattuu turvatoiminnon tapahtuessa olemaan. Venttiili Y2 voi tässä tapauksessa mahdollistaa liikkeet, vaikka sähkönsyöttö olisi katkaistu. Liikkeiden estämiseksi on käytettävä paineenpoistoventtiiliä Y4, joka

turvatoiminnon sattuessa poistaa ilman koneen paineilmajärjestelmästä, jolloin koneen liikkeet pysähtyvät. Releiden kärkien K0.0 – K0.2 ajatellaan ohjautuvan konetta ohjaavan logiikan avulla. (KUVIO 7).



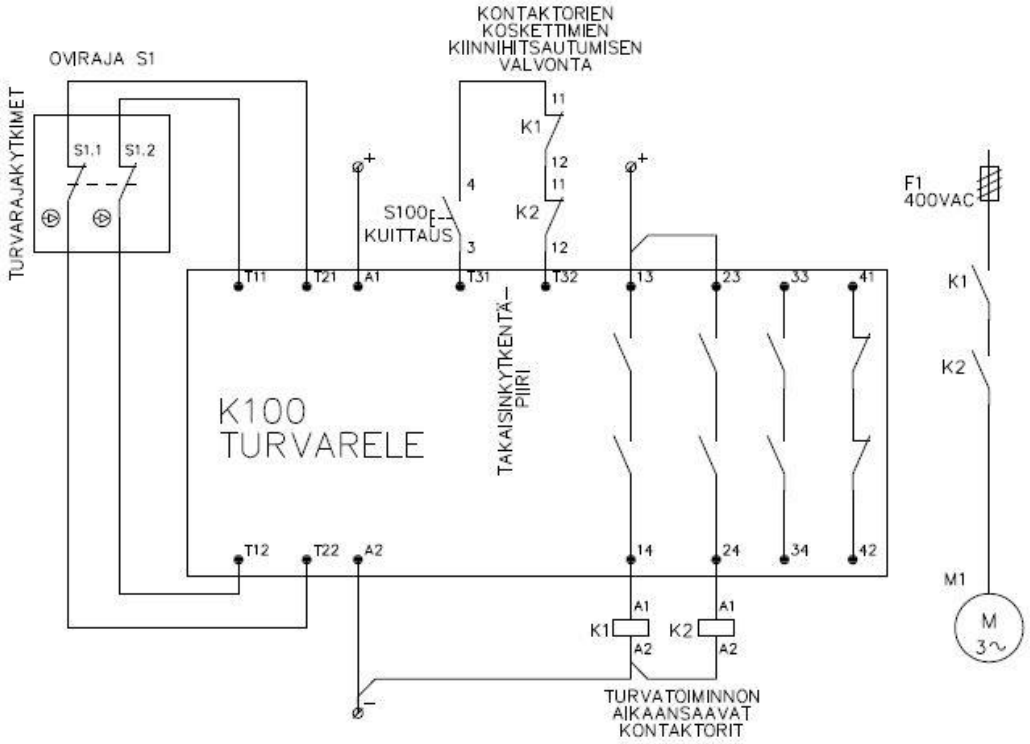
KUVIO 8. Venttiilien turvatoiminnon toteutus

Mallipiirissä 3 (LIITE 6) on esitetty kokonaisuutena kuvion 7 sisältö. Liitteestä 6 voidaan havaita, että turvapiiri on muilta osin rakenteeltaan kahdennettu, mutta venttiilit ovat rakenteeltaan luokkaa 1. Tästä seuraa, että turvapiirillä voidaan saavuttaa vain suoritustaso c. Jos ohjausjärjestelmän vaadittu suoritustaso olisi korkeampi, venttiilit pitäisi vaihtaa kahdennettuihin turvaventtiileihin tai niiden asentotietoa valvoa.

4.4 Sistema-ohjelmistotyökalu

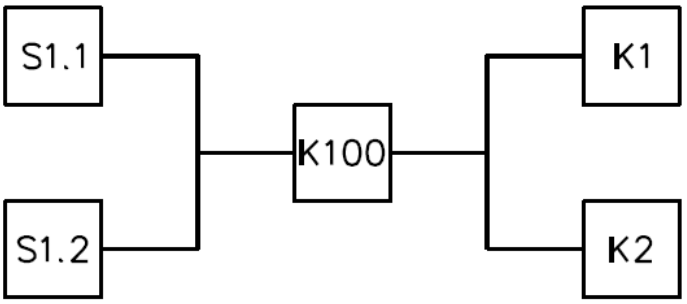
Sistema on Saksassa IFA:ssa kehitetty tietokoneavusteinen suunnitteluohjelma koneiden turvallisuuteen liittyvien ohjausjärjestelmien suunnitteluun. Ohjelmisto on ilmainen, ja siitä on tehty myös suomennos. Sistema kattaa kaikilla eri teknologioilla toteutettavat koneiden ohjausjärjestelmät. Se perustuu kaikilta osin standardin SFS-EN ISO 13849-1 määräyksiin. Ohjelmiston automaattisella laskennalla voidaan selvittää suunnitellun ohjausjärjestelmän saavuttama suoritustaso. Ohjelmiston käytön etuna on, että vältytään hankalilta luotettavuusteknisiltä laskelmilta, jotka perustuvat Markovin dynaamisiin malliratkaisuihin. Yhdenmukaisten käsitteiden ja menetelmien seurauksena suunnitteluvirheet ja väärinkäsitykset vähenevät. Lisäksi vaatimustenmukaisuuden varmistamisesta ja dokumenttien laadinnasta tulee helpompaa. (Sundquist 2009.)

Ennen varsinaisen ohjelman käyttöä suunnittelijan pitää laatia toiminnallinen piirikaavio turvatoiminnosta, jonka hän haluaa ohjelmistolla todentaa (KUVIO 9). Toiminnallisella piirikaaviolla tarkoitetaan yksinkertaistettua piirikaaviota, johon on piirretty kaikki turvapiirin kannalta olennaiset komponentit. Sellaisia komponentteja, jotka eivät vaikuta turvatoiminnon suorittamiseen, ei tarvitse esittää toiminnallisessa piirikaaviossa.



KUVIO 9. Turvatoiminnon toiminnallinen piirikaavio

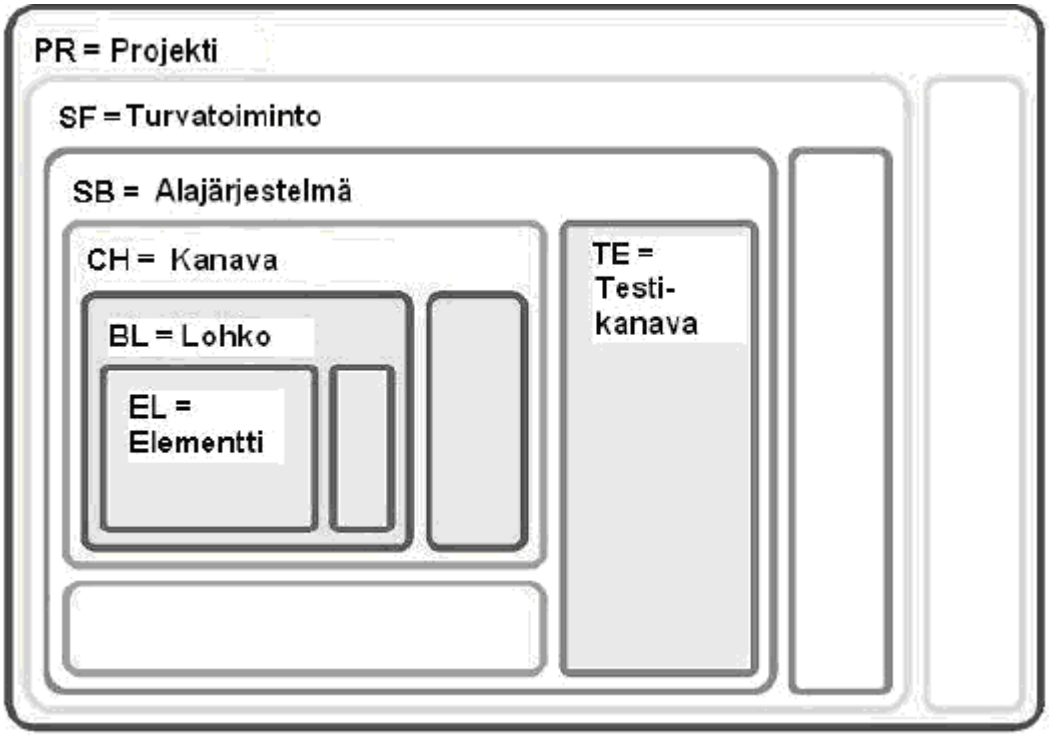
Toiminnallisesta piirikaaviosta muodostetaan turvallisuuteen liittyvä lohkokaavio, jossa näkyy jokainen turvallisuuteen vaikuttava komponentti anturista toimilaitteeseen (KUVIO 10). Jos turvatoiminnossa käytetään kaksikanavaista rakennetta, molempien kanavien tulee näkyä lohkokaaviossa.



KUVIO 10. Turvallisuuteen liittyvä lohkokaavio

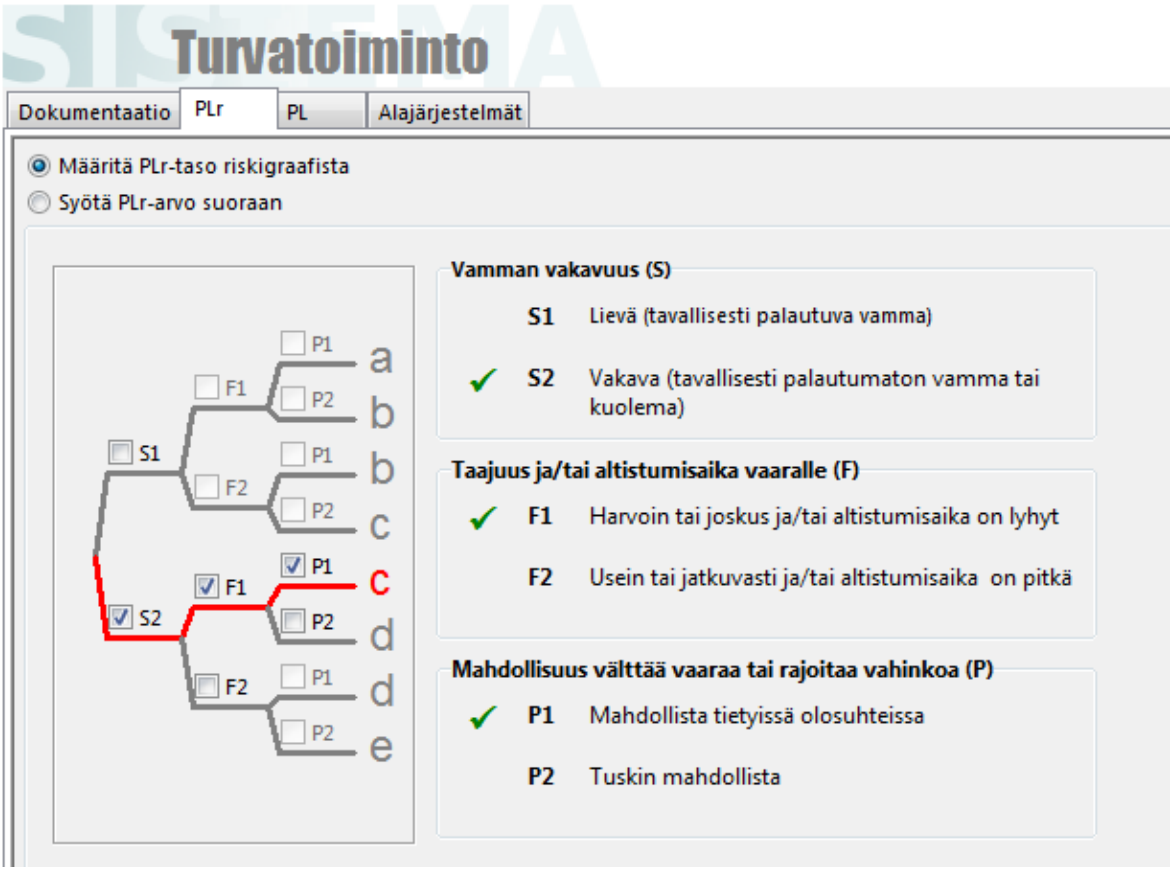
Turvallisuuteen liittyvän lohkokaavion avulla voidaan aloittaa varsinainen ohjelmiston käyttö. Sen aloitus alkaa luomalla uusi projekti (PR) ohjelmaan. Ohjelma käyt-

tää hierarkiaa, jossa projekti on jaettu turvatoimintoihin ja ne edelleen pienempiin osiin laitetasolle (KUVIO 11).



