TURVAJÄRJESTELMÄN SUUNNITTELU OPETUSKÄYTTÖÖN

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Sähkö- ja automaatiotekniikka, Valkeakoski

Syksy 2020

Tuomas Vänni

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Sähkö- ja automaatiotekniikka Tiivistelmä

Valkeakoski

Tekijä	Tuomas Vänni	Vuosi 2020
Työn nimi	Turvajärjestelmän suunnittelu opetuskäyttöön	
Ohjaajat	Mika Oinonen, Juha Sarkula	

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli suunnitella turvajärjestelmä opetuskäyttöön Hämeen ammattikorkeakoulun Valkeakosken kampukselle, käyttäen standardien mukaisia ohjeita. Tavoitteena oli myös, että turvajärjestelmä voidaan toistaa opinnäytetyön avulla.

Opinnäytetyön aikana käydään läpi turvajärjestelmiin liittyviä standardeja. Opinnäytetyössä käsitellään tarkasti riskinarviointia ja turvallisuuden tason määrittelyä. Riskinarviointia tarkastellaan standardien EN ISO 13849-1 ja EN IEC 62061 avulla. Opinnäytetyön aikana esitellään turvajärjestelmiin liittyviä komponentteja, sekä käydään TwinCAT 3- ja TwinSAFE-ohjelmointia läpi.

Opinnäytetyön aikana saadaan hyvä käsitys turvajärjestelmien standardeista ja huomataan, kuinka vaativia ne ovat. Työn lopputuloksena on oikein suunniteltu ja toteutettu turvajärjestelmä, joka on tehty käyttäen turvavalopuomeja. Uskon opinnäytetyöstä olevan hyötyä opiskelijoille turvajärjestelmiin tutustumisessa.

Avainsanat	Riskinarviointi, turva-automaatio, turvajärjestelmä
Sivut	44 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Electrical and Automation Engineering
Valkeakoski

Abstract

Author Tuomas Vänni
Year 2020

Subject Design of a safety system for educational purposes

Supervisors Mika Oinonen, Juha Sarkula

ABSTRACT

The aim of the project was to design a safety system for educational purposes to the use of Häme University of Applied Sciences Valkeakoski campus by using instructions defined in the standards of the machine safety. The aim was that the safety system could be replicated with the help of the project.

During the project, standards related to safety systems were examined. This thesis studies risk assessment and determines the safety level of a safety system in detail. Risk assessment is examined using the standards EN ISO 1349-1 and EN IEC 62061. During the project, common components related to safety systems and programming with TwinCAT 3 and TwinSAFE were studied.

During the project, a good understanding of the standards of the safety systems was gained by the author and this thesis also illustrates how demanding they are. The result of the project is a properly designed and built safety system, made using safety light barriers. I believe that this thesis will be useful for engineering students when getting acquainted with safety systems.

Keywords Risk assessment, safety automation, safety system

Pages 44 pages

Sisällys

Kuvat, taulukot ja kaavat

1 Johdanto

Opinnäytetyön tavoitteena on suunnitella turvajärjestelmä opetuskäyttöön Beckhoffin turvalogiikalla ja SICKin turvavalopuomeilla, joka voidaan yhdistää robottiin ja esimerkiksi hidastaa kyseisen robotin liikkeitä turvallisuuden vuoksi. Opinnäytetyö toteutetaan käyttäen koneturvallisuus standardeja.

Turvajärjestelmät ovat erittäin tärkeitä prosessiteollisuudessa ja tuotantojärjestelmissä, missä voi olla vaaralliset olosuhteet, sekä nopeita ja vaarallisia liikeitä tekeviä laitteita. Opinnäytetyö tarjoaa tietopohjaa turvajärjestelmiin ja niiden standardeihin.

Opinnäytetyö toimii oppaana opiskelijoille turvajärjestelmän suunnittelussa ja toteuttamisessa, jonka pohjalta projekti voidaan toistaa. Ohjelmointi toteutetaan Beckhoffin TwinCAT-ohjelmistolla, mitä käytetään usein koulussa.

Opinnäytetyö on rajattu keskittymään turvajärjestelmään ja aiheeseen liittyviin komponentteihin, sekä ohjelmointiin. Opinnäytetyössä ei asenneta tai ohjelmoida robottia, mikä voidaan halutessa liittää myöhemmin työhön.

Tavoitteena opinnäyteyön aikana on oppia ymmärtämään yleisesti turvajärjestelmiä ja laitteita, sekä saada tietopohjaa turvajärjestelmien suunnitteluun ja toteutukseen standardien avulla. Tavoitteena on myös oppia käyttämään TwinCAT-ohjelmiston TwinSAFE-osuutta, mitä tarvitaan turvajärjestelmien toteutuksessa. Työn aikana opetellaan myös turvajärjestelmän riskinarviointimenetelmiä, sekä tutustutaan turvajärjestelmän komponenttien vaatimuksiin.

Tilaajan eli Hämeen ammattikorkeakoulun Valkeakosken kampuksen tavoitteina opinnäytetyössä on saada esimerkkijärjestelmä opetuskäyttöön. Työn tavoitteisiin kuuluu turvajärjestelmän oikeaoppinen suunnittelu, sekä avata työn aikana standardeja, mitkä liittyvät turvajärjestelmiin.

2 Turvajärjestelmien perusteet

2.1 Turvajärjestelmä

Turvajärjestelmien tärkeys kasvaa vuosi vuodelta ja ne vaikuttavat merkittävästi erilaisten prosessien ja laitteiden turvallisuuteen. Turva-automaatiojärjestelmän tehtävänä on vakavissa vaara- tai häiriötilanteissa pysäyttää laitteet ja prosessi tai vaihtoehtoisesti ohjata liikkuvat laitteet turvalliseen tilaan. Turva-automaatiojärjestelmä ottaa ohjat käsiinsä, mikäli käyttöautomaatiojärjestelmä lakkaa jostain syystä toimimasta. Turvajärjestelmän toimivuus on erittäin tärkeää, sillä jos turvajärjestelmä pettää, niin jälkiseurauksina voi olla pahoja ympäristö-, laitteisto- tai henkilövahinkoja. (Tukes, 2007, s. 3)

Turva-automaatiojärjestelmä toimii varautumismenetelmänä toiminnallisessa turvallisuudessa, millä tarkoitetaan järjestelmien ja laitteiden suunniteltua ja ennakoitua toimintaa osana kokonaisturvallisuutta. Toiminnallinen turvallisuus on riittävä, kun kaikki laitteet ja järjestelmät toimivat kuten on suunniteltu ja luotettavasti, eivätkä aiheuta mitään lisävaaroja. (Tukes, 2007, s. 4)

Tukesin (2007, s. 4) dokumentissa on lueteltu turva-automaatiojärjestelmille asetettuja vaatimuksia, tässä osa näistä vaatimuksista.

- Turva-automaatiojärjestelmän tulee toimia käyttöautomaatiosta riippumatta.
- Vikatilanteessa toimilaitteet pysähtyvät tai siirtyvät määritettyyn vaarattomaan tilaan.
- Järjestelmän täytyy toimia tarpeeksi suurella varmuudella virheettömästi vaaratilanteessa, joka voi sattua laitoksen elinkaaren aikana vain kerran.
- Prosessissa täytyy olla mahdollisuus käsikäyttöiseen pysäytykseen, joka on järjestelmästä riippumaton.
- Järjestelmästä ei saa aiheutua vaarallisia ja turhia pysäytyksiä tai alasajoja.

Koneen tai laitteen valmistajan/valtuutetun edustajan on varmistettava, että riskinarviointi suoritetaan. Riskinarvioinnin avulla koneeseen voidaan määrittää sovellettavat terveys- ja

turvallisuusvaatimukset. Kone on tämän jälkeen valmistettava ja suunniteltava riskinarvioinnin tulokset huomioon ottaen. (Konedirektiivi 42/EY/2006)

Riskinarviointi ja riskin pienentäminen on toistuva prosessi, minkä aikana koneen valmistajan tai tämän valtuutetun edustajan tehtävinä ovat seuraavat asiat. (Konedirektiivi 42/EY/2006)

- Koneen raja-arvot tulee määrittää, mihin sisältyy koneen asianmukainen käyttö ja ennakoitavissa oleva väärinkäyttö.
- Koneen mahdolliset vaarat ja niihin liittyvät vaaratilanteet on tunnistettava.
- Riskin suuruus täytyy arvioida ottaen huomioon mahdolliset vammat ja terveyshaitat, sekä niiden vakavuus ja todennäköisyys
- Arvioida riskin merkitys, että voidaan määrittää, täytyykö riskiä pienentää konedirektiivin tavoitteiden mukaisesti.
- Vaarat tai näihin vaaroihin liittyviä riskejä on pienennettävä tai poistettava soveltamalla suojaustoimenpiteitä.

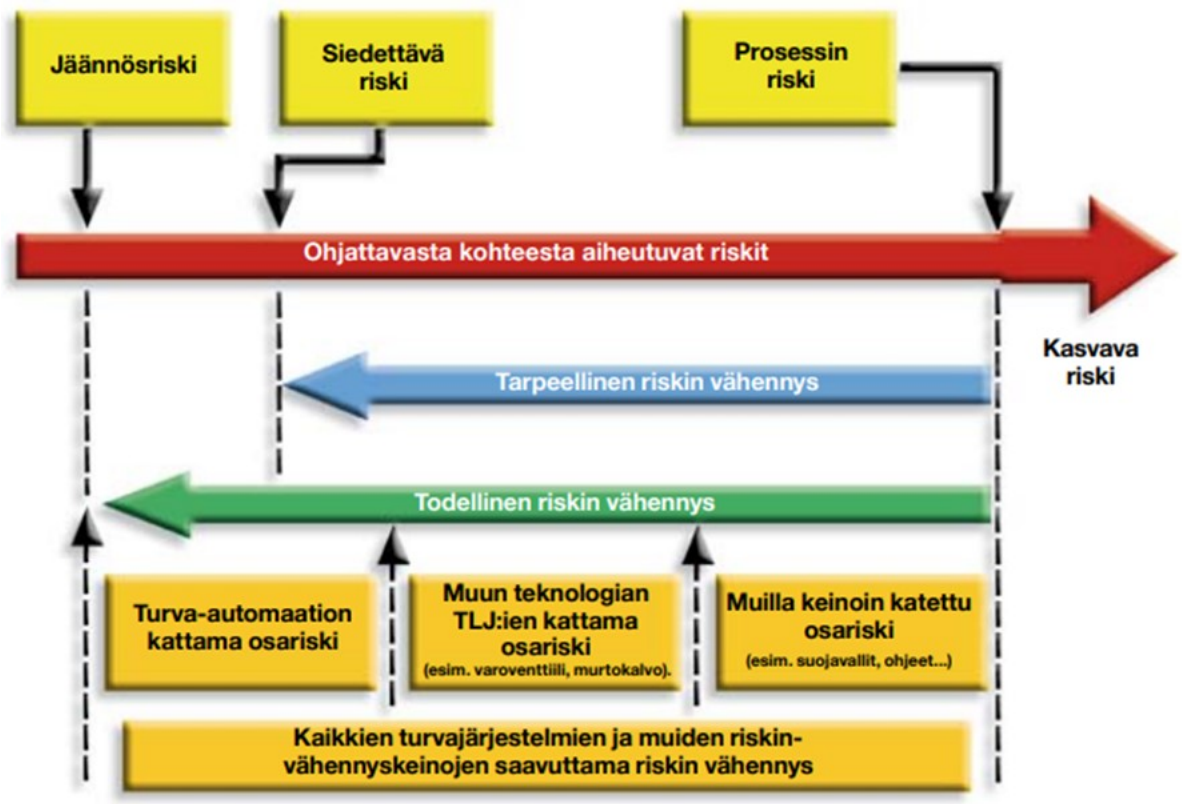
Konetta suunniteltaessa ja valmistettaessa on otettava huomioon, että kone soveltuu tarkoitukseensa, sekä sitä voidaan käyttää ja huoltaa vaarantamatta henkilöitä, kun toimitaan ohjeiden mukaisesti ja huomioitava myös kohtuudella ennakoitava väärinkäyttö. Riskin poistaminen on toteutettava koneen koko ennakoitavan elinkaaren ajalle, mukaan lukien mm. kuljetus- ja romuttamisvaihe. (Konedirektiivi 42/EY/2006)

Valittaessa tarkoituksenmukaisia ratkaisuja, valmistajan tai tämän valtuutetun edustajan täytyy noudattaa seuraavia periaatteita. Ensimmäisenä on poistettava tai pienennettävä riskejä niin paljon kuin mahdollista koneen turvallisella suunnittelulla ja rakenteella. Seuraavaksi on toteutettava suojaustoimenpiteet riskeille, joita ei voida poistaa. Lopuksi valmistajan täytyy tiedottaa koneen käyttäjälle mahdollisista jäännösriskeistä ja ilmoitettava, vaaditaanko koneen käyttöön erikoiskoulutusta, sekä määritellä henkilösuojainten tarve. (Konedirektiivi 42/EY/2006)

Riskinarviointi ja niihin varautuminen toimii usein lähtökohtana, kun suunnitellaan turvajärjestelmää prosessilaitokselle tai vaaralliselle laitteelle. Vaarallisemmat prosessit ja laitteet vaativat riskin vähennykseltä enemmän luotettavuutta ja turvajärjestelmän

riittävyyden osoittamista. Turva-automaatio on kuitenkin vain osa turvajärjestelmän kokonaisriskin vähentämistä, mihin kuuluu esimerkiksi erilaiset fyysiset suojat. Kuva 1 esitetty yleiset periaatteet mitä tulee riskin vähennykseen. (Tukes, 2007, s. 5)

Kuva 1. Riskin vähennys: yleiset periaatteet. (Tukes 2007, s. 5).



