Kari Rahikkala-Ahlqvist

Tyypillisen satamanosturin turvatoimintojen toteutustapa ohjelmoitavalla logiikalla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkövoimatekniikka

Insinöörityö

24.11.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Kari Rahikkala Tyypillisen satamanosturin turvatoimintojen toteutustapa ohjelmoitavalla logiikalla 44 sivua 24.11.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Sähkötekniikka
Suuntautumisvaihtoehto	Sähkövoimatekniikka
Ohjaaja(t)	Lehtori Jukka Karppinen, Metropolia Suunnittelupäällikkö Juha Santala, Konecranes Oy

Tavoitteena tässä työssä oli määritellä tyypillisen satamanosturin turvatoiminnot ja saada luotua tapa toteuttaa turvatoiminnot siten, että ne voidaan toteuttaa ohjelmoitavalla logiikalla vaadittuun suoritustasoon. Tutkittavana oli vertailla, onko turvatoimintoihin liittyvät toiminnot tarkoituksenmukaisempaa toteuttaa erillisenä kokonaisuutena vai integroituna nosturissa olemassa olevaan ohjauslogiikkaan. Tämän valitun tavan on täytettävä nosturin turvatoimintoja määrittelevien standardien vaatimukset. Turvatoiminnoista tehtiin työn aikana suunnittelun tarpeisiin ohje, jonka mukaan suunnittelu tulisi toteuttaa. Samalla dokumentilla voitaisiin myös perustella asiakkaille riittävän selkeästi toteutuksen lähtökohdat ja perusteet siitä, että toteutettu tapa on hyväksytty ja koeteltu riittävästi. Valitun tavan on täytettävä myös asiakkaiden vaatimat turvallisuuskriteerit.

Tämän insinöörityön alussa on esitetty ne direktiivit, asetukset ja standardit, joita koneenvalmistajien on noudatettava turvatoimintojen määrittelyssä ja suunnittelussa. Lähtökohtana on konedirektiivi 2006/42/EY, jota konevalmistajien on noudatettava. Tämän lisäksi tässä insinöörityössä on esitetty turvatoimintoja koskevaa standardien hierarkiaa.

Tämän insinöörityön tuloksena löydettiin selkein tapa ehdottaa turvatoiminnot toteutettavaksi logiikalla. Tuloksiin voidaan lukea myös eräästä projektista tehty turvatoimintojen dokumentaatio ja turvatoiminnoista ja turvatoimintojen suunnittelijoille suunnattu suunnitteluohje. Suunnitteluohjetta voidaan käyttää hyväksi yleisesti satamanostureiden turvatoimintoihin liittyvän tietoisuuden jakamisessa.

Avainsanat	Siemens S7, ohjelmoitavat logiikat, turvatoiminnot

Author Title Number of Pages Date	Kari Rahikkala-Ahlqvist Typical Port Crane Safety Features Execution Way with Logic 44 pages 24.November 2015
Degree	Bachelor of Engineering
Degree Programme	Electrical engineering
Specialisation option	Electrical power engineering
Instructor(s)	Senior Lecturer Jukka Karppinen, Metropolia Engineering Manager Juha Santala, Konecranes Plc

The aim of this thesis was to determine the safety features of a typical crane and to create a method, with which the safety functions can be implemented using logic to the required level of performance. Under investigation was to compare the implementation of the activities related to the safety-related functions, whether it is more appropriate to take this as a separate entity or as integrated to the crane existing control logic. The selected method must comply with the requirements of the standards, which determine the security functions of the crane. Also the selected method must comply with requirements of safety related standards. During this work instruction for electrical designing of safety features were created. With the same instructions, it is possible clarify to the customer clear enough the fundamentals of executed safety features and that these are approved and tried well enough. The chosen execution method of safety features must comply with all safety requirements of customers.

At the beginning of this thesis, directives, regulations and standards, that machine manufacturers must comply with in the definition and design of safety functions are presented. The starting point is the machinery directive 2006/42/EC, which the manufacturers must comply with. After this, the hierarchy of standards related to safety functions is presented.

As a result of this thesis, the best alternative to propose execution of safety functions with automation, by evaluating all possibilities, was chosen and approved to be executed in practice. During this study, a documentation phase of one project safety functions was done in practice. Also a guide of safety functions for designers, which is possible to use as a guide to share knowledge of safety features on general level, was created.

Keywords	Safety functions, Siemens, PLC Programmable Logic Controller

Sisällys

Lyhenteet

CPU	Central processor unit; keskusprosessori
DCavg	Average diagnostic coverage; diagnostiikan keskimääräinen kattavuus
EN	Euroopan standardoimisjärjestö
F-CALL	Failsafe Call; turvaohjelma kutsu
IEC	International Electrotechnical Commission; kansainvälinen sähköalan standardointiorganisaatio
ISO	Kansainvälinen standardoimisjärjestö
KC	Konecranes Finland Oy
METSTA	Metalliteollisuuden Standardisointiyhdistys ry
MTTFd	Mean Time To dangerous Failure; keskimääräinen vaarallinen vikaantumisväli
PFDavg	Average probability of (random hardware) Failure on Demand; turvatoiminnon menetyksen (satunnaisen laitevian) todennäköisyys sitä vaadittaessa
PHF	Probability of a dangerous random Hardware Failure per hour; turvatoiminnon menetyksen todennäköisyys tuntia kohden (vaarallisen vikaantumisen taajuus tuntia kohden)
PL	Performance Level; suoritustaso
PLC	Programmable Logic Controller: ohjelmoitava logiikka
RTG	Rubber Tyred Gantry; kumipyöräinen konttinosturi
SFS	Suomen standardoimisliitto

SIL	Safety Integrity Level; turvalisuuden eheystaso
SSI	Siemens Safety Integrated
STO	Safe Torque Off; turvatoiminto hallitusti momenttia laskemalla
STS	Ship To Shore
Tm	Mission time; toiminnon vaatima aika
TÜV	Technischer Überwachungs-Verein; Saksan tekninen tarkastuslaitos

1 Johdanto

Nostureiden (satama- ja telakkanostureiden) ohjausjärjestelmien turvatoimintojen määrittelyssä, standardien noudattamisessa ja toteutuksessa ohjelmoitavalla logiikalla on aiheuttanut epäselvyyksiä niin asiakkaille, kuin myös Konecranes Finland Oy:n henkilökunnalle. Usein asiakkaiden toimitusvaatimuksissa on turvatoimintojen osalta toteutustapa, vaatimustenmukaisuus lauselma.

Asiakkaiden kysyessä tai vaatiessa toimitusvaatimuksissa turvatoimintojen toteutuksesta, niiden vaatimustenmukaisuudesta, standardin noudattamisesta ja turvalogiikkatoteutuksesta tai sen puuttumisesta, Konecranesilla ei ole antaa asiakkaalle tällä hetkellä yhtä tutkittua ja kaikkien hyväksymää vastausta ohjausjärjestelmien turvatoimintojen toteutuksen mallista. Usein on päädytty antamaan asiakkaalle epäselviä selityksiä ja perusteita, miten kussakin projektissa on päädytty kulloinkin kyseessä olevaan toteutukseen.

Tämän insinöörityön ensimmäisenä tavoitteena oli määritellä mitä kuuluu nostureiden ohjausjärjestelmien turvatoimintojen piiriin. Toinen tavoite oli saada luotua toteutusmalli, jolla saadaan tehtyä turvatoimintojen toteutustapa logiikalla tai sellaisella tutkitulla ja hyväksi havaitulla tavalla, jolla voidaan täyttää satama nostureihin kohdistuvien standardien vaatimukset ja antaa henkilökunnalle riittävän selkeät ohjeet Konecranesin tavasta toteuttaa turvatoiminnot satamanostureissa niin myyntiin, kuin automaatio- ja sähkösuunnitteluun. Samankaltaisella tuotettavalla dokumentilla on tavoitteena saada perusteltua asiakkaille riittävän selkeästi toteutuksen lähtökohdat ja perusteet siitä, että toteutettu tapa on hyväksytty ja koeteltu riittävästi ja se myös täyttää heidän turvallisuuskriteerinsä. Kaikella tällä on perimmäinen tarkoitus suojella ihmisiä, koneita, laitteita ja ympäristöä.

Tämä insinöörityö ei ota kantaa turvatoimintoihin liittyvään juridiseen puoleen, eikä yleensä juridiikkaan liittyviin seikkoihin.

2 Konecranes Oy yrityksenä

Konecranes Oy (KC) on yksi maailman johtavista nostolaitevalmistajista, jolla on toimintaa 48 eri maassa ja työntekijöitä noin 11 800. Liikevaihdosta noin 48 % tulee Laitteetliiketoiminnasta ja 42 % kunnossapidosta. Elokuussa 2015 lehdistötiedotteessa (1, s.1) kerrottiin, että Konecranes Oy yhdistyy Amerikkalaisen nostolaitevalmistaja Terex Corporationin kanssa. Yhdistyminen on käytännössä tämän työn tekohetkellä kesken. Toteutuessaan yhdistyminen tekee tulevasta yhtiöstä maailman johtavan nostolaitevalmistajan. (2, s.72.)

Konecranes Oy:n nosturitarjonta kattaa lähes kaikki teollisuudenalat, pienistä muutamien kymmenien kilojen nostokapasiteetin omaavista työpiste- ja ketjunostimista suuriin telakkapukkinostureihin, joiden nostokapasiteetti saattaa olla jopa 2 000 tonnia. Teknologian ja automaatioinnovaatioiden avulla pyritään avaamaan Konecranes Oy:lle liiketoimintamahdollisuuksia, joilla parannetaan samalla asiakasturvallisuutta ja asiakkaan prosessien tuottavuutta. Kuvassa 1 on tuotteen havainnollistamiseksi kuvattu ehkä tunnetuin, tai ainakin näkyvimmillä satamissa olevin tuote, laiturikonttinosturi (STS). (2, s.66.)

Kuva 1. Konttinosturit; Laiturikonttinosturi (2, s.66)

Konecranes Oy:n kunnossapito kattaa noin 4 000 ammattitaitoisen huoltoteknikon myötä omille, sekä muiden valmistajien nostureille kunnossapidon palveluita, jotka ovat tärkeä osa yrityksen toimintaa. Kunnossapito tarjoaa asiakkailleen mm. modernisaatiopalveluja ja huoltoa. Huoltosopimukset kattavat n. 450 000 erimerkkistä laitetta. (2, s.72.)

Trueconnect® tuotemerkillä on lanseerattu etäpalveluita 25 eri maassa. Trueconnect® on yrityksen nostureiden etäpalveluihin tarkoitettu järjestelmä. Etätuen avulla on mahdollista seurata nosturin liikkeitä ja kommunikoida nosturin kanssa tietoliikenneverkon kautta. Tämän avulla voidaan asiakkaalle tarjota mm. etätuen ja vianmäärityksen palveluja mahdollisen nosturin konerikon tai muun vian esiintyessä. Trueconnect® on yksi erinomainen esimerkki yrityksen innovatiivisesta ajattelusta hoitaa asiakkaan huoltotarpeita reaaliaikaisesti. (2, s. 58.)

3 Turvatoimintojen toteutuksen nykytilanne

Aikaisemmin Konecranesin satamanostureissa ei ole käytetty turvalogiikkaa toiminnallisen turvallisuuden ohjausjärjestelmissä lainkaan. Turvalogiikan oikeasta toteutustavasta on ollut eriäviä mielipiteitä mm. siitä, miten toiminnalliset turvallisuusasiat turvalogiikalla tulisi toteuttaa.

KC:llä on tehty turvatoiminnoista automaatiosuunnittelijoille aiemmin ohje siitä, kuinka turvatoiminnot tulisi suunnitella ohjelmallisesti. Tämä selvitys aiheellinen kyseisen ohjeen soveltamiseen ja siihen, miten se olisi toteutettava käytännössä, koska ohjeen sisältö ei ota kantaa käytännön toteutustapaan. Tulevaisuuden tarpeita ajatellen nostureita koskevat turvaratkaisut tulisi suunnitella siten, että samaa ratkaisua voidaan käyttää mahdollisimman monessa satama- ja telakkanosturityypissä.

4 Koneturvallisuuteen liittyvä lainsäädäntö, säädökset ja standardit

4.1 Konedirektiivien merkitys konevalmistajille

Koneita koskevat direktiivit, säädökset, lait ja standardit on tehty henkilöiden turvallisuuden varmistamiseksi ja koneiden valmistajien avuksi, sekä saattaa markkinoille kyseiseen käyttötarkoitukseen soveltuvia määräysten mukaisia koneita. Lainsäädäntö edellyttää, että koneen valmistaja ottaa turvallisuuden huomioon koneen suunnittelussa siten, ettei se aiheuta tapaturman vaaraa ja soveltuu tarkoitettuun käyttöön. Aikaa myöten on yleensä kustannustehokkaampaa suunnitella kone hyvin etukäteen, kuin tehdä korjauksia myöhemmässä vaiheessa. Kustannustehokkaammaksi etukäteen suunnitellut koneet tekee se, että vaikutusmahdollisuudet ovat myöhemmässä vaiheessa pienemmät, tai joitakin seikkoja on myöhemmin vaikea toteuttaa. (3 s. 12)

4.2 Konedirektiivi 2006/42/EY

Konedirektiivi 2006/42/EY on Euroopan unionin alueella koneisiin ja koneyhdistelmiin sovellettu direktiivi, joka on saatettu voimaan valtioneuvoksen koneasetuksella 400/2008. Koneiden valmistajien velvollisuus on varmistaa, että kone täyttää lain vaatimukset. Uusin konedirektiivi 2006/42/EY on tullut voimaan vuonna 2009. Seuraavaksi on selitetty lyhyesti kyseisen konedirektiivin tarkoitus sekä direktiivin sitovuus nostureihin.

> Koneturvallisuuden standardeilla tarkoitetaan koneiden sekä niissä olevien järjestelmien, laitteiden ja toisinaan myös komponenttien turvallisuuskysymyksiä käsitteleviä standardeja. Koneturvallisuuden standardit liittyvät tyypillisesti koneiden suunnitteluvaiheessa sovellettavissa oleviin kysymyksiin, mutta voivat toisinaan käsitellä myös koneen elinkaaren muissa vaiheissa sovellettavissa olevia aiheita. Koneet voivat olla joko kuluttajatuotteita tai tuotantovälineitä, kädessä pidettäviä tai laajoja konelinjoja, kiinteästi asennettuja tai liikkuvia koneita. Euroopan unionissa koneilla tarkoitetaan yleensä konedirektiivin 2006/42/EY soveltamisalaan kuuluvia tuotteita, jotka nekään eivät rajoitu pelkästään sellaisiin tuotteisiin, joita arkikielessä aina kutsuttaisiin varsinaisesti koneiksi. (19, s.1.)

Konedirektiivissä on määritetty ne koneet, joita kyseinen direktiivi koskee. Direktiivin 2 artiklan mukaan direktiivi koskee myös nostureita, koska nosturi on laite, joka on konedirektiivissä mainittu laite seuraavan lainauksen mukaan:

> Toisiinsa liitettyjen osien tai komponenttien yhdistelmä, jossa on tai joka on tarkoitettu varustettavaksi muulla kuin välittömällä ihmis- tai eläinvoimalla toimivalla voimansiirtojärjestelmällä ja jossa ainakin yksi osa tai komponentti on liikkuva ja joka on kokoonpantu erityistä toimintoa varten.(5, s. 4.)

4.3 Standardien merkitys käytännössä

Suomen standardoimisliiton verkkosivuilla on kerrottu hyvin se, mitä standardeilla tehdään ja mihin niitä käytetään (6, s. 1).

> Standardit helpottavat jokapäiväistä elämää. Niillä lisätään turvallisuutta ja järkeistetään toimintaa. Standardisoinnin ansioista tuotteet, palvelut ja menetelmät sopivat siihen käyttöön ja niihin olosuhteisiin, joihin ne on tarkoitettu. Se varmistaa, että tuotteet ja järjestelmät sopivat toisiinsa ja toimivat yhdessä. Standardien mukaan valmistettu tuote hyväksytään kansainvälisille markkinoille. Niiden avulla poistetaan kaupan esteitä. (6, s. 1.)