KUVIO 11. Sistema-ohjelmiston hierarkia (Sundquist 2010, 11)

Projektin luomisen jälkeen sille voidaan lisätä turvatoiminto (SF), jolle määritellään riskien arvioinnista saatu vaadittava suoritustaso PLr. Jos riskien arviointia ei ole tehty erikseen, voidaan vaadittava suoritustaso määrittää ohjelmistossa olevalla riskigraafilla (KUVIO 12). Se perustuu täysin standardissa SFS-EN ISO 13849-1 esitettyyn riskien arviointimenetelmään.



KUVIO 12. Sistema-ohjelmiston riskigraafi

Kun turvatoiminto ja siltä vaadittava suoritustaso on määritelty, voidaan aloittaa turvallisuuteen liittyvän lohkokaavion tietojen lisääminen turvatoimintoon. Tässä vaiheessa komponenttivalintojen pitää olla tehtynä, koska niiden toiminta-arvot täytyy tuntea laskennassa. Komponentit lisätään turvatoiminnon alajärjestelmään (SB) komponenttikohtaisesti. Jos samaa komponenttia käytetään usein samassa turvatoiminnossa, riittää, kun se lisätään kerran alajärjestelmään. Jos järjestelmä sisältää kahdennuksia, nämä lisätään alajärjestelmissä oleviin kanaviin (CH).

Komponentin syöttäminen onnistuu kahdella tavalla. Useimmilla valmistajilla on ladattavissa ohjelmistoon turvakomponenteistaan kirjasto, josta komponentin voi lisätä laskentaan. Valmistaja on määrittänyt kirjastossa oleville komponenteille luokan, MTTFd-arvon ja DCavg-arvon, joten komponentti täytyy vain lisätä alajärjestelmään, eikä muita muutoksia tarvitse tehdä. Toinen tapa on määrittää komponentti manuaalisesti. Tätä tapaa tarvitaan, jos valmistajan kirjastosta ei löydy ky-

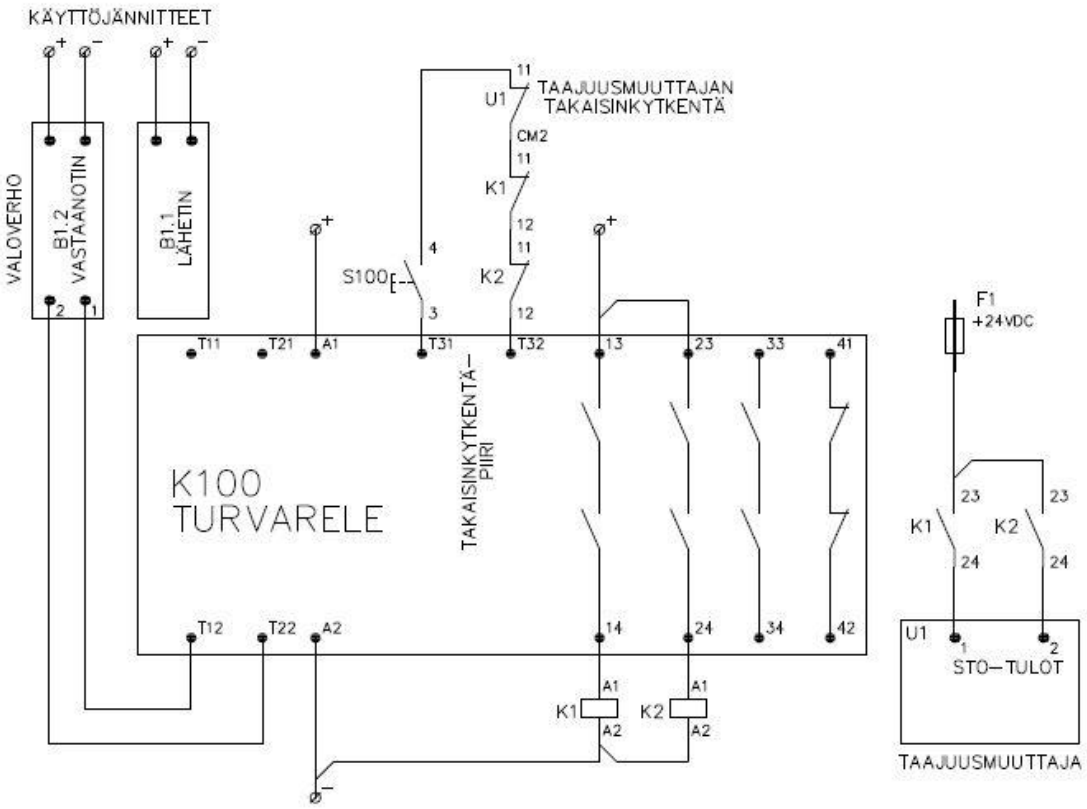
seistä komponenttia. Jotkut valmistajat voivat ilmoittaa suoraan laitteelleen suoritustason, jonka vaatimukset se täyttää. Tällöin voidaan lisätylle alajärjestelmälle syöttää tieto täytetystä suoritustasosta, eikä muuta tietoa tarvita

Monille komponenteille valmistaja on ilmoittanut datalehdessään vain B10d-arvon. Tällaisissa tapauksissa komponentille on määriteltävä luokka ja DCavg-arvo. Lisäksi B10d-arvo on lisättävä elementtitasolle (EL). Käytettäessä komponentin B10d-arvoa täytyy ohjelmalle syöttää arvioitu komponentin käyttökertojen määrä, jonka avulla ohjelma laskee komponentille MTTFd-arvon todennuslaskentaan.

Kun kaikki turvallisuuteen liittyvän lohkokaavion laitteet on lisätty laskentaohjelmistoon ja laitteille syötetty tarvittavat arvot, voidaan suorittaa todentamislaskenta. Sistema laskee syötetyillä arvoilla turvapiirin saavuttaman suoritustason PL ja vertaa sitä riskigraafilla tai riskien arvioinnilla saatuun tasoon PLr. Turvapiiri hyväksytään, jos sen saavuttama suoritustaso on vähintään sama kuin vaadittu suoritustaso. Ohjelma antaa raportin turvapiirien saavuttamista suoritustasoista (LIITE 4). Raportit liitetään koneen dokumentteihin todistamaan sitä, että koneen ohjausjärjestelmä täyttää sille määritellyt turvallisuusvaatimukset.

4.5 Turvapiirin todentaminen Sistema-ohjelmistotyökalulla

Käsittelen tässä kappaleessa esimerkkitapauksen turvapiirin todentamisesta edellisessä luvussa mainittujen ohjeiden mukaisesti. Esimerkki kattaa kolme eri tapaa lisätä komponentti laskentaan. Käytän esimerkkipiirinä valoverholla valvottua taajuusmuuttajaohjattua kuljetinta. Taajuusmuuttajassa turvapysäytyksen toteuttamiseen on käytetty turvapiirin ohjaamia turvatuloja (KUVIO 13).



KUVIO 13. Todennettavan turvatoiminnon toiminnallinen piirikaavio

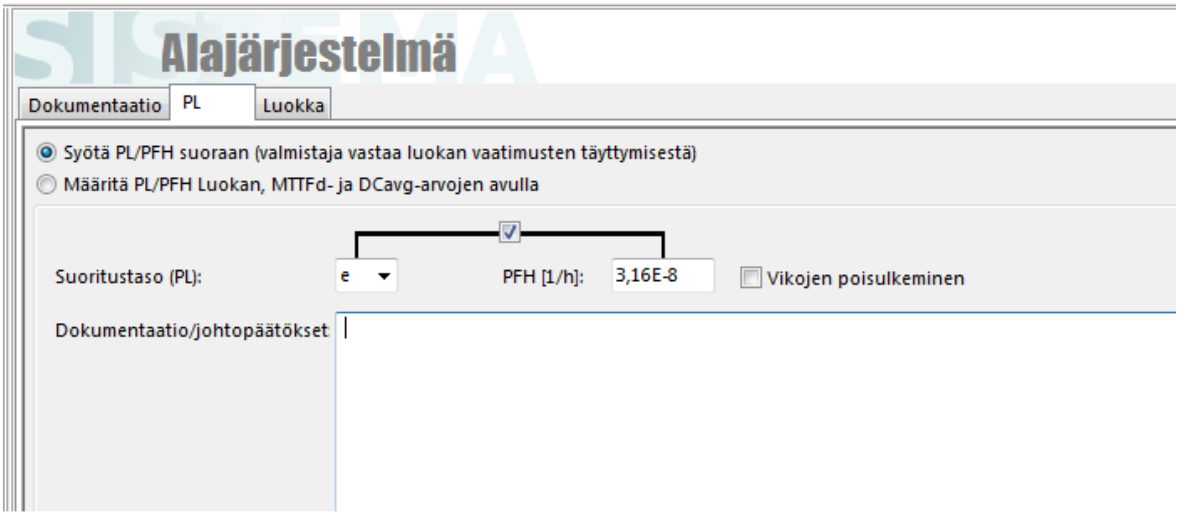
Ennen turvapiirin syöttämistä ohjelmistoon on syytä ladata laitevalmistajien komponenteistaan laatimat kirjastot ja avata ne ohjelmistoon. Kirjastot ovat ladattavissa ilmaiseksi ohjelmiston verkkosivujen kautta.

Todentaminen aloitetaan perustamalla uusi projekti. Projektille perustetaan turvatoiminto ja nimetään se esimerkiksi Kuljettimen valvonta. Turvatoiminnolle määritellään riskien arvioinnilla saatu vaadittu suoritustaso. Ajatellaan sen olevan tässä esimerkissä PLd.

4.5.1 Valoverho

Turvapiirissä (KUVIO 13) olevat komponentit B1.1 ja B1.2 on Omronin valmistama valoverho F3S-TGR-CL4, jossa on lähetin ja vastaanotin. Valmistaja ilmoittaa datalehdessään valoverhon täyttävän suoritustason PLe vaatimukset.

Valoverhon lisääminen laskentaan tapahtuu perustamalla turvatoiminnolle uusi alajärjestelmä, joka nimetään välilehdellä Dokumentaatio nimellä Valoverho. Siirrytään välilehdelle PL, jossa määritellään komponentille suoraan suoritustaso PLe, koska valmistaja ilmoittaa datalehdessään sen täyttyvän (KUVIO 14). Muita muutoksia komponentille ei tarvitse tehdä, koska ohjelmiston automatiikka vaihtaa välilehdellä Luokka olevan luokan automaattisesti tasolle 4.

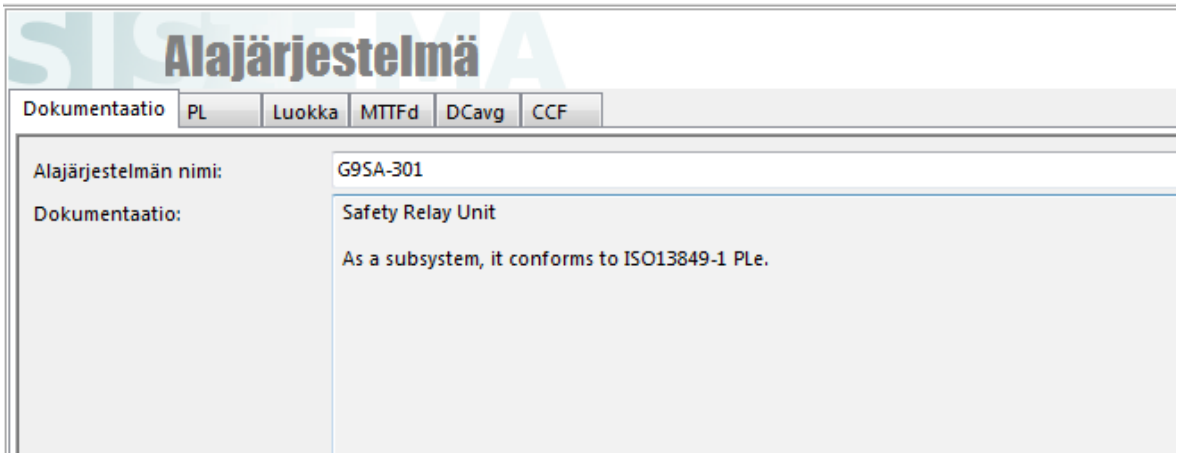


KUVIO 14. Suoritustason määrittäminen suoraan komponentille

4.5.2 Turvarele

Turvapiirissä (KUVIO 13) oleva komponentti K100 on Omronin valmistama turvarele G9SA-301. Laite löytyy suoraan Omronin laatimasta turvakomponenttien kirjastosta.

