Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

JOONA JUNNILA

Suolistamon turvallistaminen

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN
TUTKINTO-OHJELMA
2023

Tekijä(t) Junnila, Joona	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Huhtikuu 2023
	Sivumäärä 50+1	Julkaisun kieli Suomi
Julkaisun nimi **Suolistamon turvallistaminen**		
Tutkinto-ohjelma Sähkö- ja automaatiotekniikka		

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa hätäpysäytysjärjestelmä HKScan Rauman tehtaan suolistamoon, tavoitteena suolistamon turvallisuuden parantaminen.

Työn teoriaosuudessa tutustutaan standardien asettamiin määrittelyihin ja vaatimuksiin hätäpysäytysjärjestelmille sekä niiden suunnittelulle. Suunnitteluosuudessa varmistettiin hätäpysäytysjärjestelmän vaatimustenmukaisuus sekä suunniteltiin hätäpysäytyslaitteiden asennus, turvalogiikkakeskus ja siinä käytettävät komponentit.

Työn käytännönosuudessa hätäpysäytyslaitteet asennettiin ja turvalogiikkakeskus rakennettiin suunnitelmien mukaisesti. Lisäksi järjestelmässä käytettävä turvalogiikka ohjelmoitiin sekä järjestelmän käyttöpaneelille tehtiin käyttöliittymä. Hätäpysäytysjärjestelmän valmistuttua se testattiin, otettiin käyttöön ja dokumentoitiin.

Lopputuloksena suolistamon laitteille saatiin rakennettua toimiva hätäpysäytysjärjestelmä, joka parantaa suolistamon turvallisuutta ja täytti asiakkaan toiveet ja vaatimukset.

Avainsanat
Hätäpysäytys, Hätäpysäytysjärjestelmä

Author(s)
Junnila, Joona

Type of Publication
Bachelor's thesis

Date
April 2023

Number of pages
50+1

Language of publication:
Finnish

Title of publication
Emergency stop system for evisceration line

Degree program
Electrical and Automation engineering

Abstract

The purpose of this thesis was to design and implement an emergency stop system for the evisceration line of the HKScan Rauma factory, with the goal of improving the safety of the evisceration line.

The theory section contains information about the definitions and requirements set by standards for emergency stop systems and their design. In the planning section, it was ensured that the emergency stop system for the evisceration line was compliant to standards. The installation of the emergency stop devices, the safety PLC-cabinet and the components used in it were also planned.

In the practical part of the work, the emergency stop devices were installed and the safety PLC-cabin was built according to plans. In addition, the safety PLC used in the system was programmed and a user interface was made for the system's control panel. After the emergency stop system was completed, it was tested, put into use and documented.

As a result, a functional emergency stop system was built for the machines of the evisceration line, which improves the safety of the evisceration line and met the wishes and requirements of the customer.

Keywords
Emergency stop, Emergency stop system

SISÄLLYS

1 JOHDANTO

Teollisuudessa työturvallisuudella on suuri merkitys, sillä hyvä työympäristö on turvallinen ja tuottava. Turvallisen työympäristön aikaansaaminen edellyttää työpaikalla sattuvien tapaturmien ennalta ehkäisemistä. Työturvallisuus on jatkuva kehityksen kohde, jonka tavoitteena on nolla tapaturmaa. Aineellisten vahinkojen ja kustannusten lisäksi, työtapaturmat aiheuttavat ennen kaikkea inhimillistä kärsimystä. Tämä luokin painetta yrityksille työturvallisuuden jatkuvaan kehittämiseen.

Tämän opinnäytetyön tarkoituksena on suunnitella ja toteuttaa hätäpysäytysjärjestelmä asiakkaan toiveiden ja vaatimusten mukaan, HKScan Rauman tehtaan suolistamoon. Hätäpysäytysjärjestelmä pitää sisällään hätäpysäytyslaitteet, turvalogiikkakeskuksen, sekä käyttöliittymän järjestelmän diagnostiikka varten.

Työn tavoitteena on parantaa suolistamon laitteiden turvallisuutta sekä helpottaa käyttäjien ja kunnossapidon työtä käyttöliittymältä saatavan diagnostiikan myötä. Opinnäytetyö tehdään Notra Oy:n toimeksiantona HKScan Rauman tehtaan suolistamoon. Asiakkaan toiveina ja vaatimuksina oli erilaisten hätäpysäytyslaitteiden lisäys suolistamon laitteille sekä järjestelmän käyttöliittymä, josta voitaisiin nähdä jokaisen hätäpysäytyslaitteen tilat.

Työssä tutustutaan standardien määritelmiin ja opastuksiin hätäpysäytysjärjestelmille sekä niiden suunnittelulle. Työn suunnittelu osuudessa varmistetaan ja suunnitellaan asiakkaan esittämien hätäpysäytyslaitteiden vaatimustenmukaisuus ja asennustapa sekä suunnitellaan järjestelmän turvalogiikkakeskus. Työn käytännön osuudessa perehdytään turvalogiikkakeskuksen rakentamiseen, turvalogiikan ohjelmointiin sekä käyttöliittymän toteutukseen.

2 SUUNNITTELUN LÄHTÖKOHDAT

Suunnittelun lähtökohdat saadaan EU:n konedirektiivistä 2006/42/EY, joka asettaa koneita koskevat turvallisuusvaatimukset. Konedirektiivi on pantu Suomessa toimeen valtioneuvoston asetuksella koneiden turvallisuudesta 400/2008, eli ns. koneasetuksella. Koneasetuksessa määritellään koneiden valmistajien velvollisuudet, koneiden suunnitteluun ja rakentamiseen liittyvät turvallisuus- ja terveysvaatimukset sekä menettelyt koneiden vaatimustenmukaisuuden osoittamiselle. (Tukes, n.d.) Standardit esittävät opastusta näiden vaatimusten täyttymisen toteutuksessa. Koneita koskevat turvallisuusstandardit jakautuvat A, B ja C-tyypin standardeihin. A-tyypin standardit esittävät kaikkiin koneisiin sovellettavat perusteet, suunnitteluperiaatteet ja yleiset näkökohdat. B-tyypin standardit käsittelevät yhtä tai useampaa turvallisuus näkökohtaa tai suojausteknistä laitetta, jota voidaan käyttää useissa koneryhmissä. B-tyypin standardi jakautuu B1- ja B2-tyypin standardeihin. B1-tyypin standardit koskevat tiettyjä yksittäisiä turvallisuusnäkökohtia ja B2-tyypin standardit suojausteknisiä laitteita. C-tyypin standardit käsittelevät yksityiskohtaisia turvallisuusvaatimuksia tietylle koneelle tai koneryhmälle. (SFS-EN ISO 12100:2010, 2010, s. 5.)

2.1 Standardit

Standardi SFS-EN ISO 12100 määrittelee peruskäsitteet, periaatteet ja menetelmät turvallisuuden aikaansaamiseksi koneita suunniteltaessa. Standardi määrittelee riskin arvioinnin ja riskin pienentämisen periaatteet, perustuen tietämykseen ja kokemukseen koneiden suunnittelusta, käytöstä, epätavallisista tapahtumista, tapaturmista ja riskeistä. Tämä on A-luokan standardi ja toimii perustana muita A-, B- tai C-tyypin standardeja laadittaessa. (SFS-EN ISO 12100:2010, 2010, s. 6.)

Standardi SFS-EN ISO 13849-1 esittää turvallisuusvaatimukset sekä ohjeita turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelun ja integroinnin periaatteista. Standardi määrittelee näille turvallisuuteen liittyville ohjausjärjestelmän osille ominaisuudet, joihin kuuluu turvatoiminnon toteuttamiseen vaadittava suoritustaso sekä esitetään erityisvaatimukset turvallisuuteen liittyville ohjausjärjestelmän osille, joissa

käytetään ohjelmoitavia elektronisia järjestelmiä. (SFS-EN ISO 13849-1:2015, 2015, s. 8.)

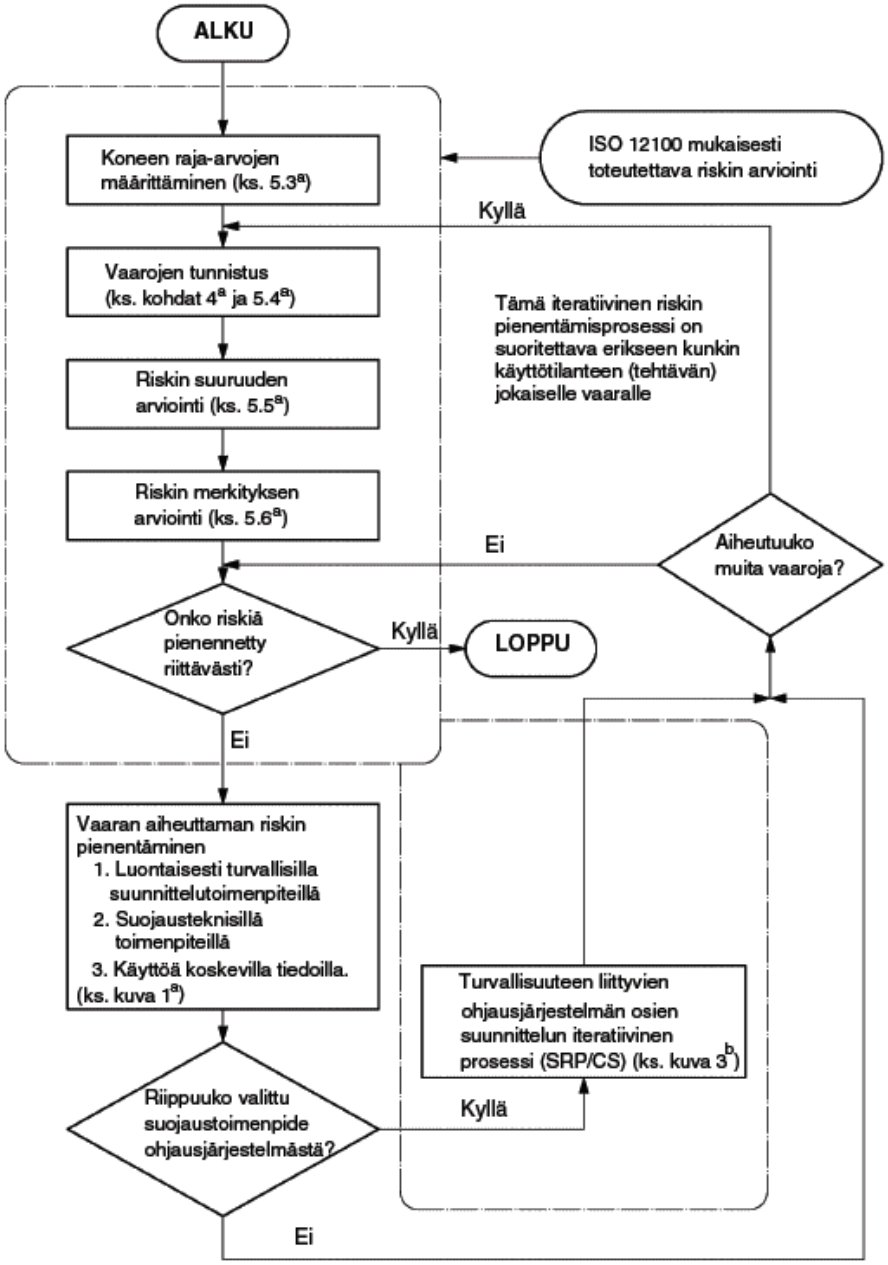
Standardi SFS-EN IEC 62061 määrittelee vaatimukset turvallisuuteen liittyvien ohjausjärjestelmien suunnittelua, integrointia ja kelpuutusta varten. Standardia voidaan soveltaa ohjausjärjestelmiin, joita käytetään yksin tai yhdistelmänä turvatoimintoihin koneissa, jotka eivät ole työskentelyn aikana kädessä kannettavia. (SFS-EN IEC 62061:2021, 2021, s. 10.)

Suunniteltaessa koneiden turvallisuuteen liittyviä ohjausjärjestelmiä, voidaan käyttää standardeja IEC 62061 ja ISO 13849. Molemmat standardit määrittelevät vaatimuksia koneen turvallisuuteen liittyvien ohjausjärjestelmien suunnitteluun ja toteuttamiseen. Kumpaa tahansa standardia käyttämällä, niiden soveltamisalojen mukaisesti, voidaan merkityksellisten turvallisuusvaatimusten olettaa tulevan täytetyksi. (SFS-EN ISO 13849-1:2015, 2015, s. 7.)

Standardeissa IEC 62061 ja ISO 13849-1 määritellään turvallisuuden eheyden taso SIL sekä vaadittu suoritustaso $PL_{r,}$ jotka tulee ottaa huomioon turvallisuuteen liittyvää ohjausjärjestelmää suunniteltaessa. Hätäpysäytystoiminto on täydentävä suojaustoimenpide, eikä sitä tule käyttää korvaamaan suojausteknisiä toimenpiteitä ja muita toimintoja tai turvatoimintoja (SFS-EN ISO 13850:2015, 2015, s. 8). Hätäpysäytystoiminto voidaan toteuttaa osana turvallisuuteen liittyvää ohjausjärjestelmää, jolloin sen toiminnon suorittavien osien tulee täyttää standardin ISO 13849-1 ja/tai IEC 62061 vaatimukset. Tässä työssä sovellettiin standardia ISO 13849-1.

2.2 Riskin arviointi ja pienentäminen

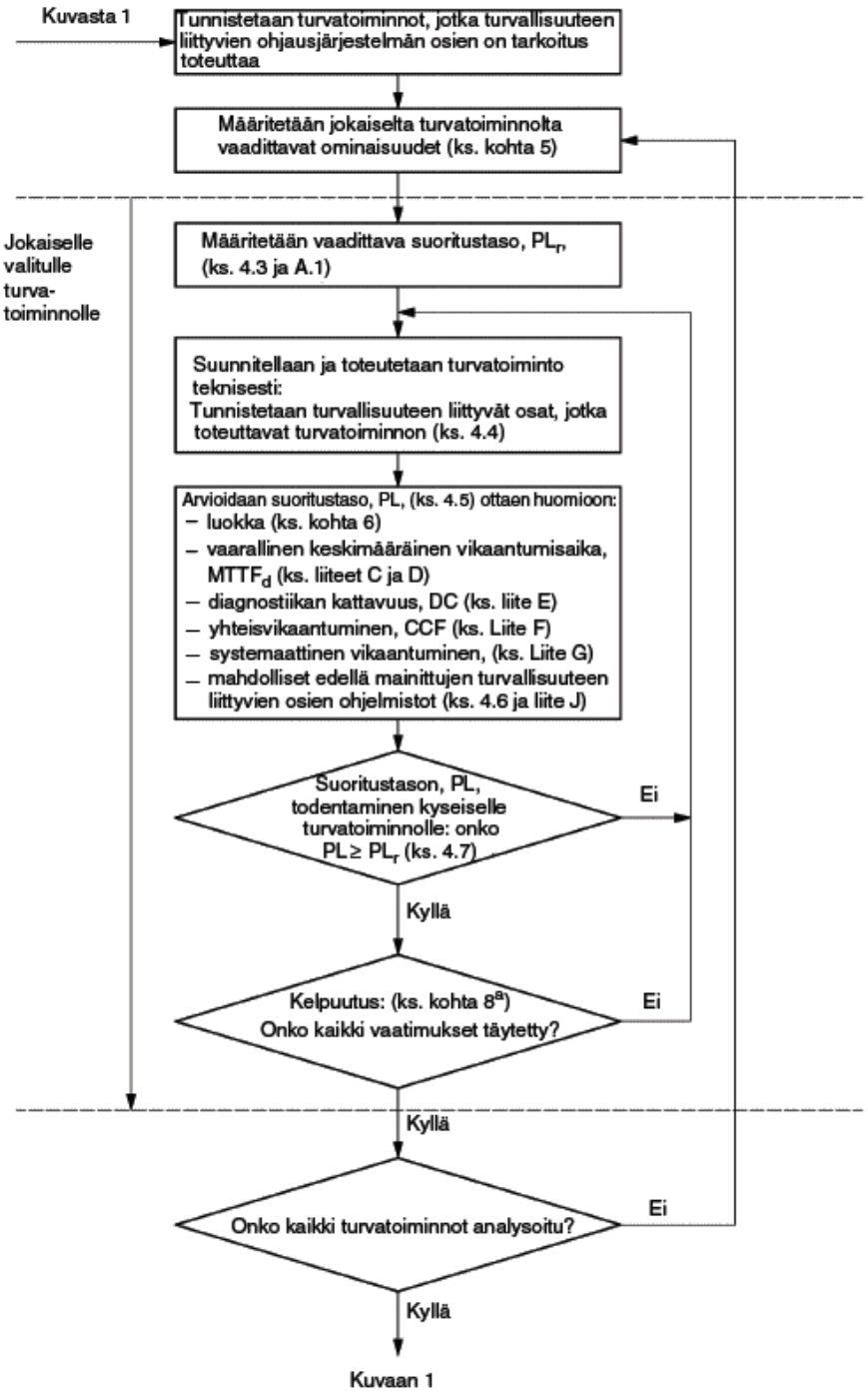
Turvallisuuteen liittyvien ohjausjärjestelmien osat tulee suunnitella ja toteuttaa siten, että noudatetaan kaikilta osin standardin ISO 12100 periaatteita (SFS-EN ISO 13849-1:2015, 2015, s. 17). Kuvassa 1 esitetään yleiskuva standardin ISO 12100 mukaisesta riskin arvioinnista ja pienentämisestä.