2.2 Standardit

Standardit, joiden etuliitteenä on EN, voidaan käyttää koko Euroopassa. Koneturvallisuutta koskevat EN-standardit jaetaan kolmeen ryhmään A-, B- ja C-tyypin standardeihin. A-tyyppi on perusstandardi, jossa käsitellään suunnittelua, turvallisuuden perusstandardeja ja työmenetelmiä, jotka koskevat kaikkia laitteita. B-tyyppi on ryhmästandardi, joka keskittyy turvapuoleen ja suojaaviin laitteisiin, joita voidaan käyttää useissa laitteissa ja koneissa. B-tyyppi jaetaan vielä B1- ja B2-luokkiin, B1 koskee erityisiä turvallisuusnäkökohtia, kuten turvaetäisyyksiä ja B2 puolestaan koskee turvallisuuteen liittyviä laitteita, kuten hätäseis- ja kaksin käsinohjauksia. C-tyyppi on tuotestandardi, joka keskittyy tiettyjen laitteiden tai laiteryhmien turvallisuusvaatimuksiin. (SICK, 2015a, s. 11–14)

Toiminnallisen turvallisuuden kattostandardi EN 61508 käsittelee turvallisuuteen liittyvien sähköisten- , ohjelmoitavien- ja elektronisten järjestelmien toiminnallista turvallisuutta. Standardista EN 61508 on johdettu standardit EN ISO 13849-1 ja EN 62061. Standardilla EN ISO 13849-1 kuvataan ohjausten turvalaitteiden rakennetta ja standardin avulla voidaan määritellä suorituskykytaso (PL). EN 62061 standardi määrittelee toiminnalliset turvallisuusnäkökulmat turvallisuuteen liittyville sähköisille- , ohjelmoitaville- ja elektronisille järjestelmille. EN 62061 standardilla voidaan määritellä myös turvallisuuden eheystaso (SIL). (Phoenix Contact, n.d.)

Valmistajan tuodessa laitetta tai konetta Euroopan markkinoille, täytyy laitteesta löytyä CE-merkintä. Laite tai kone voi saada CE-merkinnän, jos se noudattaa konedirektiivin olennaisia terveys- ja turvallisuusmääräyksiä. Kuva 2 on standardin mukainen CE-merkki. (SICK, 2015a, s. 8)

Kuva 2. CE-merkintä. (Tukes 2014).

2.3 Riskinarviointi

Riskinarviointi voidaan toteuttaa standardin EN/IEC 62061 SIL-riskinarviointimenetelmällä, mikä olisi hyvä suorittaa järjestelmän kaikille vaaroille, joissa riskiä tulisi pienentää. SIL eli turvallisuuden eheysluokitus, saadaan SIL-matriisista, jota ennen täytyy arvioida vamman vakavuus, vaaralle altistumisen kesto, vaaran aiheuttaman tapahtuman todennäköisyys ja mahdollisuus välttää tai rajoittaa vahinkoa. Taulukko 1 on vamman vakavuuden arviointi luokat. (Pilz, n.d.a)

Taulukko 1. Vakavuuden luokittelu. (Pilz n.d.a).

Vaikutus	Vakavuus (S)
Peruuttamaton: kuolema, silmän tai käsien menetys	4
Peruuttamaton: murtuneet raajat, yhden/useamman sormen menetys	3
Peruuntuva: vaatii lääkärin hoitoa	2
Peruuntuva: vaatii ensiapua	1

Taulukko 2 on luokitukset vaaralle altistumisen kestolle.

Taulukko 2. Vaaralle altistumisen taajuus ja/tai kesto. (Pilz n.d.a).

Altistumisen taajuus	Kesto (F) > 10 m
<= 1 h	5
> 1 tunti - <= 1 päivä	5
> 1 tunti - <= 2 viikkoa	4
> 2 viikkoa - <= 1 vuosi	3
> 1 vuosi	2

Taulukko 3 luokitellaan vaarallisen tapahtuman todennäköisyydet.

Taulukko 3. Todennäköisyyden luokittelu. (Pilz n.d.a).

Tapahtuman todennäköisyys	Todennäköisyys (W)
Erittäin todennäköinen	5
Todennäköinen	4
Mahdollinen	3
Harvinainen	2
Ei merkittävä	1

Taulukko 4 on luokiteltu vahingon välttämisen tai rajoittamisen mahdollisuudet.

Taulukko 4. Vahingon välttämisen tai rajoittamisen luokittelu. (Pilz n.d.a).

Mahdollisuus välttää tai rajoittaa vahinkoa	Välttäminen ja rajoittaminen (P)
Mahdoton	5
Harvinainen	3
Todennäköinen	1

SIL-luokitus määritetään edellisten taulukoiden avulla. SIL-matriisiin sijoitetaan ensiksi vahingon vakavuus, jonka jälkeen lasketaan luokka (K) Kaava 1.

Kaava 1. SIL-luokituksen laskenta.

$$K = F + W + P$$

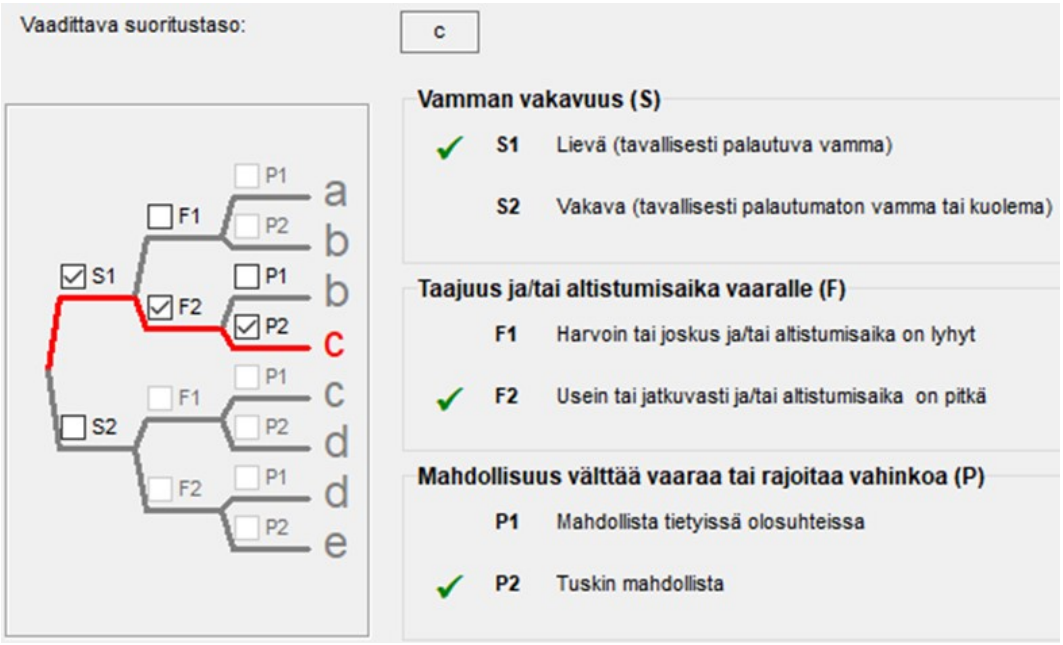
Missä, F on vahingon kesto, W on vahingon todennäköisyys ja P on vahingon välttäminen. Taulukko 5 on SIL-matriisi, josta saadaan SIL-luokitus.

Taulukko 5. SIL-matriisi. (Pilz n.d.a).

Vakavuus (S)	Luokka (K) 3 – 4	Luokka (K) 5 – 7	Luokka (K) 8 – 10	Luokka (K) 11 – 13	Luokka (K) 14 – 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3			SIL 1	SIL 2	SIL 3
2				SIL 1	SIL 2
1					SIL 1

Vaadittu riskinarviointi voidaan suorittaa myös, EN ISO 13849-1 standardin avulla, josta saadaan PL-taso eli suorituskykytaso. PL-tasot jaetaan viiteen eri kategoriaan a - e, joista PL ”a” on matalin ja PL ”e” korkein. PL-riskinarviointi on hyvin samanlainen kuin SIL-riskinarviointi ja ne ovatkin verrattavissa toisiinsa. Kuva 3 on SISTEMA ohjelmistotyökalun PL-riskigraafi. (Pilz, n.d.b)

Kuva 3. PL-riskigraafi.



Arvioitaessa turvallisuuteen liittyvän ohjausjärjestelmän suoritustasoa, katsotaan käsitettä PFHd eli keskimääräistä vaarallisen vian todennäköisyyttä tunnissa. Komponenttien luotettavuutta taas mitataan MTTFd-arvolla, joka tarkoittaa keskimääräistä aikaa vaaralliseen vikaantumiseen. Näillä arvoilla voidaan tarkistaa, onko laitteet ja järjestelmät tarpeeksi luotettavia. Taulukko 6 nähdään PL- ja SIL-tasojen vastaavuus. (Sundquist, 2011, s. 13)

Taulukko 6. Suoritustason PL ja eheystason SIL vastaavuus. (VTT, 2009, s. 19).