EU-alueen sisämarkkinoille, käytännön toteuttamista varten Euroopan alueella on oma standardointi, jota ilman yhteiset markkinat eivät voisi toimia. Edellä mainituilla verkkosivuilla on kerrottu eri standardoimisjärjestöjen merkityksestä ja kirjainyhdistelmistä seuraavaa:

> Kirjainyhdistelmät SFS, EN, ISO jne. ilmoittavat organisaation, jossa standardin teksti on vahvistettu. Suomessa vahvistetun standardin tunnus on SFS, eurooppalaisessa standardisoimisjärjestössä CENissä vahvistetun EN ja kansainvälisessä standardisoimisjärjestössä ISOssa julkaistun ISO. Tunnusyhdistelmä SFS-EN tarkoittaa, että sama standardi on voimassa sekä Suomessa että Euroopassa, SFS-ISO puolestaan sitä, että standardi on voimassa Suomessa ja ISOssa, mutta sitä ei ole vahvistettu CENissä. SFS-EN ISO tarkoittaa, että standardi on vahvistettu kaikissa kolmessa organisaatiossa. (6, s. 1.)

4.4 Koneturvallisuusstandardien kolmiportainen hierarkia

Koneturvallisuuden standardit jaetaan standardin EN ISO 12100 mukaan kolmeen ryhmään, A-, B- ja C-tyypin standardeihin. Näiden standardi tyyppien tarkoituksena on ollut nopeuttaa standardien laadintaprosessia ja varmistaa turvallisuussuunnittelun perusperiaatteiden olevan yhtäläiset kaikenlaisia koneita suunniteltaessa. (7, s.1.)

METSTA on laatinut verkkosivuilleen taulukon, jossa on selkeästi kerrottu standardien jaottelun periaatteet:

A-tyypin standardi (turvallisuuden perusstandardi)

Perusteet, suunnitteluperiaatteet ja yleiset näkökohdat kaikkiin koneisiin sovellettaviksi

A-tyypin standardit ovat: SFS-EN ISO 12100 (terminologia, perusteet ja tekniset periaatteet) sekä SFS-EN ISO 14121-1 (riskin arviointi).

B-tyypin standardi (turvallisuuden ryhmästandardi)

Käsitellään yhtä turvallisuusnäkökohtaa tai suojausteknistä laitetta.

B1-tyypin standardit koskevat tiettyjä yksittäisiä turvallisuusnäkökohtia (esim. turvaetäisyyksiä, pintalämpötiloja, melua).

B2-tyypin standardit koskevat suojausteknisiä laitteita (esim. kaksinkäsin hallintalaitteita, toimintaankytkentälaitteita, suojuksia).

C-tyypin standardi (konekohtainen turvallisuusstandardi)

Koskevat koneen tai koneryhmän yksityiskohtaisia turvallisuusvaatimuksia (esimerkiksi maansiirtokoneet, pakkauskoneet, kuljettimet, pumput, nosturit) (7, s.1.)

4.5 Nostureita koskevia standardeja

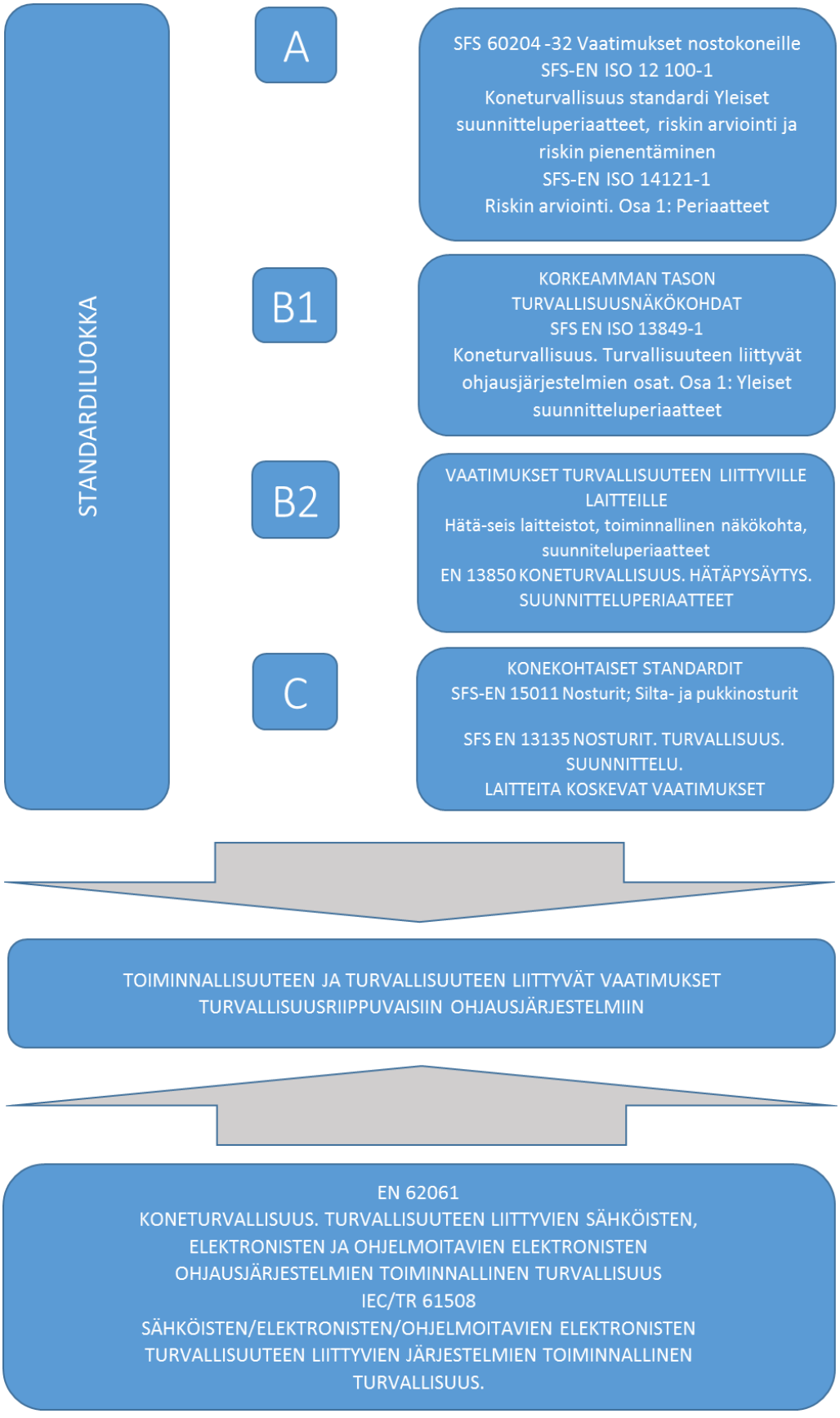
Seuraavan luetelman standardit ovat vain pieni osa nostureita koskevista standardeista. Nostureihin kohdistuvissa standardeissa on myös paljon muita sähkötekniikkaan ja mekaniikkaan sovellettavia standardeja, joita ei luetelmassa ole mainittu. Tämä kuvastaa hyvin tilannetta varsin kattavasta ja laajasta standardien määrästä ja on hyvin työlästä seurata, mitä standardia milloinkin tulee noudattaa. Käytettävät standardit ovat mm. seuraavat:

- SFS 60204 -32 Vaatimukset nostokoneille
- IEC 61131 Ohjelmoitavat logiikat
- SFS EN 15011 Silta- ja pukkinosturit
- IEC 61508 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus.
- IEC 61508-3 Ohjelmalliset vaatimukset
- IEC 61511 Functional safety – Safety instrumented systems for the process industry sector

- DIN/EN 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet 9
- SFS-EN ISO 13849-2 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus, 2008
- IEC 62 061, koneiden ohjausjärjestelmät.
- SFS-EN 15011 Nosturit; Silta- ja pukkinosturit
- SFS-EN ISO 12 100-1 Koneturvallisuusstandardi. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Hätätoiminnot (hätäpysäytys, sähkön syötön hätä poiskytkentä)
- IEC 60364-5-53 Sähkön syötön hätäpoiskytkennän toiminnalliset näkökohdat esitetään standardin kohdassa 536.4.
- IEC 61131-3 Hätäpysäytyslaitteiston suunnitteluperiaatteet ja toiminnalliset periaatteet
- SFS-EN ISO 13850 Koneturvallisuus. Hätäpysäytys. Suunnitteluperiaatteet, 2008
- SFS-EN 13135 Nosturit. Turvallisuus. Suunnittelu. Laitteita koskevat vaatimukset

IEC 61508 on kattostandardi ja IEC 61511 puolestaan prosessiteollisuutta koskeva alastandardi. Standardi IEC 62 061 koskee erityisesti konesektoria standardin IEC 61508 viitekehyksen mukaisesti. Standardin tavoitteena on helpottaa koneiden merkittävien vaarojen turvallisuuteen liittyvien sähköisten ohjausjärjestelmien suorituskyvyn määrittelyä (ks. standardin ISO 12100-1 kohta 3.8). Standardi on tarkoitettu käytettäväksi standardissa ISO 12100-1 kuvattavassa järjestelmällisessä riskin pienentämisen viitekehyksessä ja riskin arvioinnin osalta standardissa ISO 14121 (EN 1050) kuvattavien periaatteiden mukaisesti. Opastavassa liitteessä A esitettävää menetelmää suositellaan käytettäväksi turvallisuuden eheystasojen (SIL) asettamiseen.

Seuraavalla sivulla esitetty kuva 2 selkeyttää tässä työssä tarkasteltavana olevaa nostureiden turvatoimintoihin liittyviin toimintoihin sovellettavia standardeja.

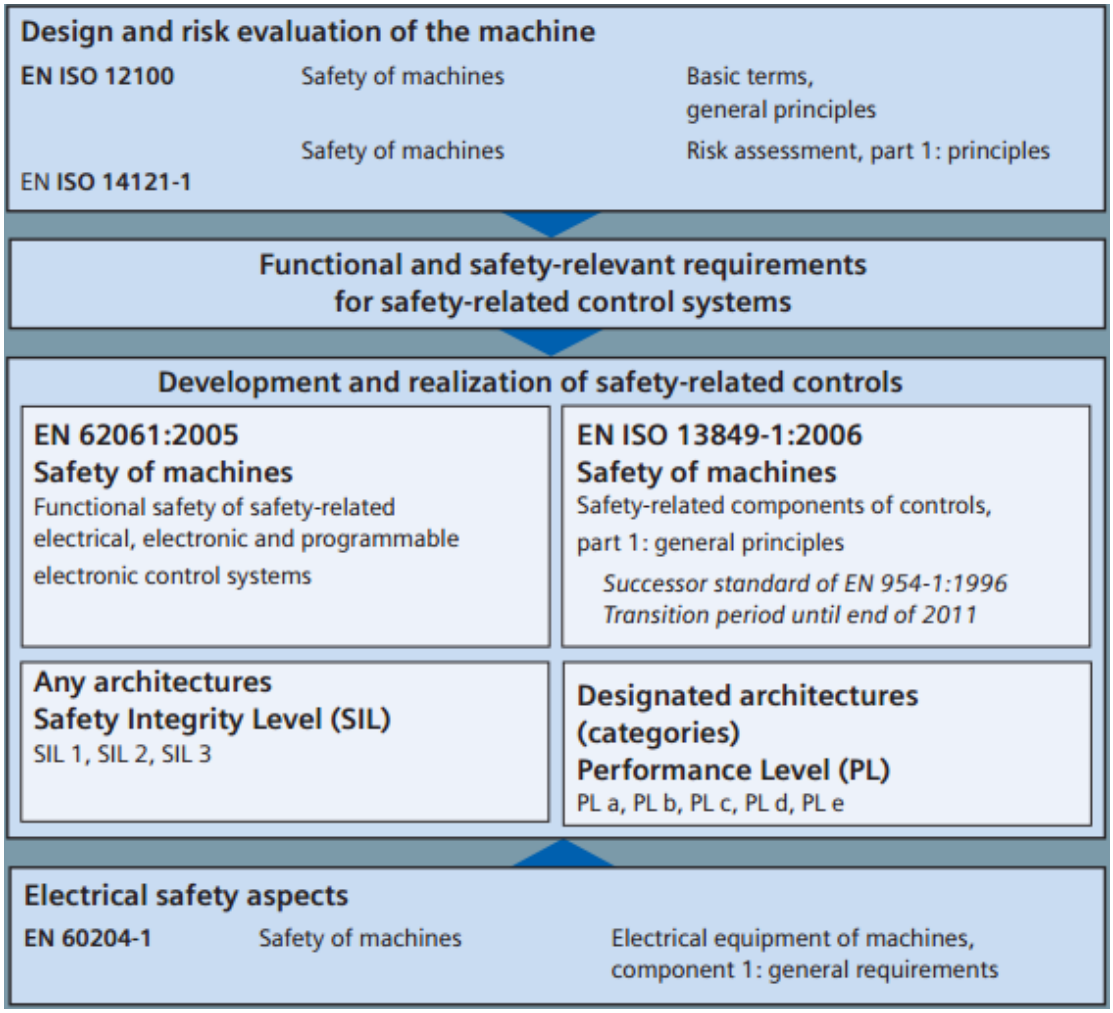


Kuva 2. Nostureiden turvatoimintoihin liittyvät pääasialliset standardit

4.6 Ohjaustoimintojen standardit

Taulukossa 1 esitetään, kuinka ohjaustoimintojen kehittämisessä standardeja voidaan soveltaa ohjaustoimintoja suunniteltaessa. (8, s.5.)

Taulukko 1. Ohjaustoimintojen perusstandardit. (8, s.5.)



Taulukossa 2 on esitetty kuinka standardeja EN 62061 EN ISO 13849 voidaan soveltaa rinnakkain ohjausjärjestelmien turvatoimintojen suunnitteluun ja toteuttamiseen.

Taulukko 2. Standardien IEC 62061 ja ISO 13849-1 soveltamissuositus (11, s.12.)

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

4.7 Ohjausjärjestelmän määritys

Tässä työssä puhutaan ohjausjärjestelmistä. Standardissa SFS-EN 62061 ohjausjärjestelmä on määritetty seuraavalla tavalla:

> Järjestelmä, joka reagoi esimerkiksi prosessista, muista koneen osista, käyttäjältä tai ulkoisista ohjauslaitteista tuleviin tietoihin ja joka saa aikaan lähtötiedot, joiden avulla kone saadaan toimimaan tarkoitetulla tavalla.(21, s.24.)

Tyypillisesti satamanostureissa käytetään ohjausjärjestelmissä tai sen osina erilaisia releitä, ylivirtasuojia, taajuusmuuttajia, kontrollereita, antureita, ohjelmoitavaa logiikkaa ja monia muita sähköisiä laitteita ohjaamassa nosturia tai sen määrättyä osaa.

5 Riskin arvioinnista yleisesti

Koneasetus VNa 400/2008 vaatii, että koneille on aina tehtävä riskin arviointi. Koneasetuksessa VNa 400/2008 on seuraava vaatimus:

> Koneen valmistajan tai tämän valtuutetun edustajan on varmistettava, että tehdään riskin arviointi, jotta koneeseen sovellettavat terveys- ja turvallisuusvaatimukset voidaan määrittää. Kone on sen jälkeen suunniteltava ja rakennettava ottaen huomioon riskin arvioinnin tulokset.(22, s.7, Liite I)

Riskin arviointi on tarkoitettu tehtäväksi koko tuotekehityksen prosessin aikana, kun tietoa saadaan lisää järjestelmästä. Tuotekehitysprosessin aikana tehtyjä korjausehdotuksia analysoidaan jälkeenpäin ja niiden perusteella muodostetaan uusia kyseisen sovelluksen turvallisuusvaatimuksia. Korjausehdotusten toteutustavan mukaan tehdään riskin arviointi standardi SFS-EN ISO 14121-1 mukaan. Jälkeenpäin on pystyttävä osoittamaan, että riskianalyysissä havaitut riskien pienentämistarpeet on viety suunnitteluun ja toteutus on testattu. Jälkiseurantadokumentaatiossa täytyisi olla merkittynä perustelut, joiden vuoksi korjausehdotuksia on hylätty tai toteutettu toisin kuin riskianalyysissä on ehdotettu.(23, s.16)

6 Toiminnallisen turvallisuuden suoritustason luokittelu

Toiminnallisen turvallisuuden luokitteluun voidaan käyttää kahta standardia, SFS-EN ISO 13849-1 sekä SFS EN 62061, jotka vastaavat toisiaan turvallisuuden luokittelun osalta. Standardissa SFS-EN ISO 13849-1 luokittelu perustuu PL-tason liittyviin vaatimuksiin ja rajoituksiin, ja siinä viitataan paljon IEC 61508 standardiperheeseen. (10, s.14). Kyseisessä standardissa luokittelu ottaa huomioon myös kategorian ja siinä otetaan huomioon lisäksi keskimääräinen vaarallisten vikojen väli (MTTFd), diagnostiikan kattavuus (DC), ja monia muita kuhunkin PL-Tasoon liittyviä vaatimuksia ja rajoituksia. Myös ohjelmoitavat järjestelmät ovat käsiteltävänä.