Kuva 1. Yleiskuva riskin arvioinnista ja pienentämisestä (SFS-EN ISO 13849-1:2015, 2015, s. 18)

Koneen yleisen suunnittelumenettelyn noudattamisen tarkoituksena on turvallisuustavoitteiden saavuttaminen. Se riskin pienentämisen osuus, joka saadaan aikaan turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelulla, on osa koneen yleistä suunnittelumenettelyä. Turvallisuuteen liittyvät ohjausjärjestelmän osat toteuttavat turvatoiminnon tai turvatoimintoja sellaisella suoritustasolla, jolla vaadittava riskin pienentäminen saavutetaan. Turvatoimintojen aikaansaaminen osana luontaisesti turvallista suunnittelua tai osana toimintaan kytketyn suojuksen tai suojalaitteen ohjausta, on turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelu osana riskin

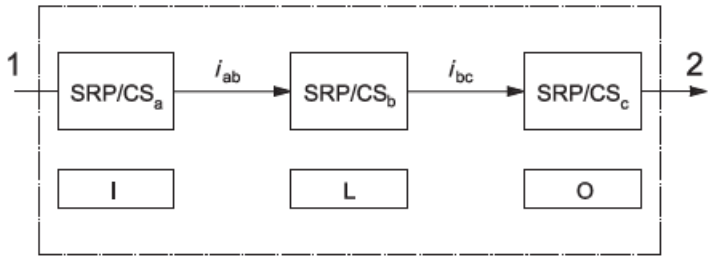
pienentämisen strategiaa. (SFS-EN ISO 13849-1:2015, 2015, s. 19.) Kuvassa 2 esitetään turvallisuuteen liittyvien ohjausjärjestelmien suunnittelun iteratiivinen prosessi.



Kuva 2. Turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelun iteratiivinen prosessi (SFS-EN ISO 13849-1:2015, 2015, s. 21)

Koneen turvatoimintojen määrittäminen on osa riskin pienentämisprosessia ja siihen kuuluvat ohjausjärjestelmän turvatoiminnot. Turvatoiminto voidaan toteuttaa yhdellä tai useammalla turvallisuuteen liittyvällä ohjausjärjestelmän osalla ja useampi

turvatoiminto voi käyttää yhtä tai useampaa turvallisuuteen liittyvää ohjausjärjestelmän osaa. Turvallisuuteen liittyvät ohjausjärjestelmän osat voivat myös toteuttaa sekä turvatoimintoja että tavallisia ohjaustoimintoja. Kun ohjausjärjestelmän turvatoiminnot on tunnistettu, suunnittelijan tulee tunnistaa turvallisuuteen liittyvät ohjausjärjestelmän osat ja tarvittaessa osoittaa niille tulot, logiikat ja lähdöt sekä erilliset kanavat varmennetuissa järjestelmissä. (SFS-EN ISO 13849-1:2015, 2015, s. 22.) Kuvassa 3 esitetään turvallisuuteen liittyvien ohjausjärjestelmien osien toteuttaman turvatoiminnon kaaviollinen esitys.



Selite

I Tulo (esim. rajakytkin, tunnistin, aktiivinen valosähköinen turvalaite)

L Logiikka

O Lähtö (esim. venttiili, kosketin, virranmuunnin)

1 Toiminnon aloittava tapahtuma (esim. painikkeeseen vaikuttaminen, suojuksen avaaminen, valosähköisen turvalaitteen valonsäteen katkaisu)

2 Koneen toimilaite (esim. moottori, sylinteri)

Kuva 3. Turvatoiminnon kaaviollinen esitys (SFS-EN ISO 13849-1:2015, 2015, s. 23)

2.3 Suoritustaso PL

Suoritustasoa PL käytetään määrittelemään turvallisuuteen liittyvien ohjausjärjestelmien osien kyky suorittaa turvatoiminto ennakoitavissa olevissa olosuhteissa (SFS-EN ISO 13849-1:2015, 2015, s. 12). Standardissa ISO 13849-1 suoritustasot määritellään vaarallisen vikaantumisen todennäköisyytenä tuntia kohden (PFHD). Suoritustasoja on viisi, joista ylin on PL e ja alin PL a. (SFS-EN ISO 13849-1:2015, 2015, s. 19.) Kuvassa 4 näkyvät kullekin suoritustasolle määritellyt vaihtelualueet vaarallisen vikaantumisen todennäköisyydelle tuntia kohden.

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

Kuva 4. Suoritustasot (PL) (SFS-EN ISO 13849-1:2015, 2015, s. 19)

Turvallisuuteen liittyvän ohjausjärjestelmän osan suoritustaso on määritettävä arvioimalla vaarallinen keskimääräinen vikaantumisaika ($MTTF_D$) jokaiselle yksittäiselle komponentille, diagnostiikan kattavuus (DC), yhteisvikaantuminen (CCF), rakenne, turvatoiminnon käyttäytyminen vikatilanteessa, turvallisuuteen liittyvä ohjelmisto, systemaattinen vikaantuminen sekä kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa. (SFS-EN ISO 13849-1:2015, 2015, s. 23.)

2.3.1 Kanavan vaarallinen keskimääräinen vikaantumisaika ($MTTF_D$)

Kanavan vaarallisen keskimääräisen vikaantumisajan ($MTTF_D$) arvo ilmaistaan kullekin kanavalle käyttäen kolmea kuvassa 5 näkyvää tasoa, ja se on otettava huomioon jokaiselle yksittäiselle kanavalle tai redundanttisen järjestelmän jokaiselle kanavalle. Tietojen hankinta komponentin vaarallisen keskimääräisen vikaantumisajan arviointia varten tulisi tehdä seuraavanlaisessa ensisijaisuusjärjestyksessä: käyttämällä valmistajan antamia tietoja, käyttämällä standardissa SFS-EN ISO 13849-1 liitteissä C ja D esitettyjä menetelmiä tai valitaan 10 vuotta. (SFS-EN ISO 13849-1:2015, 2015, s. 25-26.)

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

Kuva 5. Kanavan vaarallinen keskimääräinen vikaantumisaika ($MTTF_D$) (SFS-EN ISO 13849-1:2015, 2015, s. 25)

Standardin SFS-EN ISO 13849-1 liitteessä C esitetään useita menetelmiä yksittäisten komponenttien vaarallisen keskimääräisen vikaantumisajan arvioimiseksi tai laskemiseksi. Liitteessä esitetään menetelmiä, jotka perustuvat hyvien valmistuskäytäntöjen

huomioon ottamisessa erilaisille komponenteille, menetelmiä vaarallisen keskimääräisen vikaantumisajan laskemiseksi pneumaattisille, mekaanisille ja sähkömekaanisille komponenteille B_{10} -arvojen avulla sekä luettelo sähköisten komponenttien vaarallisista keskimääräisistä vikaantumisajoista. (SFS-EN ISO 13849-1:2015, 2015, s. 59.)

2.3.2 Diagnostiikan kattavuus (DC)

Diagnostiikan kattavuutta ilmaistaan neljällä kuvassa 6 esitetyllä tasolla. Diagnostiikan kattavuuden arvioimiseen voidaan useimmissa tapauksissa käyttää vika- ja vaikutusanalyysiä tai muuta vastaavaa menetelmää. Tällaisissa tapauksissa kaikki kyseeseen tulevat viat ja vikaantumismuodot tulisi ottaa huomioon. Standardin SFS-EN ISO 13849-1 liitteessä E, esitetään yksinkertaistettu lähestymistapa diagnostiikan kattavuuden arvioimiseksi. (SFS-EN ISO 13849-1:2015, 2015, s. 26.)

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

Kuva 6. Diagnostiikan kattavuus (DC) (SFS-EN ISO 13849-1:2015, 2015, s. 26)

2.3.3 Yhteisvikaantuminen (CCF)

Yhteisvikaantumisen vaikutuksen arviointi on laadullinen prosessi ja sillä olisi käytävä läpi koko järjestelmä. Jokainen turvallisuuteen liittyvien ohjausjärjestelmän osa olisi otettava tarkasteluun. Standardin SFS-EN ISO 13849-1 liitteessä F luetteloidaan toimenpiteet ja niihin liittyvät pisteet, jotka perustuvat teknisiin arviointeihin ja jotka edustavat näiden toimenpiteiden osuutta yhteisvikaantumisen vähentämiseen. Luettelossa esitetyille toimenpiteille voidaan esittää vain täydet pisteet tai ei mitään. Jos toimenpiteet toteutuvat vain osittain, ei pisteitä tämän menetelmän mukaisesti anneta. (SFS-EN ISO 13849-1:2015, 2015, s. 73.)

2.3.4 Luokat

Luokan B mukaiset turvallisuuteen liittyvät ohjausjärjestelmän osat tulee vähintäänkin suunnitella ja rakentaa siten, että ne kestävät odotettavissa olevat käyttökuormitukset, käsiteltävien aineiden vaikutukset sekä muut merkittävät ulkoiset tekijät kuten tehonsyötön katkeamiset ja häiriöt, sähkömagneettiset häiriöt ja tärinä. Tämän luokan järjestelmillä ei ole lainkaan diagnostiikan kattavuutta (DC_{avg} = nolla) ja kanavien keskimääräinen vaarallinen vikaantumisaika ($MTTF_D$) voi olla pieni tai keskitasoa. Luokassa B suurin saavutettavissa oleva suoritustaso on PL b. (SFS-EN ISO 13849-1:2015, 2015, s. 41-42.) Kuvassa 7 esitetään luokan B mukaisen turvallisuuteen liittyvän ohjausjärjestelmän rakenne.

Selite

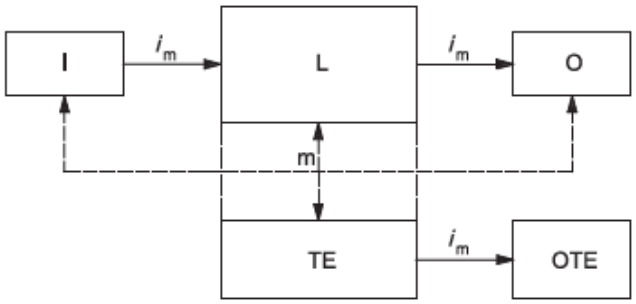
i_m	Liitäntävälineet
I	Tuloyksikkö (esim. anturi)
L	Logiikka
O	Lähtöyksikkö (esim. pääkontaktori)

Kuva 7. Luokan B rakenne (SFS-EN ISO 13849-1:2015, 2015, s. 42)

Luokassa 1 on sovellettava luokan B vaatimuksia. Lisäksi luokassa 1 on käytettävä hyvin koeteltuja komponentteja ja noudatettava hyvin koeteltuja turvallisuusperiaatteita. Hyvin koetelluksi komponentiksi katsotaan komponentti, jota on käytetty aikaisemmin laajasti ja josta on hyviä kokemuksia vastaavissa sovelluksissa, tai se on valmistettu ja todennettu noudattamalla periaatteita, joilla osoitetaan sen sopivuus ja luotettavuus turvallisuuteen liittyvissä sovelluksissa. Luokan 1 järjestelmillä ei myöskään ole lainkaan diagnostiikan kattavuutta (DC_{avg} = nolla), ja kanavien vaarallisen keskimääräisen vikaantumisajan ($MTTF_D$) on oltava korkea. Luokassa 1 suurin saavutettavissa oleva suoritustaso on PL c. (SFS-EN ISO 13849-1:2015, 2015, s. 42-43.) Luokan 1 rakenne vastaa luokan B rakennetta.

Luokassa 2 on sovellettava luokan B vaatimuksia sekä hyvin koeteltuja turvallisuusperiaatteita on noudatettava. Lisäksi luokassa 2 turvallisuuteen liittyvät

ohjausjärjestelmän osat tulee suunnitella siten, että koneen ohjausjärjestelmä tarkistaa niiden toiminnot sopivin väliajoin. Tarkistuksen on tapahduttava koneen käynnistyksen yhteydessä ja ennen yhdenkään vaaratilanteen alkamista. Tarkistuksen käynnistyminen voi alkaa automaattisesti ja sen on sallittava käyttötoiminta, jos vikoja ei ole paljastunut. Vian paljastuessa sen on saatava aikaan lähtösignaali, joka käynnistää tarvittavan ohjaustoiminnon. Suoritustasolla PLr d lähtösignaalin tulee käynnistää turvallinen tila, joka pysyy päällä, kunnes vika on korjattu. Suoritustasoon PLr c asti lähtösignaalin on mahdollisuuksien mukaan käynnistettävä turvallinen tila, joka pysyy päällä, kunnes vika on korjattu. Voi olla riittävää, että lähtösignaali antaa vain varoituksen, jos turvallisen tilan käynnistäminen ja ylläpitäminen ei ole käytännössä mahdollista. Luokassa 2 on kanavan diagnostiikan keskimääräisen kattavuuden (DC_{avg}) oltava vähintään matala, kanavan vaarallisen keskimääräisen vikaantumisajan ($MTTF_D$) on oltava matala tai korkea, riippuen vaadittavasta suoritustasosta (PLr) sekä toimenpiteitä yhteisvikaantumista (CCF) vastaan on käytettävä. Suurin saavutettava suoritustaso luokassa 2 on PL d. (SFS-EN ISO 13849-1:2015, 2015, s. 43-44.) Kuvassa 8 esitetään luokan 2 mukaisen turvallisuuteen liittyvän ohjausjärjestelmän rakenne.



Selite

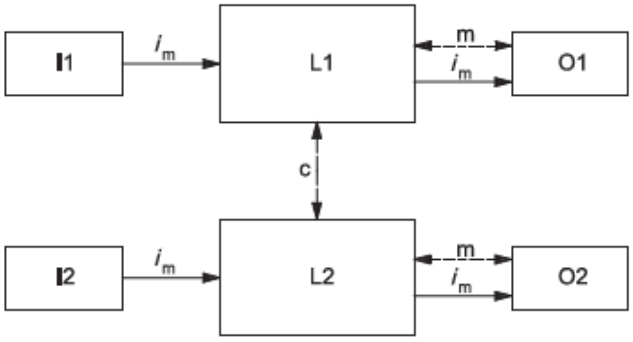
i_m	Liitäntävälineet
I	Tuloyksikkö (esim. anturi)
L	Logiikka
m	Valvonta
O	Lähtöyksikkö (esim. pääkontaktori)
TE	Testauslaitteisto
OTE	Testauslaitteiston lähdöt

Katkoviivat esittävät kohtuudella mahdollista vikojen paljastamista

Kuva 8. Luokan 2 rakenne (SFS-EN ISO 13849-1:2015, 2015, s. 45)

Luokassa 3 on sovellettava luokan B vaatimuksia, sekä hyvin koeteltuja turvallisuusperiaatteita on noudatettava. Lisäksi luokassa 3 turvallisuuteen liittyvät ohjausjärjestelmän osat tulee suunnitella siten, että yksittäiset viat missä tahansa turvallisuuteen

liittyvässä ohjausjärjestelmän osassa ei johda turvatoiminnon menettämiseen. Yksittäisen vian tulee myös paljastua turvatoiminnon seuraavaan vaateen yhteydessä tai ennen sitä, jos se on kohtuudella mahdollista. Luokassa 3 on turvallisuuteen liittyvien osien kokonaisuuden diagnostiikan keskimääräisen kattavuuden (DC_{avg}) oltava vähintään matala, redundanttisten kanavien vaarallisen keskimääräisen vikaantumisajan ($MTTF_D$) on oltava matala tai korkea, riippuen vaadittavasta suoritustasosta (PLr) sekä toimenpiteitä yhteisvikaantumista (CCF) vastaan on käytettävä. (SFS-EN ISO 13849-1:2015, 2015, s. 45.) Kuvassa 9 esitetään luokan 3 mukaisen turvallisuuteen liittyvän ohjausjärjestelmän rakenne.



Selite

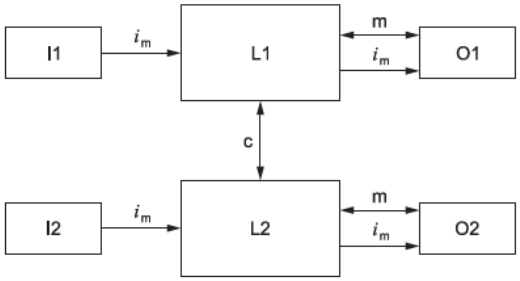
i_m	Liitäntävälineet
c	Ristiinvalvonta
I1, I2	Tuloyksikkö (esim. anturi)
L1, L2	Logiikka
m	Valvonta
O1, O_2	Lähtöyksikkö (esim. pääkontaktori)

Katkoviivat esittävät kohtuudella mahdollista vikojen paljastamista

Kuva 9. Luokan 3 rakenne (SFS-EN ISO 13849-1:2015, 2015, s. 46)

Luokassa 4 on sovellettava luokan B vaatimuksia, sekä hyvin koeteltuja turvallisuusperiaatteita on noudatettava. Lisäksi luokassa 4 turvallisuuteen liittyvät ohjausjärjestelmän osat tulee suunnitella siten, että yksittäiset viat turvallisuuteen liittyvissä ohjausjärjestelmän osissa ei johda turvatoiminnon menettämiseen ja yksittäiset viat paljastuvat turvatoiminnon seuraavan vaateen yhteydessä tai ennen sitä. Jos vikojen paljastuminen ei ole mahdollista, ei niiden kertyminen saa johtaa turvavoiminnon menettämiseen. Luokassa 4 on turvallisuuteen liittyvien osien kokonaisuuden diagnostiikan keskimääräisen kattavuuden (DC_{avg}) oltava korkea, redundanttisten kanavien vaarallisen keskimääräisen vikaantumisajan ($MTTF_D$) on oltava korkea, sekä toimenpiteitä yhteisvikaantumista (CCF) vastaan on käytettävä. (SFS-EN ISO 13849-1:2015, 2015,

s. 46.) Kuvassa 10 esitetään luokan 4 mukaisen turvallisuuteen liittyvän ohjausjärjestelmän rakenne.