Suoritustaso (PL)	Keskimääräinen vikaväli (vuotta)	Keskimääräinen vaarallisen vian todennäköisyys tunnissa (1/h)	Vastaavuus eheystasoihin (SIL)
a	1,14–11,4	$10^{-5} \leq PFH_d < 10^{-4}$	ei
b	11,4–38,1	$3 \cdot 10^{-6} \leq PFH_d < 10^{-5}$	1
c	38,1–114	$10^{-6} \leq PFH_d < 3 \cdot 10^{-6}$	1
d	114–1412	$10^{-7} \leq PFH_d < 10^{-6}$	2
e	1142–11416	$10^{-8} \leq PFH_d < 10^{-7}$	3

Turvallisuuteen liittyvillä dokumenteilla voidaan varmistaa riittävät tiedot laitoksen koko elinkaaren aikana, että järjestelmä on hallittavissa. Järjestelmien ja riskin vähennyksen riittävyys voidaan todentaa ja arvioida näistä dokumenteista. Dokumentointi pitää koostaa seuraavista aiheista: raportit, suunnitelmat, kuvaukset ja määrittelyt. Tarvittavia

dokumentteja ovat esimerkiksi kokonaisuuden turvallisuussuunnitelma, vaara- ja riskianalyysien tulokset, sekä määräaikaistestaus suunnitelma, ohjeistus ja raportti. (Tukes, 2007, s. 10)

2.4 Turvajärjestelmän turvallisuuden tason määrittäminen

Turvajärjestelmän turvallisuuden taso voidaan määritellä ja tarkistaa kahdella eri menetelmällä: standardin EN ISO 13849-1 suoritustasolla PL ja standardin EN IEC 62061 turvallisuuden eheysluokituksella SIL. Turvallisuuden taso voidaan määritellä molemmille standardeille PFHd-arvojen mukaan, jos valmistaja ei ole antanut PFHd-arvoja valmiiksi, voidaan turvallisuuden taso määritellä laskemalla yksityiskohtaisesti tiettyjen muuttujien ja arvojen mukaan. (SICK, 2015a, s. 126–134)

2.4.1 EN ISO 13849-1

Turvallisuuteen liittyvä järjestelmä voi rakentua monista eri alijärjestelmistä, sekä erilaisista komponenteista ja komponenteilla voi olla monia eri valmistajia, jos turvajärjestelmän kaikille komponenteille ei ole saatavissa PFHd-arvoja, voidaan turvallisuuden taso määrittää seuraavilla arvoilla. (SICK, 2015a, s. 126)

- Category eli kategoria, jolla tarkoitetaan järjestelmän rakennetta.
- MTTFd eli keskimääräinen vaarallisen vikaantumisen aika.
- Diagnostic coverage (DC) eli diagnostinen kattavuus.
- Common cause failure (CCF) eli yhteisvikaantuminen.
- Testing eli testaus, sisältää komponenttien ja ohjelmiston testaamisen.

Turvajärjestelmän kategoria eli rakenne on yleensä yksi- tai kaksikanavainen, ellei järjestelmälle ole tehty mitään ylimääräisiä varotoimenpiteitä. Yksikanavainen järjestelmä vastaa vikoihin yleensä vaarallisella vialla. Viat voidaan havaita, lisäämällä järjestelmään testaus komponentteja tai lisäämällä järjestelmään tuen kaksikanavaiselle järjestelmälle. Turvajärjestelmän kategorialle voidaan määrittää luokka B, 1, 2, 3 tai 4. Kategoriat B ja 1

luottavat vahvasti valittuihin komponentteihin, kun taas kategoriat 2, 3 ja 4 määritellään järjestelmän rakenteella. Kategoriaan B päästään, kun turvajärjestelmän kaikki komponentit ja laitteet on rakennettu, asennettu, valittu ja liitetty järjestelmään standardin mukaan. Kategorian B vaatimukset pätevät, myös kaikkiin muihin kategorialuokkiin ja ylemmät luokat vaativat enemmän testaus laitteita tai toisen kanavan. (SICK, 2015a, s. 127)

Keskimääräisellä vaarallisen vikaantumisen ajalla (MTTFd) kuvataan arvoa, joka ilmaisee komponentin todennäköisyyttä vikaantua vaarallisesti, komponentin koko elinaikana, koko alijärjestelmän elinaika on aina lyhyempi. MTTFd voidaan laskea koko järjestelmälle, käyttäen komponenttien arvoja apuna. MTTFd-arvo on rajattu suurimmillaan sataan vuoteen, ettei liian suuret arvot vääristä järjestelmän luotettavuutta. (SICK, 2015a, s. 128)

MTTFd-arvo voidaan luokitella kolmeen ryhmään, matala 3 – 10 vuotta, keskimääräinen 10 – 30 vuotta ja korkea 30 – 100 vuotta. MTTFd-arvo voidaan saada suoraan valmistajalta, mutta jos valmistaja ei kyseistä lukua ilmoita, voidaan se laskea B10d-arvolla, millä tarkoitetaan laitteen toimintakertojen määrää, jonka jälkeen 10 % laitteista vikaantuu. MTTFd-arvo lasketaan Kaava 2 B10d-arvon avulla. (Alanen, Hietikko & Malm, 2009, s. 20)

Kaava 2. MTTFd-arvon lasku B10d-arvon avulla.

$$\mathrm{MTTFd} = \frac{B10d}{0{,}1 * n_{op}}$$

Kaavan $\mathrm{n_{op}}$ tarkoittaa kuinka monta keskimääräisiä toimintakertoja vuodessa laitteella on. Arvo $\mathrm{n_{op}}$ voidaan myös laskea käyttämällä Kaava 3.

Kaava 3. Laitteen keskimääräisten toimintakertojen lasku vuodessa.

$$\mathrm{n_{op}} \frac{\mathrm{d_{op}} * \mathrm{h_{op}} * 3600\ \mathrm{s/h}}{\mathrm{t_{cycle}}}$$

Missä, $\mathrm{d_{op}}$ tarkoittaa toimintapäivien määrää vuodessa, $\mathrm{h_{op}}$ tarkoittaa toimintatuntien määrää vuorokaudessa ja $\mathrm{t_{cycle}}$ tarkoittaa toiminnan kestoa sekunneissa.

Turvajärjestelmän turvallisuuden tasoa voidaan nostaa, jos järjestelmään lisätään vian havaitseminen. Diagnostisella kattavuudella tarkoitetaan kykyä havaita vaaralliset viat järjestelmässä. Heikko diagnostiikka voi huomata vain muutaman vian järjestelmässä, kun taas hyvä DC voi huomata suuren osan tai jopa kaikki viat. Diagnostinen kattavuus luokitella neljään eri luokkaan, Nolla: DC on vähemmän kuin 60 %, Matala: DC on 60 % – 90 %, Keskitaso: DC on 90 % – 99 % ja Korkea: DC on yli 99 %. (SICK, 2015a, s. 129)

Yhteisvikaantumisella pyritään estämään yleisiä vikoja, joita voi aiheutua ulkoisista vaikuttajista, kuten lämpötilasta ja jännitteestä. Yleiset viat voivat tehdä identtisistä komponenteista käyttökelvottomia, vaikka komponentteja on testattu hyvin ja riippumatta niiden vikaantumistaajuudesta. Standardissa on annettu yksinkertainen pisteytys malli, millä voidaan, määrittää onko yhteisvikaantumista vähennetty tarpeeksi. Taulukko 7 on kyseinen pisteytys malli, jos mallista saa vähintään 65 pistettä, on tarvittavat CCF mittaukset tehty. (SICK, 2015a, s. 129)

Taulukko 7. CCF-malli. (SICK, 2015a).

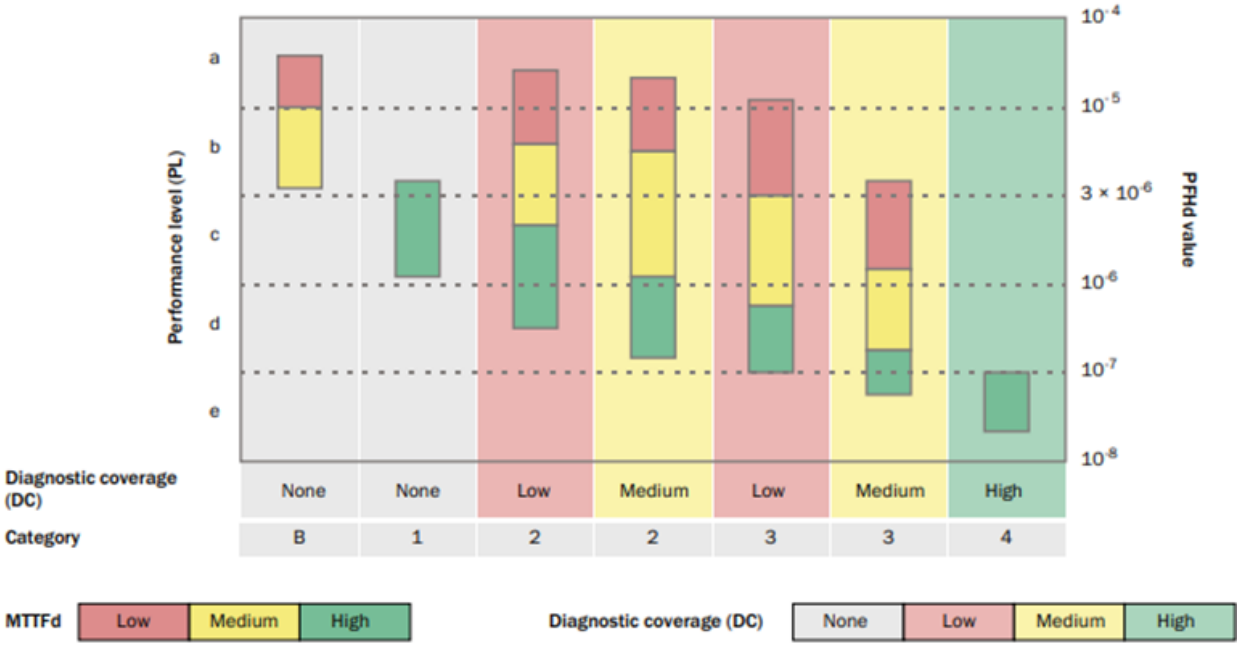
Tyyppi	Toimenpide	Pisteet
Erottelu	Signaalipolkujen välinen fyysinen erottelu	15
Diversiteetti	Käytetään erilaisia teknologioita, toteutuksia tai fysikaalisia periaatteita	20
Suunnittelu, soveltaminen ja käyttökokemukset	Suojaus jännitteen, virran, paineen, lämpötilan jne. ylitykselle	15
Suunnittelu, soveltaminen ja käyttökokemukset	Komponentit ovat hyvin koeteltuja	5
Arviointi ja analyysit	Suoritetaan vika-analyysi, jotta vältetään yhteisvikaantumista	5
Pätevyys ja koulutus	Suunnittelijat on koulutettu ymmärtämään yhteisvikaantumisen syyt ja seuraukset	5
Ympäristöolosuhteet	Sähköisten ja elektronisten järjestelmien suojaus sähkömagneettisilta häiriöiltä	25
Ympäristöolosuhteet	Otetaan huomioon haitat tärinästä, kosteudesta, lämpötilasta jne.	10

Standardi tarjoaa useita lähteitä, millä voidaan varmistaa ja testata järjestelmän toimivuus, sekä oikein asennus laitteiden ja ohjelmiston kanssa. Laitteita ja ohjelmistoa täytyy testata usein ja kunnolla, sekä säilyttää dokumentaatio muutetuista asioista. Prosessin

turvallisuuden kannalta merkittävät aiheet toteutetaan oikein ja sisältävät asianmukaisen laadunhallinnan. (SICK, 2015a, s. 129)

Kuva 4 nähdään, kuinka järjestelmän turvallisuuden taso voidaan määritellä. Esimerkiksi suoritustaso PL d, voidaan saavuttaa kategorian 2 rakenteella, diagnostiikan kattavuuden keskitasolla ja korkealla MTTFd-arvolla.

Kuva 4. Suorituskykytason määritteleminen. (SICK 2015a).



2.4.2 EN IEC 62061

Turvallisuuden tason määritteleminen turvajärjestelmälle voidaan suorittaa komponenttien avulla myös EN IEC 62061 standardin mukaan. Turvajärjestelmän saavutettu turvallisuuden eheysluokitus voidaan määritellä seuraavilla parametreilla. (SICK, 2015a, s. 134.)

- Hardware fault tolerance (HFT) eli laitteiston vikasietoisuus.
- Probability of dangerous hardware failures (PFHd) tarkoittaa keskimääräistä vaarallisen vian todennäköisyyttä tunnissa.
- DC/Safe failure fraction (SFF) eli vaarallisen vikaantumisen todennäköisyys.
- CCF.
- Testing.