Turvareleen lisääminen laskentaan tapahtuu lataamalla turvatoiminnolle kirjastosta uusi alajärjestelmä. Omronin turvakomponenttien kirjaston täytyy olla ladattuna tietokoneelle, ja se pitää lisätä ohjelmaan. Tämän jälkeen voidaan valita Omronin kirjastosta turvarele laitetunnuksella G9SA-301 ja ladata se turvatoimintoon (KUVIO 15). Muita muutoksia ei tarvitse tehdä, koska valmistaja on määrittänyt laitteen arvot kirjaston komponenteille.



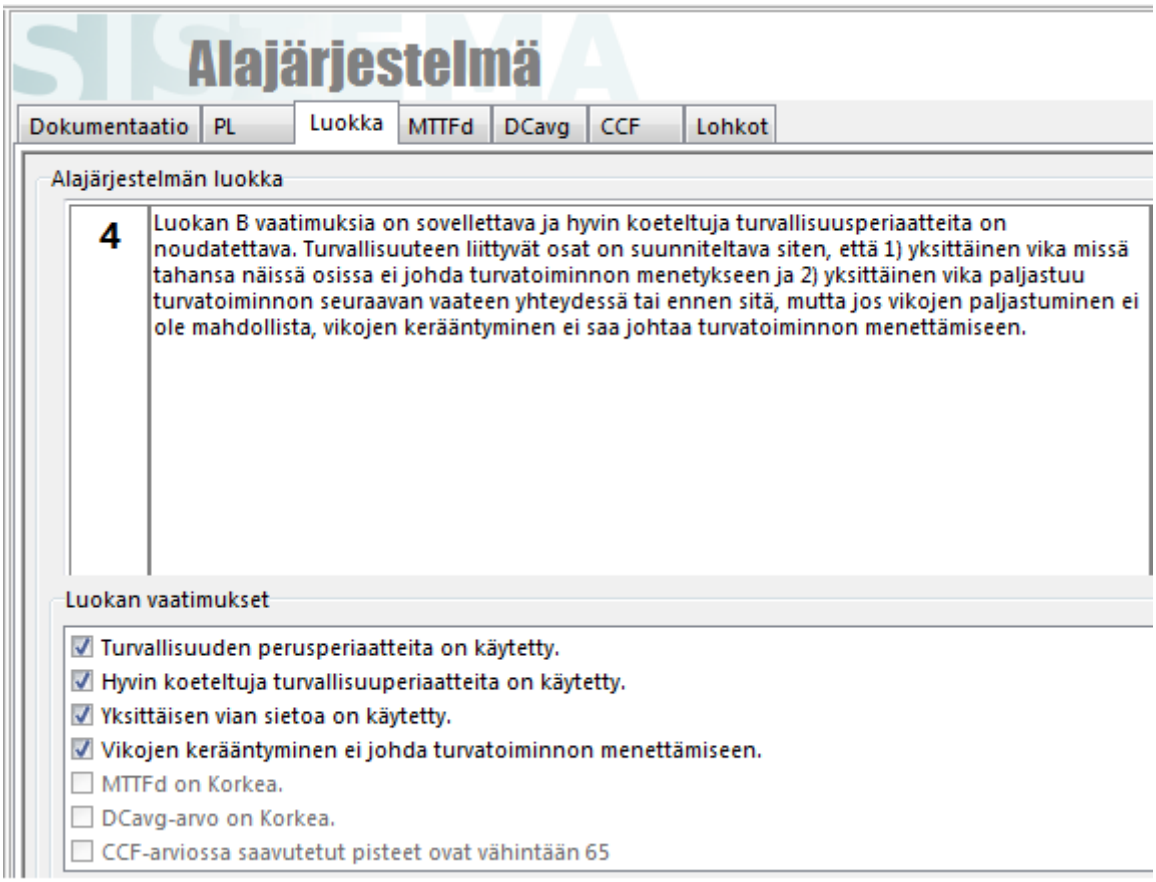
KUVIO 15. Komponenttikirjastosta lisätty turvarele

4.5.3 Turvakäyttöön hyväksytty rele

Turvapiirissä (KUVIO 13) olevat komponentit K1 ja K2 ovat Omronin valmistamia G7SA turvakäyttöön hyväksyttyjä releitä. Komponentteja ei ole saatavissa valmis-

tajan kirjastosta, eikä niille ole määritelty niiden täyttämää suoritustasoa, joten komponentit on lisättävä manuaalisesti laskentaan. Valmistaja ilmoittaa komponenttien mekaaniseksi eliniäksi 10 miljoonaa käyttökertaa.

Releiden lisääminen laskentaan aloitetaan lisäämällä uusi alajärjestelmä ja nimeämällä se G7SA-turvahyväksytyt releet. Nimeämisen jälkeen siirrytään lehdelle PL ja valitaan vaihtoehto Määritä PL/PFH Luokan, MTTFd- ja DCavg-arvojen avulla, koska releet täytyy lisätä manuaalisesti. Tämän jälkeen siirrytään välilehdelle Luokka, jossa määritellään alajärjestelmän luokaksi 4, koska turvapiiri on kahdennettu ja releiden avautuvat koskettimet kytketty turvareleen takaisinkytkentäpiiriin (KUVIO 16). Takaisinkytkennällä mahdolliset viat paljastuvat.

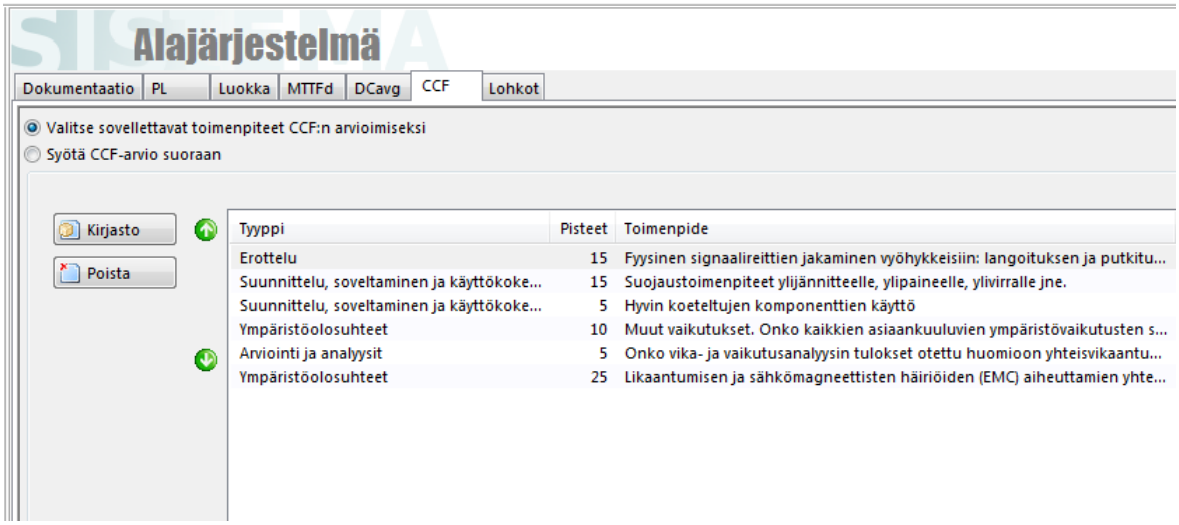


KUVIO 16. Alajärjestelmän luokan valinta ja lisävaatimukset

Luokan 4 lisävaatimuksena on, että turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita on käytetty. Olen esittänyt nämä asiat kappaleessa Turvapiirin suunnittelu. Jos vaatimukset täytetään, ne voidaan valita täytetyksi yllä olevan kuvan mukaisesti. Lisäksi vaatimuksena on yksittäisen vian sieto ja se, että vikojen kerääntyminen ei saa johtaa turvatoiminnon menettämiseen. Kun turvapiirin valvontalaitteena on turvarele, viat havaitaan, joten niitä ei pääse kertymään. Piirin kahdennuksella saadaan aikaan yhden vian sieto, joten vaatimukset yksittäisestä viansiedosta ja vikojen kerääntymisestä tulevat täytetyiksi.

Kun alajärjestelmän luokka 4 on valittu, ohjelmisto tekee piiristä automaattisesti kahdennetun. Koska releen arvot syötetään manuaalisesti ja piiri on kahdennettu, voidaan valita välilehdillä MTTFd ja DCavg valinnat Määritä arvo lohkojen avulla.

Näiden valintojen jälkeen siirrytään välilehdelle CCF. Tällä välilehdellä täytyy määrittää toimet, jotka on tehty yhteisvikaantumisen välttämiseksi. Ohjelmassa on valmis kirjasto, josta löytyy standardin SFS-EN ISO 13849-1 mukainen luettelo toimintoja yhteisvikaantumisen välttämiseksi (KUVIO 17). Kirjastosta valitaan ne toimet, jotka on otettu huomioon suunnittelussa. Valituista toimenpiteistä pitää saada vähintään 65 pistettä, jotta vaatimukset yhteisvikaantumisen välttämisestä täyttyvät. Jos pistemäärä on arvioitu standardin taulukon mukaan, sen voi syöttää myös suoraan ohjelmaan.



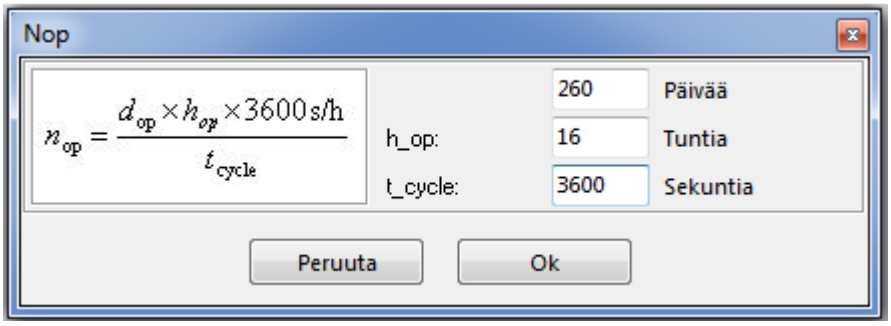
KUVIO 17. Yhteisvikaantumisen välttämiseksi tehdyt toimet

Seuraavaksi siirrytään välilehdelle Lohkot, valitaan Tuntematon lohko ja Muokkaa. Annetaan lohkolle nimi K1. Sen jälkeen siirrytään välilehdille MTTFd ja DC ja valitaan Määritä arvo elementin avulla, jonka jälkeen siirrytään välilehdelle Elementit. Tällä välilehdellä valitaan Tuntematon elementti (EL) ja valitaan Muokkaa. Annetaan elementille nimi K1 ja valitaan sen teknologiaksi Sähkömekaaninen.

Siirrytään lehdelle MTTFd ja valitaan vaihtoehto Määritä MTTFd-arvo B10d-arvon avulla. Valmistaja antaa releen mekaaniseksi eliniäksi 10 miljoonaa kertaa. Mekaanista elinikää voidaan käyttää B10d-arvona, kun komponenttia kuormitetaan alle puolella sen nimellisvirrasta. Tämän releen kärjen virrankesto on kuusi ampeeria, joten turvatulokäytössä virta jää varmasti alle kolmen ampeerin. B10d-arvoksi voidaan syöttää 10 miljoonaa.

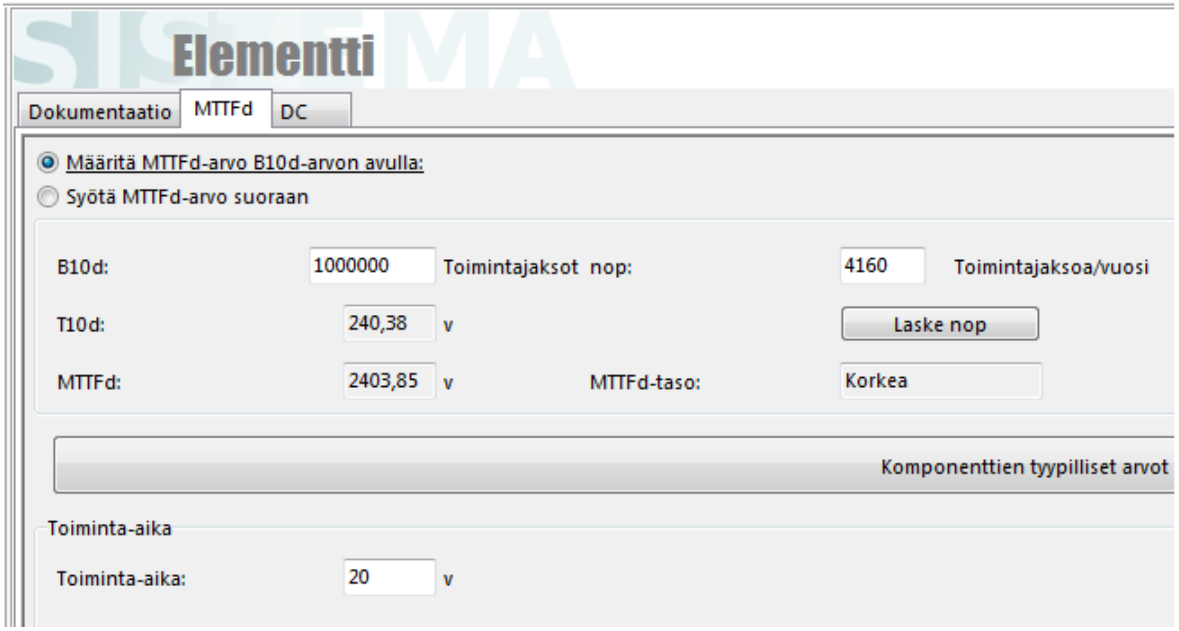
Tämän jälkeen täytyy määrittää turvatoiminnon toimintakertojen määrä vuodessa. Se voidaan laskea ohjelmalla, kun tiedetään koneen käyttötunnit vuodessa ja arvio siitä, kuinka usein turvapysäytystä tarvitaan.