Selite

i_m	Liitäntävälineet
c	Ristiinvalvonta
I1, I2	Tuloyksikkö (esim. anturi)
L1, L2	Logiikka
m	Valvonta
O1, O_2	Lähtöyksikkö (esim. pääkontaktori)

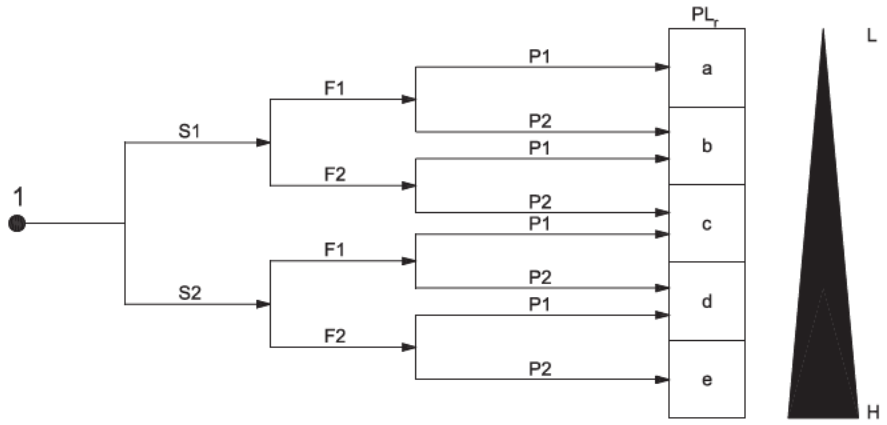
Yhtenäiset viivat valvontatoiminnoissa esittävät diagnostiikan kattavuutta, jonka taso on korkeampi kuin luokkaan 3 kuuluvassa nimetyssä rakenteessa

Kuva 10. Luokan 4 rakenne (SFS-EN ISO 13849-1:2015, 2015, s. 47)

2.4 Vaadittavan suoritustason (PL_r) määrittäminen.

Vaadittava suoritustaso (PL_r) on määritettävä jokaiselle turvatoiminnolle, jotka on tarkoitus toteuttaa ohjausjärjestelmän turvallisuuteen liittyvillä osilla ja se on dokumentoitava. Vaadittava suoritustaso määritetään riskin arvioinnin tuloksena ja sillä viitataan siihen riskin pienentämisen määrään, jonka turvallisuuteen liittyvien ohjausjärjestelmien osien on tarkoitus toteuttaa. (SFS-EN ISO 13849-1:2015, 2015, s. 22).

Kuvassa 11 esitetty kuvaaja perustuu tilanteeseen ennen turvatoiminnon lisäämistä. Turvatoiminnolta vaadittavaa suoritustasoa määritettäessä on otettava huomioon riskin pienentäminen ohjausjärjestelmästä riippumattomilla teknisillä toimenpiteillä, esimerkiksi mekaanisilla suojuksilla tai täydentävillä turvatoiminnoilla. Tämän kaltaisissa tilanteissa tulisi kuvassa 11 esitetyn kuvaajan aloituskohdaksi valita näiden toimenpiteiden toteuttamisen jälkeinen tilanne. (SFS-EN ISO 13849-1:2015, 2015, s. 53.)



Selite

1	Aloituskohta turvatoiminnon osuudenarvioimiseksi riskin pienentämisessä
L	Osuus riskin pienentämisessä pieni
H	Osuus riskin pienentämisessä suuri
PL_r	Vaadittava suoritustaso
Riskimuuttujat:	
S	Vamman vakavuus
S1	Lievä (tavallisesti palautuva vamma)
S2	Vakava (tavallisesti palautumaton vamma tai kuolema)
F	Vaaralle altistumisen taajuus ja/tai kesto
F1	Harvoin...toisinaan ja/tai lyhyt altistumisaika
F2	Toistuvasti...jatkuvasti ja/tai pitkä altistumisaika
P	Mahdollisuus välttää vaaraa tai rajoittaa vahinkoa
P1	Mahdollista tietyissä olosuhteissa
P2	Tuskin mahdollista

Kuva 11. Vaadittavan suoritustason (PL_r) määrittäminen turvatoiminnolle (SFS-EN ISO 13849-1:2015, 2015, s. 55)

Riskin suuruuttaa arvioitaessa käytetään apumuuttujia: vamman vakavuus (S), vaaralle altistumisen taajuus ja kesto (F) sekä mahdollisuus välttää vaaraa tai rajoittaa vahinkoa (P). Standardin SFS-EN ISO 13849-1 mukaan kokemus osoittaa, että nämä muuttujat voidaan yhdistää kuvassa 11 esiintyvällä tavalla, siten että saadaan riskin luokitus matalasta korkeaan. Tämä on kuitenkin vain laadullinen prosessi, joka tuottaa vain arvion riskin suuruudesta. (SFS-EN ISO 13849-1:2015, 2015, s. 53.)

Kun arvioidaan turvatoiminnon vikaantumisesta syntyvien riskien suuruutta, tarkastellaan vain lieviä tavallisesti palautuvia vammoja tai vakavia tavallisesti palautumattomia vammoja ja kuolemantapauksia. Vamman vakavuus (S) luokitellaan muuttujilla S1 ja S2. Näiden muuttujien valinnassa tulisi ottaa huomioon tapaturmien tavanomiaset seuraukset sekä niiden tavanomaiset paranemisprosessit. Esimerkiksi ruhjeet ilman komplikaatiota voitaisiin luokitella muuttujan S1 avulla, kun taas irtileikkautuminen tai kuolema voitaisiin luokitella muuttujan S2 avulla. (SFS-EN ISO 13849-1:2015, 2015, s. 53.)

Vaaralle altistumisen taajuutta ja kestoa (F) luokitellaan muuttujilla F1 ja F2. Standardin SFS-EN ISO 13849-1 mukaan näille muuttujille ei kuitenkaan voida määrittää yleisesti pätevää aikaväliä. Standardissa kuitenkin esitetään selostus, joka voi epäselvissä tapauksissa helpottaa oikean valinnan tekemistä. Jos henkilö on toistuvasti tai jatkuvasti altistuneena kyseiselle vaaralle, olisi valittava muuttuja F2. On epäolennaista, onko kyseisissä tapauksissa vaaralla altistuneena sama vai eri henkilö. Tämä muuttuja olisi valittava vaaralla alttiiksi joutumisen taajuuden ja kestoajan perusteella. Vaaralle altistumisen aikaa tulisi arvioida keskimääräisen arvon avulla, jota voidaan tarkastella suhteessa laitteen kokonaiskäyttöaikaan. Muuttuja F2 tulisi valita tilanteissa, joissa joudutaan esimerkiksi työkappaleita syötettäessä ja siirrettäessä säännöllisesti ulottumaan koneen työkalujen väliin tai jos muita perusteluita ei ole, mutta taajuus on suurempi kuin kerran 15 minuutissa. Muuttuja F1 voidaan valita, jos kertyvä altistusaika ei ylitä 1/20 laitteen kokonaiskäyttöajasta tai taajuus ei ole suurempi kuin kerran 15 minuutissa. (SFS-EN ISO 13849-1:2015, 2015, s. 53-54.)

Mahdollisuus välttää vaaraa tai rajoittaa vahinkoa (P) luokitellaan muuttujilla P1 ja P2. Muuttuja P1 tulisi valita ainoastaan, jos vaaratilanteen esiintyessä on todella mahdollista välttää vaaraa tai rajoittaa sen vahinkoa. Muissa tapauksissa muuttujaksi tulisi valita P2. (SFS-EN ISO 13849-1:2015, 2015, s. 54.)

3 HÄTÄPYSÄYTYS

3.1 Hätäpysäytystoiminto

Hätäpysäytystoiminnon tarkoituksena on estää henkilöiden käyttäytymisestä tai odottamattoman vaarallisen tapahtuman aiheuttamat uhkaavat tai todelliset hätätilanteet. Hätäpysäytystoiminto on oltava saatavilla ja toimintakuntoinen koko ajan sekä sen on oltava käynnistettävissä yhdellä ihmisen suorittamalla toimenpiteellä. Sen on myös oltava ensisijainen koneen muihin toimintoihin ja käyttötoimenpiteisiin nähden koneen

kaikkien toimintatapojen aikana heikentämättä muita suojaavia toimintoja. (SFS-EN ISO 13850:2015, 2015, s. 8.)

Hätäpysäytystoiminnon on käynnistyksen jälkeen pysyttävä käynnissä, kunnes se kuitataan käsikäyttöisesti. Minkään hätäpysäytystoiminnolla pysäytetyn toiminnon käynnistyskäsky ei saa aiheuttaa toiminnon käynnistymistä hätäpysäytyksen ollessa käynnissä. Hätäpysäytyksen toimintavalmiiksi palauttaminen on tapahduttava ihmisen suorittamalla tarkoituksellisella toimenpiteellä. Hätäpysäytystoiminnon toimintavalmiuden palauttaminen on tapahduttava vapauttamalla hätäpysäytyslaite lukinnasta, toimintavalmiuden palauttaminen ei kuitenkaan saa käynnistää konetta. (SFS-EN ISO 13850:2015, 2015, s. 8.)

Hätäpysäytystoiminto on täydentävä suojaustoimenpide. Hätäpysäytystoimintoa ei saa käyttää suojausteknisten toimenpiteiden ja muiden toimintojen tai turvatoimintojen korvaamiseen. Hätäpysäytystoiminto on suunniteltava siten, että hätäpysäytyslaitteeseen vaikuttamisen jälkeen koneen vaaralliset liikkeet pysäytetään aiheuttamatta lisävaaroja ja ilman muuta toimintaan puuttumista, eikä päätös hätäpysäytyslaitteeseen vaikuttamisesta vaadi ottamaan huomioon siitä koituvia seurauksia. Riippuen koneesta ja kyseessä olevista riskeistä hätäpysäytystoiminto voi käynnistää vahinkoriskin minimoimiseksi tarkoitettujen pysäytystoimintojen lisäksi muita toimintoja, kuten peruutus, liikkeen rajoitus tai jarrutusvoiman säätö. (SFS-EN ISO 13850:2015, 2015, s. 8-9.)

3.2 Hätäpysäytysvyöhyke

Hätäpysäytysvyöhyke on alue, jonka sisällä oleviin koneisiin vyöhykkeen hätäpysäytyslaite vaikuttaa. Jokaisen hätäpysäytyslaitteen aikaansaamaan toiminnon on vaikutettava koko koneeseen. Poikkeuksellisesti koko koneeseen vaikuttava hätäpysäytystoiminto saattaa olla soveltumaton tilanteissa joissa, kaikkien toisiinsa kytkettyjen koneiden pysäyttäminen voisi aiheuttaa lisävaaroja tai vaikuttaa tarpeettomasti tuotantoon. Hätäpysäytysvyöhyke voi kattaa osan koneesta, koko koneen tai koneryhmän. Vyöhykkeet voivat myös olla osittain päällekkäin. (SFS-EN ISO 13850:2015, 2015, s. 9.)

Hätäpysäytysvyöhykkeitä määritettäessä on otettava huomioon koneen sijoittelu koneen näkyvissä oleviin alueisiin perustuen. Vaaratilanteiden tunnistamisen mahdollisuus esimerkiksi näkyvyyden, äänien tai hajujen perusteella. Tuotantoprosessiin liittyvät muut vaaratekijät. Ennakoitavissa oleville vaaratekijöille altistuminen sekä mahdolliset muut lähistöllä olevat vaaratekijät. (SFS-EN ISO 13850:2015, 2015, s. 9.)

3.3 Pysäytysluokat

Hätäpysäytystoiminnoille pysäytysluokkia on kaksi, pysäytysluokka 0 ja pysäytysluokka 1. Hätäpysäytystoiminnon on toimittava seuraavien pysäytysluokkien mukaisesti. Vaadittava pysäytysluokka valitaan riskin arvioinnin perusteella. (SFS-EN ISO 13850:2015, 2015, s. 10.)

Pysäytysluokassa 0 pysäytys tapahtuu katkaisemalla tehonsyöttö välittömästi koneen toimilaitteisiin. Pysäytysluokassa 0 on myös otettava huomioon mahdollinen jarrutuksen tarve, tehonsyötön katkaisun lisäksi. Pysäytys voidaan toteuttaa katkaisemalla tehonsyöttö koneen sähkömoottoreilta sähkömekaanisilla kytkinlaitteilla, sekä sähkömoottorille vääntömomentin tai voiman tuottamiseen tarvittavan tehon poisto käyttämällä standardin IEC 61800-5-2 mukaista voimansiirtojärjestelmän turvallista vääntömomentin katkaisutoimintoa (Safe Torque Off, STO). Pysäytys voidaan myös toteuttaa sulkemalla pneumaattinen tai hydraulinen tehonsyöttö pneumaattisilta tai hydraulisilta toimilaitteilta. (SFS-EN ISO 13850:2015, 2015, s. 10.)

Pysäytysluokassa 1 pysäytys tapahtuu säilyttämällä tehonsyöttö koneen toimilaitteille pysähtymisen aikaansaamiseksi sekä katkaisemalla tehonsyöttö, kun pysähtyminen on saatu aikaan. Pysäytysluokassa 1 pysäytys voidaan toteuttaa liikettä hidastamalla, pysähtymisen jälkeen katkaistaan sähkömoottorin tehonsyöttö sähkömekaanisilla kytkimillä. Pysäytys voidaan myös toteuttaa käyttämällä standardin IEC 61800-5-2 mukaista voimansiirtojärjestelmän turvapysäytystoimintoa 1 (Safe Stop 1, SS1). (SFS-EN ISO 13850:2015, 2015, s. 10.)

3.4 Hätäpysäytyslaite

Hätäpysäytyslaitteet on suunniteltava siten, että käyttäjät, joilla voisi olla tarve niiden käyttöön, voivat tunnistaa ja vaikuttaa niihin helposti (SFS-EN ISO 13850:2015, 2015, s. 12). Hätäpysäytyslaitteen hallintaelimen on oltava väriltään punainen. Hallintaelimen taustan on oltava väriltään keltainen, kun se käytännössä on mahdollista. (SFS-EN ISO 13850:2015, 2015, s. 13.) Hätäpysäytyslaitteen hallintaelin voi olla tyypiltään helposti kämmenellä vaikutettava painike, naru, köysi, tanko tai käsikahva. Muiden ratkaisujen ollessa epäkäytännöllisiä, voidaan hallintaelimenä käyttää jalkapoljinta, jossa ei ole suojakantta. (SFS-EN ISO 13850:2015, 2015, s. 12.)

Hätäpysäytyslaite on sijoitettava jokaiseen käyttäjän ohjauspaikkaan, ellei riskinarviointi osoita sen olevan tarpeetonta. Hätäpysäytyslaite on myös sijoitettava jokaiseen muuhun riskinarvioinnin määrittämään kohtaan, esimerkiksi koneen sisään- ja ulosmenokohdat, kohdat, joissa käyttäjän tarvitsee puuttua koneen toimintaan sekä paikoissa, joissa koneen rakenteen vuoksi on odotettavissa ihmisen ja koneen välistä vuorovaikutusta. Hätäpysäytyslaitteen sijoituksessa on otettava huomioon, että siihen pystytään vaikuttamaan ilman vaaraa, eikä sen vaikuttamista pystytä helposti estämään. Kädellä vaikutettavan hätäpysäytyslaitteen hallintaelin tulisi kiinnittää 0,6–1,7 metrin korkeudelle kulkutasosta, kun taas jalkapolkimet tulisi kiinnittää kiinteästi suoraan kulkutasoon. (SFS-EN ISO 13850:2015, 2015, s. 12.)

3.4.1 Narujen ja köysien käyttö ohjaimena

Hätäpysäytyslaitteiden hallintaeliminä voidaan käyttää myös naruja ja köysiä, muiden hallintaelinten tapaan ovat nekin suunniteltava ja sijoitettava helposti käytettäväksi. Naruja ja köysiä käytettäessä on otettava huomioon tarvittava poikkeutuksen suuruus sekä tarvittava voima ja sen suunta, joka naruun tai köyteen on kohdistettava, jolla hätäpysäytyskäsky saadaan aikaiseksi. Huomioon on otettava myös narun tai köyden suurin mahdollinen poikkeutus, sekä niiden ja lähimmän esineen välinen vähimmäisetäisyys. (SFS-EN ISO 13850:2015, 2015, s. 14.)

Narujen ja köysien on myös oltava väriltään punaisia. Punaisesta väristä huolimatta, saattaa narun tai köyden näkyvyys olla heikko. Narujen ja köysien näkyvyyttä

voidaankin parantaa käyttämällä merkintälippuja. Merkintälippuja käytettäessä on niiden oltava väriltään punaisia ja keltaisia, esimerkiksi punakeltaraidoitettuja tai niin että punaisen ja keltaisen väriset merkintäliput vuorottelevat. (SFS-EN ISO 13850:2015, 2015, s. 14.)

Jos on todennäköistä että, naruun yritetään vaikuttaa vetämällä sitä sen akselin suuntaisesti, on narun vetäminen kumpaan suuntaan tahansa saatava aikaan hätäpysäytyskäsky. Hätäpysäytyskäskyn on myös käynnistyttävä tilanteissa, joissa naru tai köysi on löystynyt, mennyt poikki tai irronnut. Välineet hätäpysäytyslaitteen toimintavalmiiksi palauttamiseen on sijoitettava siten, että naru tai köysi näkyy koko pituudeltaan niiden sijaintikohdasta. (SFS-EN ISO 13850:2015, 2015, s. 14.)

4 HÄTÄPYSÄYTYSJÄRJESTELMÄN SUUNNITTELU

4.1 Hätäpysäytyslaitteiden asennuksen suunnittelu

Suolistamon hätäpysäytysjärjestelmän suunnittelu aloitettiin tekemällä kierros suolistamon alueella, yhdessä esimieheni, suolistamon alueen kunnossapidosta vastaavan esimiehen sekä asiakkaan puolelta toimihenkilöiden ja työturvallisuusvastaavien kanssa. Kierroksella käytiin läpi suolistamon koneet ja alueet, joiden turvallisuudessa oli havaittu puutteita. Asiakas esitti toiveensa, millainen hätäpysäytyslaite kullekin koneelle haluttaisiin. Jo kierroksen aikana käytiin keskustelua siitä, oliko jokin hätäpysäytyslaite soveltuva kyseiselle koneelle ottamalla huomioon koneen normaali toiminta ja käyttö sekä voisiko kone tai koneessa oleva tuote päästä vaikuttamaan hätäpysäytyslaitteeseen, aiheuttaen turhia pysähdyksiä tuotannolle. Kierroksen aikana esitetyt toiveet ja ratkaisut kirjattiin ylös ja ne toimivat suunnittelun lähtötietoina.

Kierrokselta saatujen lähtötietojen jälkeen, käytiin koneet vielä uudestaan läpi ja suunniteltiin hätäpysäytysvaijereiden kulkureitit, ottamalla huomioon vaijerin vaatima poikkeutus sekä hätäpysäytyspainikkeiden paikat. Suunnitelmasta luotiin kirjallinen raportti, jossa esitettiin erikseen jokainen suolistamon kone johon hätäpysäytyslaite

haluttiin sekä hätäpysäytyslaitteiden asennuksen toteutustavat. Kun suunnitelma saatiin valmiiksi, hyväksytettiin se asiakkaalla. Suunnitelman hyväksytyksen jälkeen tehtiin suolistamossa uusi kierros yrityksen mekaanisten asentajien kanssa, jotka rakentaisivat koneisiin tarvittavat kiinnikkeet hätäpysäytyslaitteille ja vaijereiden kulkureiteille. Lopuksi suunniteltiin vielä paikka hätäpysäytysjärjestelmän keskukselle tehtaan välikatolta sekä kaapelireitit keskukselta hätäpysäytyslaitteille. Kaapelireitit suunniteltiin niin, että pystyttiin hyödyntämään olemassa olevia läpivientejä ja kaapelihyllyjä välikaton ja suolistamon välillä.