EN IEC 62061 määrittelee turvajärjestelmän rakenteen alijärjestelmien ja laitteiston vikasietoisuuden avulla. HFT luokituksia ovat 0 ja 1, 0-luokassa vika laitteistossa voi johtaa turvatoiminnon menetykseen yksikanavaisessa järjestelmässä. 1-luokassa, jos laitteistossa on vika, niin turvatoimintoa ei menetetä kaksikanavaisessa järjestelmässä. (SICK, 2015a, s. 134)

Turvajärjestelmän rakenteen lisäksi, tulee ottaa huomioon PFHd jokaiselle alijärjestelmälle. PFHd-arvo voidaan laskea erilaisille alijärjestelmille tietyllä kaavalla. Kaavan toimivuuteen tarvitaan DC-arvo, toiminta-aika, diagnostinen testiväli, komponenttien vikaantumistaajuus ja CCF-arvo. Kaava 4 on kaksikanavaisen alijärjestelmän sievennetty laskukaava. (SICK, 2015a, s. 134)

Kaava 4. PFHd-arvon laskeminen kaksikanavaiselle alijärjestelmälle.

$$\mathrm{PFHd} \approx \beta * \frac{\lambda_{D1} + \lambda_{D2}}{2}$$

Kaavan 4, β tarkoittaa yhteisvikaantumisen murto-osaa ja λ_D tarkoittaa komponenttien vikaantumistaajuutta. Yhteisvikaantumisen murto-osa saadaan CCF-mallin pisteiden avulla. 35 pistettä tai vähemmän on 10 %, 36 – 65 pistettä on 5 %, 66 – 85 pistettä on 2 % ja 86 – 100 pistettä on 1 %.

SSF-arvolla kuvataan osaa turvallisista ja havaituista vaarallisista vioista, verrattaessa kokonaisvika määriin. Viat katsotaan turvallisiksi, jos vian sattuessa järjestelmä tuodaan turvalliseen tilaan tai järjestelmä pidetään turvallisessa tilassa. Korkeampi SSF-arvo tarkoittaa, pienempää todennäköisyyttä vaaralliselle vialle järjestelmässä. (Auma, n.d., s. 10)

Turvajärjestelmän turvallisuuden paras mahdollinen eheysluokitus voidaan määritellä, kun järjestelmän vikasietoisuus ja SFF-arvo on tiedossa. Kuva 5 avulla voidaan päätellä, että kaksikanavainen ja SFF-arvon 60 % omaava järjestelmä voi saada parhaimmillaan eheysluokituksen SIL 2. (SICK, 2015a, s. 135)

Kuva 5. SIL-rajat. (SICK 2015a).

Safe failure fraction (SFF)	Hardware fault tolerance	
	0	1
< 60%	-	SIL1
60 to < 90%	SIL1	SIL2
90 to < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

2.5 Turvajärjestelmän komponentteja

Seuraavaksi perehdytään yleisesti turvajärjestelmissä käytettäviin komponentteihin, sekä normaalissakin automaatiojärjestelmässä käytettäviin tärkeisiin komponentteihin. Komponenteille voidaan määritellä myös turvaluokitukset, mikä tehdään yleensä riskinarvioinnissa ja vaadittuihin ominaisuuksiin päästään oikeanlaisilla laitteilla ja järjestelmillä. Vaarallisemmat prosessit ja laitteet tarvitsevat luotettavammat turvajärjestelmät.

2.5.1 Turvalogiikka

Turvalogiikka on ohjelmoitava logiikka, joka on suunniteltu käytettäväksi vaarallisiin tehtäviin ja suojaamaan ihmisiä, sekä laitteita. Turvalogiikan mentäessä vikatilaan tai huomatessaan jonkun vian, se ohjaa laitteet turvalliseen tilaan, vahingoittamatta ihmisiä ja laitteita. Turvallisella tilalla tarkoitetaan yleensä laitteiden pysäyttämistä tai vientiä alkuasentoon. (Realpars, n.d.)

Turvalogiikkaa verrattaessa normaaliin logiikkaan, turvalogiikalla on sisäinen redundanssi, mikä on toteutettu kaksoisprosessoreilla ja tämän ansiosta järjestelmästä saadaan luotettavampaa tietoa. Turvalogiikka tarkkailee itseänsä prosessin aikana ja useimmat turvalogiikat sertifioidaan standardin IEC 61508 mukaan, joten ne saavat turvallisuuden eheysluokituksen. (Control design, 2009.)

Normaalin logiikan ja turvalogiikan erot ovat suurimmaksi osin vikojen havaitsemisessa. Normaali logiikka ajaa hyvin laitteita ja prosessia, mutta sillä ei välttämättä ole tarvittavia toimintoja havaitakseen vikoja käyttöjärjestelmässä tai I/O-väylissä, jotka on kytketty logiikkaan. Normaalilla logiikalla voidaan havaita yleisiä vikoja käyttöjärjestelmässä, kuten loputtomia silmukoita. (Control design, 2009.)

Tyypillisesti normaali logiikka ei pysty havaitsemaan I/O-väylissä vääriä kytkentöjä, oikosulkuja tai maadoitus vikoja, turvalogiikka havaitsee edellä mainitut viat redundanssin ja ainutlaatuisten I/O pulssien avulla. Turvalogiikalla on kaksoisprosessorit, jotka suorittavat turvatoimintoja ja kummallakin prosessorilla on erillinen kääntäjä, joten yksittäinen virhe ei voi tapahtua kahdesti ja jäädä huomaamatta. (Control design, 2009.)

Turvalogiikkaa voidaan käyttää normaalin logiikan sijasta, mutta normaalilla logiikalla ei voida tehdä turvallisuuteen liittyviä toimintoja. Normaalilla logiikalla on myös omat puolensa kuten edullisemmat hinnat, sekä normaalilla logiikalla pystytään suorittamaan monimutkaisempia toimintoja, kuin turvalogiikalla. (Control design, 2009.)

2.5.2 PLC

PLC eli Programmable Logic Controller tarkoittaa suomeksi ohjelmoitavaa logiikkaa. Ohjelmoitava logiikka on pieni tietokone, joita käytetään kaikenlaisissa automaatiojärjestelmissä. PLC:llä voidaan automatisoida ja ohjata prosessien kulkua, laitteiden toimintoja tai kokonaisia tuotantolinjoja. (Unitronics, n.d.)

PLC vastaanottaa informaatiota tuloliitäntöihin liitetyiltä antureilta tai laitteilta ja ohjaa näiden tulosignaalien avulla lähtösignaaleja, jotka on etukäteen ohjelmoitu halutun laisiksi ja tietyillä parametreilla. PLC voi myös seurata ja tallentaa tietoa esimerkiksi tuotantolinjan tuottavuudesta, seurata lämpötilaa, asettaa hälytyksiä vikatilanteissa ja automaattisesti pysäyttää ja käynnistää laitteita. (Unitronics, n.d.)

PLC:n CPU varastoi ja prosessoi dataa, mutta tulo- ja lähtömoduulit yhdistävät PLC:n itse laitteeseen, nämä moduulit antavat tietoa CPU:lle ja käynnistävät haluttuja toimintoja. Käyttäjän halutessa käyttää PLC:tä reaaliajassa, tarvitaan HMI eli Human Machine Interface. HMI voi olla esimerkiksi perus kosketusnäyttö, jonka kautta voidaan tarkastella ja ohjata

PLC:tä. Ohjelmoitavan logiikan ohjelmointi tapahtuu tietokoneen kautta, josta se ladataan logiikkaan. PLC-valmistajat, kuten Siemens ja Beckhoff tarjoavat oman ohjelmointi sovelluksensa asiakkaan käyttöön. (Unitronics, n.d.)

2.5.3 I/O-moduuli

I/O-moduuli on automaatiojärjestelmän osa, joka yhdistää itse laitteen järjestelmän aivoille eli PLC:lle. Järjestelmässä voi olla oma moduuli inputeille eli tuloille ja outputeille eli lähdöille. Tulomoduulilla voidaan seurata signaalin tilaa esimerkiksi kytkimistä ja lämpöanturista, lähtömoduulilla voidaan ohjata esimerkiksi valoja ja releitä. (Automation.com, 2018.)

Yleisin I/O-moduuli on digitaalinen I/O, digitaalinen I/O voi olla ainoastaan on- tai off-tilassa. Digitaalituloissa voidaan käyttää esimerkiksi painonappeja ja valokatkaisijoita ja digitaalilähtöjä puolestaan voidaan käyttää esimerkiksi valojen kanssa ja venttiilien avaamiseen ja sulkemiseen. (Automation.com, 2018.)

Toinen yleinen I/O on analoginen I/O, analoginen I/O voi saada signaaleista suurempia arvoja kuin 0 ja 1. Analoginen I/O voi lukea ja käyttää esimerkiksi arvoja 0 – 10 VDC ja 4 – 20 mA. Analoginen tulomoduuli periaatteessa mittaa joko jännitettä tai virtaa ja analoginen lähtömoduuli voi syöttää jännitettä tai virtaa, tietyillä asteikoilla. Analogiseen tulomoduuliin voidaan liittää esimerkiksi lämpöanturi tai paineanturi ja analogisella lähtömoduulilla voidaan ohjata esimerkiksi generaattorin tehon ulostuloa. (Automation.com, 2018.)

2.5.4 Turvavalopuomi

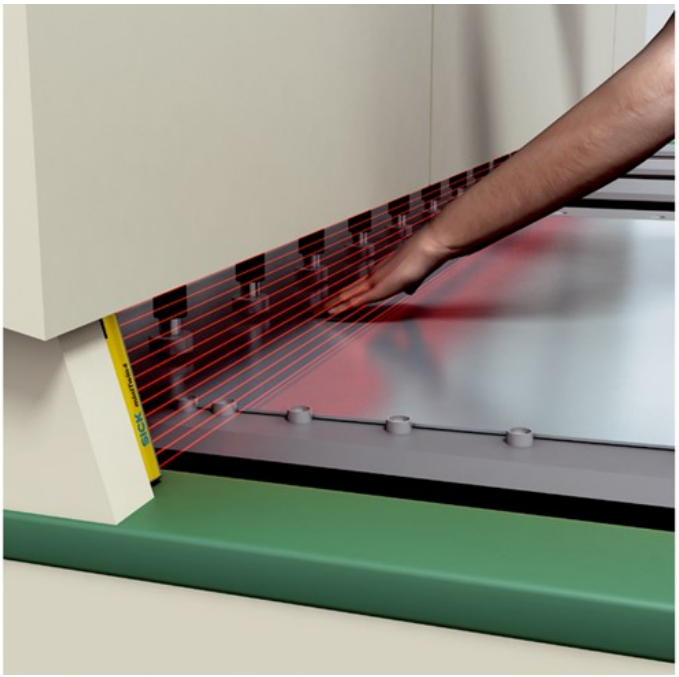
Turvavalopuomeilla voidaan järjestää automaattinen pysäytys laitteille, jos esimerkiksi ihminen on menossa puomien läpi vaaralliselle alueelle. Turvavalopuomeilla voidaan taata turvallinen työskentely laitteiden huoltajille, sekä saada laitteiden käyttäjälle joustavuutta ja vapautta teollisissa tiloissa. (Arrow, 2018.)

Turvavalopuomijärjestelmä sisältää kaksi puomia, joista toinen on lähetin ja toinen on vastaanotin. Lähetin voi sisältää monta led-valoa, mitkä lähettävät infrapuna pulsseja

vastaanottimeen. Pulssit lähetetään tietyssä järjestyksessä, kuten ylhäältä alas ja jokaisella pulssilla on tietty taajuus. Vastaanotin taas osaa odottaa näitä pulsseja oikeassa ajassa ja järjestyksessä. Kun puomien välistä menee jokin esine tai henkilö, katkeaa pulssit ja tämä aiheuttaa koneen tai laitteen pysähtymisen. Turvavalopuomit sisältävät itsevalvontapiirin, minkä avulla vian sattuessa kesken operaation, itsevalvontapiiri lähettää automaattisen pysäytys signaalin. (Arrow, 2018.)

Puomit voidaan sijoittaa suoraan toiminta-alueelle, kuten hydraulisen puristimen luo, ettei vaara-alueelle pääse työntämään sormia. Puomit voidaan asentaa myös eristämään kokonaisia huoneita, ettei kukaan pääse esimerkiksi robotin toiminta-alueelle. Suunniteltaessa toimivaa turvajärjestelmää turvavalopuomeilla, täytyy laitteen tai koneen aktivointi- ja resetointipainike, sijoittaa puomeilla suojatun alueen ulkopuolelle. Turvavalopuomeja tulee käyttää vain laitteissa, jotka voivat pysähtyä heti ja missä tahansa operaation kohdassa. Kuva 6 on esimerkki toiminta-alueelle sijoitettavista turvavalopuomeista. (Arrow, 2018.)