Kuvitellaan, että kuljetinta käytettäisiin koko vuoden ajan, kahdessa vuorossa, viisi päivää viikossa, ja turvatoiminto olisi tarpeen suorittaa kerran tunnissa. Tämä laskenta tekee yhteensä 260 päivää ja käyttöaika on 16 tuntia päivässä. Toimintakertojen laskentaikkuna voidaan täyttää kuvion 18 mukaisesti.



KUVIO 18. Turvatoiminnon toimintakertojen määrän laskenta

Määritetyillä arvoilla ohjelma laskee releen K1 MTTFd-arvon. Se kertoo releen vaarallisen vikaantumisen keskimääräisen ajan, jonka jälkeen se on vaihdettava (KUVIO 19).



KUVIO 19. B10d-arvon avulla laskettu MTTFd-arvo

Lopuksi siirrytään välilehdelle DC ja määritellään elementin diagnostiikan kattavuus. Ohjelmassa on valmis kirjasto, josta löytyy standardin SFS-EN ISO 13849-1 mukainen luettelo diagnostiikan kattavuuden toimenpiteitä ja niiden arvoja. Arvo on mahdollista syöttää myös suoraan elementille. Koska releen K1 avautuva kosketin on kytketty turvareleen takaisinkytkentäpiiriin, voidaan diagnostiikan kattavuudeksi asettaa 99 %.

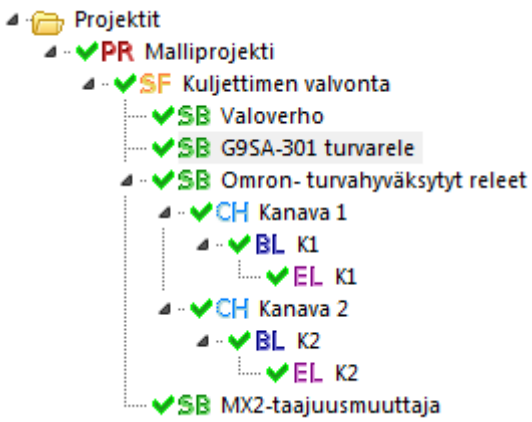
Nyt turvahyväksytty rele K1 on lisätty ja määritetty kanavaan 1. Tämän jälkeen releen K2 määrittäminen kanavaan 2 on helppoa, koska releet ovat samanlaiset ja suorittavat samaa turvatoimintoa. Avataan ohjelmassa vasemmalla sijaitsevasta polusta Kanava 1 ja valitaan lohko K1. Kopioidaan lohko K1 kanavaan 2 ja nimetään lohko ja lohkon sisässä oleva elementti nimellä K2. Nyt kopioidut lohkot ovat määrityksiltään identtiset ja kaikki tarpeellinen releiden määrittämiseksi on tehty.

4.5.4 Taajuusmuuttaja

Turvapiirissä (KUVIO 13) oleva komponentti U1 on Omronin valmistama taajuusmuuttaja MX2. Laitetta ei löydy valmistajan kirjastosta, mutta laitteen tuoteesitteessä ilmoitetaan sen täyttävän suoritustason PLd, kun turvatuloja ja laitteen takaisinkytkentää käytetään. Taajuusmuuttajan takaisinkytkentä näkyy kuviossa 13 koskettimena 11-CM2.

Taajuusmuuttajan lisääminen tapahtuu samoin kuin valoverhonkin lisääminen. Turvatoiminnolle lisätään uusi alajärjestelmä, nimetään se MX2-taajuusmuuttajaksi ja ilmoitetaan sen täyttävän suoritustason PLd. Ohjelman automatiikka valitsee komponentin luokaksi automaattisesti luokan 4. Sitä voidaan käyttää, koska taajuusmuuttajan turvatuloissa on kahdennettu rakenne ja taajuusmuuttajan avautuva kosketin on kytketty turvareleen takaisinkytkentäpiiriin.

Kun kaikki turvapiirin laitteet on syötetty ohjelmaan lohkokaavion mukaisessa järjestyksessä valmistajan antamien arvojen mukaisesti, kaikki tarvittavat määritykset ovat valmiina. Tämän jälkeen laskentapolun tulisi näyttää kuvion 20 mukaiselta. Jos ohjelmalle ei ole syötetty kaikkia todennuslaskentaan tarvittavia tietoja, se ilmoittaa siitä komponenttikohtaisesti. Ohjelman oletuksena on, että todennettavan turvapiirin käyttöikä on 20 vuotta. Jos turvapiirissä on sellaisia komponentteja, jotka eivät täytä vaadittua käyttöikää, ohjelma ilmoittaa komponenttien vaihdon tarpeesta tietyn käyttöajan jälkeen. Kun laskenta on saatu suoritettua ja turvapiirille asetetut vaatimukset täytettyä, voidaan ohjelmasta tulostaa yksityiskohtainen raportti piirin vaatimustenmukaisuudesta (LIITE 7).



KUVIO 20. Turvatoiminnon polku Sistema-ohjelmistossa

5 JOHTOPÄÄTÖKSET JA POHDINTA

Työn tarkoituksena oli selvittää koneiden sähkölaitteistoja ja ohjausjärjestelmiä käsittelevien standardien vaatimuksia sähkösuunnittelijan näkökulmasta. Työ vaati paljon perehtymistä aihetta käsitteleviin standardeihin ja alan kirjallisuuteen. Koneturvallisuutta käsitteleviä standardeja ja kirjallisuutta on saatavilla paljon, joten ongelmana oli työn rajaaminen ja olennaisten asioiden käsittely. Tähän työhön on kerätty paljon keskeistä tietoa siitä, mitä koneen sähkösuunnittelijan tulee perussuunnittelutaitojen lisäksi tietää ohjausjärjestelmästä ja sen vaatimuksista. Luonnollisesti kirjallisuudessa ja standardeissa on paljon hyödyllistä lisätietoa, jota tässä työssä ei käsitellä.

Tarkoituksena oli myös tutkia, millaisilla ohjausjärjestelmäratkaisuilla saavutetaan haluttu suoritustaso ja miten sen vaatimustenmukaisuus todennetaan. Suoritustason määräytymiseen vaikuttavia tekijöitä ovat ohjausjärjestelmän luokka, komponenttien vaarallinen keskimääräinen vikaantumisaika, diagnostiikan kattavuuden keskiarvo ja yhteisvikaantumisen välttämiseksi tehdyt toimet. Koska vaikuttavia tekijöitä on monia, suoritustason lopullinen todentaminen on syytä tehdä siihen suunnitellulla ohjelmistolla.

Sistema-ohjelmisotyökalun käyttäminen on suositeltavaa turvallisuuteen liittyvän ohjausjärjestelmän suunnittelussa. Ohjelmiston avulla voidaan määrittää ohjausjärjestelmän vaadittu suoritustaso ja selvittää suunnitellun ohjausjärjestelmän saavuttama suoritustaso, kun komponenttitiedot ja ohjausjärjestelmän rakenne ovat tiedossa. Ohjelmisto suorittaa vaativat matemaattiset todentamislaskelmat automaattisesti, joten laskuvirheiltä vältytään. Suunnittelijan on kuitenkin tunnettava ohjausjärjestelmää koskevan standardin SFS-EN ISO 13849-1 sisältö, jotta todennettavan ohjausjärjestelmän tiedot syötetään oikein laskentaan. Ohjelmistoon on saatavilla useilta laitevalmistajilta laajat komponenttikirjastot, joten tietojen syöttäminen ohjelmistoon onnistuu tehokkaasti.

LÄHTEET

Apfeld, R., Hauke, M., Schaefer, M., Rempel, P., Ostermann, B. 2010. The SISTEMA Cookbook 1. Sankt Augustin: Institute for Occupational Safety and Health of DGUV (IFA).

Apex Automation Oy. 2011. Www-dokumentti. Saatavissa: http://www.apexautomation.fi/fi. Luettu 21.3.2013

SFS-EN ISO 13849-1. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 2006. Helsinki: Suomen Standardisoimisliitto SFS. Standardien lainaukset on julkaistu Suomen Standardisoimisliito SFS ry:n luvalla.

SFS-EN ISO 13849-2. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. 2008. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-EN 60204-1. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset. 2006. Helsinki: Suomen Standardisoimisliitto SFS.

Siirilä, T. 2013 AMSC-koneturvaseminaari 16.4.2013. Advancetec Oy. Vantaa

Siirilä, T. 2009. KONETURVALLISUUS Ohjausjärjestelmät ja turvalaitteet. 2. uudistettu painos. Keuruu: Inspecta Koulutus Oy.

Siirilä, T., Kerttula, T. 2007. KONETURVALLISUUDEN PERUSTEET. Keuruu: Opiks-Tiimi Oy.

Sundcon Oy. Apex-SKT-koulutusmateriaali, Apex Automation Oy.

Sundquist, M. 2010. Ohjelmistotyökalun Sistema käyttö koneiden turvatoimintojen suunnittelussa. MetSta ry, verkkojulkaisut. Www-dokumentti. Saatavissa: http://www.metsta.fi/www/koneturvallisuuden_teemasivut/artikkelit/2010_nro_004.pdf. Luettu 3.4.2013

Sundquist, M. 2009. Koneiden ohjausjärjestelmien suunnittelutyökalu Sistema. Sesko. Www-dokumentti. Saatavissa: http://www.sesko.fi/attachments/ohjeet/osio_6.pdf. Luettu 2.4.2013

LIITTEET

LIITE 1. SFS-EN ISO 13849-1 Liite C

LIITE 2. SFS-EN ISO 13849-1 Liite E

LIITE 3. SFS-EN ISO 13849-1 Liite F

LIITE 4. Mallipiirikaavio 1. Suoran moottorilähdön turvapysäytys kahta turvarelettä käyttäen

LIITE 5. Mallipiirikaavio 2. Taajuusmuuttajalla ohjatun moottorin turvapysäytys turvalogiikkaa käyttäen

LIITE 6. Mallipiirikaavio 3. Turvataajuusmuuttajan ja venttiileiden turvatoiminnon toteuttaminen turvalogiikkaa käyttäen

LIITE 7. Sisteman raportti todennetusta turvatoiminnosta

Liite C
(opastava)
Vaarallisen keskimääräisen vikaantumisajan ($MTTF_d$) laskenta tai arviointi yksittäisille komponenteille

C.1 Yleistä

Tässä liitteessä esitetään useita menetelmiä vaarallisen keskimääräisen vikaantumisajan arvioimiseksi tai laskemiseksi yksittäisille komponenteille: kohdassa C.2 esitettävä menetelmä perustuu hyvien valmistuskäytäntöjen huomioon ottamiseen erilaisille komponenteille; kohdassa C.3 esitettävä menetelmä on sovellettavissa hydraulisille komponenteille; kohdassa C.4 esitetään menetelmä vaarallisen keskimääräisen vikaantumisajan laskemiseksi pneumaattisille, mekaanisille ja sähkömekaanisille komponenteille B_{10} -arvojen avulla (ks. C.4.1) ja kohdassa C.5 esitetään luettelo sähköisten komponenttien vaarallisista keskimääräisistä vikaantumisajoista.

C.2 Hyvän valmistuskäytännön menetelmä

Jos seuraavat kriteerit täyttyvät, voidaan komponenttien $MTTF_d$- tai B_{10d} -arvot arvioida taulukon C.1 avulla.

a) Komponentit valmistetaan noudattamalla turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita standardin ISO 13849-2:2003 mukaisesti tai komponentin suunnittelu tehdään asiaan kuuluvan standardin (ks. tämän standardin taulukko C.1) mukaisesti (vahvistus tästä on komponentin tuotetiedoissa).