4.2 Turvalogiikkakeskuksen suunnittelu ja komponenttien valinta

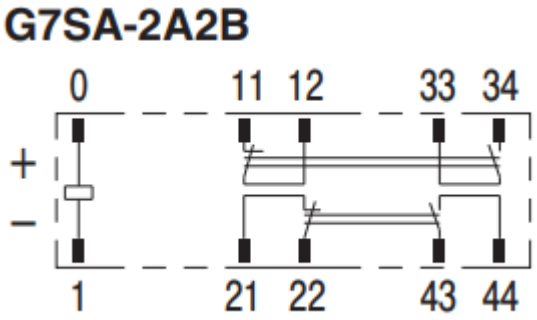
Hätäpysäytyslaitteiden asennuksen suunnittelun jälkeen aloitettiin järjestelmälle tulevan keskuksen suunnittelu. Suunnitteluvaiheessa valittiin järjestelmässä käytettävät komponentit, jonka jälkeen piirrettiin laitteistosta alustavat sähköpiirustukset. Järjestelmässä käytettävä turvalogiikka I/O-moduuleineen oli jo ennalta hankittu, joten turvalaitteiston kannalta oleellisista osista vain vaatimustenmukaisten releiden valinta tuli tehdä. Muiden komponenttien osalta valittiin komponentteja, joita oli käytössä muissakin tehtaan laitteissa ja olivat hyväksi todettuja.

Hätäpysäytysjärjestelmän turvalogiikaksi oli valittu ABB:n AC500-S, joka täyttää SIL 3 ja PL e tasojen vaatimukset. Turvalogiikkaan kuului SM560-S turva-CPU, PM5630-2ETH tavallinen CPU, kolme DI581-S turvatulomoduulia, DX581-S turvatulo- ja lähtömoduuli sekä tavallinen digitaalitulo- ja lähtömoduuli DC532.

ABB:n AC500-sarjan logiikoilla voidaan yhdistää tavallisia ja turva I/O-moduuleja, erilaisten automaatiojärjestelmien rakentamiseksi. Tavallisia AC500 moduuleita ei käytetä AC500-S turvalogiikassa turvatoimintojen suorittamiseen, eikä näissä esiintyvät mahdolliset viat vaikuta negatiivisesti turvatoimintojen suorittamiseen (ABB, 2022, s. 66). Turvalogiikan turva-CPU SM560-S asennetaan tavallisen CPU:n vasemmalle puolelle kommunikointiväylään, jonka kautta ne voivat kommunikoida keskenään. Turva-CPU:n ollessa erillinen laite, voidaan turvaohjelmaa ajaa erillään tavallisen CPU:n ohjelmasta.

Turvatulomoduuli DI581-S sisältää 16 turvadigitaalitulokanavaa ja 8 test pulse-lähtöä. Test pulse-lähdöt tarjoavat 24 V signaalin lyhyillä yhden millisekunnin mittaisilla uniikeilla vaihesiirretyillä 0 V pulsseilla, joita voidaan käyttää valvomaan vääriä signaaleja tulokanavissa (ABB, 2022, s. 66). Test pulse-lähdöt on omistettu tietyille tulokanaville, esimerkiksi test pulse-lähtöä T0 voidaan käyttää vain tulokanavien I0 ja I1 kanssa. Turvatulo- ja lähtömoduuli DX581-S sisältää 8 turvadigitaalitulokanavaa, 8 turvadigitaalilähtökanavaa sekä 4 test pulse-lähtöä. Kuten turvatulomoduulissakin, test-pulse-lähdöt on omistettu tietyille tulokanaville

Järjestelmässä käytettäviksi releiksi valittiin Omronin G7SA-2A2B. G7SA tuoteperheen pakko-ohjatut releet on suunniteltu käytettäviksi erilaisissa turvallisuuteen liittyvissä järjestelmissä. G7SA-2A2B releessä on kaksi, kuvassa 12 näkyvää avautuvaa ja sulkeutuvaa kosketinta, jotka on yhdistetty toisiinsa mekaanisesti. Koskettimien mekaaninen yhdistäminen mahdollistaa esimerkiksi koskettimien kiinni hitsaantumisen havaitsemisen.

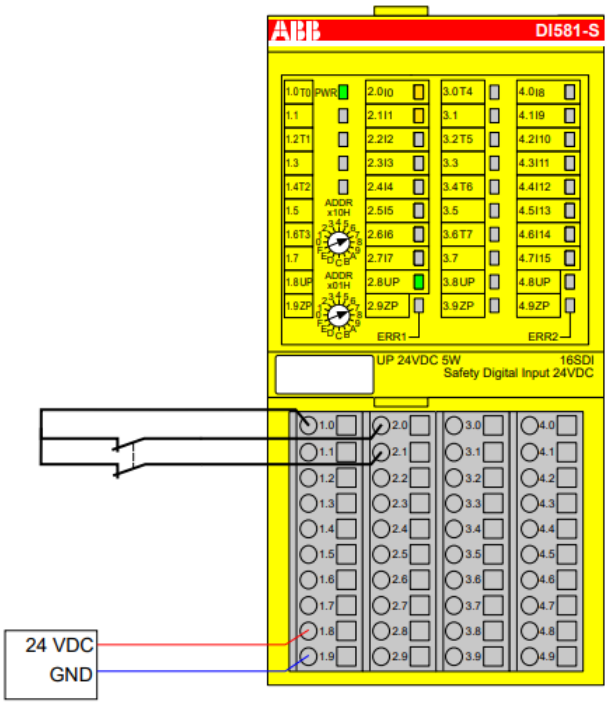


Kuva 12. G7SA-2A2B releen koskettimet (Omron, n.d., s. 8)

Kun järjestelmässä käyttävät komponentit oli saatu valittua, aloitettiin alustavien sähköpiirustusten teko. Sähköpiirustuksia tehdessä perehdyttiin paremmin ABB:n ohjekirjaan ”AC500-S Safety User Manual V1.3.0”, josta löytyi suoraan kytkentä esimerkkejä turvatulo- ja lähtömoduuleille.

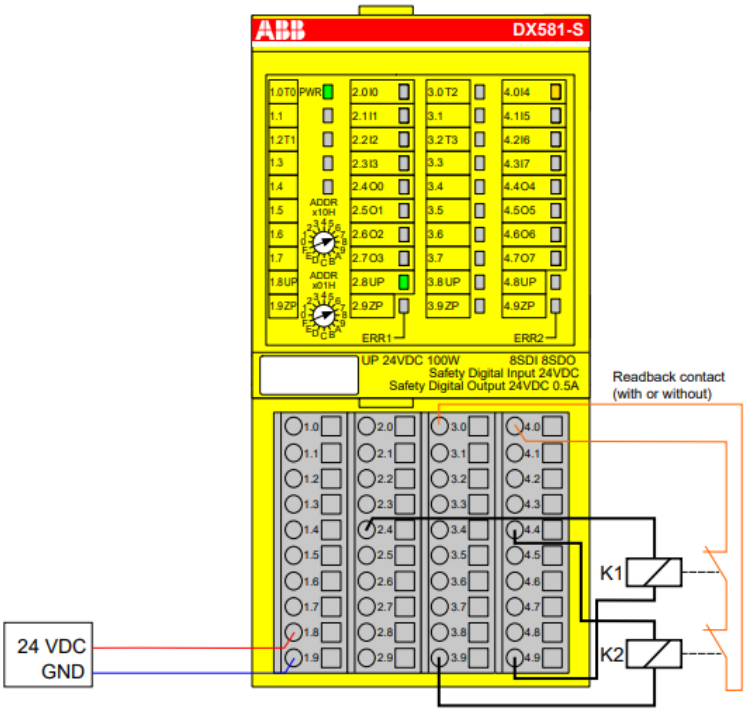
Hätäpysäytyslaitteiden kytkennät turvatulomoduuleille tehtäisiin kuvassa 13 esiintyvän esimerkin mukaisesti. Hätäpysäytyslaitteen molemmat kanavat saisivat syöttönsä turvatulomoduulin test pulse-lähdöstä ja kanavien tulosignaalit kytkettäisiin kyseiselle

test pulse-lähdölle omistettuihin tulokanaviin. Tällä kytkennällä ja virheiden poissulkemisella voitaisiin saavuttaa SIL 3 ja PL e tasojen vaatimukset.



Kuva 13. Hätäpysäytyslaitteiden kytkentä turvatulomoduuliin (ABB, 2022, s. 80)

Hätäpysäytysjärjestelmän releiden ohjaus tehtäisiin turvatulo- ja lähtömoduulilla kuvassa 14 esiintyvän esimerkin mukaisesti. Kummallekin releelle tulisi oma ohjauksensa moduulin lähtökanavista. Releiden takaisinkytkentä saataisiin releiden avautuvien koskettimien sarjaan kytkennästä, joka saisi syöttönsä moduulin test pulse-lähdösta ja takaisinkytkennän signaali tuotaisiin test pulse-lähdölle omistettuun tulokanavaan. Tällä kytkennällä voitaisiin saavuttaa SIL 3 ja PL e tasojen vaatimukset.

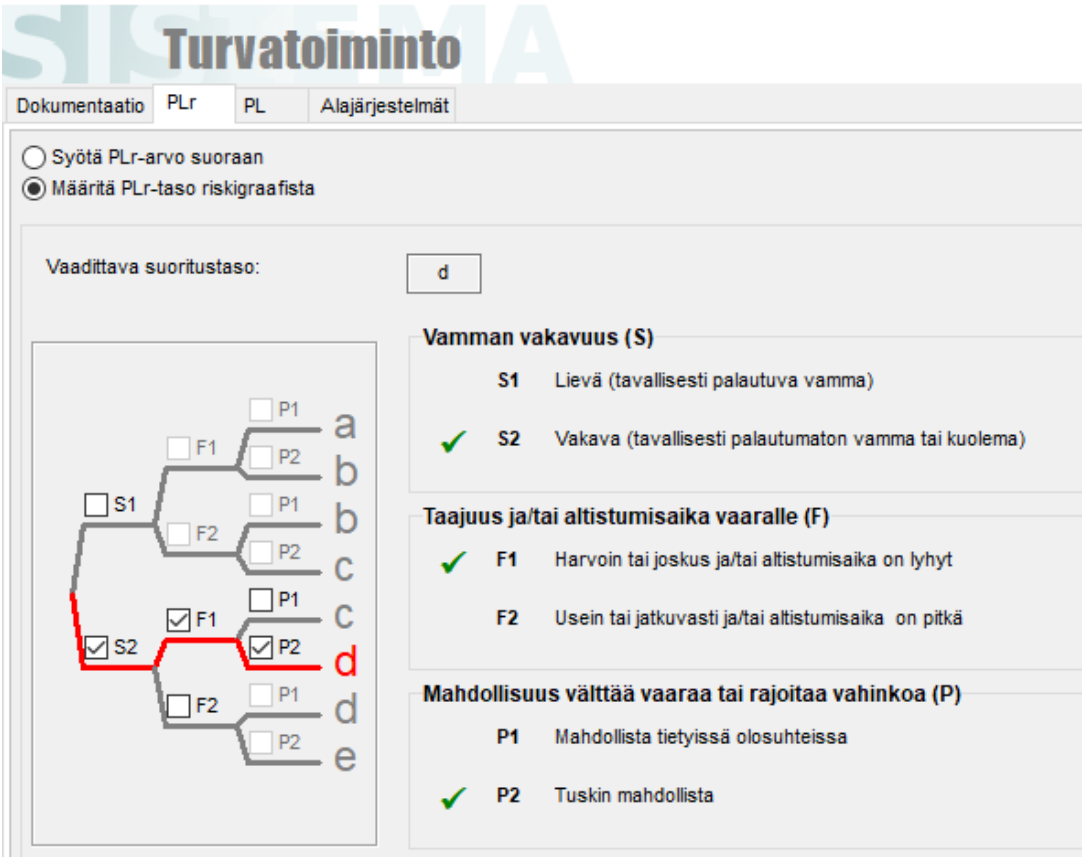


Kuva 14. Releiden kytkentä turvatulo- ja lähtömoduuliin (ABB, 2022, s. 102)

4.3 Hätäpysäytysjärjestelmän todentaminen

Komponentti valintojen sekä alustavien sähköpiirustusten jälkeen tuli vielä varmistaa hätäpysäytysjärjestelmän osien suoritustasojen riittävyys. Suoritustasot todennettiin Sistema-ohjelmistotyökalulla. Sistema-ohjelmistotyökalu on Saksassa/IFA:ssa kehitetty tietokoneavusteinen suunnittelumenetelmä. Sistema on tarkoitettu koneiden turvallisuuteen liittyvien ohjausjärjestelmien suunnitteluun ja se perustuu kaikilta osin ISO 13849-1 standardiin. (Sundcon Oy, n.d.)

Ohjelmiston käyttö aloitettiin luomalla uusi projekti. Projektin nimeksi annettiin tässä tapauksessa ”Suolistamo hätäpysäytysjärjestelmä”. Projektin luomisen jälkeen sille lisättiin turvatoiminto (SF). Turvatoiminnolle annettiin nimeksi ”Hätäpysäytys”, ja sille määriteltiin vaadittu suoritustaso PL_r. Vaadittu suoritustaso määritettiin kuvassa 15 esitetyllä ohjelmistossa olevalla riskigraafilla.



Kuva 15. Riskigraafi

Vamman vakavuutta (S) arvioitaessa tarkasteltiin suolistamon laitteiden vaaroja. Vaaroiksi tunnistettiin liikkuvat ja pyörivät kone-elimet sekä viiltävät osat. Näiden vaarojen mahdolliset seuraukset voivat olla puristuminen, viiltyminen tai irtileikkaantuminen, takertuminen, loukkuunjääminen, nieluunjoutuminen, hankautuminen ja hiertyminen sekä isku. Vamman vakavuudeksi (S) valittiin muuttuja S2, joka on vakava, tavallisesti palautumaton vamma tai kuolema.

Vaaralle altistumisen taajuus ja/tai kesto (F), koneet ovat suojattu suojuksilla, jotka estävät pääsyn vaaravyöhykkeille. Tilanteissa, joissa koneet ovat päällä ja suojukset ovat auki, esimerkiksi kun koneita pestään, on vaaralla altistumisen kesto lyhyt. Vaaralle altistumisen taajuudeksi ja/tai ajaksi valittiin muuttuja F1. F1 voidaan valita, jos altistusaika ei ylitä määrää 1/20 kokonaiskäyttöajasta tai vaaralla altistumisen taajuus ei ole suurempi kuin kerran 15 minuutissa (SFS-EN ISO 13849-1:2015, 2015, s. 54).

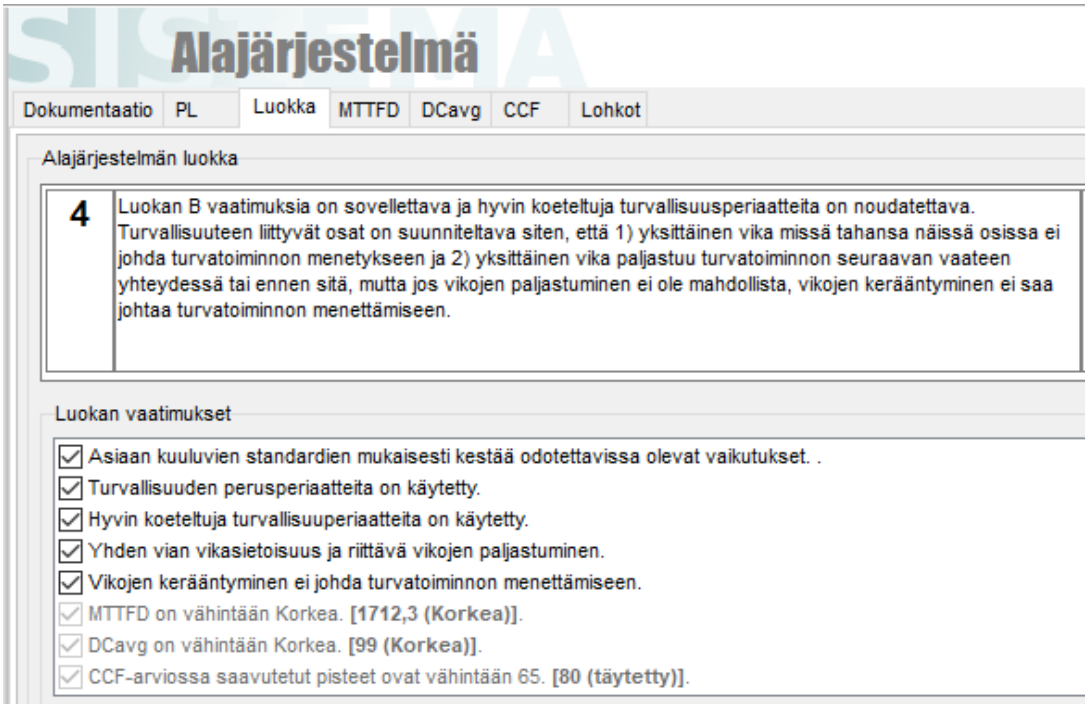
Mahdollisuus välttää vaaraa tai rajoittaa vahinkoa (P). Vaaratilanteen esiintyessä olisi valittava P1 ainoastaan, jos vaaran välttäminen on todella mahdollista tai sen vaikutusta voidaan merkittävästi vähentää, muutoin olisi valittava P2 (SFS-EN ISO 13849-

1:2015, 2015, s. 54). Esimerkiksi kun koneita pestään, on koneiden suojukset avattava, eikä vaaraa voida välttää, joten valittiin muuttuja P2. Nämä riskimuuttuja valinnat määrittelivät vaadituksi suoritustasoksi PL_r d.