Standardissa SFS EN 62061 luokittelu on tarkoitettu ohjelmoitaviin järjestelmiin ja järjestelmäsovelluksiin. Luokittelu perustuu vaarallisten vikojen todennäköisyyteen, ja siinä on SIL- tasoihin liittyviä rajoituksia ja vaatimuksia. (10, s.14)

VTT:n tutkimusraportin VTT-R-04369-10 mukaan

> Standardeja SFS EN 62061 ja SFS-EN ISO 13849-1 voidaan käyttää ristiin siten, että muutamat järjestelmän osat käsitellään ensimmäisellä ja loput toisella standardilla. Siten esim. hydrauliikka ja pneumatiikka voidaan käsitellä 13849-1 mukaan ja elektroniikka 62061:n mukaan. Taulukko 5 esittää PL-tasojen, SIL-tasojen ja kategorioiden vastaavuuden. Kategorioiden osalta vertailu on suuntaa antava. (10, s.14.)

Taulukossa 3 on esitetty SIL-tasojen ja PL-tasojen vastaavuudet toisiinsa.

Taulukko 3. Suoritustason PL, turvallisuuden eheyden tason, sekä SIL luokan vastaavuus. (9, s.14)

Suoritustaso (PL)	Luokka (kategoria)	Keskimääräinen vaarallisen vian todennäköisyys tunnissa (1/h)	Vastaavuus eheystasoihin (SIL)
a	B	$10^{-5} \leq PFH_d < 10^{-4}$	ei
b	1-2	$3 \cdot 10^{-6} \leq PFH_d < 10^{-5}$	1
c	1-3	$10^{-6} \leq PFH_d < 3 \cdot 10^{-6}$	1
d	3	$10^{-7} \leq PFH_d < 10^{-6}$	2
e	4	$10^{-8} \leq PFH_d < 10^{-7}$	3

7 Turvallisuuteen liittyvien ohjausjärjestelmien suunnittelu

EN ISO 13849-1-standardin mukainen suunnitteluprosessi voidaan määrittää seuraavan luetelman avulla:

- kuvaa suunnitteluprosessi
- suorita tarvittaessa riskin arvioiminen
- määritä turvatoiminnot (ks. 7.1)
- arvioi vaadittava suoritustaso PLr (ks. 7.2)
- suunnittele ja luo toteutus turvatoiminnoille (ks.7.3)
- määritä suoritustaso PL jokaiselle turvallisuuteen liittyvälle osalle (ks.7.4)
- tarkista, että vaadittava suoritustaso on saavutettu (ks.7.5)
- suorita ohjelmiston kehittäminen, konfigurointi ja parametrointi
- suorita testaukset
- toteuta ja kelpuuta suunnitellun mukaisesti
- dokumentoi järjestelmä
- tee muutosten hallinnan dokumentointi

Turvallisuuteen liittyvät ohjausjärjestelmän osat on suunniteltava ja toteutettava siten, että noudatetaan kaikilta osin standardien SFS-EN ISO 12100 ja SFS-EN ISO 14121 riskin pienentämisen periaatteita. Standardi SFS-EN ISO 12100 on perusstandardi, joka sisältää konedirektiivi 2006/42/EY:n soveltamiseksi tarvittavat perusteet vaarojen tunnistamiseksi. Siinä esitetään myös hyväksyttävä tapa konedirektiivin pakollisen riskin arvioinnin suorittamiseksi ja dokumentoinniksi.

7.1 Turvatoimintojen suunnittelu ja toteutus

Turvallisuuteen liittyvien ohjausjärjestelmän osien kyky toteuttaa turvatoiminto ilmaistaan suoritustason määrittämisen avulla. Suoritustaso PL määritellään arvioimalla seuraavassa luetelmassa lueteltuja näkökohtia. Viittaukset ovat suoraan standardin EN 13849-1 alakohtiin.

-vaarallinen keskimääräinen vikaantumisaika (MTTFd) jokaiselle yksittäiselle komponentille

-diagnostiikan kattavuus (DC), (ks. liite E)

-yhteisvikaantuminen (CCF), (ks. liite 6.)

-rakenne eli luokat (ks. 6.2)

-turvatoiminnon käyttäytyminen vikatilanteessa (-tilanteissa), (ks. 6)

-turvallisuuteen liittyvä ohjelmisto (ks. 4.6 ja liite J)

-systemaattinen vikaantuminen (ks. liite G)

-kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa (11, s.42.)

Turva-automaatio on suunniteltava siten, että määrittelyvaiheen vaatimukset otetaan huomioon. Riskien vähennystarve, sekä muut tekijät sellaiset tekijät, joilla on mahdollista varmistaa koneen tai laitteen turvallisuus koko sen eliniän ajan, on myös otettava huomioon. Turva-automaation tulee pysäyttää koneen työtehtävä ja saattaa kone turvalliseen tilaan häiriön sattuessa. Kone ei myöskään saa aiheuttaa tarpeettomia pysähdyksiä turvallisuuden kannalta. Turva-automaation tulee olla luotettavaa ja soveltuvaa kuhunkin käyttöolosuhteeseen. Huoltoa ja koestusta koskevat vaatimukset on otettava

huomioon myös turva-automaatiota toteutettaessa. Turvatoimintojen turvalaitteiden tulee olla muista vakiolaitteistoista riippumattomia, paitsi jos muut turvalaitteet eivät vaaranna turvapuolen toimintaa. Toteutusvaiheessa toteutetaan suunnittelussa tehdyt hyväksytyt suunnitelmat asianmukaisesti. Koneeseen liitetty turvajärjestelmä ja siihen liittyvät kenttälaitteet tulee merkitä ja niistä on laadittava tarvittavat asiakirjat sekä käyttöohjeet. Koneen käyttöönotossa todetaan, että koneen turvallisessa tilassa pitävät laitteet toimivat suunnitellulla tavalla valmistajan laatimien ohjeiden mukaisesti. Mikäli turva-automaatioon tehdään muutoksia, on silloin käytävä läpi kaikki ne kohdat, joihin muutos vaikuttaa alakohtineen. Suuremmissa modernisaatioissa, kannattaa koko suunnitteluprosessi alkaa uudestaan alusta saakka, riskien hallinnan kautta jalkautuen suunnitteluun ja käyttöönottoon. (30, s.137).

7.2 Turvatoimintojen määritys

Turvatoimintojen määritys ja vaadittavan suoritustason arviointi voidaan toteuttaa standardin SFS EN 13849 mukaan kahdella eri tavalla. Ensimmäisessä tavassa määritellään ohjausjärjestelmän vaarakohdille välttämättömät turvatoiminnot, tarkennetaan näiden toimintojen vaatimukset ja määritetään turvatoiminnoille vaadittava suoritustaso (PLr). Toisessa tavassa määritetään ohjausjärjestelmälle suoraan korkein suoritustaso ja tämän jälkeen määritetään suoritustason täyttävät turvallisuustoiminnot. (11, s.38) Suoritustason valinta suoraan korkeimmalle tasolle on yleinen tapa, mutta sarjatuotteessa se saattaa kustannusten nousun vuoksi olla mahdoton toteutustapa.

Standardi EN ISO 13849 ohjaa turvatoimintojen tunnistamisesta seuraavasti:

> Turvatoimintoja tunnistettaessa ja eriteltäessä on otettava huomioon vähintäänkin seuraavat seikat:
>
> a) jokaista erityistä vaaraa tai vaaratilannetta koskevan riskin arvioinnin tulokset
>
> b) koneen käyttötoimintaan liittyvät ominaisuudet mukaan lukien
>
> — koneen tarkoitettu käyttö (mukaan lukien kohtuudella ennakoitavissa oleva väärinkäyttö)
>
> — käyttötavat (esim. paikalliskäyttö, automaattikäyttö, koneen tiettyä osaa tai vyöhykettä koskeva käyttö)

— toimintajakson aika ja

— vasteaika

c) hätätoiminto

d) erilaisten työprosessien ja käsikäyttöisten toimien keskinäisen vuorovaikutuksen kuvaus (korjaus, asetus, puhdistus, vianetsintä jne.)

e) koneen käyttäytyminen, jonka turvatoiminnon on tarkoitus saada aikaan tai estää

f) koneen tila(t) (esim. toimintatapa), jossa sen on tarkoitus olla toimiva tai sen toiminta on estettynä

g) käyttötoiminnan taajuus

h) niiden toimintojen ensisijaisuus, jotka voivat olla yhtä aikaa toimivia ja jotka voivat aiheuttaa ristiriitaisia tilanteita. (10 s.58.)

7.3 Tyypillisen satamanosturin turvatoimintojen rajoittimet

Tarvittavat turvatoiminnot määritetään standardeissa ISO 1200-1, ISO 1200-2 ja ISO 14121 kuvattujen riskin pienentämisen strategioiden mukaisesti. Satamanostureissa tyypillisesti esiintyviä turvatoimintojen rajoittimia on esitetty seuraavassa luetelmassa(8, s.84)

- hätäpysäytyspainikkeet
- nostokyvyn rajoittimet
- liikkeenrajoittimet: nostoliikkeen yläraja ja alaraja, kaikkien siirtoliikkeiden äärirajat
- törmäyksen estolaitteet tapauksissa, joissa ei pystytä puskureilla estämään seuraavassa luetelmassa luetellut ja standardissa SFS-EN15011 mainitut seikat:

  a) nosturien komponenttien lujuuden ylitys

  b) nosturien tai vaunujen putoaminen tai kaatuminen

  c) kuorman putoaminen

  d) kuorman heilunta vaarallisella tavalla

- nosto- tai ajonopeuden ja/tai kiihtyvyyden/hidastuvuuden rajoittimet riippuen nostetusta kuormasta

Muita samanlaisia toimintoja ovat lisäksi (ajo)nopeuden ja/tai kiihtyvyyden/hidastuvuuden rajoittimet riippuen tuulioloista, henkilöiden havaitsemiseen suunnitellut turvalaitteet ja logiikkayksiköt turvatoimintoja varten.

Edellä luetelluista turvatoimintojen rajoitinlaitteista ei kaikissa nosturisovelluksissa ole välttämättä käytössä kaikkia luetelman toimintoja, kuten esimerkiksi henkilöiden havaitsemiseen suunniteltuja turvalaitteita. Näitä toimintoja on sovellettu joissakin satama-aluetta koskevissa laitteistoissa käyttämällä esimerkiksi valoverhoja, joilla on tarkoitus havaita henkilöiden meneminen vaaralliselle alueelle.

7.4 Tyypillisen satamanosturin turvatoiminnot

Satamanosturisovelluksien erilaisuuden vuoksi on haastavaa soveltaa standardin vaatimuksia kaikkiin sovelluksiin, niiden nykyisten teknisten ratkaisujen vuoksi. Ne onkin suunniteltava erikseen sovelluskohtaisesti ja arvioitava turvatoimintojen osalta tarkasti siten, että ne täyttävät kaikki standardissa vaadittavat seikat. Suunnittelijoiden tai c-tyypin standardin laatijoiden on otettava huomioon näistä tarpeelliset kohdat.(11, s.64) Esimerkiksi käyttötoiminnot, normaali käynnistys tai pysäytys, voivat olla myös turvatoimintoja. Tämä voidaan varmistaa vasta koneen riskin arvioinnin toteuttamisen jälkeen. Turvatoiminnolla tarkoitetaan sellaista koneen toimintoa, jonka vikaantuminen voi aiheuttaa välittömän riskin kasvamisen. Standardin EN13849-1 mukaan turvatoiminnoksi tarkoitetaan riskien pienentämiseksi sellaisia laitteita, joilla on yksi tai useampi turvatoiminto. Turvallisuuteen liittyviksi ohjausjärjestelmän osiksi kutsutaan osia, joiden tehtävänä on turvatoimintojen toteuttaminen. Standardissa SFS-EN 15011 mainitaan nostureiden ohjaustoimintojen suoritustasosta, että kaikkien turvallisuuteen liittyvien ohjausjärjestelmien osien on täytettävä vähintään standardin EN ISO 13849-1 suoritustaso c. Vaikka em. standardissa on määritelty saavuttamaan suoritustaso c, se ei kuitenkaan välttämättä ole asiakkaan vaatimus, vaan se saattaa poiketa mainitusta arvosta. Tyypillisessä satamanosturissa on oltava ainakin seuraavassa luetelmassa mainitut turvatoiminnot, ellei vaaratekijöitä ole poistettu muilla tavoin.

- ylikuormasuojaus
- nopeussäätöisten käyttöjen ylinopeusvahti
- hätä-seis-piirit. Sisältäen radiot, nosturissa sijaitsevat piirit, ulkoisessa ohjainhuoneessa tai rakennuksessa sijaitsevat piirit ja muut ulkoiset piirit.

- asiaan kuuluvien liikkeiden rajoitukset, eli kaikkien liikkeiden pysäytysrajat
- törmäyksenesto (8, s.84)

Turvatoiminnot ovat otettu luetelmaan standardista SFS-EN 13135, jossa toiminnot määritellään turvallisuuteen liittyviksi ohjausjärjestelmän toiminnoiksi. Huomioitavaa on, että nostureita koskevissa standardeissa mainitaan puskurien olevan sopiva liikkeenrajoitin. KC: n nostureissa lähestulkoon kaikissa liikkeenrajoittimet ovat toteutettu sähköisinä toimintoina, sekä mekaanisilla puskureilla. (8, s.84)

Standardissa EN ISO 13849 mainitaan edellisen luettelon lisäksi turvatoiminnoiksi seuraavan luettelon toiminnot, jotka ovat toteutettavissa nostureissa turvatoimintoina.(11, s.66)

- käynnistys tai uudelleenkäynnistystoiminto
- tehonsyötön vaihtelut, menetys ja palautuminen
- ohjaustavat ja ohjaustavan valinta
- turvallisuuteen liittyvien ohjausjärjestelmien osien vuorovaikutus

7.5 Pysähtymistoimintojen määrittäminen

Pysähtymistoiminnot määritellään nostureiden osalta standardissa SFS EN 60204-32, jossa pysähtymistoiminnot jaetaan kolmeen luokkaan

1. luokka 0: pysäyttäminen poistamalla välittömästi teho nostokoneen toimilaitteilta (ts. valvomaton pysähtyminen, ks. 3.69)

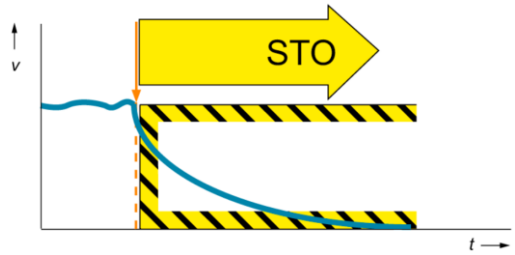
2. luokka 1: valvottu pysähtyminen (ks. 3.12), jossa nostokoneen toimilaitteilla on teho pysähtymisen aikaan saamiseksi. Pysähtymisen jälkeen teho poistetaan toimilaitteilta.