   HUOM. Nämä tiedot voidaan selvittää komponentin valmistajan tuotetiedoista.

b) Komponentin valmistaja erittelee käyttäjälle soveltuvat käyttötarkoitukset ja käyttöolosuhteet.

c) Komponentin toteutuksen ja toiminnan osalta turvallisuuteen liittyvän ohjausjärjestelmän suunnitelma täyttää turvallisuuden perusperiaatteet ja hyvin koetellut turvallisuusperiaatteet standardin ISO 13849-2:2003 mukaisesti.

C.3 Hydrauliset komponentit

Jos seuraavat kriteerit täyttyvät, voidaan yksittäisen hydraulisen komponentin (esim. venttiilin) $MTTF_d$ -arvoksi arvioida 150 vuotta:

a) Hydrauliset komponentit valmistetaan noudattamalla turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita standardin ISO 13849-2:2003 (taulukot C.1 ja C.2) mukaisesti hydraulisen komponentin suunnitteluun (vahvistus tästä on komponentin tuotetiedoissa).

   HUOM. Nämä tiedot voidaan selvittää komponentin valmistajan tuotetiedoista.

b) Hydraulisen komponentin valmistaja erittelee käyttäjälle soveltuvat käyttötarkoitukset ja käyttöolosuhteet. Turvallisuuteen liittyvän ohjausjärjestelmän osan valmistajan on toimitettava tietoja, jotka liittyvät hänen velvollisuuksiinsa soveltaa hydraulisten komponenttien toteutuksen ja toiminnan osalta turvallisuuden perusperiaatteita ja hyvin koeteltuja turvallisuusperiaatteita standardin ISO 13849-2:2003 (taulukoiden C.1 ja C.2) mukaisesti.

Jos joko kriteeriä a) tai b) ei saada täytettyä, valmistajan on ilmoitettava yksittäisen hydraulisen komponentin $MTTF_d$ -arvo.

Taulukko C.1 $MTTF_d$- tai B_{10d}- arvoja käsitteleviä kansainvälisiä standardeja

	Standardin ISO 13849-2:2003 mukaiset turvallisuuden perusperiaatteet ja hyvin koetellut turvallisuusperiaatteet	**Muut merkitykselliset standardit**	**Tyypilliset arvot: $MTTF_d$ (vuotta) B_{10d} (jaksoa)**
Mekaaniset komponentit	Taulukot A.1 ja A.2	–	$MTTF_d$ = 150
Hydrauliset komponentit	Taulukot C.1 ja C.2	EN 982	$MTTF_d$ = 150
Pneumaattiset komponentit	Taulukot B.1 ja B.2	EN 983	B_{10d} = 20 000 000
Releet ja apukontaktorit pienellä kuormituksella (mekaaninen kuormitus)	Taulukot D.1 ja D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Releet ja apukontaktorit maksimikuormituksella	Taulukot D.1 ja D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Lähestymiskytkimet pienellä kuormituksella (mekaaninen kuormitus)	Taulukot D.1 ja D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Lähestymiskytkimet maksimikuormituksella	Taulukot D.1 ja D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Kontaktorit pienellä kuormituksella (mekaaninen kuormitus)	Taulukot D.1 ja D.2	IEC 60947	B_{10d} = 20 000 000
Kontaktorit nimelliskuormituksella	Taulukot D.1 ja D.2	IEC 60947	B_{10d} = 2 000 000
Asemantuntokytkimet kuormituksesta riippumatta [a]	Taulukot D.1 ja D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Asemantuntokytkimet (erillisellä vaikutuselimellä, suojuksen lukinnalla) kuormituksesta riippumatta [a]	Taulukot D.1 ja D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Hätäpysäytyslaitteet kuormituksesta riippumatta [a]	Taulukot D.1 ja D.2	IEC 60947 ISO 13850	B_{10d} = 100 000
Hätäpysäytyslaitteet suurimmalla toimintojen lukumäärällä	Taulukot D.1 ja D.2	IEC 60947 ISO 13850	B_{10d} = 6 050
Painikkeet (esim. sallintakytkimet) kuormituksesta riippumatta [a]	Taulukot D.1 ja D.2	IEC 60947	B_{10d} = 100 000
Suureen B_{10d} määritelmä ja käyttö: ks. kohta C.4. HUOM. 1 B_{10d} -arvon arvioidaan olevan kaksi kertaa B_{10} (50 % vaarallisia vikaantumisia). HUOM. 2 "Pienellä kuormituksella" tarkoittaa esimerkiksi 20 % nimellisarvosta (ks. lisätietoja ISO 13849-2).			
[a] Jos vian poissulkeminen pakkotoimiselle avautumiselle on mahdollista.			

C.4 Pneumaattisten, mekaanisten ja sähkömekaanisten komponenttien vaarallinen keskimääräinen vikaantumisaika

C.4.1 Yleistä

Pneumaattisille, mekaanisille ja sähkömekaanisille komponenteille (pneumaattiset venttiilit, releet, kontaktorit, asemantuntokytkimet, asemantuntokytkimien nokkapyörät jne.) voi olla vaikeata laskea vaarallista keskimääräistä vikaantumisaikaa (komponenttien $MTTF_d$), joka ilmoitetaan vuosina ja jota standardin ISO 13849 tämä osa edellyttää. Useimmissa tapauk-

Liite E
(opastava)
Esimerkkejä toimintojen ja moduulien diagnostiikan kattavuudesta

E.1 Esimerkkejä diagnostiikan kattavuudesta (DC)

Ks. taulukko E.1

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.	

E.2 Keskimääräisen diagnostiikan kattavuuden (DC_{avg}) arviointi

Monissa järjestelmissä voidaan käyttää useita erilaisia toimenpiteitä vikojen paljastamiseen. Näillä menetelmillä voidaan tarkistaa turvallisuuteen liittyviä ohjausjärjestelmän osia ja niillä voi olla erilaiset diagnostiikan kattavuudet. Arvioitaessa suoritustasoa kuvan 5 mukaisesti voidaan soveltaa vain yhtä, eli keskimääräistä, diagnostiikan kattavuuden arvoa turvatoimintoa suorittavien turvallisuuteen liittyvien ohjausjärjestelmän osien kokonaisuudelle.

Diagnostiikan kattavuus voidaan määrittää paljastuneiden vaarallisten vikaantumisten vikaantumistaajuuden ja kaikkien vaarallisten vikaantumisten vikaantumistaajuuden suhteena. Tämän määritelmän mukaisesti keskimääräinen diagnostiikan kattavuuden (DC_{avg}) arvio saadaan seuraavan yhtälön avulla:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \qquad (E.1)$$

Tässä turvallisuuteen liittyvän ohjausjärjestelmän osan kaikki komponentit on otettava huomioon ja niitä on tarkasteltava yhdessä ilman vikojen poissulkemista. Jokaisen lohkon vaarallinen keskimääräinen vikaantumisaika ($MTTF_d$) ja diagnostiikan kattavuus (DC) otetaan huomioon. DC merkitsee tässä yhtälössä ohjausjärjestelmän osassa (riippumatta vikojen paljastamiseen käytettävästä menetelmästä) paljastuneiden vaarallisten vikaantumisten vikaantumistaajuuden ja kaikkien vaarallisten vikaantumisten vikaantumistaajuuden suhdetta. Siten DC viittaa testattuun osaan eikä testauslaitteeseen. Komponenteilla, joille ei ole vikaantumisen paljastamista (esim. joita ei testata), on DC = 0 ja se vaikuttaa DC_{avg} -arvon laskennassa vain yhtälön nimittäjään.

Liite F
(opastava)
Yhteisvikaantumisen (CCF) arviointi

F.1 Vaatimukset yhteisvikaantumiselle

Esimerkiksi standardin IEC 61508-6:2000 liitteessä D esitetään kattava proseduuri toimenpiteille anturien ja toimilaitteiden sekä erikseen logiikan yhteisvikaantumisten estämiseen. Kaikki siinä esitettävät toimenpiteet eivät ole sovellettavissa konesovelluksissa. Tärkeimmät toimenpiteet esitellään seuraavassa.

HUOM. Standardin ISO 13849 tässä osassa oletetaan, että redundanttisille järjestelmille standardin IEC 61508-6:2000 liitteen D mukaisen β-tekijän olisi oltava enintään 2 %.

F.2 Yhteisvikaantumisen vaikutuksen arviointi

Tällä laadullisella prosessilla olisi käytävä läpi koko järjestelmä. Turvallisuuteen liittyvien ohjausjärjestelmän osien kukin osa olisi otettava tarkasteluun.

Taulukossa F.1 luetteloidaan toimenpiteet ja niihin liittyvät numeroarvot, jotka perustuvat teknisiin arviointeihin ja jotka edustavat kunkin toimenpiteen osuutta yhteisvikaantumisen vähentämiseen.

Jokaiselle luetteloidulle toimenpiteelle voidaan esittää vain joko täydet pisteet tai ei mitään. Jos toimenpide toteutetaan vain osittain, ei pisteitä tämän menetelmän mukaisesti anneta.

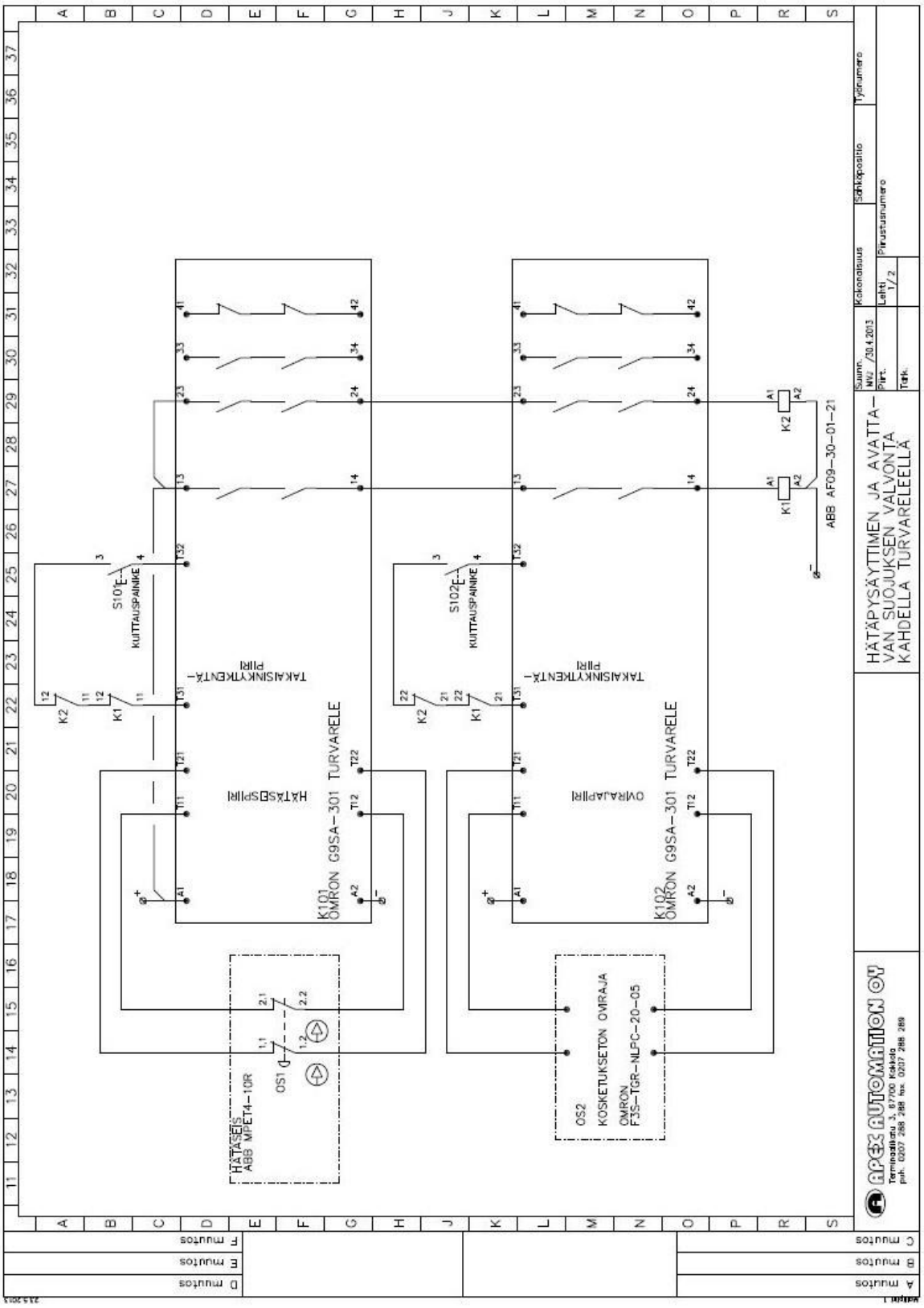
Taulukossa F.1 esitetään yhteisvikaantumisen vähentämisen määrällinen arvio.