Turvatoiminnon ja siltä vaadittavan suoritustason määrittelyn jälkeen aloitettiin tietojen lisääminen turvatoimintoon. Komponentit lisättiin turvatoiminnon alajärjestelmään (SB) ja järjestelmässä olevat kahdennukset lisättiin alajärjestelmissä oleviin kanaviin (CH). Komponentteja voitiin lisätä ohjelmaan kahdella eri tavalla. Osalle komponenteista löytyi valmistajilta ohjelmaan ladattavia kirjastoja, joista komponentit voidaan lisätä ohjelmaan suoraan. Näille komponenteille valmistaja on määrittänyt suoraan luokan ja suoritustason. Komponentit voidaan myös lisätä ohjelmaan manuaalisesti. Kun komponentti lisätään ohjelmaan manuaalisesti, voidaan sen suoritustaso määrittää suoraan, jos valmistaja sen ilmoittaa. Monille sähkömekaanisille komponenteille ilmoitetaan kuitenkin vain $B10_D$-arvo, jolloin komponentille on määriteltävä luokka, DC_{avg}-arvo sekä arvioitava komponentin käyttökertojen määrä, jonka avulla ohjelma laskee komponentille $MTTF_D$-arvon $B10_D$-arvon avulla.

4.3.1 Hätäpysäytyslaitteet

Hätäpysäytysjärjestelmässä on 16 hätäpysäytyslaitetta, joista kolmetoista on vaijereita, kaksi painiketta ja yksi kahva. Jokainen hätäpysäytyslaite lisättiin ohjelmaan omana alajärjestelmänään koska ne olivat kytketty turvalogiikalle erikseen. Turvatoiminnolle lisättiin alajärjestelmä ja sille annettiin nimeksi ”Pyrstösulannyppijä Hätäseisvaijeri”. Tämän jälkeen valittiin PL-välilehdeltä: Määritä PL/PFH luokan, $MTTF_D$- ja DC_{avg}-arvojen avulla. Kuvassa 16 näkyvältä luokka välilehdeltä valittiin luokka 4 ja merkittiin luokan vaatimukset täytetyiksi. Hätäpysäytyslaitteet ovat kytketty turvalogiikan testipulssi kanaviin, joten vikoja ei pääse kertymään. Valitsemalla luokaksi 4, tekee ohjelma alajärjestelmästä kaksikanavaisen.



Kuva 16. Alajärjestelmän luokan määritys

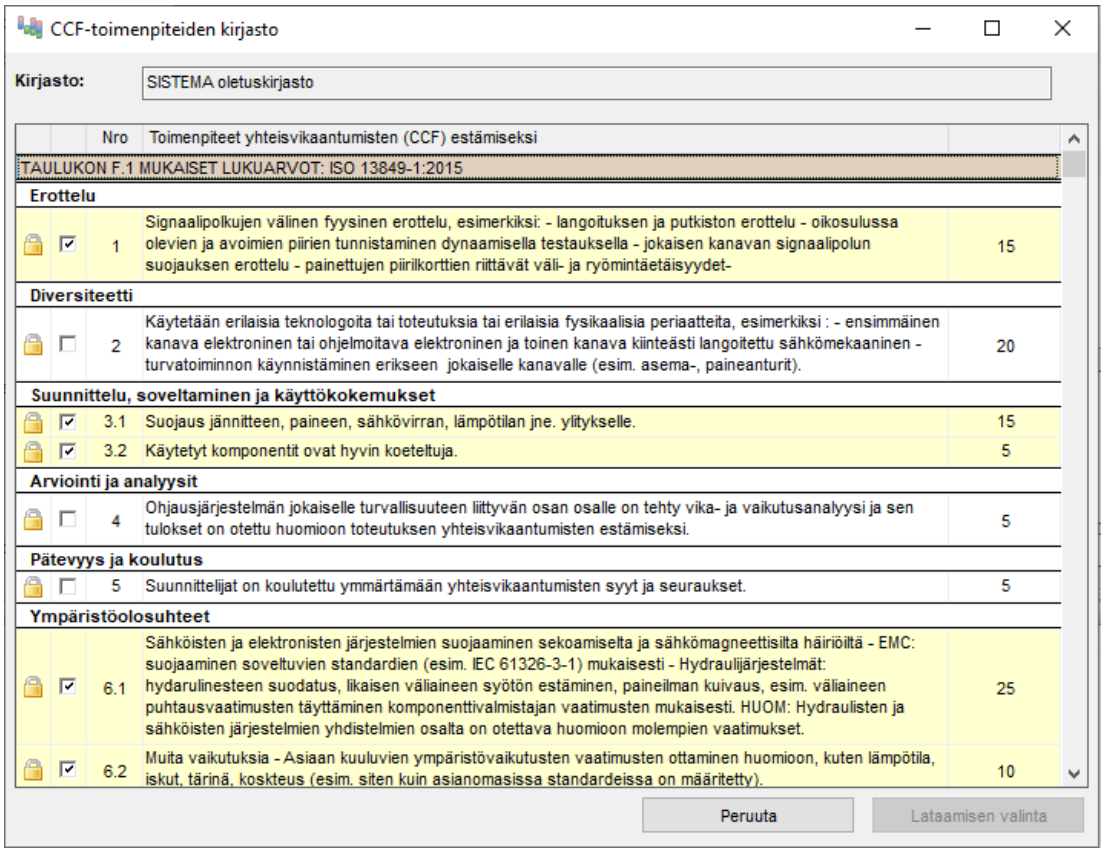
$MTTF_D$ ja DC_{avg} välilehdiltä valittiin arvojen määrittäminen lohkojen avulla. Lohkot välilehdeltä lisättiin kanavaan 1, lohko (BL) joka nimettiin ”Kosketin 1 NC”.

Lohkon $MTTF_D$-välilehdeltä, joka esitetään kuvassa 17, valittiin: Määritä $MTTF_D$-arvo $B10_D$-/B10-arvon avulla. Valmistaja oli ilmoittanut $B10_D$-arvoksi $1{,}5 \times 10^6$, joka syötettiin ohjelmaan, tämän jälkeen piti vielä arvioida toimintakertojen määrä vuodessa. Arvioitiin että koneita käytettäisiin 365 päivää vuodessa, 24 tuntia päivässä ja turvatoiminto suoritettaisiin kerran tunnissa. Määritetyillä arvoilla ohjelma laskee hätäpysäytyslaitteen $MTTF_D$-arvon. Standardissa ISO 13849 määritellään myös, että komponentin toiminta-aika ei saa olla alle 20 vuotta. 20 vuoden aikarajoitus pätee myös $T10_D$-arvoon, kun sitä käytetään. Yli 20 vuoden toiminta-aika ei myöskään anna hyötyä PL:n laskemisessa. Komponentin todellinen käyttöaika ei saisi koskaan ylittää toiminta-aikaa, jolloin tulee huolehtia, että komponentti vaihdetaan ajoissa.

Kuva 17. Hätäpysäytyslaitteen $MTTF_D$-arvon määritys $B10_D$-arvon avulla

Lohkon DC-välilehdeltä löytyy valmis kirjasto, jossa on standardin SFS-EN ISO 13849-1 mukainen luettelo toimenpiteistä diagnostiikan kattavuuden määrittelemiselle. DC-arvo voidaan syöttää myös suoraan, jos se on tiedossa. DC-arvoksi saatiin 99 %, koska hätäpysäytyslaite on kytketty turvalogiikan testipulssi kanavaan, eikä vikoja pääse kertymään. Kun ensimmäisen kanavan lohko oli saatu määriteltyä, voitiin se kopioida kanavaan 2 ja muuttaa lohkon nimeksi ”kosketin 2 NC”, koska molemmat koskettimet ovat samanlaisia.

Lopuksi määriteltiin vielä tehdyt toimenpiteet alajärjestelmän yhteisvikaantumisen (CCF) estämiseksi. CCF-välilehdeltä valittiin kuvassa 18 näkyvästä valmiista kirjastosta sovellettavat toimenpiteet CCF:n arvioimiseksi. Vähimmäisvaatimuksena on 65 pistettä ja kokonaispisteiksi saatiin 70.



Kuva 18. Toimenpiteet yhteisvikaantumisen (CCF) estämiseksi

Kun ensimmäinen hätäpysäytyslaite saatiin määriteltyä, oli muiden lisääminen helppoa. Muut hätäseisvaijerit voitiin lisätä suoraan kopioimalla ja nimeämällä komponentit uudestaan. Hätäseispainikkeiden ja kahvan osalta piti $MTTF_D$-arvot laskea näiden valmistajien antamien $B10_D$-arvojen avulla.

4.3.2 Turvalogiikka ja I/O-moduulit

Turvalogiikan CPU sekä turvatulo- ja lähtömoduulit löytyivät suoraan ABB:n komponenttikirjastosta, joka saatiin ladattua ABB:n verkkosivuilta. Turvalogiikan komponenteille oli valmiiksi määritelty suoritustaso PL, joten komponentit voitiin lisätä ohjelmaan suoraan omina alajärjestelminään.

4.3.3 Releet

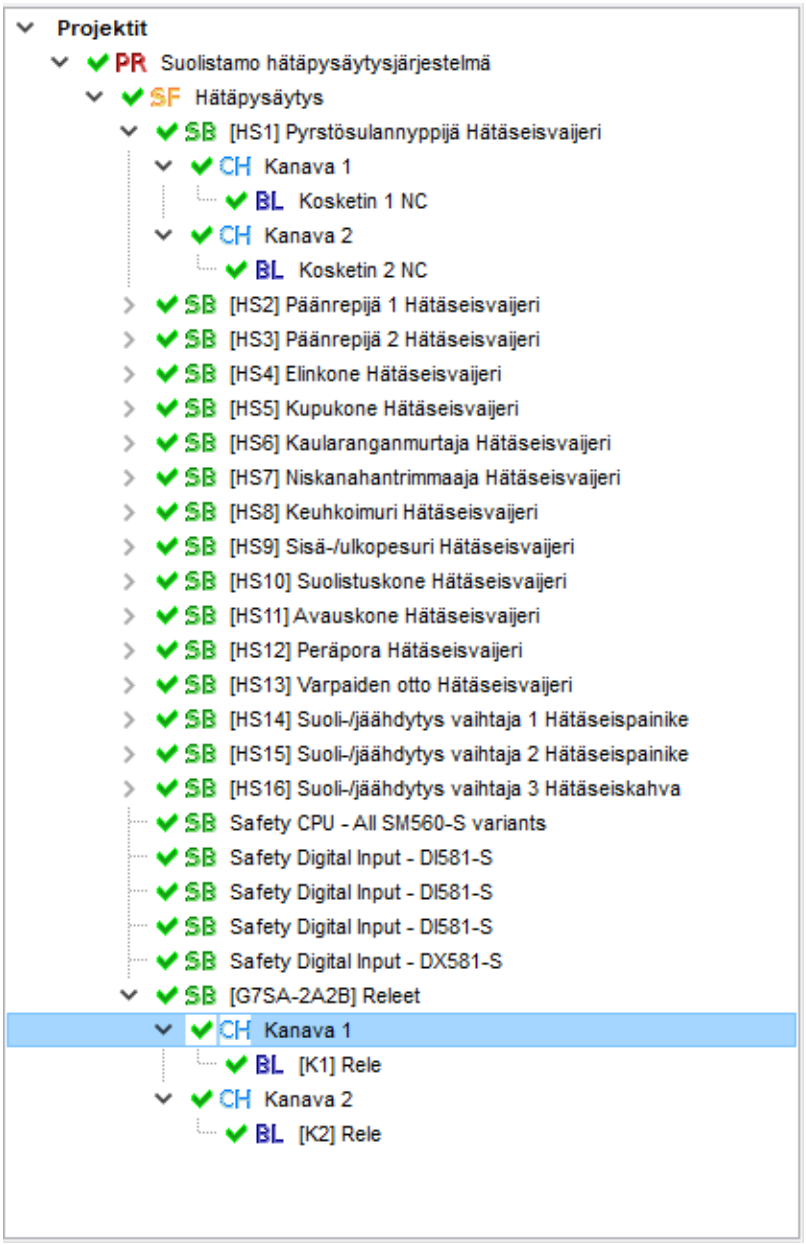
Hätäpysäytysjärjestelmän releet lisättiin ohjelmaan omaksi alajärjestelmäksi. Järjestelmässä käytettyjä Omronin G7SA-tuoteperheen releitä ei ollut valmiina valmistajan

komponenttikirjastoissa, eikä niiden suoritustasoa ollut määritelty. Releet lisättiin ohjelmaan manuaalisesti, samalla tavalla kuin hätäpysäytyslaitteetkin. Luotiin uusi alajärjestelmä, jolle annettiin nimi ”Releet” sekä tunnus ”G7SA-2A2B”. PL-välilehdeltä valitaan: Määritä PL/PFH luokan, $MTTF_D$- ja DC_{avg}-arvojen avulla. Luokka välilehdeltä valitaan luokka 4, ja merkitään luokan vaatimukset täytetyiksi. Releet ovat kahdennettu ja niiden avautuvien koskettimien kautta kulkeva takaisinkytkentä on kytketty turvalogiikan testipulssi kanavaan. Kahdennuksen ansiosta saadaan aikaan yhden vian sieto ja takaisinkytkennällä sekä testipulssi kanavaa käyttämällä viat havaitaan eikä niitä pääse kertymään. $MTTF_D$ ja DC_{avg} välilehdiltä valitaan arvojen määrittäminen lohkojen avulla. Lohkot välilehdeltä lisätään kanavaan 1, lohko (BL) jolle annettiin nimeksi ”Rele” ja tunnukseksi ”K1”.

Lohkon $MTTF_D$-välilehdeltä valittiin: Määritä $MTTF_D$-arvo $B10_D$-/B10-arvon avulla. Valmistaja oli ilmoittanut $B10_D$-arvoksi $10x10^6$, joka syötettiin ohjelmaan, tämän jälkeen piti vielä arvioida toimintakertojen määrä vuodessa. Arvioitiin että koneita käytettäisiin 365 päivää vuodessa, 24 tuntia päivässä ja turvatoiminto suoritettaisiin kerran tunnissa. Määritetyillä arvoilla ohjelma laskee releen K1 $MTTF_D$-arvon.

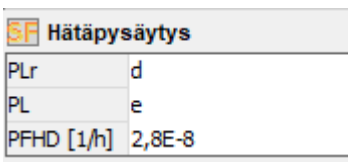
DC-arvoksi saadaan 99 %, koska releen avautuvalla koskettimella saadaan takaisinkytkentätieto turvalogiikalle, sekä takaisinkytkentä on kytketty turvalogiikan testipulssi kanavaan. Näin viat havaitaan, eikä niitä pääse kertymään. Kun ensimmäisen kanavan lohko on saatu määriteltyä, voidaan se kopioida kanavaan 2 ja muuttaa lohkon tunnukseksi ”K2”, koska molemmat releet ovat samanlaisia

Lopuksi määriteltiin vielä tehdyt toimenpiteet alajärjestelmän yhteisvikaantumisen (CCF) estämiseksi. CCF-välilehdeltä valittiin valmiista kirjastosta sovellettavat toimenpiteet CCF:n arvioimiseksi. Vähimmäisvaatimuksena on 65 pistettä ja kokonaispisteiksi saatiin 70.



Kuva 19. Sistema projektipuu

Lopputuloksena hätäpysäytysjärjestelmän suoritustasoksi saatiin PL e, joka on riittävä. Kuvassa 19 kuvakaappaus ohjelmistosta, jossa näkyy vaadittu suoritustaso PL_r d sekä saavutettu suoritustaso PL e. Lisäksi liitteenä 1 on Sistemasta saatu raportti turvatoiminnon vaatimusten täyttymisestä.



SF Hätäpysäytys	
PLr	d
PL	e
PFHD [1/h]	2,8E-8

Kuva 20. Vaadittu ja saavutettu suoritustaso

5 HÄTÄPYSÄYTYSJÄRJESTELMÄN TOTEUTUS

5.1 Turvalogiikkakeskuksen toteutus

Alustavien sähköpiirustusten sekä komponentti valintojen valmistuttua aloitettiin keskuksen rakentaminen. Keskuskaapiksi valittiin Rittalin 800x1000 kompakti kytkentäkaappi AX. Kyseinen kaappi valittiin, koska haluttiin että keskukseen jäisi vielä runsaasti tilaa mahdollisia tulevaisuuden muutoksia varten, sekä sellainen löytyi valmiiksi hyllystä.

Keskuskaapin valinnan jälkeen otettiin pohjalevy irti kaapista, jolloin sen kalustaminen ja johdotusten tekeminen olisi vaivattomampaa. Pohjalevy asetettiin asennuslineeseen ja siihen kiinnitettiin tarvittavat johdotuskourut sekä DIN-kiskot, jonka jälkeen aloitettiin keskuksen kalustaminen. DIN-kiskoille kiinnitettiin turvalogiikka I/O-moduuleineen, releet, 24V teholähde, termostaatti kotelon jäähdytykselle, pistorasia sekä tarvittavat sulakkeet, vikavirtasuoja ja riviliittimet. Keskuksen kalustamisen jälkeen merkittiin keskuksen komponentit sekä riviliittimet. Logiikan turvatulo ja -lähtö sekä tavalliselle digitaalitulo- ja lähtömoduulille tehtiin omat riviliitin positiot. Riviliittimet pyrittiin asentamaan mahdollisimman lähelle kotelon pohjaa, jolloin keskukselle tulevien ja sieltä lähtevien kaapeleiden kytkentä olisi mahdollisimman vaivatonta.

Komponenttien ja riviliitinten merkitsemisen jälkeen aloitettiin keskuksen johdotus. Keskuksen sisäiset 230 VAC kytkennät toteutettiin mustalla 1,5 mm^2 monisäikeisellä johtimella, 24 VDC kytkennät tummansinisellä 0,75 mm^2 monisäikeisellä johtimella sekä 0 VDC kytkennät sinivalkoisella 0,75 mm^2 monisäikeisellä johtimella. Johdotuksen jälkeen asennettiin pohjalevy takaisin keskuskaappiin. Lopuksi keskuskaapin läpivientilaipat otettiin irti ja niihin tehtiin tarvittavat läpiviennit. Läpivientejä tehtiin hieman enemmän kuin oli tarpeen, jotta niitä olisi varalle mahdollisia tulevaisuuden muutoksia varten. Keskuksen valmistuttua, asennettiin se paikalleen tehtaan välikatolle, jossa se on suojassa kosteudelta.