3. luokka 2: valvottu pysähtyminen, jossa nostokoneen toimilaitteilla säilytetään teho. (26, s.104)

Jos pysäyttämistoimintoa käytetään turvallisuuteen liittyvänä ohjaustoimintona, hyväksymättömiä ohjauspoikkeamia ei sallita. (ks. 9.4.4) Tällöin poikkeamia vastaan pitää toteuttaa esim. käyttämällä käyttöjärjestelmiä, jotka takaavat tarvittavat turvallisuuteen liittyvät ohjaustoiminnot standardin IEC 61800-5-2 mukaisesti. (26, s.104)

7.6 Safe Torque Off; Taajuusmuuttajan turvatoiminto (STO)

Safety Torque Off on useimpiin markkinoilla oleviin taajuusmuuttajiin integroitu turvatoiminto. Tässä kyseisessä turvatoiminnossa estetään taajuusmuuttajan modulaatio, eli ohjauspulssien tuottaminen estetään moottoria ohjaavilta transistoreilta. STO-toiminnossa moottori pysähtyy kitkan tai vastamomentin seurauksena. Tätä toimintoa voidaan käyttää toiminnoissa, joissa pysäytys on tarpeellista tehdä nopeasti. STO-toiminto on standardin SFS EN 60204-1 pysähtymistoimintoluokan 0 vaatimusten mukainen. Seuraavassa kuvassa on esitetty STO-toiminnon periaate, jossa sininen käyrä esittää moottorin pyörimisnopeutta (v) ajan (t) funktiona. Oranssi nuoli esittää hetkeä, jolloin turvatoiminto aktivoidaan. (16, s.1)



Kuva 3. Graafinen esitys STO toiminnosta nopeuden ja ajan funktiona (16, s.1.)

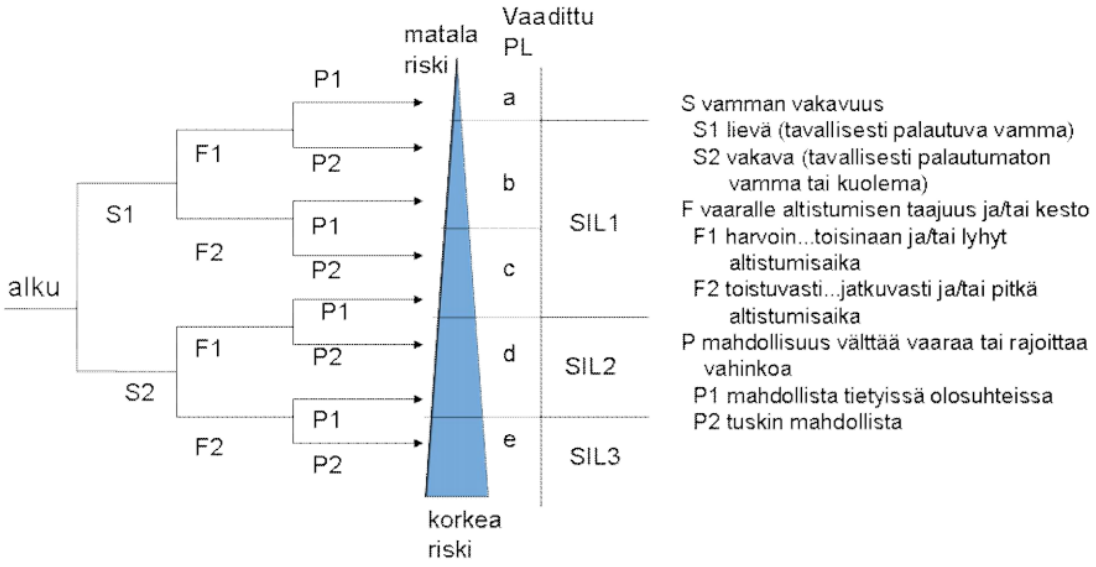
7.7 Standardin EN ISO 13849 mukainen suoritustaso

Otsikossa mainitun EN ISO 13849-standardin mukaisesti turvallisuuden tasoa kuvataan kirjaimella a, b, c, d tai e, jolla ilmaistaan turvallisuuteen liittyvien ohjausjärjestelmän osien kykyä suorittaa turvatoiminto ennakoitavissa olosuhteissa. Jokaiselle valitulle turvallisuuteen liittyvälle ohjausjärjestelmän osalle ja/tai niiden yhdistelmälle, joka toteuttaa turvatoiminnon, on arvioitava suoritustaso PLr.

Toiminnallisen turvallisuuden taso saadaan likiarvona suoraan standardista tai riskinarvion perusteella (10, s.15).

> Jos standardeista ei löydy turvatoiminnoille PLtasoa, pitää päätös tehdä riskin arvioinnin perusteella. SFS-EN ISO 13849-1 esittää riskin arvioinnin perustaksi riskigraafia (ks. Kuva 4). Menetelmässä vaadittava PL-taso saadaan määriteltyä kolmella kysymyksellä:
>
> - mikä on vamman vakavuus?
>
> - mikä on vaaralle altistumisen taajuus (tai kesto)?
>
> - onko mahdollista välttää vaara tai pienentää vahinkoa? (10, s.15).

Standardin SFS-EN ISO 13849-1 mukainen riskigraafi on esitetty kuvassa 4. Riskigraafilla voidaan määrittää vaadittava suoritustaso PLr riskin arvioinnin perusteella. (11, s.100).



Kuva 4. Standardin SFS-EN ISO 13849-1 mukainen riskigraafi. (11, s100.)

7.8 Suoritustason arvioinnin yksinkertaistettu menetelmä

Nimettyjä rakenteita kuvataan lohkokaavioilla ja ne luetellaan kappaleessa 7.7.1 kunkin luokan yhteydessä. Nimetyt rakenteet kuvataan turvallisuuteen liittyvien ohjausjärjestelmän osien yhdistelminä, joka alkaa kohdasta, jossa turvallisuuteen liittyvät signaalit syntyvät ja päättyy tehonohjauselimien ns. *lähtöihin* (ks. myös ISO 12100-1:2003 liite A).

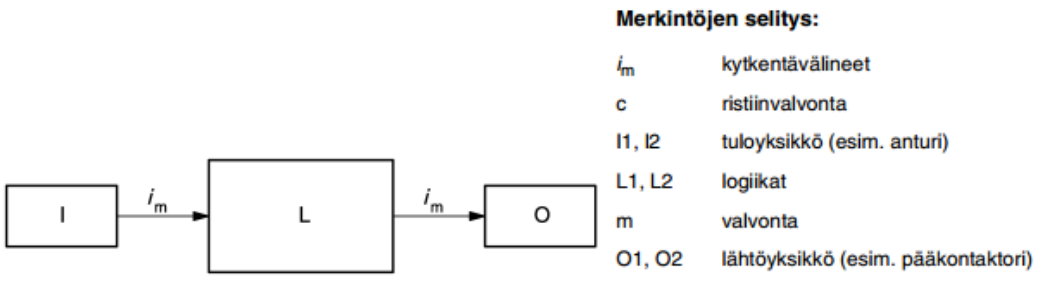
Nimettyjä rakenteita voidaan myös käyttää kuvaamaan ohjausjärjestelmän alajärjestelmää tai sen osaa, joka vastaa tulosignaaleihin ja tuottaa turvallisuuteen liittyvän lähtösignaalin. Siten tulo-yksikkö voi tarkoittaa esimerkiksi valoverhoa, ohjauslogiikkaelementtien tulopiirejä tai tulopuolen kytkimiä. Ns. lähdöt voivat vastaavasti tarkoittaa esimerkiksi lähtösignaalien kytkintä tai laserskannerien lähtöjä. (11, s.48)

Turvallisuuteen liittyvien ohjausjärjestelmien luokat

Turvallisuuteen liittyvien ohjausjärjestelmän osien on oltava yhden tai useamman alla lueteltujen viiden luokan vaatimusten mukaisia. Luokat ovat perusmuuttujia, joita käytetään halutun suoritustason saavuttamiseen. Standardin ISO 13849-1 määrittelemiä, nimettyjä rakenteita eli luokkia on yhteensä viisi: B, 1, 2, 3 ja 4.

Luokat B, 1 ja 2 ovat yksikanavaisia, kun taas luokat 3 ja 4 ovat kaksikanavaisia, eli niissä on kaksi erillistä toisistaan riippumatonta, toimivaa kanavaa, jotka pystyvät suorittamaan turvatoiminnon. Tämä tekee luokista 3 ja 4 kalleimmat toteuttaa, mutta niillä saadaan korkeimmat suoritustasot. Järjestelmän rakenteella on siis suuri merkitys sille, mihin suoritustasoon päädytään. Luokkien arkkitehtuuri yleensä kuvataan lohkokaavioesityksenä (ks. kuva 8). (11, s.74) Luokkarakenteiden määritelmät ovat seuraavat:

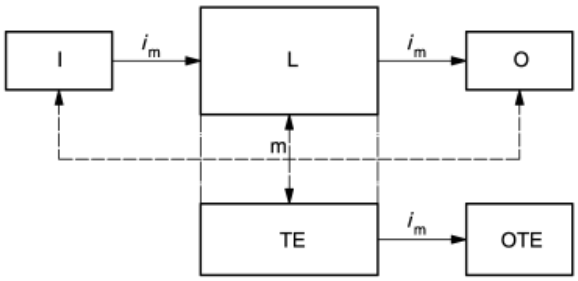
- Luokan B yleisiä tuvallisuusperiaatteita (suojamaadoitus, eristyksen valvonta, jännitepiikkien vaimennus yms.) on noudatettava. Käyttö- ja ympäristöolosuhteet on otettava huomioon käytettävissä komponenteissa. Vaarallisten vikaantumisten välinen keskimääräinen aika, MTTFd-arvo, on oltava 3–30 vuotta. (11, s.74)
- Luokassa 1 on noudatettava luokan B vaatimuksia sekä hyvin koeteltuja komponentteja ja hyvin koeteltuja turvallisuusperiaatteita (ylimitoittaminen, pakkotoimisuus yms.). MTTFd on oltava 30–100 vuotta. (11, s.74)
- Luokassa 1 suurin saavutettavissa oleva suoritustaso on PL c.



Kuvio 1. Luokan B ja 1 mukainen nimetty rakenne (11, s.74.)

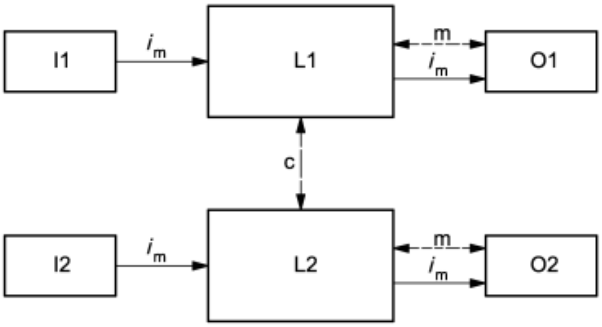
- Luokassa 2 on noudatettava luokkien B ja 1 vaatimuksia, sekä koneen ohjausjärjestelmän on koetettava turvatoimintojen toimivuus tietyin väliajoin. MTTFd on oltava 3–100 vuotta vaaditun PL-tason mukaan ja yhteisvikaantumisen (CCF) todennäköisyys on oltava pieni (CCF-arvon määrittäminen; kpl 2.3.6). (11, s.74)

- Luokassa 2 suurin saavutettavissa oleva suoritustaso on PL d.



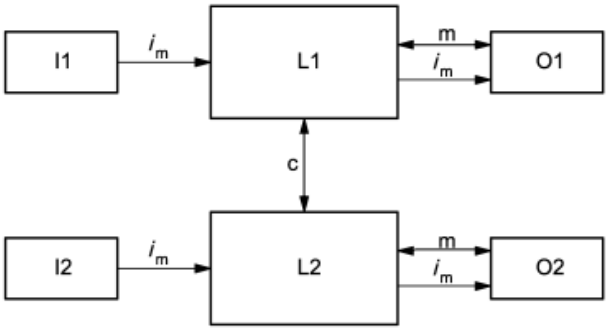
Kuvio 2. Luokan 2 mukainen esitystapa (11, s.74.)

- Luokassa 3 on noudatettava luokkien B ja 1 vaatimuksia. Yksittäisen vian sattuessa ohjausjärjestelmän on pystyttävä suorittamaan turvatoiminto, ja mahdollisuuksien mukaan yksittäinen vika on havaittava. Useammat viat on aina havaittava. MTTFd on oltava 30–100 vuotta vaaditusta PLtasosta riippuen. Dcavg, eli diagnostiikan kattavuuden keskiarvo on oltava vähintään 60–99 %, yhteisvikaantumisen (CCF) todennäköisyys oltava pieni. (11, s.74)



Kuvio 3. Luokan 3 mukainen esitystapa (11, s.74.)

- Luokassa 4 on noudatettava luokkien B ja 1 vaatimuksia. Turvatoimintoa ei saa menettää vaikka järjestelmässä olisi yksi vika. Kaikkien vikojen on paljastuttava, eli vikoja ei saa kertyä järjestelmään, ilman että käyttäjä niistä tietää. Jos vikoja kuitenkin kertyy, ne eivät saa aiheuttaa turvatoiminnon menettämistä. Käytännössä tarkoittaa järjestelmän kahdennusta, sekä itse- että ristivalvontaa. MTTFd: n on oltava 30–100 vuotta, DCavg: n on oltava 99–100 % ja yhteisvikaantumisen (CCF) todennäköisyys on oltava pieni. (11, s.74)



Kuvio 4. Luokan 4 mukainen esitystapa (11, s.74.)

7.9 Turvatoimintojen ohjausjärjestelmien komponentit

Kokonaisuudessaan turvatoimintojen piirien kaikkien komponenttien on oltava määritellyn turvallisuustason tasolle luokiteltuja (11, s.42). Esimerkiksi KC:n käytössä olevat hätä-seis painikkeet on luokiteltu suoritustasolle PLe. Tässä insinöörityössä ei ole kaikkia turvatoimintojen komponentteja, ja niiden suoritustasoa ei ole esitelty niiden suuren määrän vuoksi. Käytännön sovelluksissa oletuksena on, että suunnittelija tekee komponenttien valinnan yhteydessä niiden turvallisuustason tarkistuksen siten, että komponentit täyttävät vaaditun tason.

KC:llä on käytetty pitkään Siemensin valmistamia logiikkakomponentteja nostureiden ohjausjärjestelmissä, joten tässä työssä keskitytään Siemensin komponentteihin ja ohjelmistoon, jotka ovat KC:n yleisesti käytössä.

Suurin ero logiikan vakio- ja turvakomponenttien välillä on, että turvakomponenttien valvonnassa on kaksikanavainen sisäinen rakenne mentäessä turvallisuustasolle PLd. Molemmat kanavat valvovat toisiaan, testaavat automaattisesti sisäänmenojen ja ulostulojen tilaa, sekä asettavat moduulin turvatilaan vikatapauksissa. Turvatoimintojen kommunikointiin voidaan käyttää mm. PROFIsafe väyläratkaisua kenttälaitteiden väliseen kommunikaatioon (ks.8.2).

8 Turvatoimintojen tulot, lähdöt ja kenttäväylä

Turvatoimintojen toteutuksessa automaatiolla on mahdollista varmentaa toiminnallista turvallisuutta, ja nykyisin turva-automaatio on yleistynyt turvallisuuden varmentamisessa niin prosessiteollisuudessa kuin koneissa.

8.1 Logiikan tulot ja lähdöt, I/O

Siemensin logiikkaperheen turva-automaatiotuotteet voidaan tunnistaa keltaisesta lipukkeesta komponentin etupaneelissa. Vakio-, sekä turvakomponentteja voidaan asentaa vierekkäin kuvassa 5 esitetyn tavoin.