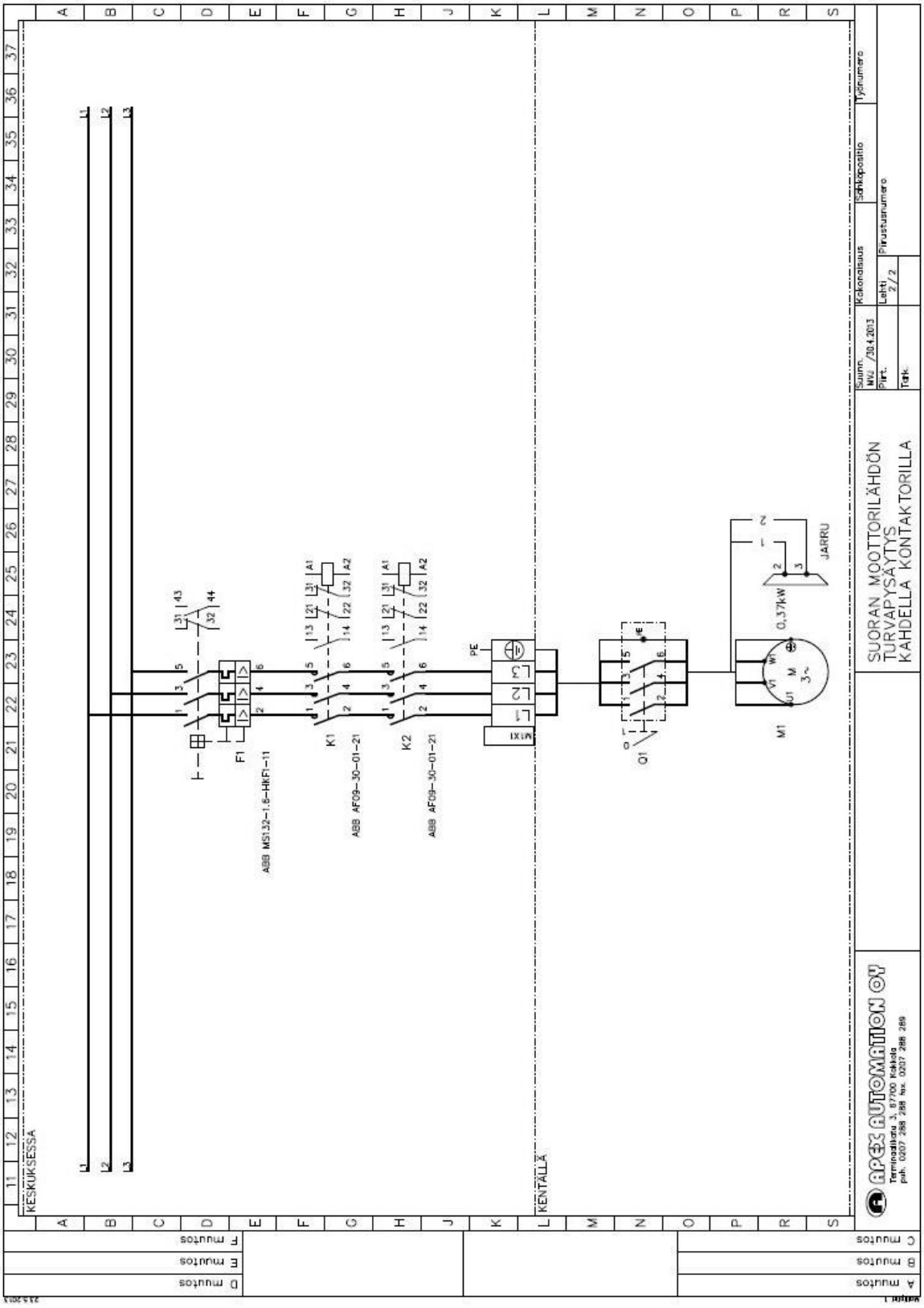
Taulukko F.1 Pisteytysprosessi ja yhteisvikaantumista estävien toimenpiteiden määrällinen arviointi

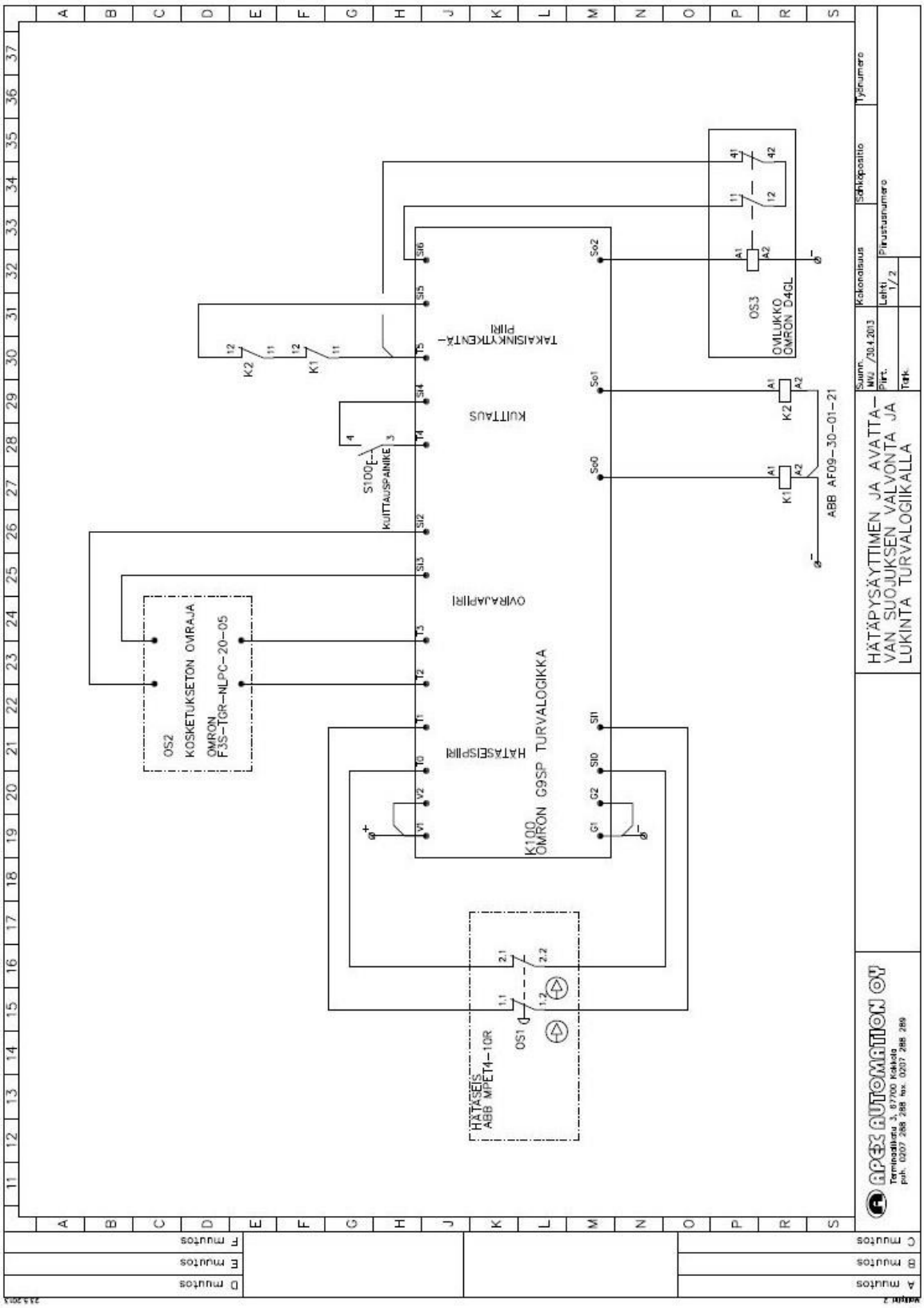
Nro	Yhteisvikaantumista estävä toimenpide	Pisteet
1	**Erottelu/erottaminen**	
	Signaalireittien fyysinen erottaminen – johdotuksen/putkituksen erilleen sijoittaminen – riittävät ilma- ja pintavälit painetuissa piirilevyissä	**15**
2	**Erilaisuus (diversiteetti)**	
	Erilaisten teknologioiden, toteutustapojen tai fyysisten periaatteiden käyttö, esimerkiksi – ensimmäinen kanava toteutetaan ohjelmoitavalla elektronikalla ja toinen kanava kiinteästi langoitettuna – toiminnan aloittamistapa – paine ja lämpötila Etäisyyden tai paineen mittaus: – digitaalinen ja analoginen Eri valmistajien komponentit	**20**
3	**Suunnittelu, soveltaminen ja kokemukset**	
3.1	Suojaustoimenpiteet ylijännitteelle, ylipaineelle, ylivirralle jne.	**15**
3.2	Käytetyt komponentit ovat hyvin koeteltuja	**5**
4	**Arviointi ja analyysit**	
	Onko vika- ja vaikutusanalyysin tulokset otettu huomioon toteutuksessa yhteisvikaantumisten estämiseksi?	**5**
5	**Pätevyys ja koulutus**	
	Onko suunnittelu- ja ylläpitohenkilöstö koulutettu ymmärtämään yhteisvikaantumisten syyt ja seuraukset?	**5**
6	**Ympäristöolosuhteisiin liittyvä toimenpiteet**	
6.1	Likaantumisen estäminen ja sähkömagneettinen yhteensopivuus yhteisvikaantumisten estämiseksi soveltuvien standardien mukaisesti Pneumaattiset- ja hydrauliset järjestelmät: väliaineen suodatus, likaisen ilmailman estäminen ja paineilman kuivatus (esim. komponentin valmistajan esittämien väliaineen puhtausvaatimusten mukaisesti) Sähköiset järjestelmät: onko järjestelmä tarkistettu sähkömagneettisen häiriönsiedon kannalta (esim. asiaankuuluvien yhteisvikaantumisen estämistä käsittelevien standardien mukaisesti)? Yhdistetyt sähköiset ja hydrauliset tai pneumaattiset järjestelmät: olisi otettava huomioon molemmat edellä mainittavat näkökohdat	**25**
6.2	Muut vaikutukset Onko kaikkien asiaankuuluvien ympäristövaikutusten sietokyky otettu huomioon kuten lämpötila, iskut, tärinä, kosteus (asiaankuuluvien standardien erittelyn mukaisesti)?	**10**
	Yhteensä	**[mahdolliset maksimi-pisteet 100]**