Kuva 21. Keskus paikalleen asennettuna

5.2 Hätäpysäytyslaitteiden asennus ja kaapelointi

Keskuksen rakennuksen aikana aloitettiin hätäpysäytyslaitteiden asennus. Laitteisiin tuli yhteensä 16 hätäpysäytyslaitetta, joista kolmetoista oli vaijereita, kaksi painiketta ja yksi kahva. Hätäpysäytyslaitteiden ja vaijereihin tarvittavien väkipyörien kiinnityksen hoiti yrityksen mekaaniset asentajat, annetun ohjeistuksen mukaisesti. Lisäksi asennettiin paikoilleen käyttöliittymän paneeli koteloineen, muiden suolistamon käyttöpaneeleiden yhteyteen.

Kuva 22. Hätäseisvaijeri

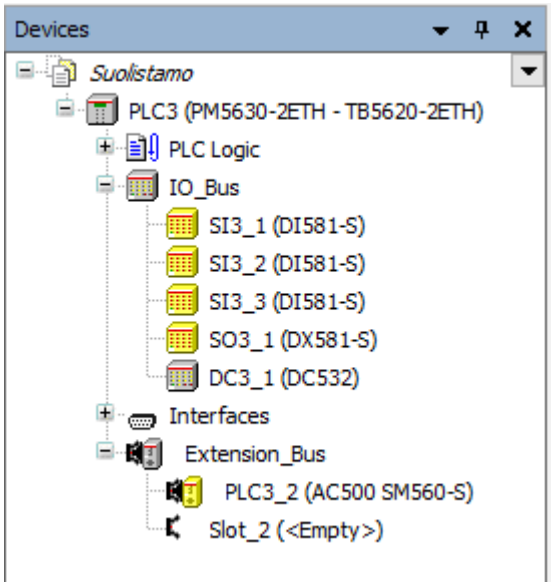
Hätäpysäytyslaitteiden ja keskuksen paikalleen asentamisen jälkeen aloitettiin kaapelointi. Keskuksen 230 V syöttö otettiin lähimmästä jakokeskuksesta missä oli vapaa 16 A vikavirtalähtö. Jokaiselle hätäpysäytyslaitteelle lähti keskukselta oma kaapelinsa, sekä paneelille tarvittava syöttökaapeli ja sen yhteyteen asennetulle kuittauspainikkeelle omansa. Lisäksi kytkettiin paneelin ja PLC:n välinen Ethernet kaapeli.

6 OHJELMOINTI JA KÄYTTÖLIITTYMÄN TOTEUTUS

Laitteiston valmistuttua oli vuorossa turvalogiikan ohjelmointi ja käyttöliittymän toteutus. Turvalogiikan ohjelmointi tehtiin ABB:n Automation Builder ohjelmistolla, versiolla 2.5. Automation Builder on ABB:n ohjelmointi, simulointi, käyttöönotto ja kunnossapidon ohjelmaympäristö ohjelmoitaville logiikoille, liikkeenohjaukselle, Ohjauspaneeleille sekä SCADA:lle (ABB, n.d.-a, s. 5). Ohjelmisto on saatavana ilmaisena Basic versiona sekä maksullisina Standard ja Premium versioina. Turvalogiikan ohjelmointi vaatii joko Standard tai Premium version sekä erillisen lisenssin. Turvalogiikan ohjelmointiin voidaan käyttää kolmea ohjelmointikieltä: LD (Ladder Diagram), FBD (Function Block Diagram) ja ST (Structured Text). (ABB, n.d.-b.)

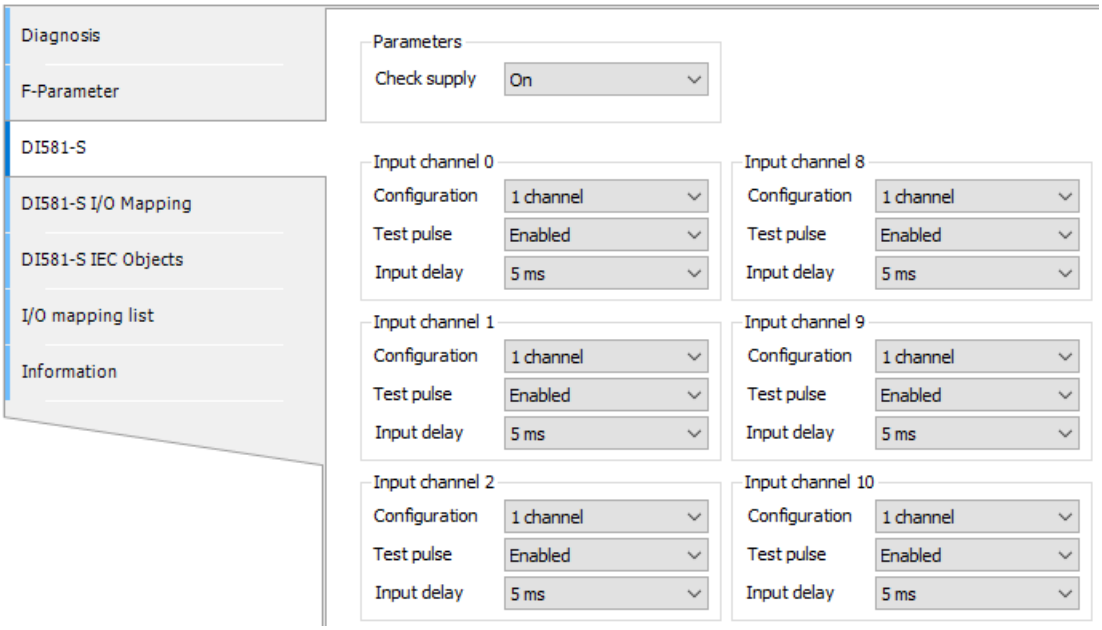
6.1 Turvalogiikan ohjelma

Ohjelmointi aloitettiin luomalla laitekonfiguraatio. Ohjelmaan luotiin uusi projekti, jonka yhteydessä ohjelmaan lisättiin järjestelmän tavallinen CPU. Seuraavaksi lisättiin logiikan laajennusväylään turva-CPU sekä I/O-väylään käytössä olevat turvatulo- ja lähtömoduulit sekä tavallinen digitaalitulo ja -lähtömoduuli. Laitteet tuotiin ohjelmaan kuvassa 23 esitetyllä tavalla, siihen järjestykseen missä ne fyysisestikin olivat. Laitteiden lisäämisen jälkeen asetettiin laitteille oikeat IP-osoitteet sekä muut asetukset CPU:n ja turva-CPU:n kommunikointia varten.



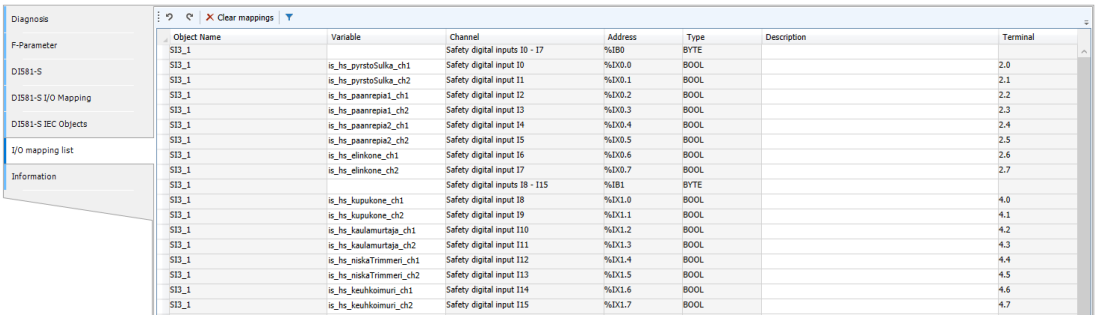
Kuva 23. Projektipuu laitekonfiguraation jälkeen

Laitekonfiguraation jälkeen tehtiin laitteistolle I/O-konfiguraatio. I/O-moduulien kanavat ovat tehdasasetuksiltaan pois käytöstä, jolloin niiden asetukset tuli vaihtaa laitteistolle sopiviksi. Tulokanavat asetettiin 1-kanavaisiksi, koska kaksikanavaisten hätäpysäytyslaitteiden signaalien valvonta suoritetaan ohjelmallisesti turva-CPU:ssa. Hätäpysäytyslaitteet saivat syöttönsä turvatulomoduulien test pulse-lähdöistä, jolloin myös ne otettiin käyttöön. Kuvassa 24 esitetään I/O-konfiguraatio yhden turvatulomoduulin osalta.



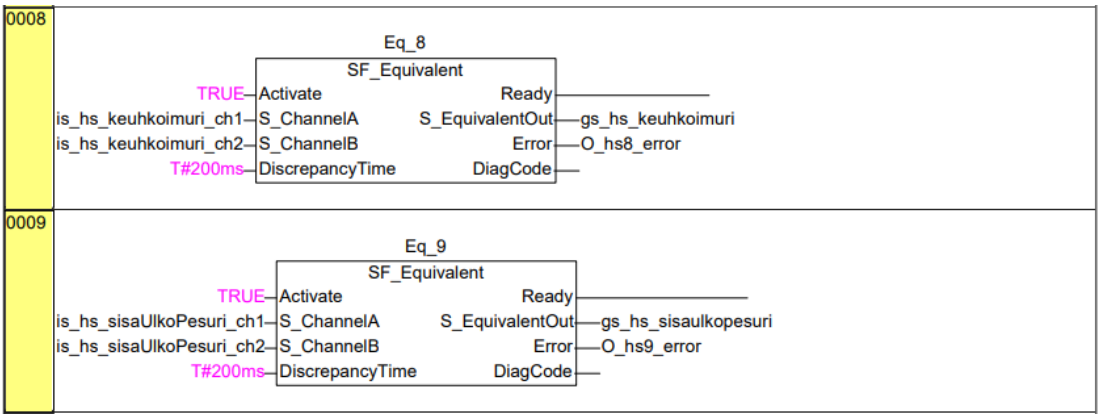
Kuva 24. Turvatulomoduulin I/O-konfiguraatio

I/O-konfiguraation jälkeen tehtiin turvatuloihin ja –lähtöihin tarvittavat muuttujat. Turvatulo- ja lähtömoduuleihin luotiin muuttujat hätäpysäytyslaitteille, releille sekä releiden takaisinkytkennälle. Turvatulomoduuleille luotiin lisäksi muuttujat kanavien kuittauspyynnölle sekä kuittaukselle. Kuvassa 25 esitetään hätäpysäytyslaitteiden muuttujat yhden turvatulomoduulin osalta.



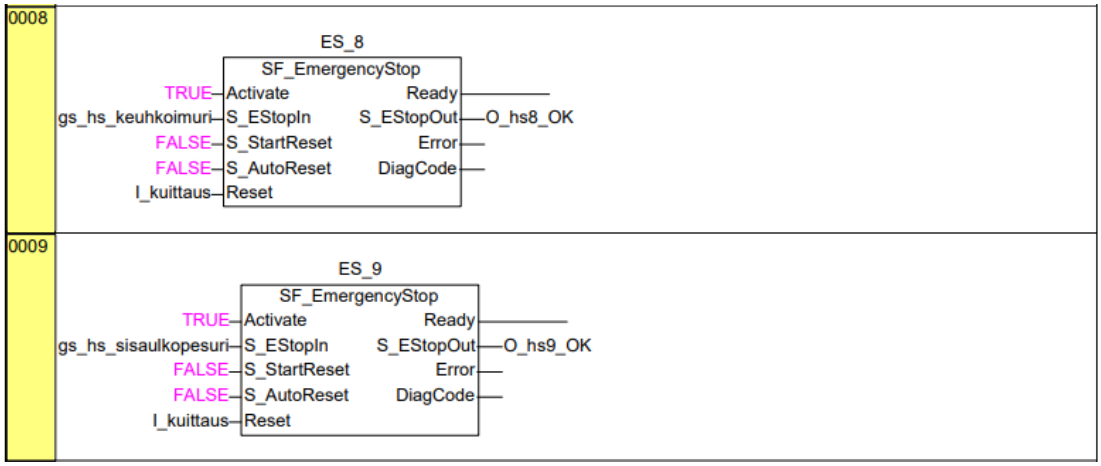
Kuva 25. Turvatulomoduulin muuttujat

Laite- ja IO-konfiguraatioiden jälkeen aloitettiin itse ohjelman luominen. Aluksi luotiin aliohjelma, jolla valvotaan hätäpysäytyslaitteilta saatavien signaalien tiloja. Jokaiselle hätäpysäytyslaitteelle tuotiin oma, kuvassa 26 esitetty SF_Equivalent funktioblokki, jolla kaksikanavaisen hätäpysäytyslaitteen signaaleista saadaan tuotettua yksi hätäpysäytyslaitteen tilaa esittävä signaali. Funktioblokin tuloihin tuotiin hätäpysäytyslaitteen molempien kanavien signaalit, sekä määritettiin diskrepanssi aika, jonka aikana molempien tulokanavien signaalien pitää muuttua. Funktioblokin lähtö S_EquivalentOut menee ja pysyy päällä niin kauan, kun molempiin tulokanaviin tulee signaali ja lähtö Error ei ole päällä. Lähtö Error menee päälle, jos tulokanavien signaalit ovat eriarvoiset asetetun diskrepanssi ajan jälkeen ja pysyy päällä niin kauan, kunnes molempien tulokanavien signaalit ovat katkenneet ja menneet takaisin päälle asetetun diskrepanssi ajan sisällä.



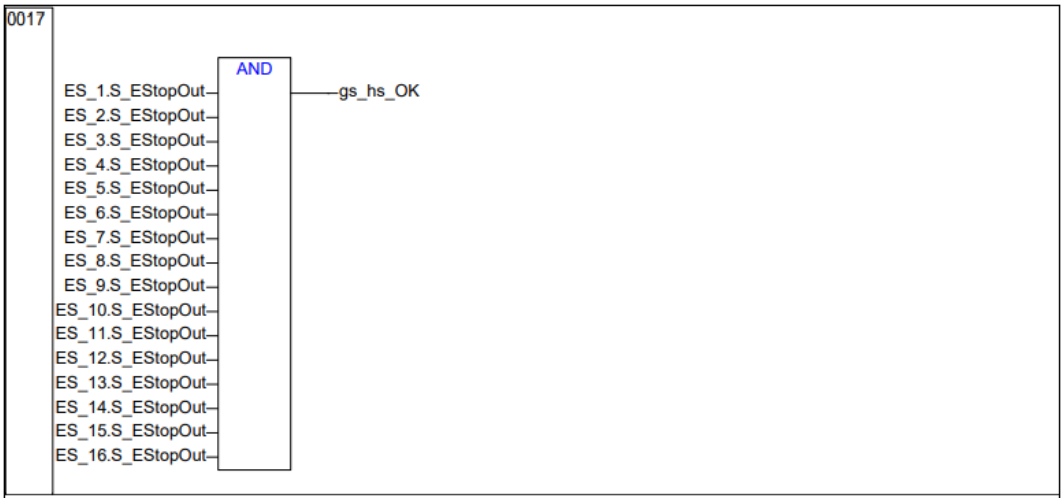
Kuva 26. Hätäpysäytyslaitteiden signaalien valvonta

Seuraavaksi luotiin aliohjelma, joka käsittelee hätäpysäytyslaitteiden tiloja sekä varmistaa uudelleenkäynnistyksen eston. Edellisen aliohjelman tapaan tuotiin jokaiselle hätäpysäytyslaitteelle oma, kuvassa 27 esitetty SF_EmergencyStop funktioblokki. Funktioblokin tulokanavaan S_EStopIn tuodaan edellisestä aliohjelmasta saatu hätäpysäytyslaitteen tilatieto. Tulokanavat S_StartReset sekä S_AutoReset asetetaan arvoon FALSE, jolloin lähdön S_EStopOut päälle asettuminen vaatii manuaalisen kuittauksen kuittauspainikkeella. Signaalin katkeaminen tulokanavasta S_EStopIn hätäpysäytyslaitteeseen vaikuttamisesta, mahdollisesta viasta tai sähkökatkosta johtuen asettaa lähdön S_EstopOut pois päältä. Lähtö pysyy pois päältä niin kauan, kunnes tuloon S_EStopIn tulee signaali sekä tulo Reset tunnistaa kuittauspainikkeen nousevan reunan. Nousevan reunan tunnistuksella estetään laitteen automaattinen käynnistyminen, kun hätäpysäytyslaitteen signaali palautuu ja kuittauspainikkeen signaali on valmiiksi aktiivinen esimerkiksi koskettimen kiinni hitsaantumisen tai painikkeen jumiutumisen myötä.



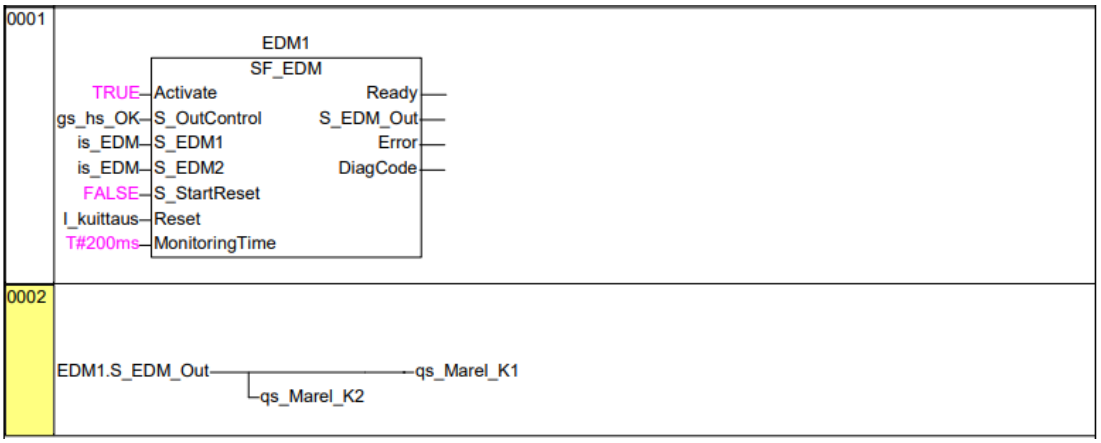
Kuva 27. Hätäpysäytyslaitteiden tilat ja uudelleenkäynnistyksen esto

Aliohjelmaan lisättiin vielä kuvassa 28 näkyvä AND-portti, jonka tuloihin lisättiin kaikkien SF_EmergencyStop funktioblokeilta saadut hätäpysäytyslaitteiden tilatiedot. AND-portilla saadaan koottua yhteen kaikkien hätäpysäytyslaitteiden tilat ja koostettua niistä yksi kaikki hätäpysäytyslaitteet kattava tilatieto.