Kuva 6. Turvavalopuomi toiminta-alueella. (SICK n.d.a).

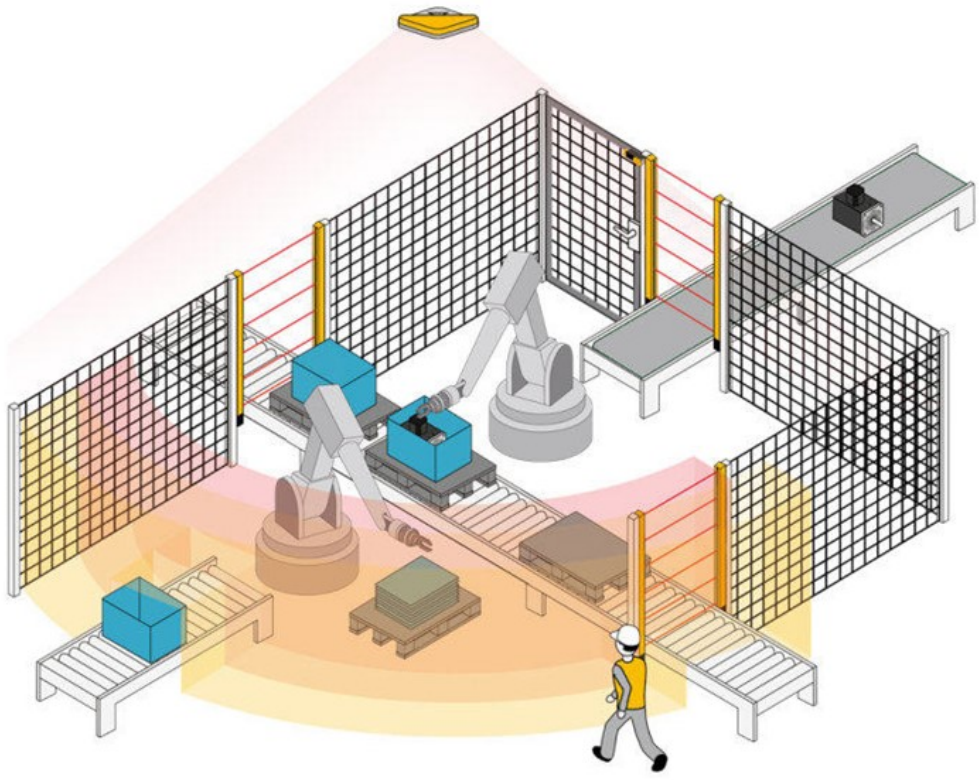


2.5.5 Turvakamerajärjestelmä

Pilz:in SafetyEYE turvakamerajärjestelmällä voidaan suojata koneita ja ihmisiä, sijoittamalla valvotun alueen yläpuolelle tunnistinyksikkö, mikä sisältää kolme kameraa. Useiden eri anturien sijasta, SafetyEYE:n avulla voidaan luoda kolmiulotteinen suoja vaara-alueen ympärille tai valvoa jotain tiettyä kohdetta. Turvakamerajärjestelmän käyttö tiloissa, missä ihminen ja kone tekevät yhteistyötä, auttaa saavuttamaan nopean tuotannon ja turvalliset työ olot. Kamerajärjestelmälle asetetaan varoitus- ja tunnistusalueet, estäen henkilöiden pääsyn vaara-alueelle. (Pilz, 2014, s. 8)

SafetyEYE-järjestelmä sisältää tunnistinyksikön ja ohjausyksikön, mikä sisältää analysointiyksikön ja turvaohjauksen. Järjestelmä havainnoi ja ilmoittaa lähestyvästä kohteesta ja pysäyttää koneen tai laitteen hätätilanteissa. Järjestelmälle voidaan määrittää halutut varoitus- ja tunnistusalueet. Järjestelmän valvottavan alueen enimmäisala on noin 72 m^2. SafetyEYE-järjestelmän suorituskykyluokka on PL d ja turvallisuuden eheysluokitus SIL 2. Kuva 7 on esimerkki SafetyEYE-turvakamerajärjestelmän toiminnasta. (Pilz, n.d.c)

Kuva 7. SafetyEYE tuotannossa. (Pilz n.d.c).



2.5.6 Turvalaserskanneri

Turvalaserskannerit käyttää kulkuaika teknologiaa, mikä tarkoittaa, että skanneri lähettää laser säteilyä ja mittaa ajan mikä laserilla kestää palata takaisin yksikköön, tämän avulla skanneri pystyy laskemaan sijaintia. Skannerille voidaan ohjelmoida halutunlainen alue tai useita alueita. Skannerille voidaan esimerkiksi ohjelmoida kaksi eri kokoista puoli ympyrän muotoista aluetta sisäkkäin, joista isompi alue hidastaa laitetta ja sisempi alue pysäyttää laitteen, kun huomataan jotain vaara-alueella. (Keyence, n.d.)

Turvalaserskannereita käytetään yleisesti niiden monipuolisuuden vuoksi. Skannerit voidaan asentaa pysty- tai vaakasuoraan ja ne ovat hyvin pieni kokoisia, joten niitä voi käyttää paikoissa, minne esimerkiksi turvavalopuomit eivät mahdu. Skanneri voidaan asentaa myös automaattiseen kuljetuskoneeseen, minkä ansiosta voidaan välttää törmäyksiä esineisiin ja ihmisiin, tästä on esimerkki Kuva 8. (Keyence, n.d.)

Kuva 8. Kuljetuskone. (SICK n.d.b).

2.6 Ohjelmointi

Työssä käytetään ohjelmoinnin osalta Beckhoffin TwinCAT 3-ohjelmistoa. TwinCAT 3-ohjelmistolla voidaan toteuttaa lukuisia erilaisia projekteja, kuten urheiluareenojen ja tuulivoimaloiden automatisointia. TwinCAT 3 voidaan yhdistää Matlab- ja Simulink-ohjelmistoihin, joista voi olla hyötyä simuloinnissa ja ohjauspiirien rakentamisessa. TwinCATin integrointi Microsoft Visual Studion kanssa mahdollistaa ohjelmoinnin, parametroinnin, konfiguroinnin ja diagnosoinnin pelkästään yhdellä sovelluksella. (Beckhoff, 2019a, s. 2 – 7)

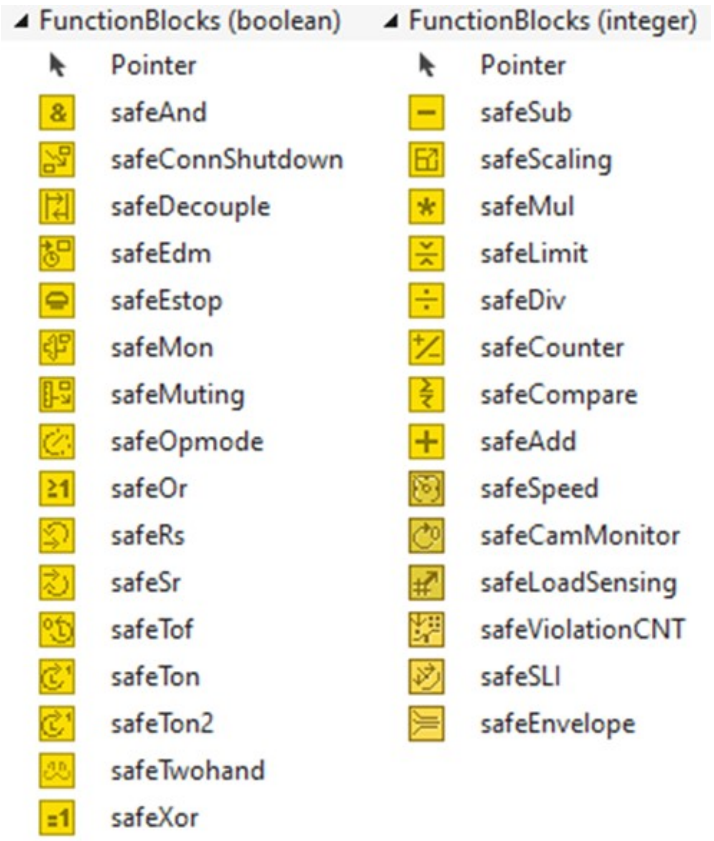
TwinCAT 3-ohjelmistolla voidaan rakentaa myös visuaalisia toimintoja ja simulaatioita, kuten painikkeita ja merkkivaloja. TwinCAT 3 tukee monia eri ohjelmointikieliä, jotka ovat listattuna seuraavaksi.

- Function Block Diagram (FBD) Toimilohkokaavio
- Ladder Logic Diagram (LD) Tikapuulogiikka kaavio
- Structured Text (ST) Rakenteinen Teksti
- Sequential Function Chart (SFC) Sekvenssivuokaavio
- C/C++
- Continuous Function Chart (CFC) Sekvenssikaavio

TwinCAT 3-ohjelmiston turvallisuuteen liittyvä ohjelmointi tehdään ohjelmiston erillisessä TwinSAFE-moduulissa. TwinSAFE-ohjelmointi suoritetaan toimilohkokaaviolla (FBD), mikä on hieman erilaista verrattuna normaaliin toimilohkokaavio-ohjelmointiin. TwinSAFE-ohjelmoinnissa käytössä on tuttuja toimilohkoja, kuten AND- ja OR-lohkot, sekä valmiiksi rakennettuja ja sertifioituja turvallisuuteen liittyviä toimilohkoja.

TwinSAFE-ohjelmoinnissa käytetään networkkeja, kuten myös normaalissa toimilohkokaaviossa, joita voidaan lisätä halutessa. Toimilohkot on jaettu kahteen ryhmään, boolean ja integer. Boolean-toimilohkot käyttävät totuusarvoja tosi ja epätosi tai nollia ja ykkösiä. Integer-toimilohkot puolestaan käyttävät kokonaislukuja, esimerkiksi laskureissa. Kuva 9 on kaikki TwinSAFE-toimilohkot.

Kuva 9. Toimilohkot



Ohjelmoitaessa pystytään rakentamaan erillisiä TwinSAFE-ryhmiä, millä voidaan loogisesti erotella ohjelmat. Esimerkiksi, jos käytössä on vain yksi turvalogiikka ja enemmän kuin yksi fyysinen laite tai moduuli, jota halutaan ohjata, on järkevää erotella ohjelmat eri ryhmiin. TwinSAFE-ryhmiä käyttämällä ainoastaan vikaantunut laite menee turvalliseen-tilaan, eli pois päältä ja toiset laitteet voivat jatkaa normaalisti. (Contact and Coil, n.d.)

3 Turvajärjestelmän toteutus

3.1 Suunnittelu

Tavoitteena on rakentaa turvajärjestelmä oviaukkoon, käyttäen SICKin turvavalopuomeja, joilla voidaan estää vahingot toiminta-alueella. Turvavalopuomeista läpi mentäessä pysäytetään haluttu kone tai laite ja varmistetaan ettei järjestelmä lähde käyntiin ennen kuin on taas turvallista. Työn tavoitteena on ohjelmoida järjestelmä, siten että se toimii pelkän PLC:n avulla. Turvajärjestelmä täytyy saada käyntiin ilman tietokonetta myös odottamattoman sähkökatkoksen jälkeen.