Kuva 5. Siemensin PLC komponenttien vakio- ja turvakomponentteja (28, s.31)

8.2 Turvalogiikan kenttäväylä

Kun käytetään hajautettua logiikkaa, kenttälaitteiden välillä on käytettävä tiedonsiirtoon kyseessä oleville laitteille soveltuvan protokollan omaavaa tiedonsiirtojärjestelmää. KC:n sovelluksissa on käytetty jo pitkään Profibus-protokollaan tukeutuvaa järjestelmää, joka on standardi väylätekniikka ja osa IEC 61158 standardia, jota lukuisat yritykset käyttävät. Siemens on ollut yrityksenä mukana kehittämässä tätä tiedonsiirtoratkaisua. Profibus-tekniikoita on olemassa kaksi eri vaihtoehtoa. PROFIBUS DP (Decentralized Perephery = hajautettu järjestelmä) ja PROFIBUS PA (Process Automation), joista PA on laajennettu versio Profibus DP. (29, s.7)

Turva-automaatiosovelluksiin on kommunikointi toteutettavissa PROFIsafe-väylätekniikalla, jossa vakiotiedonsiirto ja turvatiedonsiirto siirretään samassa väylässä toistensa kanssa. Profisafe on Profibus DP -väylän päälle suunniteltu erillinen kerros, jonka tarkoi-

tus on vähentää mahdollisia tietojen lähetys- ja vastaanottovirheitä (engl. Black Channel). Profisafe toteutusta voidaan käyttää aina standardin ISO 13849 luokitteleman turvallisuuden tasolle e. (29, s.7)

Turvakerroksen ollessa itsenäinen tiedonsiirtokerros riippumatta alustan toteutustavasta, oli sitten kyseessä kuparijohto, valokaapeli, langaton yhteys tai liitinalusta. Profisafe ei ole riippuvainen tiedonsiirtonopeuksista tai virheenhavaitsemislaitteistoista, vaan se näkee vain oman kerroksen. Turvaväylän viestit ovat hallitsevia viestejä väylässä, jotka vahvistetaan toisilleen signaalin lähteestä sen prosessointitasolle saakka. (29, s.7) Yleensä tiedonsiirrossa tapahtuu virheitä ja tämän vuoksi Profisafe tiedonsiirtoa valvotaan seuraavassa luetelmassa luetelluilla virheiltä. (29, s.10)

- toisto: vanhentuneet sanomat lähetetään uudelleen vääränä ajankohtana
- katoaminen: sanomaa ei vastaanotettu tai tunnistettu
- lisäys: sanoma lisätään ja tulee odottamattomasta tai tuntemattomasta lähteestä
- väärä järjestys: sanomien määrätty järjestys on virheelinen
- tietojen virhe: sanomat vääristyneitä
- viive: sanomat tulevat sallitun saapumisaikaikkunan ulkopuolella
- naamioitunut sanoma: sanoma, joka tulee voimassa olevalta lähteeltä
- fifo virhe: first in first out, oikeaa järjestystä ei säilytetä eli puskurointivirhe. (29, s.10)

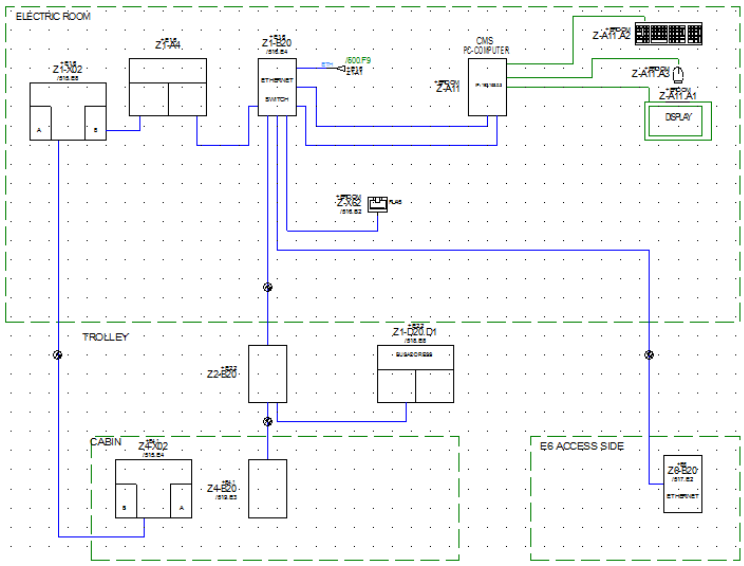
Edellisen luetelman virheen havaitsemisen jälkeen ohjainyksikkö menee vika-tilaan ja vika on poistettava, ennen kuin ohjainyksikkö sallii ohjelman jatkumisen. Tällä estetään koneen vaarallisten toimintojen suoritusta. (29, s.11)

9 Hätä-seis-piirin toteutus nykyisellä mallilla ja turva-automaatiolla

9.1 Nykyinen hätä-seis-piirin toteutuslogiikka ja toiminta

KC: n satamanosturit liiketoiminta-alueen tuotteista lähestulkoon kaikissa on hajautettu logiikka. Tämä tarkoittaa sitä, että nosturissa olevia logiikkakomponenteista koostuvia yksiköitä on asennettu sähkökeskuksiin eri puolille nosturia. Tämän tarkoituksena on sähkökeskusten välisen kaapeloinnin määrän minimoiminen. Kommunikointi laitteiden

välityksellä tapahtuu pääosin Profibus DP–väylän kautta. Valokuitua käytetään myös tiedonsiirrossa sellaisissa paikoissa, joissa ohjauskaapeleihin saattaa indusoitua häiriöitä ja näin ollen häiriöt saattavat vaarantaa oikean tiedonkulun. Esimerkkinä tähän kappaleeseen on otettu RTG- nosturin hätä-seis-toiminto turvatoimintona standardin SFS EN ISO 13849 mukaan. Kuvassa 6 on esitetty yksitiekaaviolla RTG-nosturin väylätopologia, jossa on Profibus DP-väyliä ja valokuidulla toteutettuja tiedonsiirtoväyliä. (ks. 30).



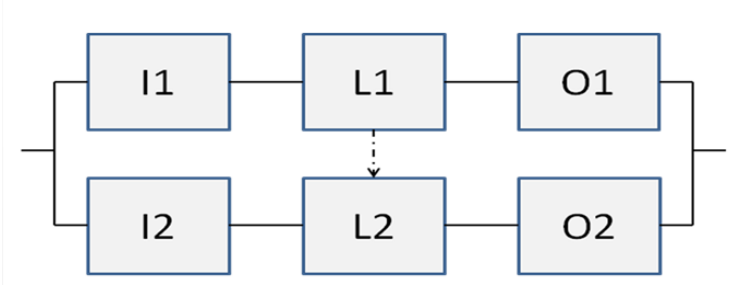
Kuva 6. RTG-Nosturin profibus-väylän topologia

Hätä-seis-painikkeita on nosturissa eri paikoissa, kuten teleissä, vaunussa, sähköhuoneessa, ohjaamossa telin kojekaapissa ja yleensäkin siellä, missä niitä mahdollisesti tarvitsee olla turvallisuuden takaamiseksi. Lyhyesti esitettynä hätä-seis-toiminto alkaa siitä, kun henkilö painaa hätä-seis-painiketta. Toiminta aiheuttaa nosturin pääliikkeiden jarrujen tehonsyötön katkeamisen ja jarrujen sulkeutumisen jousivoiman aikaansaamina pysäyttäen liikkeet. Samaan aikaan moottoreita ohjaavat invertterit putoavat pois ready-tilasta ja moottoreiden tehonsyöttö katkeaa. Tässä esitetyssä RTG-nosturissa pääliikkeiden invertterit ovat ns. common bus-laitteita, joille tehosyöttö tapahtuu yhteisen DC-välipiirin kautta. Hätä-seispainiketta painettaessa tehonsyöttö pääliikkeiden inverttereille katkeaa, invertterit menevät vika-tilaan ja käy-toiminto on estetty. Nosturin kuljettaja saa hälytyksen ohjaamoon toimintapaneelin välityksellä, ja tieto välitetään logiikan Profibus väylän kautta kuljettajalle näytön kautta.

Sähköpiirikaavio nykyisestä RTG-nosturin hätä-seis-piirin toteutuksesta löytyy esimerkinomaisesti esitettynä liitteessä 1. Hätä-seis-piiri on nykyisessä toteutusmallissa tehty

sarjassa olevilla hätä-seispainikkeiden NC-koskettimilla, jotka ohjaavat apurelettä O-K11. O-K11-koskettimet ohjaavat relettä O-K1, joka puolestaan katkaisee jännitteen kaikista samassa ryhmässä olevilta logiikan ulostuloilta, inverttereiden ready-piiristä ja koneistojen jarrunohjauspiiristä. Logiikalle on sisäänmenot myös releiltä O-K1 sekä O-K2, joiden toimintaa käsitellään PLC-ohjelman toiminnan kuvauksen yhteydessä.

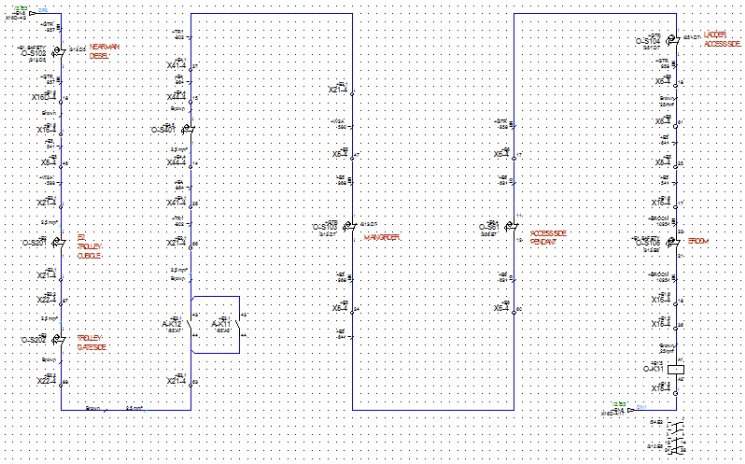
Standardin SFS EN ISO 13849 mukainen lohkokaavioesitys hätä-seis-piiristä on esitetty kuvassa 7.



Kuva 7. E-Stop-piirin lohkokaavioesitys

Nykyinen hätä-seis-toiminnon toteutus on ohjelmoitu ohjelmistoon STL-kielellä ja ohjelmiston toiminnan kuvaaminen/seuraaminen lähtee siitä, kun hätä-seis-painiketta on painettu, jolloin rele O-K11 päästää, O-K1:n apukärki aukeaa ja antaa logiikan sisäänmenolle tilatiedon jne

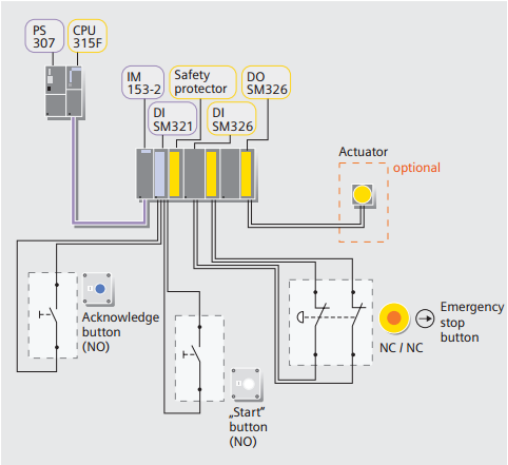
Kuvassa 8 on esitetty, nykyisen hätä-seis-piirin toteutustapa sarjaan kytketyillä hätä-seis painikkeen koskettimilla, joiden jälkeen on hätäseis-piirin releen kela. Hätä-seis painikkeen toinen kosketin on kytketty PLC:n inputiin. Jos toinen koskettimista avautuu, nosturin liikkeen pysähtyminen on aktivoitu ohjelmallisesti. PLC:llä on käytetty komponentteina vakiokomponentteja.



Kuva 8. Nykyisen mallin mukainen hätä-seis-piirin toteutus

9.2 Esimerkki hätä-seis-piirin toteutus turva-automaatiolla

Kuvassa 9 on esimerkinomaisesti kuvattu, kuinka edellisessä kappaleessa 9.1 kuvattu turvatoimintoihin lukeutuva hätä-seis-piiri voidaan toteuttaa turvalogiikkaa käyttäen.

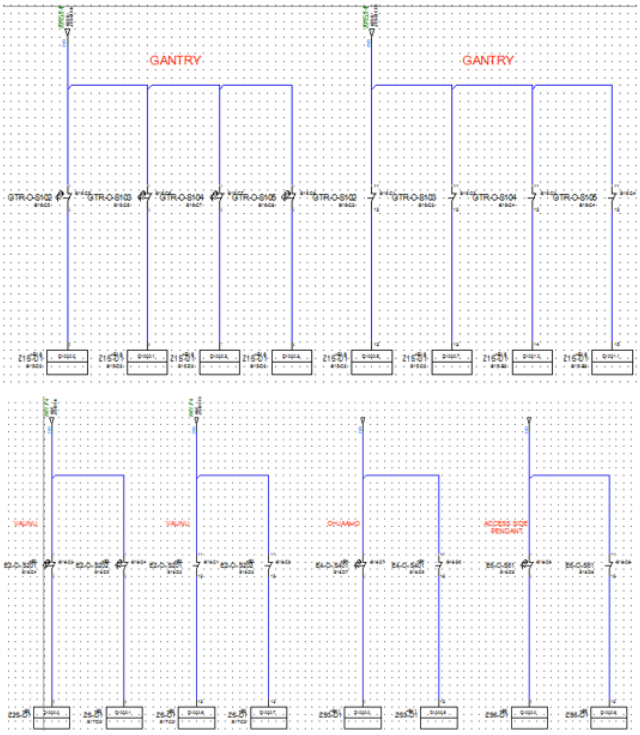


Kuva 9. Hätä-seis-piirin periaatteellinen toteutus turva-automaatiolla (28, s.174)

Mikäli hätä-seis painikkeen sijainti poikkeaa edellä esitetystä kuvasta ja hätä-seis toiminto on johdotettu PLC:n ala-asemaan, voidaan tiedonsiirto toteuttaa Profisafe-väylällä, joka on luokiteltu PLe tasolle. Verrattuna turvarelemalliin (ks. kappale 10) tämän tavan etuna on johdotuksen väheneminen. Varsinkin satamanosturissa tällä on merkitystä, koska PLC:n ala-asemat sijaitsevat eri puolella nosturia.

10 Hätä-seis-piirin toteutus turva-automaatiolla tyypillisessä satamanosturissa

Kuvassa 10 esitetään, kuinka hätä-seis-piirin toteutus turva-automaatiolla voidaan esittää sähkökuvissa.



Kuva 10. Hätä-seis-piirit toteutettu turva-automaatiolla

Kuten kuvia 9 ja 11 vertailemalla huomataan, on turva-automaatiosovelluksen toteutustapa huomattavasti selkeämpi. Vaikka kuvassa 11 ei ole merkitty liittimiä ja tarvittavia välikaapeleita, tulee niitä alemman kuvan mukaan vähemmän kuin perinteisessä mallissa. Ala-asemalta toiselle kaapeloinnin osuus vähenee huomattavasti, koska painikkeet on johdotettu suoraan turva-PLC:n sisäänmenoon ja turvapuolen kommunikointi tapahtuu olemassa olevan Profibus-väylän kautta.

10.1 Hätä-seis-piirin turva-automaatiototeutuksen ohjelmallinen osuus

Turva-automaatiota käytettäessä käytännön toimiin liittyy seuraavissa viidessä kappaleessa esitetyt pääkohdat, joista kussakin on erilaisia tehtäviä, jotka täytyy suorittaa

turva-automaatiota suunniteltaessa. Sovelluksesta riippuen, voi seuraavissa kappaleissa mainittujen toimien lisäksi olla myös muitakin asioita, jotka täytyy ottaa huomioon suunnittelussa.