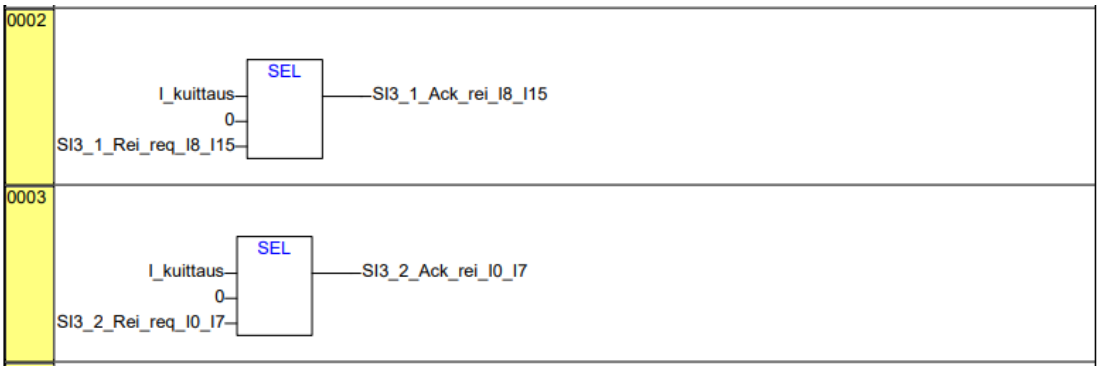
Kuva 28. Kaikkien hätäpysäytyslaitteiden tila

Seuraavaksi luotiin aliohjelma järjestelmän releiden ohjaukselle ja valvonnalle. Ohjelmaan lisättiin kuvassa 29 esitetty SF_EDM funktioblokki. Funktioblokin tuloon S_OutControl tuodaan edellisessä aliohjelmassa AND-portilla koostettu kaikkien hätäpysäyttimien tilatieto. Tuloihin S_EDM1 sekä S_EDM2 tuodaan releiltä saatava takaisinkytkentä, joka saadaan kummankin releen avautuvien koskettimien sarjaan kytkennästä. Tulo S_StartReset asetetaan arvoon FALSE, jolloin releiden kytkeytyminen päälle vaatii manuaalisen kuittauksen kuittauspainikkeelta käynnistyksen jälkeen. Tuloon MonitoringTime asetettiin aika, jonka aikana tulokanavien S_EDM1 ja S_EDM2 signaalien pitää muuttua lähdön S_EDM_Out muuttuessa. Lähdöllä S_EDM_out ohjataan järjestelmän kahta relettä. Releet kytkeytyvät päälle, kun tulo S_OutControl saa signaalin, tuloihin S_EDM1 ja S_EDM2 tulee signaali, käynnistyksen esto ei ole päällä eikä virhettä ole havaittu. Releiden kytkeytyessä päälle pitää releiden avautuvien koskettimien vaihtaa tilaansa, jolloin tulojen S_EDM1 sekä S_EDM2 signaalit katkeavat, jos signaalit eivät katkea funktioblokki havaitsee virheen ja lähtö S_EDM_Out kytkeytyy pois päältä. Tällä tavalla pystytään havaitsemaan esimerkiksi koskettimien kiinni hitsaantuminen.



Kuva 29. Releiden ohjaus ja valvonta

Seuraavaksi luotiin aliohjelma turvamoduulien kuittaukselle mahdollisen häiriön tai vikatilan jälkeen. Ohjelmassa käytettiin kuvassa 30 näkyvää SEL-funktiota, joka kirjoittaa funktion lähtöön joko arvon 0 tai 1, Rei_req bitin arvosta riippuen. Kun järjestelmä käynnistetään eikä kuittauspainiketta ole painettu lähtöön kirjoitetaan arvo 0, jolloin turvamoduulit ovat vikatilassa. Kuittauspainikkeen vaikuttumisen jälkeen kirjoitetaan lähtöön arvo 1, jolloin turvamoduulien vikatila kuittaantuu. Turvatuloissa havaitun virheen seurauksena menevät vikatilassa olevien tulojen Rei_req bitit arvoon 0 jolloin kuittaus ei onnistu. Rei_req bitit saavat arvon 1 vikatilanteen korjaantuessa.



Kuva 30. Turvamoduulien kuittaus

Lopuksi pitää kaikkia aliohjelmia vielä kutsua pääohjelmassa. Pääohjelman alkuun lisättiin kuvassa 31 esitetty watchdogin asetukset: SF_WDOG_TIME_SET, jossa määritettiin maksimi aika yhdelle ohjelmasyklille. Ajaksi määritettiin 200ms. Maksimi aika tuli määrittää, koska sitä ei ole määritetty turva-CPU:n oletusasetuksissa. Ilman ajan määrittämistä watchdogin ajaksi oletetaan 0 ms, jolloin CPU menee vikatilaan.

```
0001 PROGRAM PLC_PRG
0002 VAR
0003     SF_WDOG_TIME_SET: SF_WDOG_TIME_SET;
0004     watchDog_done : BOOL;
0005     watchDog_actTime : DWORD;
0006     watchDog_maxTime : DWORD;
0007 END_VAR
```

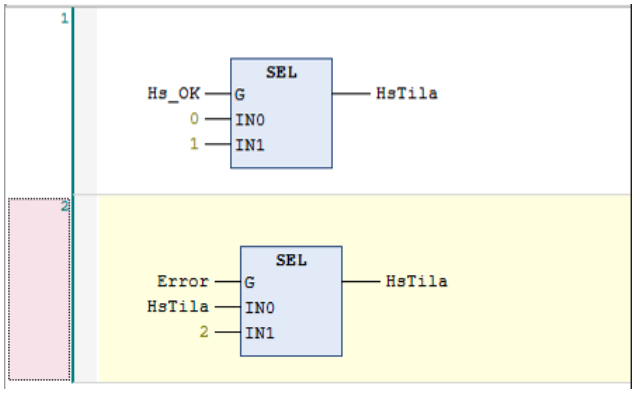
```
0001 SF_WDOG_TIME_SET(
0002     EN:= TRUE,
0003     WDOG:= 200,
0004     RESET:= FALSE,
0005     DONE=> watchDog_done,
0006     ACT_TIME=> watchDog_actTime,
0007     MAX_TIME=> watchDog_maxTime);
0008
0009
0010
0011 PRG_Ack_rei();
0012 PRG_Equivalent();
0013 PRG_Hs();
0014 PRG_Output();
```

Kuva 31. Pääohjelma ja watchdog

6.2 Käyttöliittymän ohjelma

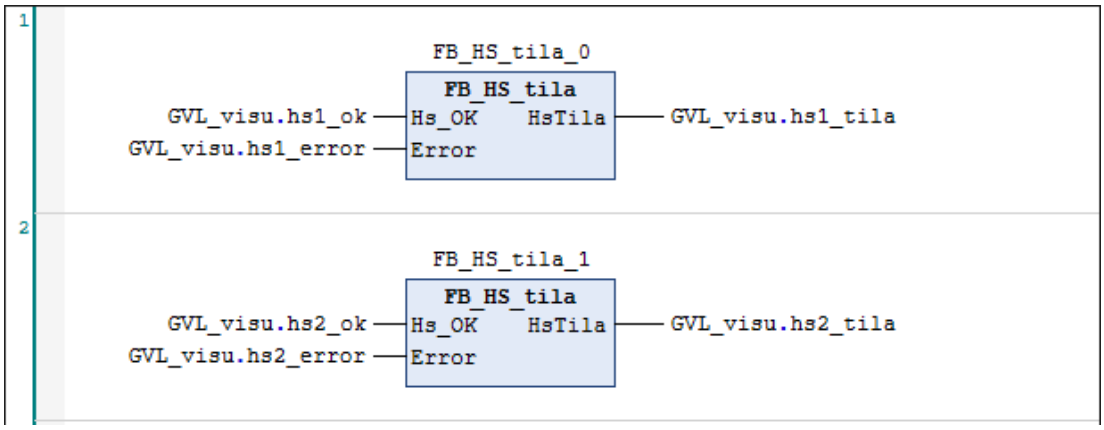
Turvapuolen ohjelman valmistuttua luotiin vielä tavallisen logiikan puolelle tarvittavat ohjelmat käyttöliittymää sekä kuittauspainiketta ja sen merkkivaloa varten. Aluksi ohjelmaan luotiin globaalit muuttujat kuittauspainikkeille ja muuttujalle, jolla kuittauspainikkeiden tiedot viedään tavallisen logiikan puolelta turvalogiikalle sekä muuttujat hätäpysäytyslaitteiden tilojen esittämistä varten käyttöliittymässä.

Hätäpysäytyslaitteiden tilojen esittämiselle käyttöliittymässä luotiin oma funktioblokki. Funktioblokissa käytettiin SEL-funktioita, jonka lähtöön kirjoitetaan arvo 0, 1 tai 2 tulosignaalin tilasta riippuen, kuvassa 32 esitetyllä tavalla. Kun hätäpysäytyslaite ei ole vaikuttuneena kirjoitetaan lähtöön arvo 0, laitteen ollessa vaikuttuneena kirjoitetaan lähtöön arvo 1 ja laitteen ollessa vikatilassa kirjoitetaan lähtöön arvo 2.



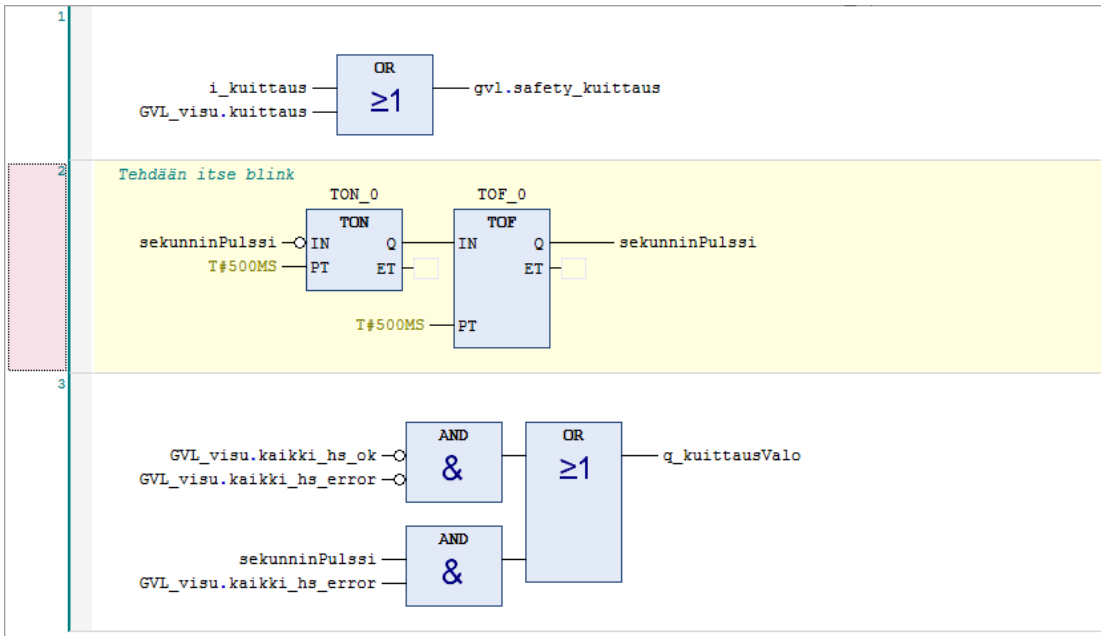
Kuva 32. Hätäpysäytyslaitteiden tilat funktioblokki

Seuraavaksi luotiin aliohjelma, jossa käytettiin kuvassa 33 näkyvää aikaisemmin luotua funktioblokkia hätäpysäytyslaitteiden tilojen esittämiselle käyttöliittymässä. Jokaiselle hätäpysäytyslaitteelle tuotiin oma funktioblokki, jonka tuloihin tuotiin hätäpysäytyslaitteiden tilatiedot. Tulosignaalien tiloista riippuen kirjoitetaan lähtömuuttujan arvoksi joko 0, 1 tai 2, jolla hätäpysäytyslaitteen tilatieto viedään käyttöliittymälle. Aliohjelman loppuun lisättiin vielä OR-portit, joilla luotiin tilatiedot kaikkien hätäpysäytyslaitteiden tiloista.



Kuva 33. Hätäpysäytyslaitteiden tilat ohjelma

Kuittauspainikkeille sekä fyysisen kuittauspainikkeen merkkivalolle luotiin oma, kuvassa 34 esitetty aliohjelma. Kuittauspainikkeille käytettiin OR-porttia, jolla fyysisen ja käyttöliittymässä olevan kuittauspainikkeen signaalit viedään OR-portin lähdössä olevalla muuttujalla turvalogiikalle. Kuittauspainikkeen merkkivalolle tehtiin ohjelma, jossa merkkivalo palaa, kun jokin hätäpysäytyslaite on tai on ollut vaikuttuneena mutta mikään hätäpysäytyslaite ei ole vikatilassa. Hätäpysäytyslaitteen ollessa vikatilassa merkkivalo vilkkuu. Merkkivalon vilkkumista varten ohjelmaan tehtiin pulssisignaali, käyttämällä veto- ja päästöhidasteisia funktioblokkeja.



Kuva 34. Kuittauspainikkeet ja merkkivalo

Lopuksi lisättiin vielä kaikkien aliohjelmien ohjelmakutsut pääohjelmaan.

POU: PLC_PRG

```
1       PROGRAM PLC_PRG
2       VAR
3       END_VAR
4
```

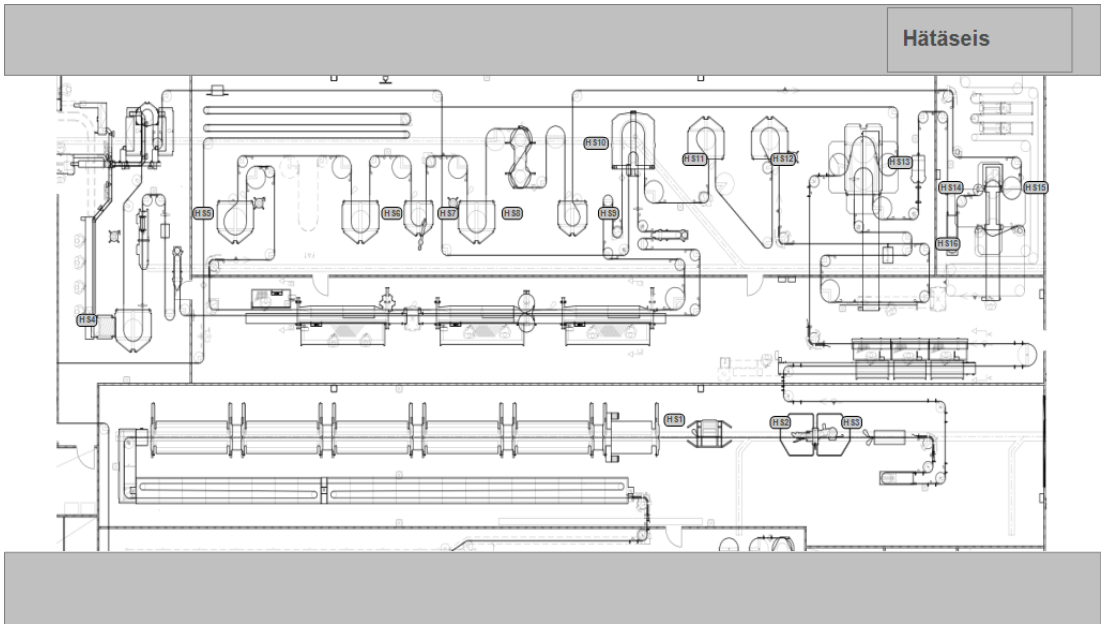
```
1       PRG_IO_ohjaukset ( ) ;
2       PRG_Visu ( ) ;
3
```

Kuva 35. Pääohjelma

6.3 käyttöliittymän toteutus

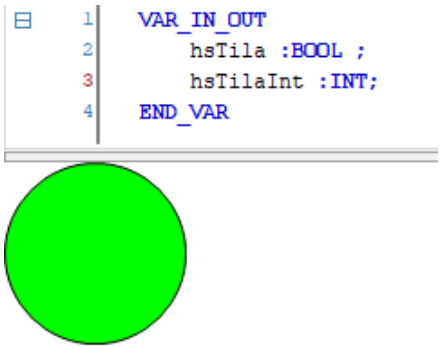
Käyttöliittymä toteutettiin ABB:n Automation Builder ohjelmistossa olevalla visualization ominaisuudella. Ensimmäiseksi käyttöliittymälle tarvittiin pohjakuva, jossa näkyisi kaikki suolistamon laitteet. Suolistamosta löytyikin jo valmis layout-kuva, jota voitaisiin käyttää käyttöliittymän pohjakuvana. Layout-kuvaa ei kuitenkaan pystytty suoraan käyttämään käyttöliittymän pohjana, koska kuvassa näkyi suurempi osa tehtaasta sekä kuvassa oli paljon erilaisia mittoja ja merkintöjä suolistamon rakenteille ja laitteille. Kuva rajattiin kattamaan vain suolistamon alue ja kuvasta poistettiin muut käyttöliittymän kannalta epäoleelliset merkinnät.

Kun pohjakuva saatiin muokattua sopivaksi, lisättiin se ohjelman ImagePool:iin. Seuraavaksi ohjelmaan lisättiin uusi visualization, johon kuva tuotiin ja skaalattiin vastaamaan käyttöpaneelin resoluutiota. Pohjakuvaan haluttiin lisätä vielä ylä- ja alapalkit, jotta saataisiin selkeä paikka käyttöliittymään tulevalle kuittauspainikkeelle sekä kaikkien hätäpysäytyslaitteiden tilaa kuvaavalle elementille. Luotiin uusi visualization johon pohjakuvan visualization tuotiin Frame-elementillä. Pohjakuvaan lisättiin myös positionumerot jokaiselle hätäpysäytys laitteelle.