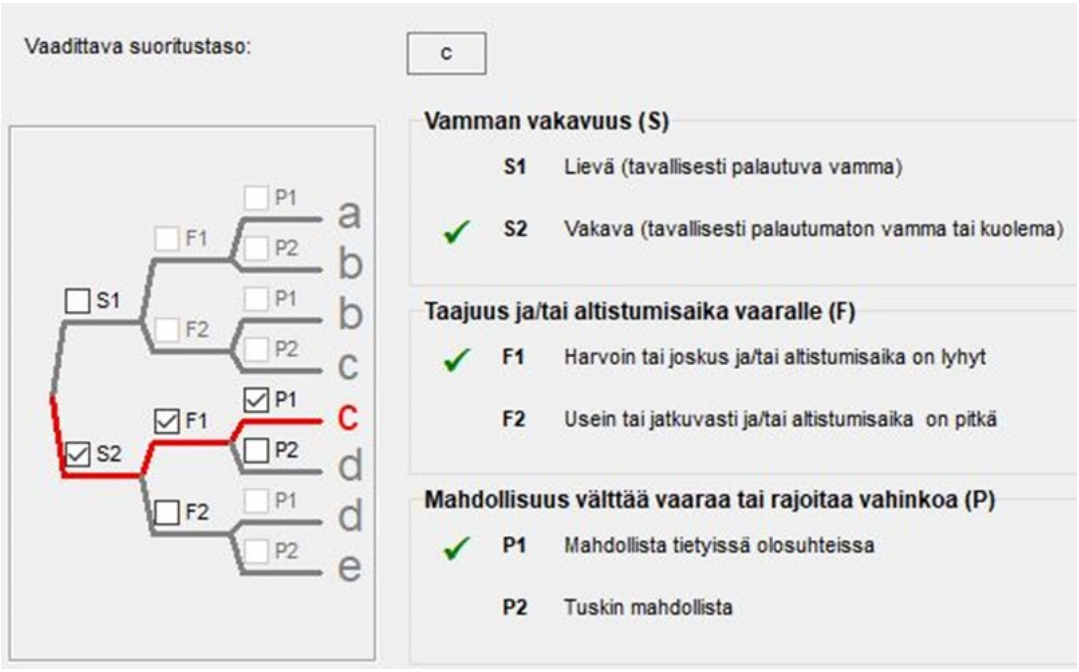
Järjestelmälle tehdään ensimmäiseksi riskinarviointi SISTEMA ohjelmistolla, josta saadaan EN ISO 13849-1 standardin mukainen suorituskykytaso PL. Riskinarvioinnin jälkeen käydään läpi kaikkien komponenttien turvaparametrit, jotka komponentin valmistaja on kertonut ja lasketaan tarpeen vaatiessa itse tarvittavat arvot. Seuraavaksi rakennetaan turvajärjestelmä SISTEMAlla ja syötetään tarvittavat arvot komponentteihin, jonka jälkeen tarkistetaan, onko suorituskykytaso tarpeeksi hyvä riskinarvioinnista saatuun tulokseen verrattaessa, jos järjestelmällä ei ole tarpeeksi hyvä suorituskykytaso, suoritetaan riskin vähennys vertaamalla muita menetelmiä ja laitteita.

Turvajärjestelmän läpäistyä riskinarviointi ja siitä mahdollisesti seuraavat riskin vähennykset, voidaan järjestelmää alkaa rakentamaan ja ohjelmoimaan. Turvajärjestelmän ohjelmointi vaiheessa tehdään monia testejä, että varmistutaan järjestelmän toimivuudesta ja turvallisuudesta.

3.2 Turvatoiminnon määrittely

Riskinarviointi tehtiin SISTEMAlla ja päädyttiin suorituskykytasoon PL c, mikä nähdään Kuva 10. Turvavalopuomit sijaitsevat oviaukolla, joka johtaa robotille, joten vamman vakavuuteen (S) valittiin S2, koska robotti voidaan ohjelmoida liikkumaan isoilla nopeuksilla. Taajuus tai altistumisaika vaaralle (F) kohtaan valittiin F1, koska osuman tullessa, se on todennäköisesti nopea ja alueella liikkuu harvoin ihmisiä. Mahdollisuus välttää vaaraa (P) kohtaan valittiin P1, koska vaara-alueelle pääsyä voidaan rajoittaa helposti ja robotin nopeuksia voidaan säätää pienemmiksi.

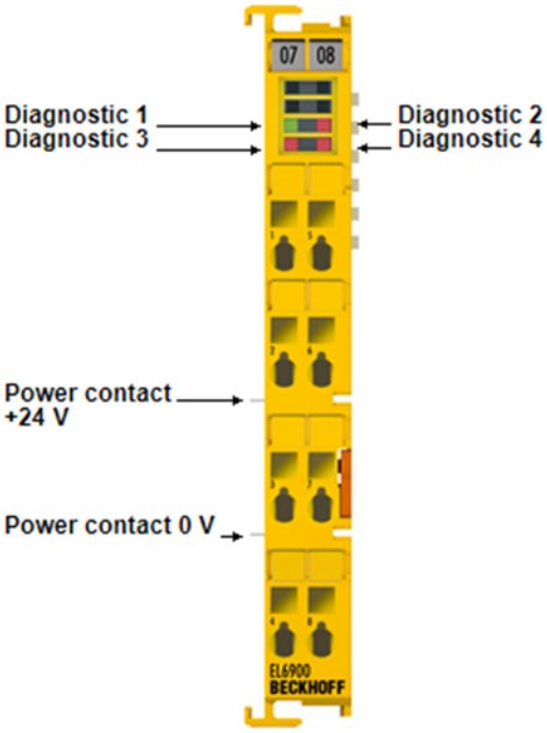
Kuva 10. Turvajärjestelmän riskinarviointi.



3.2.1 Turvalogiikka

Työssä käytettävä turvalogiikka on Beckhoffin TwinSAFE logic EL6900, kyseisellä turvalogiikalla voidaan yhdistää 128 TwinSAFE-laitetta. EL6900 käyttää Safety over EtherCAT protokollaa ja syöttöjännitteenä toimii 24 Vdc. Logiikka toimii linkki yksikkönä TwinSAFE input- ja output terminaalien välillä. Kuva 11 on EL6900-turvalogiikka, josta nähdään neljä diagnostiikka led-valoa ja jännite liittimet. (Beckhoff, 2019b.)

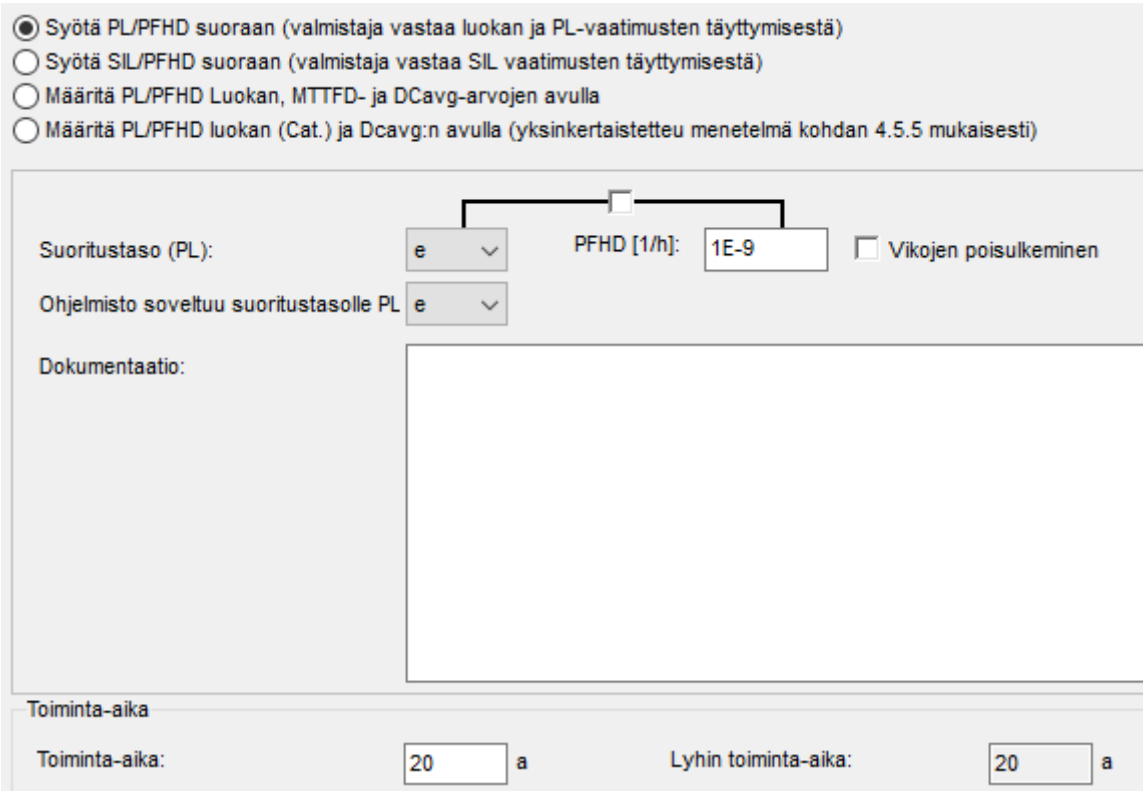
Kuva 11. EL6900. (Beckhoff 2019b).



EL6900-turvalogiikalla on valmiiksi sertifioituja turvatoimintolohkoja, kuten hätäpysäytys ja turvaovien valvonta, näitä lohkoja voidaan yhdistellä ja valittavissa on myös perusoperaattoreita, kuten AND ja OR. Halutut toiminnot tehdään TwinCAT-ohjelmistolla, josta ne ladataan kenttäväylän kautta turvalogiikkaan. Beckhoff on ilmoittanut EL6900-turvalogiikalle suorituskykytason PL e ja turvallisuuden eheysluokitus tason SIL 3. (Beckhoff, 2019b.)

Beckhoff on antanut turvalogiikan datalehdissä tarkempia tietoja turvaparametreista, jotka johtavat turvaluokituksiin PL e ja SIL 3. EL6900-turvalogiikan keskimääräinen vaarallinen vikaantumisaika (MTTFd) on korkea 20 vuotta, kategoria luokitus on 4, diagnostiikan kattavuus luokka (DC) on korkea, laitteiston vikasietoisuus luokka (HFT) on 1 ja keskimääräinen vaarallisen vian todennäköisyys tunnissa (PFHd) on 1,03 x 10^-9. SISTEMA-ohjelmistolle voi syöttää suoraan suorituskykytason ja PFHd-arvon, mikä näkyy Kuva 12. (Beckhoff, 2017a, s. 17)

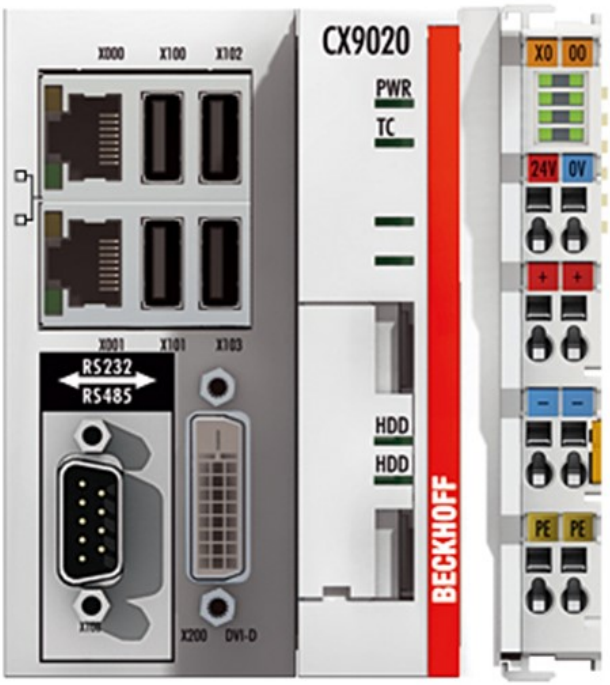
Kuva 12. EL6900 turvaluokitus.



3.2.2 PLC

Työssä käytettävä PLC on Beckhoffin CX9020. CX9020 on tietokone, mistä löytyy kaksi ethernet-liitäntää, kaksi MicroSD-kortti paikkaa, DVI-D-liitäntä ja neljä USB 2.0-liitäntää, joihin voidaan liittää esimerkiksi hiiri ja näppäimistö. CX9020 vaatii toimiakseen 24 volttia tasavirtaa (Vdc). Kuva 13 on CX9020. (Beckhoff, 2020, s. 12)

Kuva 13. CX9020. (Beckhoff 2019c).