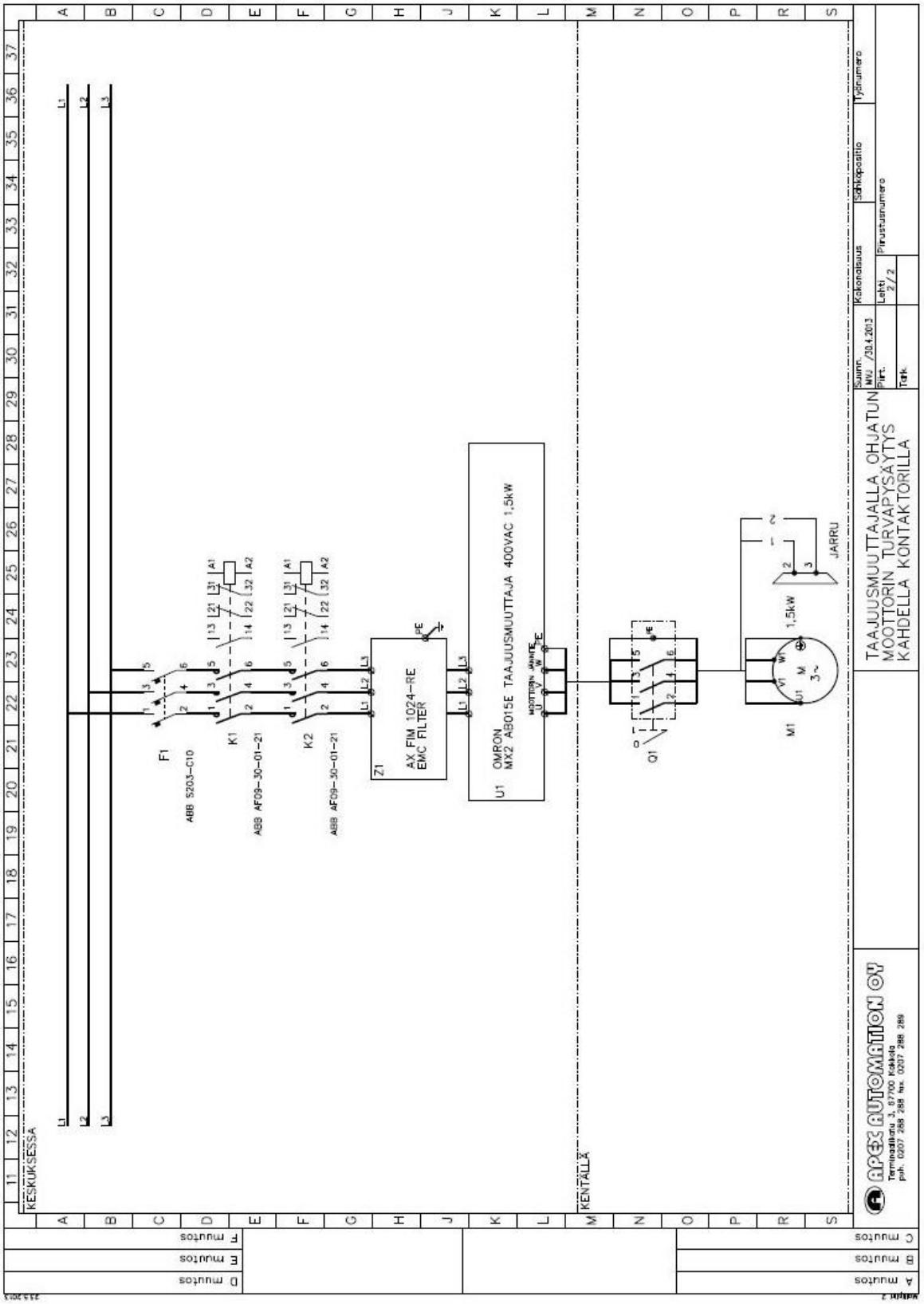
Kokonaispisteet	**Toimenpiteet yhteisvikaantumisen välttämiseksi** [a]
65 tai enemmän	Täyttää vaatimukset
vähemmän kuin 65	Ei täytä vaatimuksia ⇒ valitaan lisätoimenpiteitä

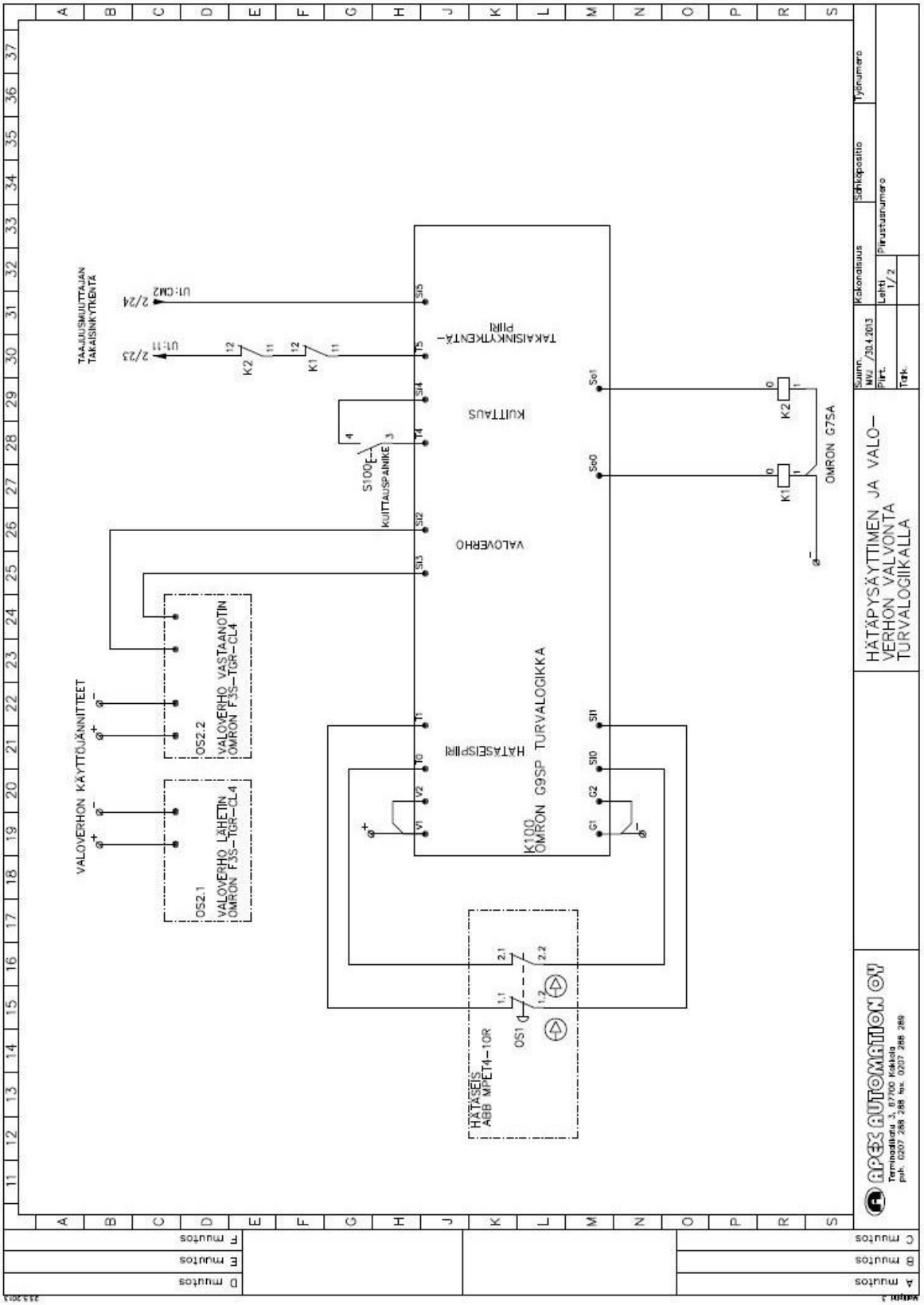
[a] Jos teknologiset toimenpiteet eivät ole merkityksellisiä, tähän sarakkeeseen liittyviä pisteitä voidaan tarkastella kokonaisvaltaisessa laskelmassa.

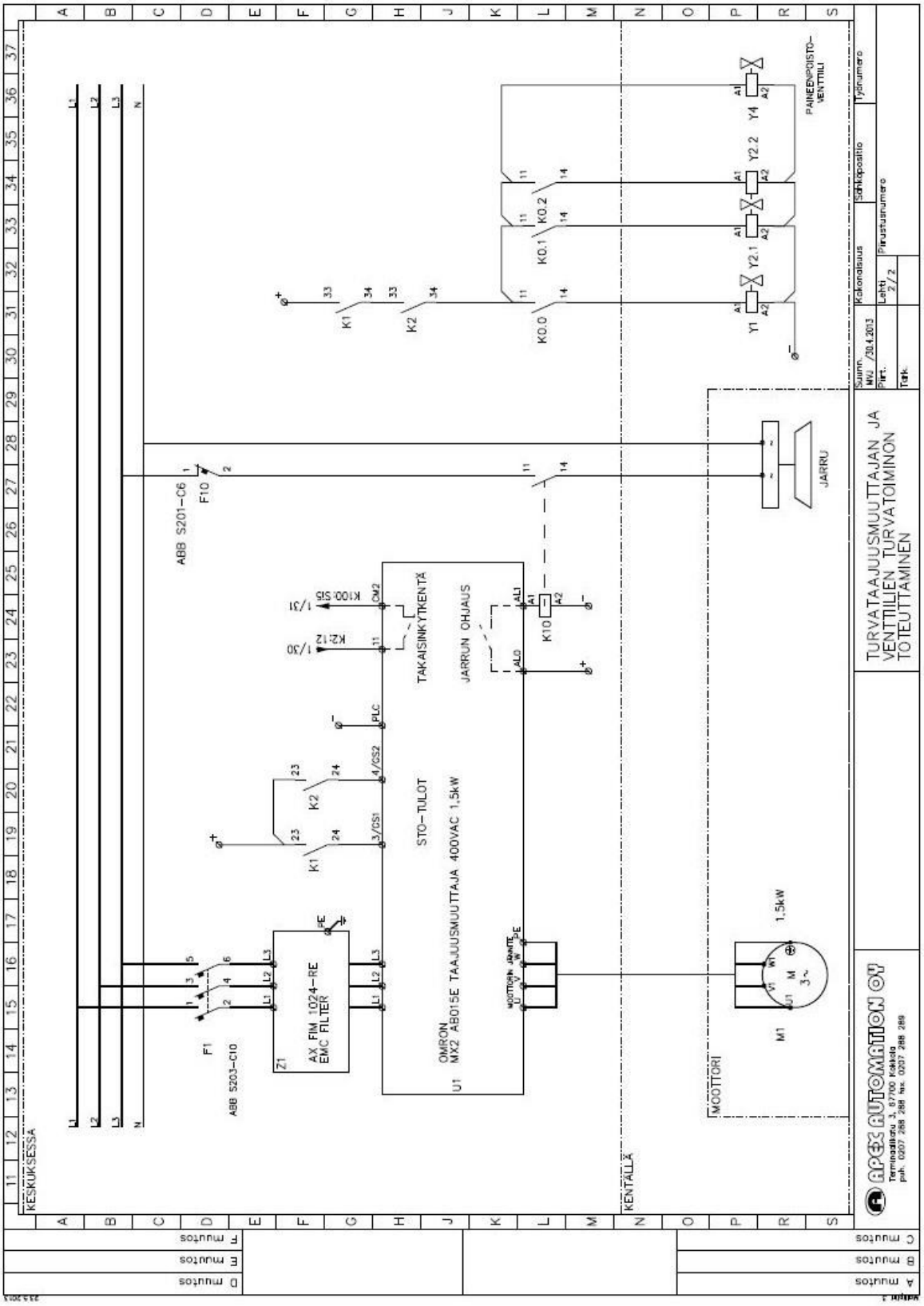

HÄTÄPYSÄYTTIMEN JA AVATTAVAN SUOJUKSEN VALVONTA KAHDELLA TURVARELEELLÄ
Suunn. MV/ 30.4.2013
Piirt.
Tark.
Kokonaisuus
Lehti 1/2
Sähkökaavio
Piirustusnumero
Työnumero
APS AUTOMATION OY
Terminaalitalo 3, 07700 Kerkkola
puh. 0207 288 288 fax. 0207 288 289
K101 OMRON G9SA-301 TURVARELE
K102 OMRON G9SA-301 TURVARELE
HÄTÄSBSPIIRI
OVIRAJAPIIRI
TAKAISINKYTKENTÄ-PIIRI
KUITTAUSPAINIKE
S101
S102
K1
K2
ABB AF09-30-01-21
HÄTÄSES ABB MPET4-10R
OS1
OS2
KOSKETUKSETON OVIRAJA
OMRON F3S-TGR-NLPC-20-05
A muutos
B muutos
C muutos
D muutos
E muutos
F muutos


KESKUKSESSÄ
KENTÄLLÄ
L1
L2
L3
PE
F1
ABB MS132-1.6-HKF1-11
K1
ABB AF09-30-01-21
K2
ABB AF09-30-01-21
Q1
M1
0,37kW
JARRU
SUORAN MOOTTORILÄHDÖN
TURVAPYSÄYTYS
KAHDELLA KONTAKTORILLA
APSI AUTOMATION OY
Terminaalitie 3, 87700 Kajaani
puh. 0207 288 288 fax. 0207 288 289
Suunn.
MVJ 30.1.2013
Piirt.
Tark.
Kokonaisuus
Lehti
2/2
Sähkökaatio
Piirustusnumero
Työnumero
A muutos
B muutos
C muutos
D muutos
E muutos
F muutos


HÄTÄPYSÄYTTIMEN JA AVATTAVAN SUOJUKSEN VALVONTA JA LUKINTA TURVALOGIIKALLA
APES AUTOMATION OY
Terminaalitie 3, 87700 Kajaani
puh. 0207 288 288 fax. 0207 288 289
K100
OMRON G9SP TURVALOGIKKA
HÄTÄSEISPIIRI
OVIRAJAPIIRI
KUITTAUS
TAKAISINKYTKENTÄ-PIIRI
OS1
HÄTÄSEIS
ABB MPET4-10R
OS2
KOSKETUKSETON OVIRAJA
OMRON
F3S-TGR-NLPC-20-05
S100
KUITTAUSPAINIKE
K1
K2
OS3
OVILUKKO
OMRON D4GL
ABB AF09-30-01-21