10.1.1 Käytettävien komponenttien ryhmittely

Tässä vaiheessa ensimmäisenä valintana on käytettävän CPU:n valinta. Valinnassa kannattaa kiinnittää huomiota ainakin seuraavassa luettelossa esitettyihin seikkoihin:

- työmuistin riittävyyteen
- osoiteavaruuden suuruuden riittävyyteen
- laskureiden ja ajastimien määrän riittävyyteen
- laajennettavuuteen
- käytettävä väyläratkaisu on tuettu (36, s.81)

Vakio- ja turvapuolen I/O: a voidaan käyttää rinnakkain samassa asemassa. Mikäli kyseessä on laajennus, niin kaikki jo olemassa olevat korttiyksiköt voidaan säilyttää entisellään ja jatkaa asemaa turvayksiköillä. Kuitenkin sillä ehdolla, että käytettävä CPU on fail-safe-yhteensopiva. Mikäli sovelluksen toteutus kuuluu turvaluokkaan SIL3/luokka 4/PLe, täytyy I/O-kortit asentaa erilliseen potentiaaliryhmään, eli kortit on erotettava vakiokomponenteista erillisellä tehokomponentilla. (36, s.52)

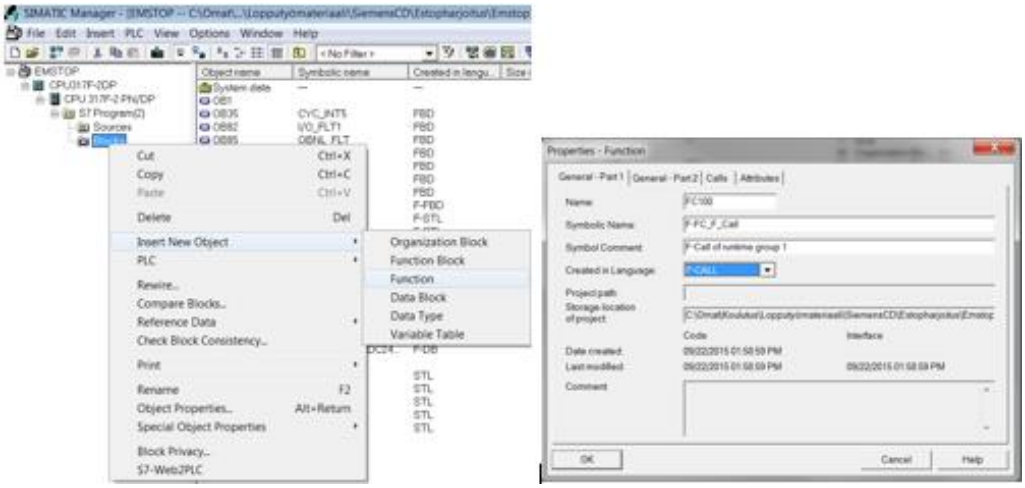
Käytettävistä korteista mainittakoon erikseen analogiainput-kortti, jossa vakio- ja turvapuolen kortit eroavat toisistaan sisääntulon lukualueen ja ohjelmoitavuuden osalta. Vakiokäytössä mahdollisuudet ovat laajemmat. Virranmittaus turvapuolella on lukualueella 4–20 mA. Vakiopuolella on valittavana 0–20 mA tai 4–20 mA sekä 0–10 V. Syynä tähän on turvapuolen sisääntulon 4-20mA mittausalueella erotettava johdinkatkosvalvonta. Turvapuolen analogiakortit osoitetaan prosessikuva-alueelle ja luku tapahtuu CPU:n prosessikuvan kautta, koska suora periferian puhuttelu ei ole sallittua turvaohjelmassa. Analogiainput-kortissa osoitetaan ohjelmassa prosessikuva-alueelle ja mittausarvon lukeminen tapahtuu CPU:n prosessikuvan kautta. Suora periferia-lukualueen puhuttelu ei ole sallittua turvaohjelmassa. Antureiden tehonlähteenä suositellaan käytettävän korttiyksikön sisäistä anturisyöttöä. Ulkoista tehonlähdettäkin voidaan käyttää, mikäli tehonlähteen stabiliteetin tulee vastata turvaluokkaa SIL2/PLd. (37, s.156)

10.1.2 Turvaohjelman rakenne ja ohjelmointi

Turva-ohjelman turvallisuuteen liittyvät ohjelmointilohkot on tehtävä Siemens S7 Manager ohjelmaan FBD- tai LAD- ohjelmointikielillä. Lohkot koostuvat kirjoitetuista toiminnallisista lohkoista ja ohjelman itse generoimista lohkoista. Ohjelma generoi itse käyttäjän ohjelmoimalohkoa vastaavan lohkon, jossa käytetään erilaisia operandeja ja operaatioita. Operandi tarkoittaa lausekkeen kohdetta, jolle operaattori tekee jotain. (36, s.99)

10.1.3 F-CALL-kutsu ja -luonti

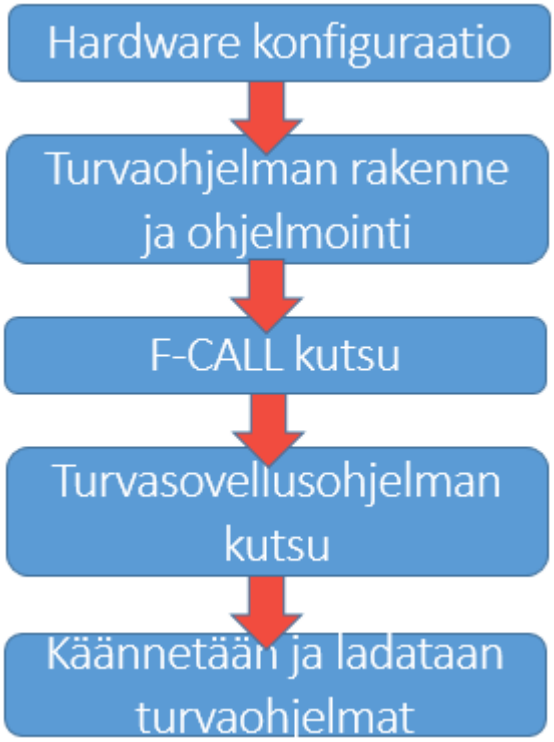
Tässä vaiheessa suunnittelija lisää kyseisen F-CALL-yksikön ohjelmaan editorin F-Call-kielellä, mutta sitä ei editoida. F-Call tarkoittaa turvaohjelman generoimaa F-FC toimintalohkoa, joka liittää turvaohjelman CPU:n kokonaisohjelmaan. Myöhemmin käännettäessä ohjelmaan, turvaohjelman puoli generoi F-Call ohjelman. Turvaohjelmat täytyy suorittaa samalla aikavälillä, eli turvaohjelmien kutsu tehdään aikakeskeytys-ohjelmalohkossa, esimerkiksi OB35:ssä. Samassa ohjelmalohkossa voidaan kutsua myös vakio-ohjelmalohkoja. F-Call kutsu täytyy olla ensimmäisenä aikakeskeytys-ohjelmalohkossa. Kuvassa 11 on esitetty, kuinka ohjelmalohko luodaan Siemens S7-ohjelmassa. (36, s.105)



Kuva 11. Ohjelmalohkon luonti

10.1.4 Turvaohjelman käsittely, kutsuryhmät

Turvaohjelma muodostuu yhdestä tai kahdesta toisistaan riippumattomasta kutsuryhmästä, jotka kutsuvat turvaohjelmia. Tällöin on mahdollista erottaa turvaohjelman aikakriittiset ja ei-aikakriittiset turvatoiminnot. Mitä lyhempi reaktioajan täytyy olla, sitä pienempi kutsuryhmän kutsuväli täytyy olla. (36, s.106) Kun kaikki turvaohjelman turvavarmennetut yksiköt mukaan lukien F-Call ja F-ohjelmalohkot on luotu, täytyy ohjelmassa määritellä kutsuryhmä. Lopuksi käännetään ja ladataan koko turvaohjelma CPU:hun. Kuvia 12 esittää koko turvaprojektin ohjelmoinnin pääkohdat. (36, s.122)



Kuva 12. Turvaprojektin ohjelmoinnin pääkohdat (36, s.122)

11 Turvarele turvatoimintojen toteutuksessa

Koska standardissa SFS EN 15011 määritellään, että sähkömekaanisilla komponenteilla toteutetun ohjausjärjestelmän on täytettävä vähintään suoritustaso c ja kategoria (luokka) 1. Luokan 1 laitteistoissa on sovellettava samoja periaatteita kuin mitä sovelletaan luokan B laitteistoon. Lisäksi standardissa SFS EN ISO 13849 mainitaan, että ohjausjärjestelmän osat on suunniteltava ja rakennettava käyttämällä hyvin koeteltuja komponentteja ja noudattamalla hyvin koeteltuja turvallisuusperiaatteita. (11 s.78)

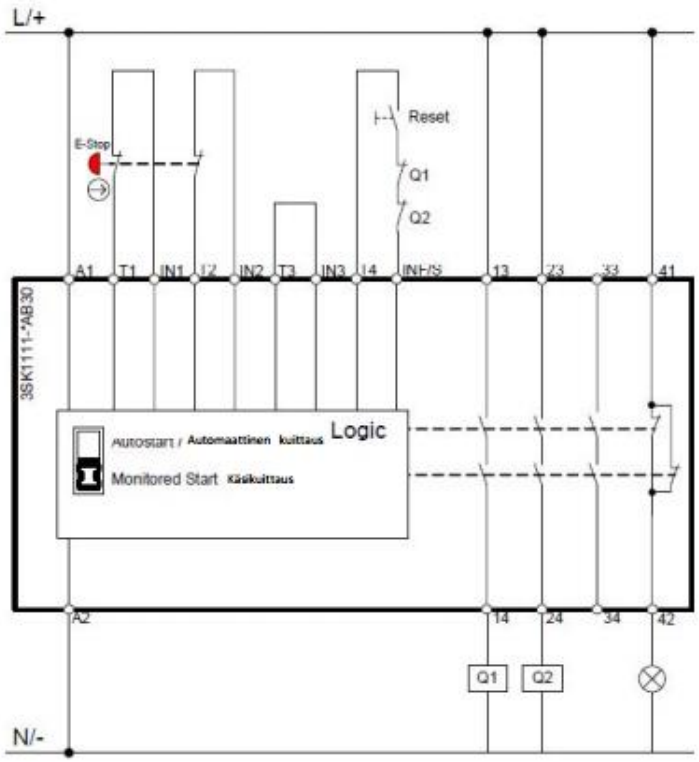
Hyvin koeteltu komponentti tarkoittaa, että sitä on käytetty aiemmin laajasti ja siitä on hyviä kokemuksia vastaavissa sovelluksissa. Se on myös varmistettu ja todennettu noudattamalla periaatteita, joilla osoitetaan komponentin sopivuus ja luotettavuus turvallisuuteen liittyvissä sovelluksissa. (33 s.162)

Päätös tietynlaisen komponentin hyväksymisestä ns. hyvin koetelluksi riippuu sovelluksesta. Luokassa 1 suurin saavutettavissa oleva suoritustaso on PL c, joka on riittävä tässä työssä aiemmin tarkasteltavalle järjestelmälle (ks. 9). Mikäli halutaan korkeamman suoritustason d mukainen ohjausjärjestelmä, täytyy mekaaniset komponentit, kuten releet ja hätä-seis painikkeet kahdentaa. Tämän vuoksi turvapiireissä saattaa olla tarkoituksenmukaista käyttää monimutkaisissa sovelluksissa turvareleitä. Esimerkiksi mainittakoon hätä-seis-piiri. Riippuen turvareleen versiosta ja toimilaitteen tai anturin ulkoisesta kytkennästä, voidaan turvareleillä toteutettu laitteisto toteuttaa jopa PL luokan e-tasolle (14 s.200). Kuvassa 13 on esitetty Siemensin Sirius tuoteperheen turvareleitä, jotka eroavat selkeimmin ulkoisesti vakioreleestä keltaisten värimerkintöjen osalta.

Kuva 13. Siemensin Sirius tuoteperheen turvareleitä (34, s.1.)

Turvarele hätä-seis-piirissä

Esimerkkinä turvareleen käyttömahdollisuudesta voidaan ottaa hätä-seis-piiri ja sen kytkentä Siemensin valmistamaan 3SK1-hätä-seis-moduuliin. Kuvassa 14 esitetty kytkentä toteutettuna 3SK1111-turvareleellä antaa standardin SFS EN ISO 13849 mukaisen turvallisuustasoluokituksen e.(11, s.213). Turvareleiden käyttö on perusteltua joissakin sovelluksissa, koska toteutettuna vakio PLC:llä johdotetulla järjestelmällä, voi järjestelmästä tulla monimutkainen suunnitella, ottaa käyttöön ja huoltaa. Tämä on mahdollista, koska turvareleissä on itsessään tilaansa valvovia ominaisuuksia, jotka edesauttavat saavuttamaan helpommin ymmärrettävillä kytkennöillä vaaditun suoritustason.



Kuva 14. Turvarele hätä-seis-piirissä (35, s.3.)

Siemens Sirius 3SK1-moduulin avulla on mahdollista toteuttaa hätä-seis ja hätäpysäytystoimintoja, monitoroida suojaavia ovia asentokytkimien avulla, sekä monitoroida valoverhoilla tai lasereilla toteutettuja suoja-alueita (12 s.45).

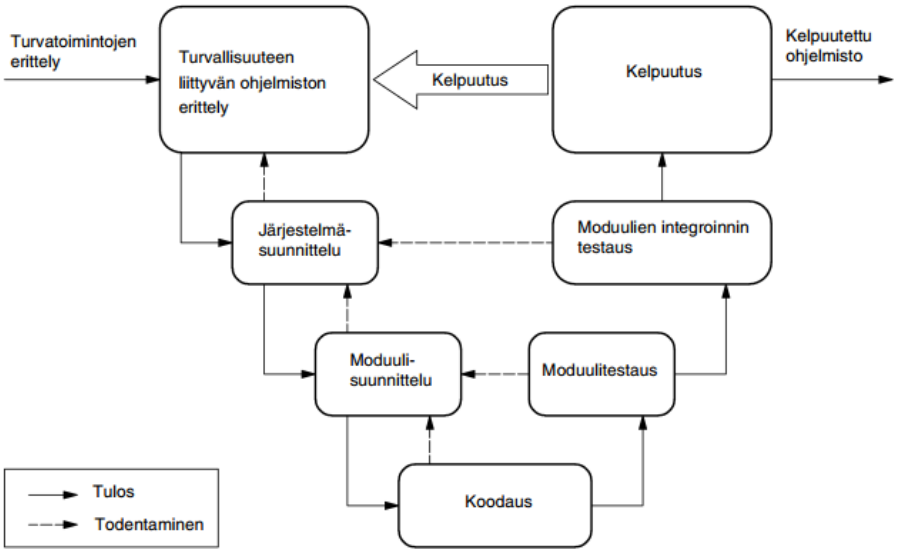
12 Turva-automaation ohjelmistojen vaatimukset

Sähköohjausjärjestelmien tullessa ajan myötä monimutkaisemiksi mm. riittävien turvallisuustoimintojen turvallisuuden tarkistaminen on yhä vaikeampaa. Ohjauksien ohjelmointirivien tarkistaminen ei välttämättä anna varmuutta siitä, että ohjelmisto toimii oikein ja turvallisesti kaikissa tilanteissa. Ohjelmistopäivityksillä ja lisäyksillä voidaan monesti lisätä luotettavuutta olennaisesti. Ohjelmoinnin suunnittelun tavoitteena on saada ohjelmistosta yksikäsitteinen ja selkeä niin, että se on ymmärrettävää, testattavaa, jäljitettävää ja ylläpidettävää. Ohjelmoinnin lähtökohtana on virheiden välttäminen koko ohjausjärjestelmän turvallisuuselinkaaren aikana. (31, s.62)

KC:lla on Siemensin Step 7-ohjelmointityökalu käytössä laajasti useassa maassa. Siemensin logiikkaa voidaan ohjelmoida samalla ohjelmistotyökalulla, niin vakio-, kuin turvatoimintojen osalta. Turvaohjelmien luomiseen täytyy olla Safety Distributed-lisäpaketti. Nämä ohjelmistot ovat kansainvälisen TÜV-luokituslaitoksen hyväksymiä turvaohjelmatyökaluja. Standardissa SFS EN ISO 13849-1 on turvallisuuteen liittyvään sovellusohjelmistoon liittyen määrittelyjä, jotka on otettu huomioon Siemensin Safety Distributed lisäpaketissa. (12, s.1)

Sovellusohjelmiston turvallisuusvaatimukset

Turvallisuuteen liittyvän sulautetun ja sovellusohjelmiston turvallisuuselinkaaren yksinkertaistettu V-malli esitetään kuvassa 15 ja SFS EN ISO 13849 standardissa. Esitetty V-malli sopii molempien ohjelmistojen kehittämiseen. (10, s.54).



Kuva 15. Ohjelmiston turvallisuuselinkaaren yksinkertaistettu V-malli (10, s.54.)