CX9020-PLC:n käyttöjärjestelmänä toimii Microsoft Windows Embedded Compact 7. Tietokoneella on 1 Gt RAM-muistia ja pysyvää muistia 128 kt, mikä pysyy tallessa esimerkiksi sähkökatkon jälkeen. CX9020-PLC sisältää myös kahdeksan diagnostiikkalediä, joista voidaan seurata esimerkiksi jännitelähteen ja ethernet-väylien tilaa. (Beckhoff, 2020, s. 8)

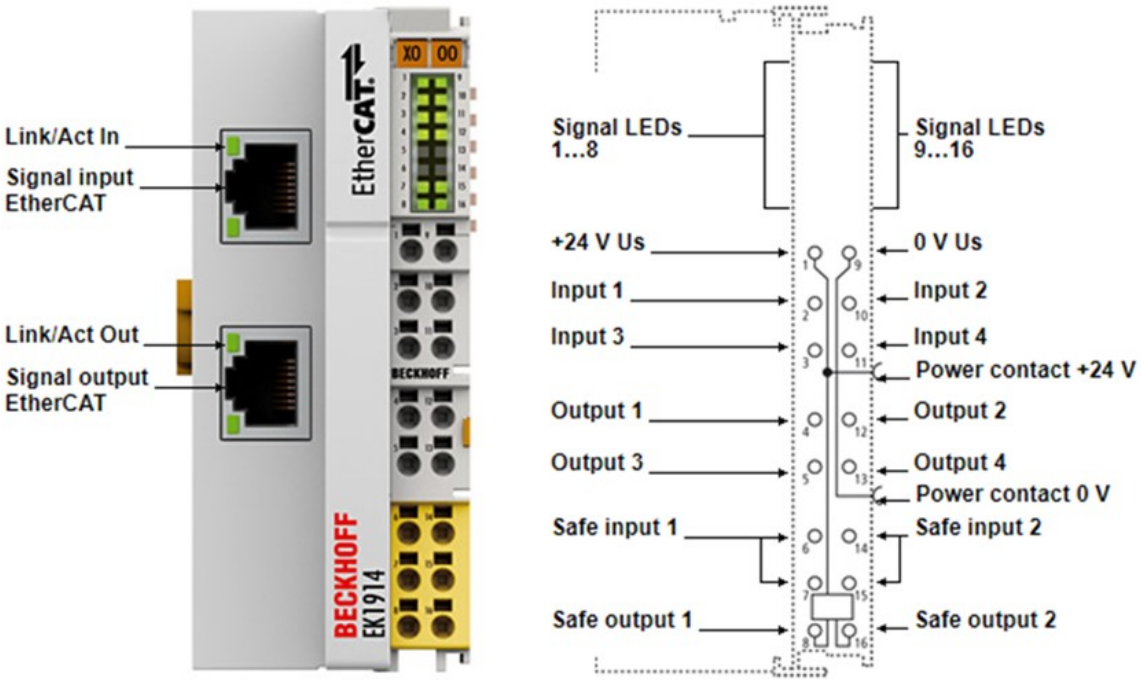
CX9020 ei kuulu itse turvajärjestelmään, mutta kyseisellä komponentilla päästään ohjelmoimaan TwinCAT 3-ohjelman kautta TwinSAFE-turvajärjestelmää ja lataamaan turvaohjelma turvalogiikalle EL6900. CX9020-PLC:tä voidaan käyttää yhdessä turvalogiikan EL6900 kanssa, vaarantamatta turvallisuuden tasoa. (Beckhoff, 2015; Beckhoff, 2019d, s. 13)

3.2.3 I/O-moduuli

Työssä käytettävä I/O-moduuli on Beckhoffin EK1914, joka täyttää suorituskykytasoltaan PL e kategorian vaatimukset. Kyseisellä I/O-moduulilla on neljä digitaalituloa ja neljä digitaalilähtöä, sekä kaksi turvatuloa ja kaksi turvalähtöä. Turvatulot ja -lähdöt voidaan tunnistaa helposti niiden keltaisesta väristä. Syöttönä I/O-moduulilla toimii 24 Vdc ja liitäntä protokollana EtherCAT. EK1914-moduulin lähtöjen ja tulojen tilaa voidaan seurata ledien

avulla, joita löytyy kuusitoista. Kuva 14 on EK1914 ja liitäntöjen osoitteet. (Beckhoff, 2017b, s. 12 – 15)

Kuva 14. EK1914. (Beckhoff 2019e).



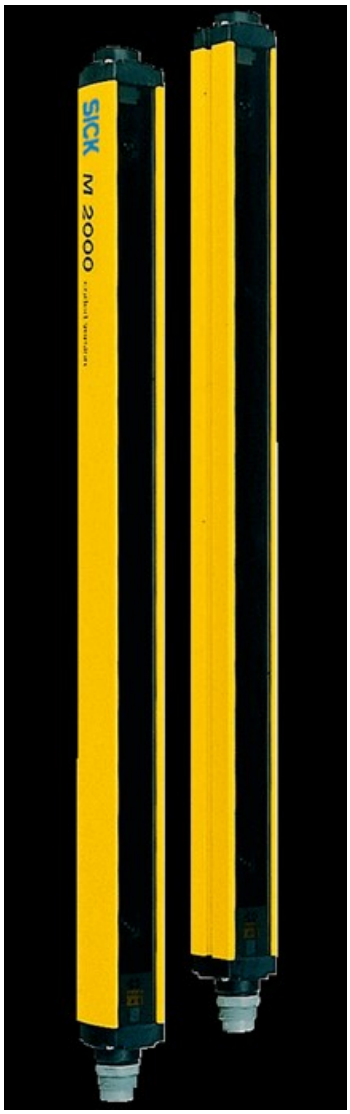
EK1914 I/O-moduulille on annettu tuotteen datalehdissä rutkasti turvallisuuteen liittyviä parametreja. I/O-moduulin MTTFd-arvo on korkea 20 vuotta, DC luokitus on korkea, kategoria 4, HFT 1 ja PFHd-arvo 2,64 x 10^-9. Koska valmistaja oli tarjonnut suorituskykytason ja PFHd-arvon, voidaan ne sijoittaa suoraan SISTEMA-ohjelmistoon. (Beckhoff, 2017b, s. 17)

3.2.4 Turvavalopuomi

Työssä käytettävät turvavalopuomit tai valoverhot ovat SICKin M2000 monisäteisiä turvavalopuomeja, kyseiset puomit ovat noin metrin pituisia. M2000-turvavalopuomeja voidaan kytkeä sarjaan kolme kappaletta, puomeja voidaan käyttää kulun valvontaan yhdeltä tai useammalta suunnalta. M2000-turvavalopuomilla on kolme sädettä, joiden toimintaetäisyys yltää 25 metriin asti, etäisyys voidaan konfiguroida tarpeen mukaan. Toinen työssä käytettävistä puomeista on lähetin ja toinen vastaanotin, lähetin lähettää kolmea

infrapuna sädettä, joita vastaanotin osaa odottaa. Kuva 15 on kaksi M2000-turvavalopuomia. (SICK, n.d.c)

Kuva 15. M2000-Turvavalopuomi. (SICK n.d.d).



M2000-turvavalopuomin syöttöjännitteenä toimii 24 Vdc ja järjestelmäliitäntä tehdään 8-napaisella M12 urosliittimellä. SICK on ilmoittanut M2000-turvavalopuomille turvallisuudeneheystason SIL1, suorituskykytason PL c, kategoria luokan 2 ja PFHd-arvon 2,2 x 10^-8. Tarvittavat arvot voidaan taas syöttää suoraan SISTEMAlle. (SICK, 2015b, s. 213 – 236)

3.2.5 Turvallisuuden taso

Turvallisuuden taso saatiin määriteltyä SISTEMAlla, vaadittu suorituskykytaso oli PL c. SISTEMAlle syötettiin turvallisuuteen vaikuttavien laitteiden PFHd-arvot ja suorituskykytaso, jotka valmistajat Beckhoff ja SICK oli tarjonnut. Turvajärjestelmällä päästiin vaadittuun PL-kategoriaan ja järjestelmän PFHd-arvoksi tuli 2,6 x 10^-8. Kuva 16 nähdään SISTEMA-ohjelmistolta saatu raportti.

Kuva 16. Turvallisuuden taso.

SF Nimi: Turvajärjestelmä

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

Tähän kuuluvat alajärjestelmät

SB Nimi: EL6900

Resulting PL: e	PFHD [1/h]: 1E-9	Luokka (Cat.): 4
MTTFD [v]: ei asiaankuuluva	DCavg [%]: ei asiaankuuluva	CCF-pisteet: ei asiaankuuluva

SB Nimi: Valoverho

Resulting PL: c	PFHD [1/h]: 2,2E-8	Luokka (Cat.): 2
MTTFD [v]: ei asiaankuuluva	DCavg [%]: ei asiaankuuluva	CCF-pisteet: ei asiaankuuluva

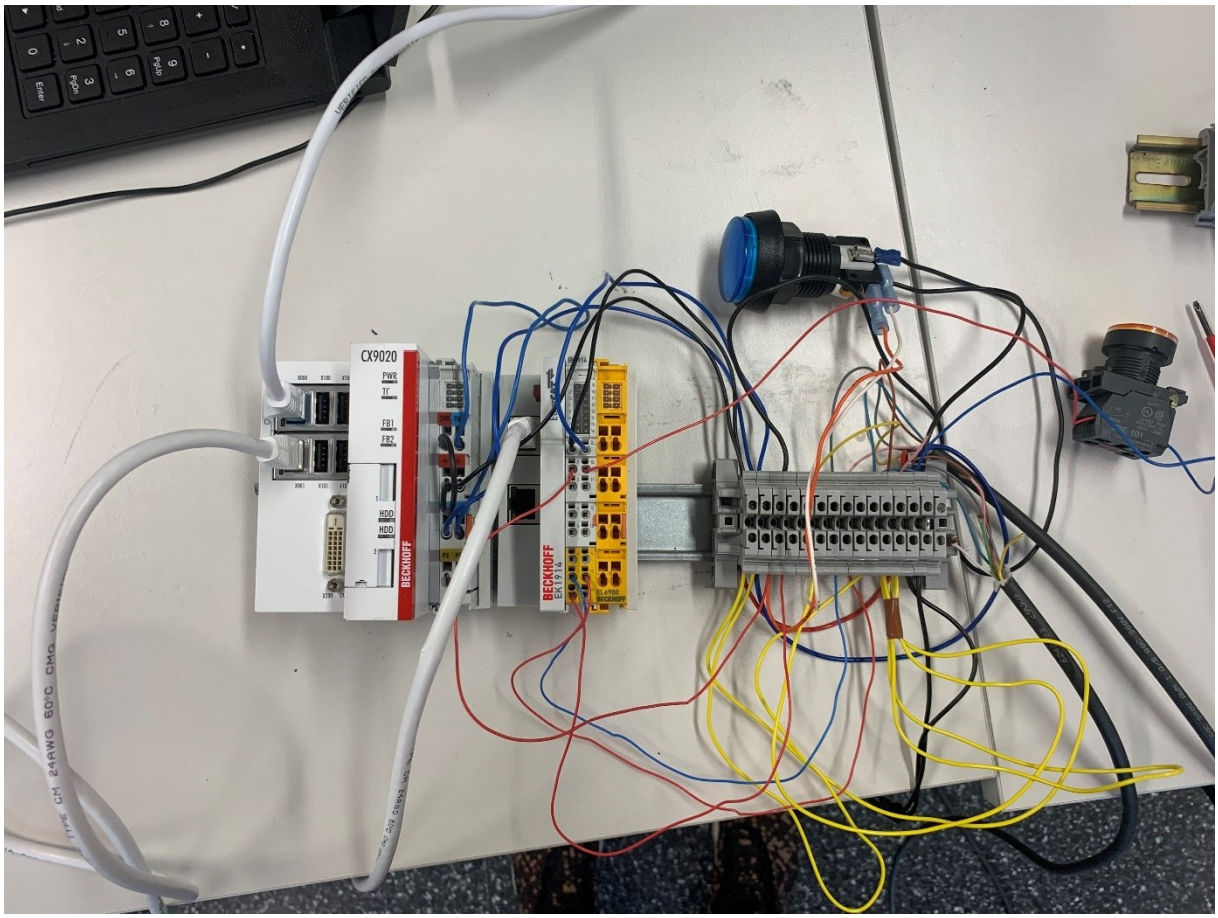
SB Nimi: EK1914

Resulting PL: e	PFHD [1/h]: 2,6E-9	Luokka (Cat.): 4
MTTFD [v]: ei asiaankuuluva	DCavg [%]: ei asiaankuuluva	CCF-pisteet: ei asiaankuuluva

3.3 Kytkennät

Kaikki komponentit kiinnitetään 35 mm:n DIN-kiskoon ja lisäksi kiskoon asennetaan noin 10 riviliitintä. PLC, I/O-moduuli ja turvalogiikka työnnetään toisiinsa kiinni, koska komponenttien takaosassa on kiinteät jännite liittimet. Turvavalopuomien kytkentään käytetään 8-napaista M12-liitintä ja johdon toinen pää avataan, missä on 7 eri väristä johdinta, joista tarvittavat liitetään järjestelmään. Järjestelmälle tuodaan jännite pistorasiasta, joka muunnetaan 24 Vdc. Kuva 17 nähdään valmiit kytkennät.