KESKUKSESSÄ
KENTÄLLÄ
L1
L2
L3
F1
ABB S203-C10
K1
ABB AF09-30-01-21
K2
ABB AF09-30-01-21
Z1
AX FIM 1024-RE
EMC FILTER
U1
OMRON
MX2 AB015E TAAJUUSMUUTTAJA 400VAC 1.5kW
MOOTTORIN JOHTO
Q1
M1
1.5kW
JARRU
TAAJUUSMUUTTAJALLA OHJATUN
MOOTTORIN TURVAPYSÄYTYS
KAHDELLA KONTAKTORILLA
Suunn.
MVJ 30.4.2013
Piirt.
Tark.
Kokonaisuus
Lehti
2/2
Sähkökaavio
Työnumero
Piirustusnumero
APES AUTOMATION OY
Terminaalitie 3, 87700 Kajaani
puh. 0207 288 288 fax. 0207 288 289
A muutos
B muutos
C muutos
D muutos
E muutos
F muutos


HÄTÄPYSÄYTTIMEN JA VALO-
VERHON VALVONTA
TURVALOGIIKALLA
APS AUTOMATION OY
Terminaalitie 3, 87700 Kajaani
puh. 0207 288 288 fax. 0207 288 289
Suunn.
MV. /30.4.2013
Piirt.
Tark.
Kokonaisuus
Lehti
1/2
Sähköpositio
Piirustusnumero
Työnumero
TAAJUUSMUUTTAJAN
TAHAISINKYTKENTÄ
U1:CM2
2/24
U1:11
2/23
K2
K1
TAKAISINKYTKENTÄ-
PIIRI
KUITTAUS
S100
KUITTAUSPAINIKE
VALOVERHO
K100
OMRON G9SP TURVALOGIKKA
HÄTÄSEISPIIRI
OS1
HÄTÄSEIS
ABB MPET4-10R
VALOVERHO KÄYTTÖJÄNNITTEET
OS2.1
VALOVERHO LÄHETIN
OMRON F3S-TGR-CL4
OS2.2
VALOVERHO VASTAANOTIN
OMRON F3S-TGR-CL4
OMRON G7SA
A muutos
B muutos
C muutos
D muutos
E muutos
F muutos


KESKUKSESSÄ
KENTÄLLÄ
L1
L2
L3
N
F1
ABB S203-C10
F10
ABB S201-C6
Z1
AX FIM 1024-RE
EMC FILTER
U1
OMRON
MX2 AB015E TAAJUUSMUUTTAJA 400VAC 1,5kW
STO-TULOT
TAKAISINKYTKENTÄ
JARRUN OHJAUS
K1
K2
K10
K0.0
K0.1
K0.2
Y1
Y2.1
Y2.2
Y4
PAINEENPOISTO-VENTTIILI
JARRU
MOOTTORI
M1
1,5kW
TURVATAAJUUSMUUTTAJAN JA VENTTIILIEN TURVATOIMINON TOTEUTTAMINEN
APES AUTOMATION OY
Terminaalitie 3, 87700 Kajaani
puh. 0207 288 288 fax. 0207 288 289
Suunn.
MVJ /30.4.2013
Piirt.
Tark.
Kokonaisuus
Lehti
2/2
Sähkökaavio
Työnumero
Piirustusnumero
A muutos
B muutos
C muutos
D muutos
E muutos
F muutos

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

PR Projektin nimi: Malliprojekti

Tekijä:	Mikko Vähäjylkkä
Vaarallinen kohta/kone:	Kuljetin
Dokumentaatio:	
Dokumentti:	
Tiedoston nimi:	F:\Opinnäytetyön sistemaprojekti\Malliprojekti.ssm
Ohjelmiston versio:	1.1.5
Standardin versio:	ISO 13849-1:2006, ISO 13849-2:2003
Tarkistussumma:	f2faa9cd38deb2d63a8710e35096e757
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:Kuljettimenvalvonta

Vaadittu: PLr d Saavutettu: PL d PFH [1/h]: 3,97E-7 Tila: vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

SF Turvatoiminto: Kuljettimen valvonta

Turvatoiminnon tyyppi:	Turvalaitteen käynnistämä turvallisuuteen liittyvä pysäytystoiminto
Laukaiseva tapahtuma:	Valoverhon vaikuttaminen saa aikaan kuljetinta ohjaavan taajuusmuuttajan turvapysäytyksen
Reaktio:	
Turvallinen tila:	Liikkeet pysähtyneet
Dokumentaatio:	
Dokumentti:	
Saavutettu PL:	d PFH [1/h]: 3,97E-7
PLr (suora syöte):	d
Dokumentaatio/johtopäätökset::	
Lähde (esim. standardi):	
Tiedosto:	
Tila:	vihreä

Alajärjestelmät:

SB Nimi:Valoverho

PL: e	PFH [1/h]: 3,16E-8
Luokka (Cat.): 4	Toimita-aika [v]: 20

DokumentaatioAlajärjestelmä

Dokumentaatio:	
Dokumentti:	

SuoritustasoAlajärjestelmä

Dokumentaatio/johtopäätökset::	

Luokka (Cat.) Alajärjestelmä

Dokumentaatio/johtopäätökset::	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.

Tila/ViestitAlajärjestelmä

Tila:	vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

SF Turvatoiminto: Kuljettimen valvonta

Alajärjestelmät:

SB Nimi: G9SA-301

PL: e	PFH [1/h]: 2,47E-8
Luokka (Cat.): 4	Toimita-aika [v]: 20
DCavg [%]: 99 (Korkea)	CCF-pisteet: 65 (täytetty)
MTTFd [v]: 100 (Korkea)	

DokumentaatioAlajärjestelmä

Dokumentaatio:	Safety Relay Unit As a subsystem, it conforms to ISO13849-1 PLe.
Dokumentti:	

Luokka (Cat.) Alajärjestelmä

Dokumentaatio/johtopäätökset::	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	
Luokan vaatimukset:	Turvallisuuden perusperiaatteita on käytetty. [täytetty] Hyvin koeteltuja turvallisuuperiaatteita on käytetty. [täytetty] Yksittäisen vian sietoa on käytetty. [täytetty] Vikojen kerääntyminen ei johda turvatoiminnon menettämiseen. [täytetty] MTTFd on Korkea. [täytetty] DCavg-arvo on Korkea. [täytetty] CCF-arviossa saavutetut pisteet ovat vähintään 65 [täytetty]

DiagnostiikankattavuusAlajärjestelmä

Dokumentaatio/johtopäätökset::	

Tila/ViestitAlajärjestelmä

Tila:	vihreä

Alajärjestelmät:

SB Nimi: G7SA-turvahyväksytyt releet

PL: e	PFH [1/h]: 2,47E-8
Luokka (Cat.): 4	Toimita-aika [v]: 20
DCavg [%]: 99 (Korkea)	CCF-pisteet: 65 (täytetty)

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

SF **Turvatoiminto: Kuljettimen valvonta**

MTTFd [v]: 100 (Korkea)

DokumentaatioAlajärjestelmä

Dokumentaatio:

Dokumentti:

Luokka (Cat.) Alajärjestelmä

Dokumentaatio/johtopäätökset::

Lähde (esim. standardi) Luokka (Cat.):

Tiedosto:

Luokan vaatimukset:	Turvallisuuden perusperiaatteita on käytetty. [täytetty]
	Hyvin koeteltuja turvallisuuperiaatteita on käytetty. [täytetty]
	Yksittäisen vian sietoa on käytetty. [täytetty]
	Vikojen kerääntyminen ei johda turvatoiminnon menettämiseen. [täytetty]
	MTTFd on Korkea. [täytetty]
	DCavg-arvo on Korkea. [täytetty]
	CCF-arviossa saavutetut pisteet ovat vähintään 65 [täytetty]

Tila / Viestit Alajärjestelmä

Tila: vihreä

Kanavat/testikanavat:

CH Nimi: Kanava 1

MTTFd [v]: 2403,85

Lohkot:

BL Nimi: **K1**

MTTFd [v]: 2403,85 (Korkea) DC [%]: 99 (Korkea)

Toimita-aika [v]: 20

Dokumentaatio Lohko

Dokumentaatio:

Dokumentti:

Tila / Viestit Lohko

Tila: vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

SF **Turvatoiminto: Kuljettimen valvonta**

Elementit:

EL Nimi: **K1**

B10d [jaksoa]: 1000000 Nop [toimintajaksoa/vuosi]: 4160

T10d [v]: 240,38 MTTFd [v] (B10d-arvon avulla): 2403,85 (Korkea)

Toimita-aika [v]: 20

DC [%]: 99 (Korkea)

DokumentaatioElementti

Teknologia: sähkömekaaninen

Dokumentaatio:

Dokumentti:

DiagnostiikankattavuusElementti

Dokumentaatio/johtopäätökset::

Tila / Viestit Elementti

Tila: vihreä

Viesti [Viestin tila]:

Kanavat/testikanavat:

CH Nimi: Kanava 2

MTTFd [v]: 2403,85

Lohkot:

BL Nimi: **K2**

MTTFd [v]: 2403,85 (Korkea) DC [%]: 99 (Korkea)

Toimita-aika [v]: 20

Dokumentaatio Lohko

Dokumentaatio:

Dokumentti:

Tila / Viestit Lohko

Tila: vihreä

Elementit:

EL Nimi: **K2**

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

SF **Turvatoiminto: Kuljettimen valvonta**

B10d [jaksoa]: 1000000	Nop [toimintajaksoa/vuosi]: 4160
T10d [v]: 240,38	MTTFd [v] (B10d-arvon avulla): 2403,85 (Korkea)
Toimita-aika [v]: 20	
	DC [%]: 99 (Korkea)

DokumentaatioElementti

Teknologia:	sähkömekaaninen
Dokumentaatio:	
Dokumentti:	

DiagnostiikankattavuusElementti

Dokumentaatio/johtopäätökset::

Tila/ViestitElementti

Tila:	vihreä
Viesti [Viestin tila]:	

Alajärjestelmät:

SB Nimi:MX2-taajuusmuuttaja

PL: d	PFH [1/h]: 3,16E-7
Luokka (Cat.): 4	Toimita-aika [v]: 20

DokumentaatioAlajärjestelmä

Dokumentaatio:	
Dokumentti:	

SuoritustasoAlajärjestelmä

Dokumentaatio/johtopäätökset::

Luokka(Cat.)Alajärjestelmä

Dokumentaatio/johtopäätökset::	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.

Tila/ViestitAlajärjestelmä

Tila:	vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden arviointiin

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Projektin nimi: Malliprojekti

Tiedoston päiväys: 29.4.2013 Raportin päiväys: 30.4.2013 Tarkistussumma: f2faa9cd38deb2d63a8710e35096e757

VASTUUVAPAUSLAUSEKE

Ohjelmiston tuotannossa on huolehdittu, että se on tehty nykytekniikan tason mukaisesti. Ohjelmisto on tarkoitettu käyttöönotettavaksi korvauksetta.

Ohjelmiston käyttö tapahtuu käyttäjän omalla riskillä. Lainsäädännön antamissa rajoissa ei hyväksytä mitään lakiin perustuvaa vastuuta ohjelmistosta. Erityisesti mitään vastuuta ei hyväksytä aineellisista tai oikeudellisista virheistä, joko ohjelmistossa tai siihen liittyvässä dokumentaatiossa ja muissa tiedoissa sekä erityisesti niiden oikeellisuudesta, virheettömyydestä, kolmansien osapuolten omistusoikeuksista ja tekijänoikeuksista, ajan tasalla pysymisestä, täydellisyydestä ja/tai käyttötarkoitukseen soveltuvuudesta lukuun ottamatta tahallista vahingoittamisen tarkoitusta.

IFA sitoutuu pitämään verkkosivut vapaina viruksista, mutta kuitenkaan ei voida varmistaa, että ohjelmisto ja sen mukana toimitettavat tiedot olisivat viruksista vapaita. Tämän vuoksi käyttäjää suositellaan ryhtymään sopiviin tietoturvan toimenpiteisiin ja käyttämään virustutkaa ennen ohjelmiston, dokumentaation ja muiden tietojen lataamista.

YHTEYS

Saksan sosiaalisen tapaturmavakuutuksen työterveyden ja työturvallisuuden laitos (IFA)
(Institute for Occupational Health and Safety of German Social Accident Insurance (IFA))
Osasto 5 (Tapaturmien ehkäisy/tuoteturvallisuus)
Osoite: Alte Heerstr. 111, 53754 Sankt Augustin
Sähköposti: sistema@dguv.de
Verkkosivu:www.dguv.de/ifa(Webcodee20543)

Tarkastajan päivämäärä, allekirjoitus

Tekijän päivämäärä, allekirjoitus