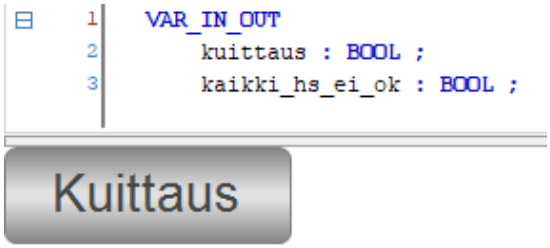
Kuva 36. Käyttöliittymän pohjakuva

Pohjakuvan valmistuttua luotiin visualization, jolla saatiin kuvattua hätäpysäytyslaitteiden tiloja. Käytettäväksi elementiksi valittiin kuvassa 37 esitetty ympyrä, jonka väri ja sisällä oleva teksti vaihtuu hätäpysäytyslaitteen tilan mukaan. Elementti luotiin omaan visualizationiinsa, jotta samaa elementtiä voitaisiin käyttää kaikille hätäpysäytyslaitteille. Elementille luotiin paikalliset muuttujat, joita käytetään elementin värin ja sisällä olevan tekstin vaihtamiseen. Muuttujalla ”hsTila” vaihdetaan elementin väri, joka on vihreä, kun hätäpysäytyslaite ei ole vaikuttuneena tai punainen kun hätäpysäytyslaite on vaikuttuneena tai vikatilassa. Elementin sisällä olevan tekstin muuttamista varten luotiin tekstilista, jonka avulla ohjelmassa saadut hätäpysäytyslaitteen tilatiedot 0, 1 ja 2 saatiin muutettua käyttöliittymällä muotoon OK, 0 ja ERR. Muuttujalla ”hsTilaInt” vaihdetaan elementin sisällä oleva teksti, joka on ”OK”, jos hätäpysäytyslaite ei ole vaikuttuneena, ”0” jos hätäpysäytyslaite on vaikuttuneena tai ”ERR” jos hätäpysäytyslaite on vikatilassa.



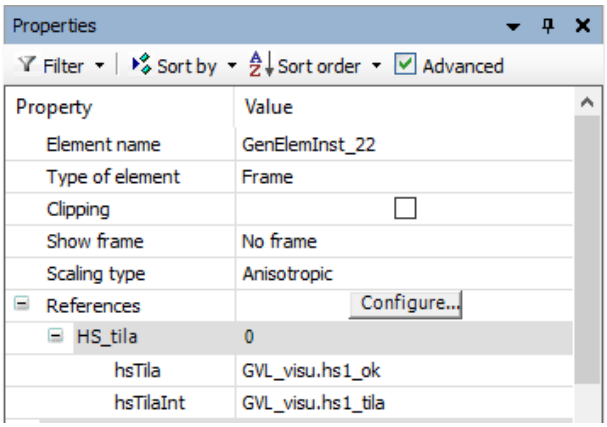
Kuva 37. Hätäpysäytyslaitteen tila visualization

Käyttöliittymässä olevalle kuittauspainikkeelle luotiin myös oma visualization. Elementtinä käytettiin kuvassa 38 näkyvää painiketta, jonka sisällä on teksti ”Kuittaus” ja jonka väri vaihtuu hätäpysäytyslaitteiden tilojen mukaan. Elementin paikallisella muuttujalla ”kuittaus” viedään tieto kuittauspainikkeen tilasta ohjelmaan ja muuttujalla ”kaikki_hs_ei_ok” vaihdetaan elementin väri siniseksi, kun jokin hätäpysäytyslaite on vaikuttunut tai mennyt vikatilaan. Normaalitilassa kuittauspainikkeen väri on harmaa.



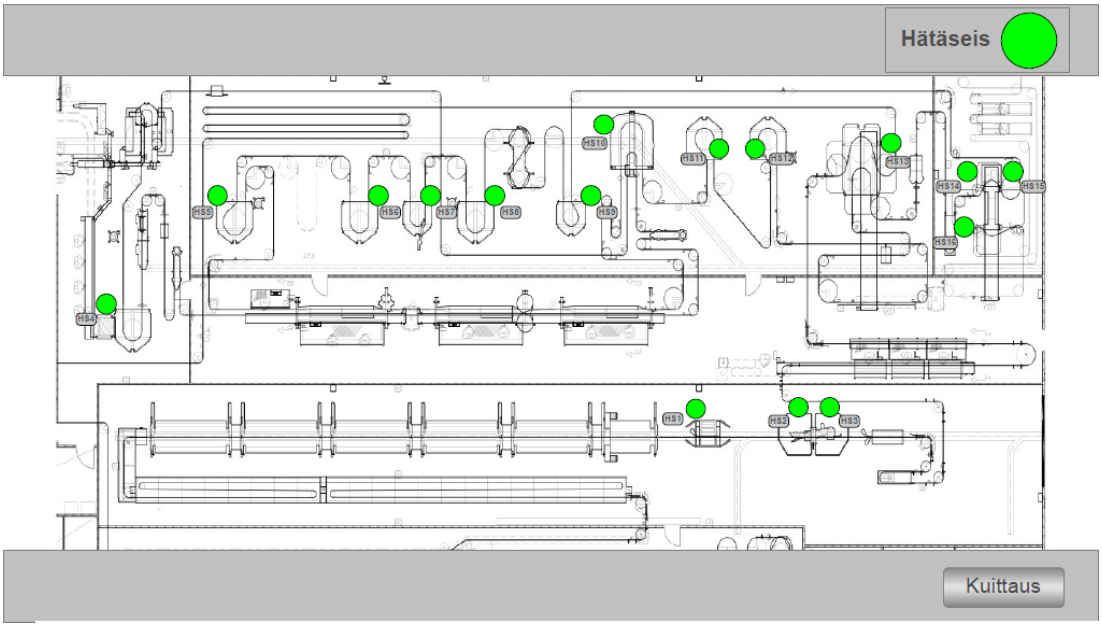
Kuva 38. Kuittauspainike visualization

Lopuksi luotiin visualization, jonka pohjalle tuotiin Frame-elementeillä aikaisemmin tehty pohjakuva, kuittauspainike sekä hätäpysäytyslaitteiden tiloja kuvaava ympyrä jokaiselle hätäpysäytyslaitteelle. Hätäpysäytyslaitteiden tiloja kuvaavat ympyrät aseteltiin pohjakuvaan niille paikoilleen, joissa ne fyysisestikin olivat. Elementit linkitettiin ohjelmassa luotuihin muuttujiin kuvassa 39 esitetyllä tavalla, jolloin ne saadaan muuttumaan hätäpysäytyslaitteiden tilojen mukaan.



Kuva 39. Hätäpysäytyslaitteen tila elementin muuttujat

Käyttöliittymän valmistumisen jälkeen, piti se vielä saada toimimaan käyttöpaneelissa. Projektipuuhun lisättiin WebVisu, johon asetettiin käyttöpaneelissa näkyvä visualization sekä paneelin resoluutio. Seuraavaksi yksi PLC:n Ethernet-portti konfiguroitiin verkkopalvelimeksi. Nyt käyttöliittymää pystyttiin käyttämään verkkoselaimella hakemalla Ethernet-portin IP-osoitetta ja lisäämällä loppuun ”/webvisu.htm”. Käyttöpaneelille asennettiin Chromium verkkoselain. Käyttöliittymän osoite määritetiin Chromiumin asetuksista kotisivuksi, jolloin se lataantuisi käyttöpaneelille aina käynnistyksen yhteydessä.



Kuva 40. Valmis käyttöliittymä

7 KÄYTTÖÖNOTTO JA DOKUMENTOINTI

7.1 Toiminnan testaus ja käyttöönotto

Ennen hätäpysäytysjärjestelmän käyttöönottoa tarkistettiin kytkennät, laitteiden oikeanlainen toiminta sekä käyttöliittymällä näkyvien tilatietojen paikkansa pitävyys. Kytkentöjen tarkistuksessa varmistettiin, että ne vastaavat alustavia sähköpiirustuksia ja muutokset merkattiin ylös.

Hätäpysäytyslaitteiden toiminta tarkistettiin laukaisemalla jokainen hätäpysäytyslaite yksittäin, jonka jälkeen tarkistettiin, että oikeat turvatulomoduulin tulokanavat menevät pois päältä, järjestelmän releet eivät vedä, hätäpysäytyslaitetta ei saada kuitattua ja käyttöliittymällä näkyvä tilatieto on oikea. Seuraavaksi hätäpysäytyslaite palautettiin normaalin toimintatilaan ja tarkistettiin että järjestelmän releet eivät vieläkään vedä ja käyttöliittymällä näkyvä tilatieto pysyy samana. Tämän jälkeen painettiin kuittauspainiketta ja tarkistettiin että hätäpysäytyslaite kuittaantuu, releet kytkeytyvät päälle ja tilatieto käyttöliittymällä muuttuu oikeaksi. Lopuksi luotiin vielä tilanteita, joilla varmistettiin järjestelmän oikeanlainen toiminta mahdollisissa vikatilanteissa. Hätäpysäytyslaitteiden toisen kanavan tulosignaali katkaistiin, jonka jälkeen tarkistettiin samat asiat kuin aikaisemmin, sillä muutoksella että kuittaus ei saanut onnistua ennen kuin molemmat hätäpysäytyslaitteen tulosignaalit katkeaisivat ja menisivät takaisin päälle ohjelmassa asetetun diskrepanssi-ajan sisällä.

Kun järjestelmä oli todettu toimintakuntoiseksi, se liitetiin osaksi suolistamon ohjausjärjestelmää ja koeajettiin. Koeajon aikana varmistettiin, että hätäpysäytyslaitteet eivät laukea esimerkiksi tärinän vaikutuksesta ja että suolistamon koneet pysähtyvät välittömästi, kun hätäpysäytyslaitteisiin vaikutetaan. Onnistuneen koeajon jälkeen järjestelmä oli valmis käyttöönotettavaksi. Järjestelmän toimintaa seurattiin seuraavien viikkojen aikana tarkemmin, jonka aikana sen todettiin toimivan moitteettomasti.

7.2 Dokumentointi

Hätäpysäytysjärjestelmän valmistuttua piirrettiin laitteiston sähkökuvat puhtaaksi. Sähkökuvat piirrettiin EPLAN Education ohjelmistolla, versiolla 2.9. Sähkökuvat piirrettiin käyttämällä samanlaista asettelua kuin muissakin yrityksen projekteista tehdyissä sähkökuvissa oli käytetty. Hätäpysäytyslaitteiden kytkennät turvatulomoduuleille eriteltiin omille sivuilleen ja niihin merkittiin hätäpysäytyslaitteen positionumero sekä kone, jossa hätäpysäytyslaite on, jolloin oikean laitteen löytäminen kentältä tai sähkökuvista helpottuu. Sähkökuviin lisättiin myös kuvat jokaisesta logiikan I/O-moduulista, joista selviää nopeasti mitä mihinkin moduuliin on kytketty ja paljonko niissä on vapaita paikkoja. Valmiit sähkökuvat tulostettiin paperisena versiona keskukseen sekä tallennettiin sähköisessä muodossa kunnossapidon tietokoneille.

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

Työn tarkoituksena oli suunnitella ja toteuttaa hätäpysäytysjärjestelmä HKScan Rauman tehtaan suolistamon laitteille, asiakkaan toivomusten mukaisesti. Työssä tutustutaan myös standardien määrittelyihin ja vaatimuksiin hätäpysäytyslaitteille sekä hätäpysäytysjärjestelmien suunnitteluun. Asiakkaan toiveena oli erilaisten hätäpysäytyslaitteiden lisääminen suolistamon laitteille, joiden turvallisuudessa oli havaittu puutteita sekä järjestelmän käyttöpaneeli, josta voitaisiin nähdä jokaisen hätäpysäytyslaiteen tilat. Työn suunnittelu osuudeksi jäi varmistaa, että asiakkaan esittämät hätäpysäytyslaitteet olivat käyttökelpoisia kullekin laitteelle, vaatimustenmukaisuuden varmistaminen sekä hätäpysäytyslaitteiden asennuksen, turvalogiikkakeskuksen ja käyttöliittymän suunnittelu. Laitteille tulevista hätäpysäytyslaitteista sekä niiden asennuksen toteutustavasta luotiin kirjallinen raportti, joka hyväksytettiin asiakkaalla.

Työn suunnitteluvaiheen jälkeen aloitettiin hätäpysäytysjärjestelmän rakentaminen käytännössä. Hätäpysäytyslaitteet asennettiin koneisiin asiakkaan hyväksymän suunnitelman mukaisesti ja turvalogiikkakeskus rakennettiin valittuja komponentteja käyttämällä alustavien sähkökuvien mukaan. Hätäpysäytyslaitteiden asennuksen ja

keskuksen valmistumisen jälkeen laitteet kaapeloitiin, turvalogiikkaan tehtiin ohjelma ja järjestelmän käyttöpaneelille tehtiin käyttöliittymä. Käyttöliittymältä nähdään jokaisen hätäpysäytyslaitteen osalta, onko laite toimintakunnossa, vaikuttuneena tai vikatilassa. Käyttöliittymältä saatu diagnostiikka helpottaa niin laitteiden käyttäjiä, kuin myös kunnossapitoa mahdollisten vikatilanteiden selvittämisessä.

Järjestelmän valmistuttua sen toiminta testattiin, jonka jälkeen se otettiin käyttöön. Käyttöönoton jälkeisinä viikkoina järjestelmän toimintaa seurattiin vielä tarkemmin, jolloin sen todettiin toimivan moitteettomasti. Lopuksi järjestelmän sähkökuvat piirrettiin puhtaaksi ja ne lisättiin järjestelmän keskukseen sekä kunnossapidon tietokoneille. Lopputuloksena, suolistamon laitteille saatiin rakennettua toimiva hätäpysäytysjärjestelmä, joka parantaa suolistamon turvallisuutta ja täytti asiakkaan toiveet ja vaatimukset.

Opinnäytetyötä tehdessäni tutustuin koneturvallisuuden standardeihin, joista sain oppia lisää turvallisuuteen liittyvien ohjausjärjestelmien suunnittelusta ja toteuttamisesta. Lisäksi hätäpysäytykselle esitetyt määrittelyt ja vaatimukset tulivat tutuiksi standardin SFS-EN ISO 13850 kautta. Näitä tietoja pääsin käyttämään käytännössä hätäpysäytysjärjestelmän suunnittelussa ja toteutuksessa. Lisäksi pääsin tutustumaan ABB:n turvalogiikan ohjelmointiin sekä käyttöliittymän tekemiseen. Ohjelmointi itsessään oli tuttua opintojeni ajalta, mutta turvapuolen ohjelman tekeminen sekä ABB:n logiikan ohjelmointi oli uutta.

LÄHTEET

ABB. (2022). AC500-S Safety user manual V1.3.0. Haettu 11.11.2022 osoitteesta https://search.abb.com/library/Download.aspx?DocumentID=3ADR025091M0210&LanguageCode=en&DocumentPartId=&Action=Launch

ABB. (n.d.-a). Automation Builder Engineering productivity [esite]. Haettu 11.11.2022 osoitteesta https://search.abb.com/library/Download.aspx?DocumentID=3ADR010137&LanguageCode=en&DocumentPartId=&Action=Launch

ABB. (n.d.-b). Automation Builder Features and target hardware. Haettu 11.11.2022 osoitteesta https://new.abb.com/plc/automationbuilder/platform/software

Omron. (n.d.). Relays with Forcibly Guided Contacts G7SA. Haettu 22.11.2022 osoitteesta https://assets.omron.eu/downloads/datasheet/en/v8/j120_g7sa_relays_with_forcibly_guided_contacts_datasheet_en.pdf

SFS-EN ISO 13850:2015. (2015). Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet. https://online.sfs.fi

SFS-EN ISO 13849-1:2015. (2015). Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. https://online.sfs.fi

SFS-EN ISO 12100:2010. (2010). Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. https://online.sfs.fi

SFS-EN IEC 62061:2021. (2021). Koneturvallisuus. Turvallisuuteen liittyvien ohjausjärjestelmien toiminnallinen turvallisuus. https://online.sfs.fi

Sundcon Oy. (n.d.). Ohjelmistotyökalu Sistema koneiden turvatoimintojen suunnitteluun. Haettu 22.12.2022 osoitteesta https://www.sundcon.fi/turvallisuus/sistema-ohjelmistotyoekalu.html

Tukes. (n.d.). Koneita koskevat vaatimukset. Haettu 16.03.2023 osoitteesta https://tukes.fi/tuotteet-ja-palvelut/koneet#f06cc837

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Suolistamo hätäpysäytysjärjestelmä

Tiedoston päiväys: 22/12/2022 14.16.54 Raportin päiväys: 15/02/2023 Tarkistussumma: 6db3c4bfb7c5f8ec7fe226dd9f253834

PR Projektin nimi: Suolistamo hätäpysäytysjärjestelmä

Projektitiedoston nimi:	C:\Users\joona\Documents\SISTEMA\Projects\Suolistamo.ssm
Valmistumisen päivämäärä:	21/12/2022 10.24.45
Projektin tila:	
Projektin numero:	
Projektin versio:	
Tekijät:	joona
Projektista vastaavat:	
Tarkastajat:	
Vaarallinen kohta/kone:	
Dokumentaatio:	
Dokumentti:	
Ohjelmiston versio:	2.0.8 build 4
Standardin versio:	ISO 13849-1:2015, ISO 13849-2:2012
Tarkistussumma:	6db3c4bfb7c5f8ec7fe226dd9f253834
Asetukset:	☑ Käytä DC:n väliarvoja PFHD:n laskentaan (tarkempi). ☐ MTTFD-arvon pienentäminen luokkaa 4 varten arvosta 2500 arvoon 100 vuotta.
Tila:	vihreä
Huomautus:	Tähän projektiin (tai siihen kuuluviin peruselementteihin) ei ole merkitty yhtään varoitusta.

Tulostusasetukset

☑ Näytä turvatoiminnot ☐ näytä myös alajärjestelmät

☐ näytä myös lohkot ☐ näytä myös elementit

Tähän kuuluvat turvatoiminnot

SF Nimi: Hätäpysäytys

Vaadittu: PLr d	Saavutettu: PL e	PFHD [1/h]: 2,8E-8	Tila: vihreä