Seuraavassa luetelmassa on esitetty vaatimuksia ja ohjeita sovellusohjelmistolle ja sen kehittämiselle. (10, s.54.)

- Turvallisuuteen liittyvän ohjelmiston katselmointi
- Työkalujen soveltuvuus. Kirjastojen oltava vaatimusten mukaisia ja ohjelmointikielten valinta standardin IEC 61311-3 mukaiseksi

- Ohjelmiston suunnitteluun tulee kuulua seuraavia: modulaarinen rakenne, ohjelmavuon puolimuodollisia menetelmiä, toimilohkot eivät saa olla liian suuria, yksi tulokohta niin yksi lähtökohta, kolmivaiheinen rakennemalli, turvalähdön asettaminen vain yhteen kohtaan ohjelmassa ja käytetään ulkoisen vikaantumisen paljastamistekniikoita turvallisen tilan aikaansaamiseksi

- turvallisuuteen liittyvän ja liittymättömän ohjelmiston yhdistäminen on koodattava eri toimilohkoihin ja näiden datan välillä ei saa olla mitään loogista yhdistelmää

- toteutettu ohjelmisto ja koodaus on oltava luettavaa, ymmärrettävää ja testattavaa, siihen on käytettävä perusteltuja tai hyväksyttäviä koodausääntöjä, datan eheyden ja mielekkyyden tarkistuksia, testaukseen simulointia ja todentaminen tehtävä ohjaus ja datavuon analyysillä(PL d ja e)

- testaukseen liittyvät vaatimukset on seuraavat: Kelpuutuksessa soveltuva testi ns. ”musta laatikko” –testaus, PL d ja e testaus raja-arvo analyysilla, suositus testaussuunnitelmasta, I/O testauksilla varmistuttava turvallisuuteen liittyvistä signaaleista että niitä käytetään oikein

- dokumentointisäännöistä on vaadittu seuraavaa: dokumenttien moduulien otsakkeissa oltava henkilön nimi, kuvaukset toiminnasta, versiotunnus, sekä riittävästi verkon tai lauseiden kommentteja tai esittelyjä

- todentamiseen esimerkeiksi katselmointi, tarkastus, läpikäynti tai muut sopivat toimenpiteet

- konfiguraation hallinta luotava toimivaksi (erityisen suositeltavaa)

- muutosten jälkeen tehtävä vaikutusanalyysi ja jos käyttöoikeuksia muutetaan, on muutosten tekeminen valvottava ja historia dokumentoitava (10, s.54).

13 Turvatoimintojen dokumentointivaatimukset

Turvallisuuteen liittyvällä dokumentoinnilla varmistetaan riittävät tiedot kaikissa elinkaaren vaiheissa, jotta järjestelmä on toteutettavissa ja hallittavissa. Dokumentointi on edellytys sille, että järjestelmien ja riskin vähennyksen riittävyys voidaan todentaa ja arvioida. Turvallisuuteen liittyvä dokumentaatio muodostetaan omaksi selkeäksi kokonaisuudekseen. Dokumentoitavia asioita ovat suunnitelmat, määrittelyt ja kuvaukset sekä raportit (esim. kokonaisuuden turvallisuussuunnitelma ja toiminnallisen turvallisuuden arviointi). (24, s.10)

Koko konetta koskevat seuraavat dokumentointivaatimukset:

- tulokset vaara- ja riskianalyyseistä, sekä niihin liittyvät lähtötiedot tai oletukset

- turvallisuussuunnitelma (jolla osoitetaan tavoitteisiin pääseminen)

- tiedot turvatoimintojen toteuttamiseen liittyvistä laitteista ja vaatimuksista
- suunnitteluun, käyttöönottoon, testaamiseen sekä kelpuutukseen liittyvät asiat
- menettelyt ja organisaatiot, jotka liittyvät turvatoimintojen toteuttamiseen, käyttöön ja ylläpitoon
- muutosmenettelyyn liittyvät vaatimukset ja toteutukset
- määräaikaiskoestus /-testaus (suunnitelma, ohje ja raportit). (24, s.10)

SFS-EN ISO 13849-1 määrittelee vaatimuksia ohjelmiston dokumentoinnille seuraavasti:

1. Turvallisuuteen liittyvä sulautetun ohjelmiston erittely ja suunnittelu tulee olla dokumentoitu. Ohjelmiston kaikki turvallisuuteen liittyvät toimenpiteet tulee olla dokumentoitu ohjelmiston elinkaaren aikana. (11, s.54)

2. Turvallisuuteen liittyvän sovellusohjelmiston turvatoimintojen erittely ja suunnittelu tulee olla dokumentoitu. (11, s.54)

3. Turvallisuuteen liittyville sovellusohjelmistoille, jotka on tarkoitettu suoritustason PLc-e komponenteille (vaatimus tai suositus) tulee kaikki ohjelmiston elinkaaren aikana tapahtuneet toimenpiteet olla dokumentoitu. Dokumentoinnin on oltava loppuun saatettua, saatavilla olevaa, luettavaa ja ymmärrettävää. Moduulien otsakkeet tulee olla dokumentaatiossa, kuten myös ohjelmoinnin tehneen henkilön tiedot, kuvaukset toiminnasta, tulojen ja lähtöjen kuvaukset, versio, toimilohkojen versio sekä riittävästi kommentteja verkon tai lauseiden esittelyistä. (11, s.54)

Näillä edellä mainituilla dokumenteilla on tarkoitus pitää turvatoimintojen koko elinkaari hallittuna ja seurattavana. Dokumentaatiosta on varmasti hyötyä myöhemmässä vaiheessa, esimerkiksi mikäli koneeseen joudutaan tekemään muutoksia. (11, s.54)

Siemensin distributed safety-ohjelmassa standardien mukainen ohjelmadokumentaatio muodostuu automaattisesti. Turvajärjestelmän tarkistusta varten Siemensin ohjelmistossa on seuraavat toiminnot: (32, s.143)

- hardware-konfiguraation ja parametroinnin tulostus
- turvaohjelmien vertailu

- turvaohjelman tulostus. (32, s.143)

Ohjelmasta saatavat tulosteet sisältävät seuraavan listan mukaiset tiedot ohjelmasta:

- funktiolohkot
- lista turvaohjelman F-lohkoista
- symbolilista
- hardware-konfiguraatio. (32, s.143)

Lisäksi tulosteista löytyy tarkistussumma, S7 Safety-versiotunnus, turvaohjelman tila sekä symbolien tunnus. Olennaisena vaatimuksena dokumentoinnissa on, että olemassa olevan konfiguraation komponentit ja parametrit täsmäävät tulosteen kanssa. (32, s.143)

14 Turvatoimintojen toteutustapavaihtoehdot logiikalla

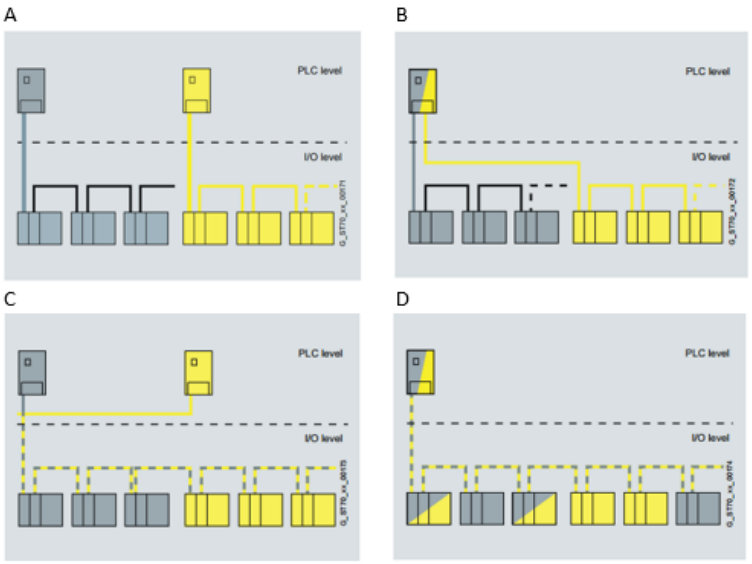
Tässä kappaleessa (ks. 14.2) on esitetty se tapa, jolla turvatoiminnot suositellaan toteutettavan logiikalla. Toteutustapa on valittu pitäen silmällä uusia projekteja, joissa turvatoimintoja toteutetaan logiikalla. Vanhoihin olemassa oleviin sovelluksiin tämä valittu tapa ei välttämättä sovellu, koska sovellukset saattavat poiketa lähtökohtaisesti teknisesti niin paljon, että valitulla tavalla toteutustapa on mahdoton. Satamanostureita on toimitettu jo vuosikymmeniä, joten kaikissa ei välttämättä ole logiikkaa olemassa. Näissä tapauksissa on turvatoimintojen suunnittelu ja arviointi tehtävä kokonaan alusta saakka, mikäli ne halutaan toteuttaa ohjelmoitavalla logiikalla.

14.1 Turva PLC:n toteutustapojen rakennevaihtoehdot

Turva-automaation rakenteen käytännön toteutuksessa on käytettävissä neljä erilaista vaihtoehtoa. Nämä edellä luetellut tavat ovat Siemensin esittämiä ratkaisuja, ja muilla valmistajilla saattaa olla tästä esityksestä poikkeavia järjestelmiä. Seuraavassa luettelossa on esitetty neljä erilaista vaihtoehtoa, jotka ovat käytännössä olemassa olevat vaihtoehdot toteutustavaksi.

- erillinen PLC, I/O ja väylä (ks. kuva A)
- sama PLC, erotetut I/O ja väylä (ks. kuva B)
- yksi väylä, erilliset turva ja vakio PLC (ks. kuva C)
- yksi PLC ja väylä, sulautettu I/O (ks. kuva D) (15, s.12)

Kuvassa 16 on esitetty graafisesti edellä mainitut toteutustavat, jotka ovat mahdollisia toteutustapoja toiminnallisen turvallisuuden toteutuksessa. (15, s.12)



Kuva 16. Neljä erilaista toteutustapaa (15, s.23.)

Tarkastellaan edellä mainituista vaihtoehdoista neljässä seuraavassa kappaleessa kutakin esitettyä eri vaihtoehtoja niiden etujen ja haittojen kannalta.

14.1.1 Vaihtoehto A: Erillinen PLC, I/O ja väylä

Tässä vaihtoehdossa on erotettu vakio- ja turvajärjestelmä kokonaan erilliseksi laitteistoiksi. Laitteistojen välillä ei ole kommunikaatiota lainkaan. Tämän vaihtoehdon hyviä puolia ovat, että turvapuolen esitystapa dokumenteissa yksinkertaista ja komponentit ovat kokonaan erillään mekaanisesti vakiokomponenteista.

Negatiivisiksi puoliksi voidaan lukea seuraavat seikat:

- kommunikointi vakio-PLC:n kanssa ei ole mahdollista.
- väyläkaapeli lisää vakio-PLC:n ja turva-PLC:n välille.
- kaksinkertaistaa väyläkaapeloinnin nykyiseen verrattuna ala-asemien ja vakio/turva-CPU:n välillä.
- yksi CPU lisää, joka kasvattaa kustannuksia.

Tämä edellä esitetty tapa on nk. perinteinen tapa toteuttaa turvatekniikkaa, joka on laajasti prosessiteollisuudessa käytetty toteutustapa. (28, s.23)

14.1.2 Vaihtoehto B: sama CPU, erotetut I/O ja väylä

Tämän vaihtoehdon hyviä puolia ei nosturisovelluksissa ole mainittavissa ainakaan uusissa toteutuksissa. Tämä voi kuitenkin olla hyvin varteenotettava vaihtoehto esimerkiksi modernisaatioissa.

Tämän vaihtoehdon negatiivisiksi puoliksi voidaan lukea väyläkaapeloinnin kaksinkertaistuminen, komponenttien lisääntyminen (mm. CPU), joka puolestaan lisää kustannuksia. Komponentteja tulee lisää myös sen vuoksi, koska etäasemaan, mikäli sellainen on, täytyy asentaa aina sovitinkortti korttipaikkaan ensimmäiseksi.

14.1.3 Vaihtoehto C: Yksi väylä, erilliset turva ja vakio PLC

Tässä vaihtoehdossa hyviä puoli on se, että olemassa olevaa väyläkaapelointia voidaan hyödyntää tiedonsiirrossa. Väyläkaapelointia täytyy rakentaa kuitenkin uusien turvatoimintojen suorittamiseen etäasemien välille, silloin kun on kyseessä hajautettu logiikka. Tämä vaihtoehto C soveltuu erinomaisesti modernisaatioiden toteutukseen.

Vaikka olemassa olevaa väyläkaapelointi voidaan hyödyntää, on uusien etäasemien välille mahdollisesti tehtävä uutta kaapelointia, joka puolestaan lisää kustannuksia. CPU:n lisääminen kasvattaa myös kustannuksia omalta osaltaan.

14.1.4 Vaihtoehto D: Yksi PLC, väylä ja sulautettu I/O

Tämän otsikossa mainitun toteutustavan hyvät puolet ovat seuraavat seikat:

- ei tarvitse lisätä väyläkaapelointia lainkaan, vaan voidaan käyttää olemassa olevaa kaapelointia
- johdotusta tarvitaan vähemmän
- komponenttien määrä ei lisäänny ja siten vältytään ylimääräisiltä kustannuksilta.
- kustannukset eivät lisäänny erillisen turva-CPU:n myötä
- I/O:ta voidaan käyttää vakio I/O:n jatkona, jolloin ei tarvitse lisätä komponentteja kaikissa tapauksissa
- yksinkertainen kommunikointi vakio- ja turvaohjelman välillä
- vähemmän suunnittelutyötä, koska ohjelmointi tapahtuu vakio suunnitteluohjelmalla.

Edellä mainittujen listojen hyvät ja huonot puolet eivät välttämättä kaikki toteudu jokaisessa sovelluksessa. Esimerkiksi modernisaatioissa kohdan 8.3.3 ratkaisu on erittäin hyvä vaihtoehto, koska modernisaatioissa voidaan tällä ratkaisulla helposti hyödyntää olemassa olevaa väylää. Myös turva-CPU:n ja ala-asemien I/O:n lisääminen on selkeää vakio I/O:n rinnalle. Tosin samankaltaisia toimia täytyy suorittaa mm. CPU:lle, oli kyseessä vanhan CPU:n korvaaminen turva CPU:a tai uuden CPU:n lisääminen vanhan CPU:n rinnalle.

14.2 Turvatoimintojen toteutustavan valintaperusteet

Edellisessä kappaleessa vertaillut toteutustavat antavat hyvän kuvan siitä, kuinka eri toteutustavat eroavat toisistaan. Satamanosturi sovelluksissa toteutustavaksi näiden esitettyjen vaihtoehtoisten toteutustapojen välillä, suositeltavaksi toteutustavaksi esitetään edellisissä kappaleissa vertaillun pohjalta vaihtoehtoa D, jossa turva- ja vakio- PLC on sulautettu yhdeksi järjestelmäksi. Tätä toteutustapaa kutsutaan integroiduksi tavaksi. Mikäli tätä toteutustapaa sovelletaan nykyisiin jo olemassa oleviin sovelluksiin, tällöin täytyy varmistaa, että käytetyt komponentit, kuten CPU ja I/O, ovat soveltuvia kyseiseen

kohteeseen. Dokumentointiin liittyen kaikki toteutustavat voidaan esittää yksitiepiirikaaviona samalla tavalla, jossa turvapuoli on eroteltu vakio PLC:tä, joten tässä suhteessa eroja toteutustapojen välillä ei juurikaan ole. Turva CPU:n lisääminen kohtien 14.1.1 ja 14.1.3 tavoin ei ole teknisesti perusteltua, ja sen olemassaolo ei anna teknisessä mielessä sellaista lisäarvoa, joka perusteella CPU:n lisääminen olisi järkevää.

Integroitu turvatekniikka sisältää koko turvaketjun antureista ja toimilaitteista ohjaukseen, mukaan lukien turvavarmennetun kommunikaation vakiokenttäväylällä. Integroitu toteutustapa tarjoaa joustavuutta ja tuottavuutta, koska vakio- ja turva-asemat ovat liitetty yhteiseen väylään, sekä vakio- ja turvakomponentteja voidaan asentaa rinnakkain.

Perinteiseen tapaan, jossa PLC:n turva-ja vakiopuoli ovat täysin toisistaan erotetut ja vaihtoehto C:hen verrattuna, on vaihtoehto D huomattavasti kustannustehokkaampi tapa, verrattuna kokonaan erillisellä turvalogiikalla toteutettuun tapaan. Integroidulla toteutustavalla voidaan turvalogiikkayksiköitä asentaa olemassa olevien asemien perään suoraan, ilman että asennusvaiheessa täytyy pakosta asentaa erillinen laajennusosion vaatimat komponentit. Toki täytyy muistaa, että aina tämä ei ole mahdollista, mikäli kyseessä on jälkeenpäin asennettava asema ja maksimimäärä kortteja on jo asennettu asemaan. Siemensin logiikan ollessa kyseessä suurin korttien määrä yhdessä etäasemassa on kahdeksan. Mikäli korttien määrä on suurempi, on niissä tapauksissa lisättävä laajennusosa, joka sallii korttien määrän lisäämisen.

Mahdollinen modernisointien yhteydessä lisättävä turvalogiikka on aina suunniteltava erikseen kuhunkin sovellukseen vaaditun toteutuksen ja asiakkaan vaatimusten mukaan. Tällöin integroidusta ratkaisusta ei välttämättä ole niin paljon hyötyä tai sitä ei voida toteuttaa halutulla tavalla, koska esimerkiksi tilanpuute saattaa estää kyseessä olevan tavan käytön ja voi olla järkevämpää toteuttaa työ muulla tavalla.

Kussakin edellä esitellyistä vaihtoehdoista logiikkaohjelmistoon täytyy tehdä konfiguraatio käytetyistä komponenteista, joten senkään puolesta käytetyllä rakenteella ei ole valinnan puolesta merkitystä. Kun ohjelmistoa ladataan PLC:n ja rakenteessa on käytetty turvalogiikkaa, Siemensin ohjelma vaatii salasanan, jolla varmistetaan mahdollinen turvatoimintojen hallittu muuttaminen. Mikäli salasanoja ei ole jaettu yleisesti, tämä on hyvä tapa suojata koneen turvatoimintojen hallittu muuttaminen. Salasanalla ohjelman suojaaminen on mahdollista kaikissa edellä esitetyissä vaihtoehdoissa ja suojaus tapahtuu

täysin samalla tavalla. Salasanasuojaus ei ole välttämättä paras mahdollinen tapa suojata ohjelmistoa muutoksilta, koska usein salasana joudutaan luovuttamaan usealle henkilölle projektin aikana ja näin ollen se ei pysy salassa. Ohjelmistossa on kuitenkin olemassa järjestelmä, joka tallentaa tehdyt muutokset ja sieltä voi myöhemmin jäljittää milloin ja mitä ohjelmaan on muutettu.

14.3 Elinkaariajattelu valintaperusteena

Usein ajatellaan, että sähkölaitteistojen kokoonpanossa varsinkaan nostureissa elinkaariajattelulla ei ole kovinkaan suurta merkitystä sähkölaitteiden määrän vähäisyyden vuoksi. On totta, että yhdessä tuotteessa sillä ei olekaan niin suurta merkitystä, mutta mitä enemmän tuotteita tehdään, sitä suuremmaksi elinkaariajattelun merkitys kasvaa. Tässä insinöörityössä toteutustavan valinnalla ei kokonaisuudessa olekaan kovin suurta merkitystä elinkaariajattelun valossa, jos saadaan vähennettyä yksi tai kaksi komponenttia logiikkaohjauksesta, ja ajatellaan vain yksittäistä tuotetta. Toimitettavien järjestelmien määrän kasvaessa, on vähemmillä komponenteilla toteutetun järjestelmän osalta suurempi merkitys myös elinkariajattelun kannalta. Ympäristömyönteisen tuotesuunnittelun perustavoitteena on materiaalien tehokas käyttö, energian käytön minimoiminen, haitallisten aineiden käytön minimoiminen, tuotteen käyttöiän pidentäminen ja kierrätettävyyden parantaminen. Tässä insinöörityössä valitussa toteutustavassa komponenttien määrän minimoimisella saadaan komponenttimäärässä optimaalisin tapa toteuttaa turvatoiminnot ekologisimmalla tavalla. Nosturit ja varsinkin satamanosturit ovat suurikokoisia ja teräksestä valmistettuja koneita. Tämän vuoksi teräsrakenteen osuus on merkittävin myös ympäristövaikutuksiltaan. Turvatoimintojen toteutuksessa komponenttimäärien pienentäminen koskee logiikkayksiköitä, joten ympäristövaikutus teräsrakenteen ja logiikkayksiköiden välillä on huomattavan suuri. Kuitenkin ajatellen sitä, mitä valmistusmateriaaleja elektroniikassa on käytetty, kuten kultaa, hopeaa ja muita harvinaisia mineraaleja, ympäristövaikutuserot alkavat merkitsemään enemmän. Tuotteen elinkaaren loppuvaiheessa myös materiaalien kierrätettävyydellä on merkitystä, koska elektroniikkakomponenttien kierrätys on haastavaa. Usein elektroniikka jäte päätyy muun jätteen sekaan, mikä ei suurempien määrien ollessa kyseessä, ole kovin ekologista. (27, s.6)

14.4 Valintaperuste asiakkaan näkökulmasta

Turvatoimintojen toteutusmallissa asiakkaan näkökulmasta yksi kriteeri on, että laitteisto on tehty tavalla, joka on käytössä muillakin valmistajilla. Tämä antaa asiakkaalle varmuutta siitä, että toteutustapa on koettu hyväksi tavaksi yleisemmällä tasolla. Toisena kriteerinä on järjestelmän laajennettavuus ja muunneltavuus. Laajennettavuus ja muunneltavuus ovat tärkeitä ajatellen koko laitteistoa elinkaaren kannalta, jolloin myöhemmässä vaiheessa tulleet mahdolliset muutostarpeet on helpompi toteuttaa. Luotettavuuden osalta asiakkaan näkökulma on selkeä. Mitä luotettavammalla tavalla toiminnot on tehty, sen parempi se on asiakkaalle. Mikäli komponenttien määrää voidaan laitteistossa vähentää, sen parempi se on asiakkaalle, koska vikaantuvia komponentteja on tällöin vähemmän. Siirryttäessä suurella komponenttimärällä toteutetusta laitteistosta ohjelmalliseen toteutukseen, on tällöin etuna laitteiston toimintavarmuus, koska ohjelmistojen vikaantuminen on harvinaisempaa, kuin mekaanisten tai sähkömekaanisten komponenttien vikaantuminen. Ohjelmallisesti oikealla laitteiston toteutustavalla toteutetun laitteen etuna on taloudellisuus, luotettavuus ja turvallisuus.

15 Yhteenveto

Tässä insinöörityössä päätavoitteena oli löytää parhaiten soveltuva vaihtoehto turvatoimintojen toteutustavaksi satamanostureissa turvatoimintojen määrittämisen jälkeen. Aiheena tämä oli erittäin mielenkiintoinen ja haastava, koska aihealue on laaja ja sovellettavia standardeja on paljon. Tosin kirjallisuutta ei aiheesta kovin montaa kirjaa ollut saatavilla, mutta verkkodokumentteja puolestaan senkin edestä. Varsinaista sovellusta turvatoimintojen soveltamisesta ei tämän insinöörityön aikana ollut aikaa tehdä, koska aiheena toteutus on laaja ja vaatii paljon aikaa. Mielestäni paras vaihtoehto tavasta toteuttaa turvatoiminnot kuitenkin tuli hyvin esille tässä insinöörityössä vertailemalla eri vaihtoehtoja keskenään ja soveltuvin ehdotettu valinta voitaisiin tehdä tässä insinöörityössä esitettyjen kriteerien perusteella. Tämän insinöörityön teon aikana tehtiin myös ohje turvatoimintojen toteutuksesta sekä dokumentaatio erään projektin turvatoiminnoista. Näiden soveltaminen jatkossa on todennäköistä, koska turvatoimintoja tullaan suunnittelemaan ja dokumentoimaan standardien mukaisesti. Turvatoimintoihin liittyy paljon muutakin direktiivien ja standardien lisäksi, joita tulee tai suositellaan noudatettaviksi tässä insinöörityössä esitellyn lisäksi.

Turvatoimintoihin ja niiden toteutukseen kiinnitetään asiakkaiden puolelta entistä enemmän huomiota myös asiakkaiden puolelta. Tämän vuoksi turvatoimintojen tekninen toteutustapa ja perusutelut ovat tulossa merkittävämpään osaan koneiden ja laitteiden toiminnan kannalta. Tämän vuoksi suosittelen turvatoimintojen toteutuksen kehittämisen jatkamista ohjelmoitavalla logiikalla vaadittujen teknisten ehtojen mukaan vaadittuun suoritustasoon. Tekniikan ja sovellusten kehittyessä, on mielenkiintoista nähdä, mihin suuntaan asetusten vaatimukset ja standardien ehdotukset, sekä tekniset ratkaisut kehittyvät tulevaisuudessa turvatoimintojen osalta, niin tekniikan alalla yleensä kuin KC:llä.

Lähteet

1 Taloussanomat lehdistötiedote 11.8.2015. Verkkodokumentti. <http://www.taloussano.mat.fi/porssi/2015/08/11/konecranes-ja-terex-yhdistyvat/201510122/170>. Luettu 20.8.2015.

2 Konecranes yritysesittely. PPTX -sarja yrityksen markkinointimateriaalista.

3 Suomen standardoimisliitto. Verkkodokumentti. <http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/mihin_standardeja_tarvitaan>. Luettu 15.8.2015.

4 Työsuojeluhallinto. Koneturvallisuus, koneiden tekniset vaatimukset ja vaatimustenmukaisuus. Verkkodokumentti. <http://www.tyosuojelu.fi/upload/tso_16-2009.pdf>. Luettu 15.9.2015.

5 Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY 17.5.2006.

6 Suomen standardoimisliitto. Verkkodokumentti. <http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/mihin_standardeja_tarvitaan>. Luettu 15.8.2015.

7 METSTA teemasivut. Koneturvallisuuden standardien suhde lainsäädäntöön. Verkkodokumentti. <http://www.metsta.fi/www/koneturvallisuuden_teemasivut/standardisointi/01-03-00.php>. Luettu 21.9.2015.

8 Suomen standardoimisliitto. SFS-EN 13135: Nosturit. Turvallisuus. Suunnittelu. Laitteita koskevat vaatimukset. Helsinki 15.4.2013.

9 Siemens esite: Easy Implementation of the European machinery directive. Verkkodokumentti. <https://www.automation.siemens.com/cd-static/material/info/e20001-a230-m103-v2-7600.pdf>. Luettu 5.8.2015.

10 VTT Tutkimusraportti VTT-R-04369-10. Verkkojulkaisu<VTT Tutkimusraportti VTT-R-0439-10>. Luettu 5.6.2015.

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

12 Siemens-Industrial controls materiaali. Verkkodokumentti. <www.siemens.com/sirius/infomaterial>. Luettu 22.8.2015.

13 Siemens internetsivut. Verkkodokumentti. <http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/kone_ja_prosessiturvallisuus_seka_atex/koneturvallisuus/simatic_turva_automaatio/turvalogiikat.htm>. Luettu 12.7.2015.

14 Siemens-Industrial controls materiaali. Verkkodokumentti. <www.siemens.com/sirius/infomaterial>. Luettu 15.9.2015.

15 Siemens-esite turva-automaatiosta. Verkkodokumentti. <http://www.automation.siemens.com/salesmaterial-as/brochure/en/brochure_safety_integrated_for_factory_automation_en.pdf>. Luettu 10.6.2015.

16 Taajuusmuuttajan integroidut turvatoiminnot. Verkkodokumentti. Siemens esite. <http://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/product-portfolio/drive-technology/safety-functions/pages/safe-torque-off.aspx>. Luettu 15.10.2015.

17 Harri Ylä-Soininmäki. 2006. Konecranes sisäinen esitys: Analysis of crane safety functions,

18 Siemens manuaali turvareleistä. Verkkodokumentti <https://support.industry.siemens.com/cs/attachments/67585885/manual_safety_relay_3SK1_en-US.pdf?download=true>. Luettu 1.6.2015.

19 Metsta teemasivut. Verkkodokumentti. <http://www.metsta.fi/www/koneturvallisuuden_teemasivut/standardisointi/index.php>. Luettu 15.9.2015.

20 Suomen standardointiliitto. Standardit tutuksi. Verkkodokumentti. <http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/sfs_en_iso>. Luettu 15.9.2015.

21 SFS-EN 62061 Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Helsinki 26.9.2005.

22 Valtioneuvoston asetus. VNa 400/2008. Verkkodokumentti. < http://www.edilex.fi/saadoskokoelma/20080063.pdf>. Luettu 20.10.2015.

23 Marita Hietikko, Timo Malm & Jarmo Alanen VTT tiedote 2485. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Verkkodokumentti. <http://www.vtt.fi/inf/pdf/tiedotteet/2009/T2485.pdf>. Luettu 16.6.2015.

24 Turvatekniikan keskus. Tukes opas. Verkkodokumentti <http://www.tukes.fi/Tiedostot/kemikaalit_kaasu/Turva-automaatio_prosessiteollisuudessa.pdf>. Luettu 10.6.2015.

25 Suomen standardoimisliitto. Standardi SFS-EN ISO 13850 Koneturvallisuus. Hätäpysäytys. Turvallisuusperiaatteet. Helsinki 24.11.2008.

26 Suomen standardoimisliitto Standardi SFS-EN 60204-32 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 32:Vaatimukset nostokoneille. Helsinki 24.11.2008

27 FIMECC_Result Publications_1_2014_Elinkaariarviointi tuotesuunnittelussa_0.pdf. Verkkodokumentti. < https://www.teknologiainfo.net/fi/content/elinkaariarviointi-tuotesuunnittelussa-opas-metalli-ja-konepajateollisuudelle>. Luettu 30.9.2015.

28 Siemens esite SIMATIC Safety Integrated for Factory Automation. Verkkodokumentti<http://www.industry.siemens.com/topics/global/en/safety-integrated/pages/functional-safety.aspx>. Luettu 23.8.2015.

29 PROFIsafe_system_description_v_2010_English.pdf. Verkkodokumentti <http://www.profibus.com/nc/pi-organization/regional-pi-associations/homepage-italia/downloads/downloads/profisafe-technology-and-application-system-description/display/>. Luettu 10.6.2015.

30 Siirilä, Tapio. 2009. Koneturvallisuus, Ohjausjärjestelmät ja turvalaitteet III. Luettu 22.5.2015.

31 Suomen standardoimisliitto. SFS-EN 61508-3 Sähköisten/Elektronisten/Ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 3: Ohjelmistovaatimukset.

32 Siemens koulutusmateriaali. ArtikkeliSiemensKoulutusmateriaali.pdf. Luettu 12.11.2015.

33 Tapio Siirilä ja Tuiri Kerttula 2007. Koneturvallisuuden perusteet. Luettu 15.7.2015.

34 Internet. Verkkodokumentti <http://www.digchip.com/datasheets/5497611-sirius-3sk1-safety-relays.html>. Luettu 15.11.2015.

35 Siemens osakeyhtiö. S3K1 Turvareleen peruskytkennät. Verkkodokumentti <http://www.siemens.fi/pool/products/industry/iadt_is/tuotteet/kone_ja_prosessiturvallisuus_seka_atex/koneturvallisuus/turvareleet_ja_hatapysaytys/3sk1_kaeyttoe_ja_asennusohje_v1_3_fi.pdf>. Luettu 13.8.2015.

36 Siemens. Automaatiokoulutus, Distributed safety projektointi ja ohjelmointi. Luettu 7.8.2015.

37 Siemens. Automation system S7-300 Fail-Safe SIgnal modules. Verkkodokumentti <https://www.automatyka.siemens.pl/docs/docs_ia/S7300_Fail-Safe_Modules_e.pdf>. Luettu 28.7.2015