Kuva 17. Valmiit kytkennät.



PLC-CX9020:n liitin 24 V yhdistetään + liittimeen ja toisesta + liittimestä yhdistetään 24 Vdc jännitteeseen. PLC:n 0 V liitin yhdistetään – liittimeen ja toisesta – liittimestä yhdistetään nollaan. PLC:n ethernet-porteista toinen liitetään tietokoneelle ohjelmointi varten ja toisesta portista viedään kaapeli I/O-moduulille.

Turvalogiikalle EL6900 ei tarvitse johdotuksia ollenkaan. Turvalogiikka on liitettynä sen takaosassa olevien jännite liitinten avulla I/O-moduuliin. Turvalogiikalle ladataan ohjelma I/O-moduulin kautta.

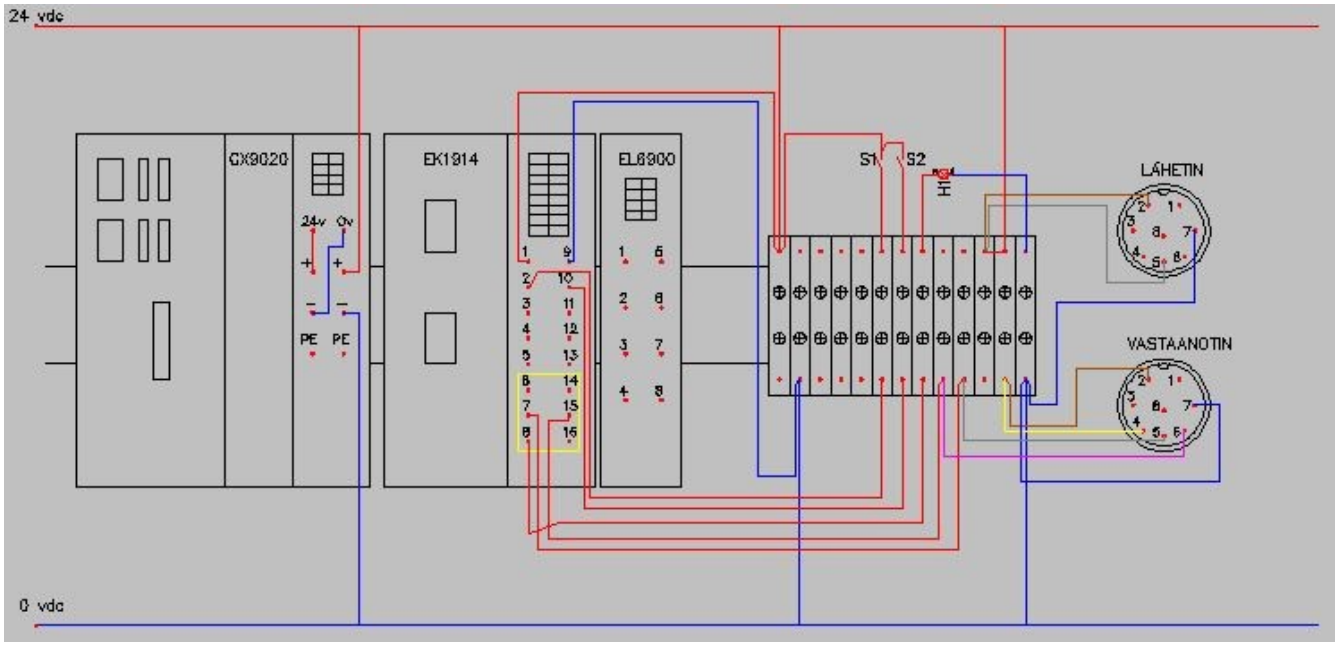
I/O-moduuli EK1914:n liittimeen 1 tuodaan jännite ja liitin 9 yhdistetään nollaan. Turvatulo 1, mikä on liittimessä 7 yhdistetään riviliittimen kautta vastaanotin turvavalopuomin harmaaseen johtimeen, mikä on OSSD 1-signaali. Turvatulo 2, mikä on liittimessä 15 yhdistetään saman vastaanotin puomin vaaleanpunaiseen johtimeen, mikä on OSSD 2-signaali. Turvalähtö 1, joka sijaitsee liittimessä 8 on yhdistetty merkkivaloon, jonka avulla voidaan seurata turvalähdön tilaa. Koska työssä ei tehty mitään ohjauksia laitteille oli

merkkivalo helpoin tapa seurata turvalähdön tilaa. I/O-moduulin tulot 1 ja 2 on yhdistetty normaalisti auki oleviin kytkimiin.

Lähetin turvavalopuomin ruskeaan johtimeen, mikä toimii käyttöjännitteenä, tuodaan 24 Vdc ja lähettimen sininen johdin yhdistetään nollaan. Lähettimen itsetestaus, mikä on harmaa johdin, yhdistetään myös suoraan 24 Vdc jännitteeseen. Vastaanotin puomin keltainen johdin on EDM-signaali, jolla voidaan suorittaa kontaktorivalvontaa, yhdistetään suoraan 24 Vdc jännitteeseen, koska sillä ei ole käyttöä työssä. Vastaanottimen OSSD 1- ja OSSD 2-johtimet on yhdistetty I/O-moduulille. Vastaanottimen ruskea johdin yhdistetään jännitteeseen ja sininen johdin yhdistetään nollaan. Turvavalopuomien johdoista jää monia johtimia vapaiksi, joita voidaan käyttää esimerkiksi puomien konfigurointiin.

Kuva 18 on CADS Electric ohjelmalla piirretty piirikaavio. Turvavalopuomien M12-liitäntää ei saa laitettua väärin päin, joten puomien työssä tarvittavien johtimien oikeat värit on lisätty selkeyttämään kuvaa.

Kuva 18. Turvajärjestelmän piirikaavio.



Turvajärjestelmän tarkoituksena on siis seurata, onko ihmisiä menossa vaaralliseen tilaan turvavalopuomien avulla, jotka sijaitsevat oviaukossa. Turvavalopuomien infrapunasäteet huomaavat ja katkaisevat jännitteen turvalähdöltä 1, jos säde/säteet katkeavat.

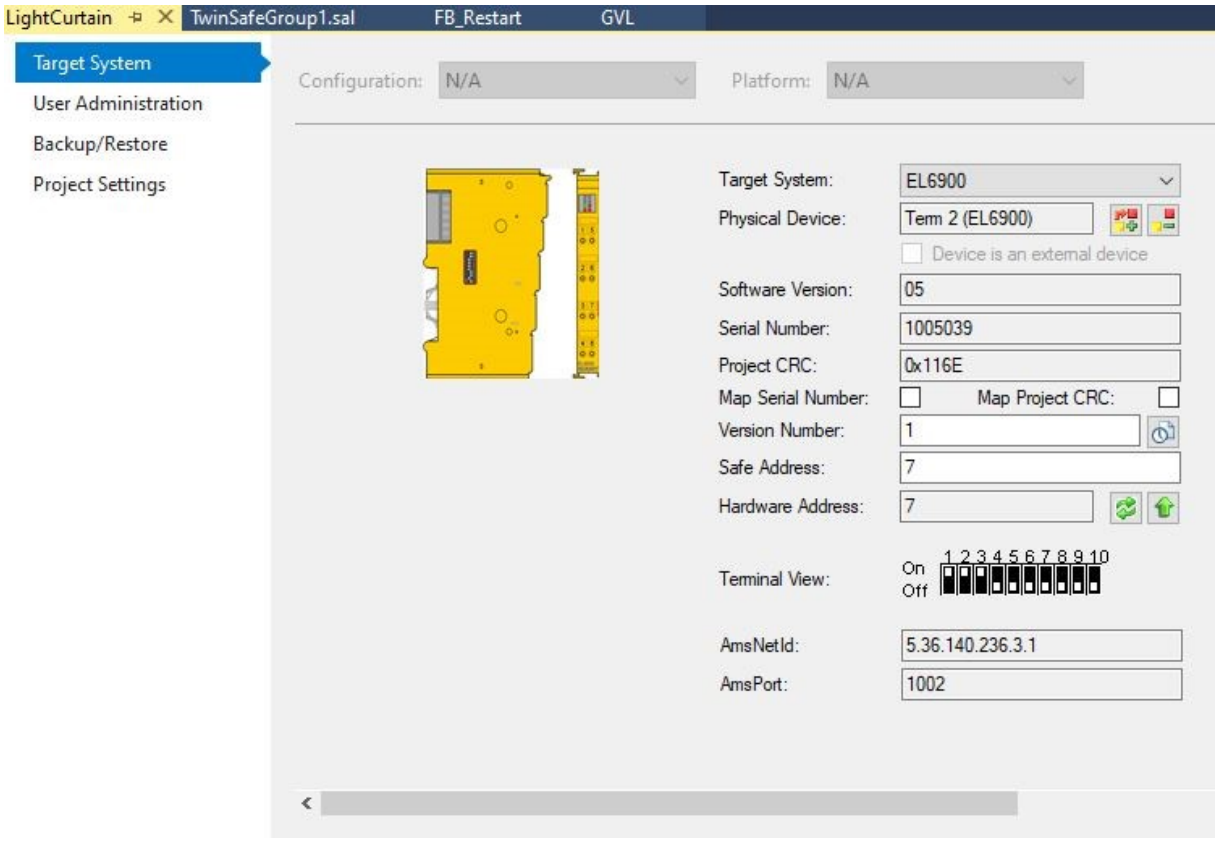
Turvajärjestelmän virheiden kuittaus tehdään kytkimellä S2. Virheiden kuittauksen jälkeen järjestelmä resetoidaan kytkimellä S1, jonka jälkeen järjestelmä on toiminnassa. Turvavalopuomien infrapunasäteiden katketessa, järjestelmä menee turvalliseen tilaan ja pysäyttää lähdöt, toiminta voidaan taas käynnistää kytkimellä S1. Turvajärjestelmän tilaa voidaan seurata merkkivalon H1 avulla, joka on liitetty turvalähtöön 1. Turvajärjestelmä on käynnissä, kun merkkivalo H1 palaa ja pysäytettynä, kun H1 on sammuksissa.

3.4 Ohjelmointi

Ohjelmointi vaiheen alkaessa, tarkistetaan ensin kaikki kytkennät ja asetetaan turvavalopuomit vastakkain, puomit kohdistetaan kunnolla, kun järjestelmä kytketään päälle. Käynnistetään TwinCAT 3 ja luodaan projekti, kun projekti on luotu, haetaan PLC-CX9020 kohdejärjestelmäksi. Seuraavaksi haetaan kaikki loput komponentit TwinCATin Solution Explorer-palkin kohdasta Devices, josta suoritetaan Scan toiminto. Scan toiminnolla saadaan kaikki komponentit mukaan projektiin.

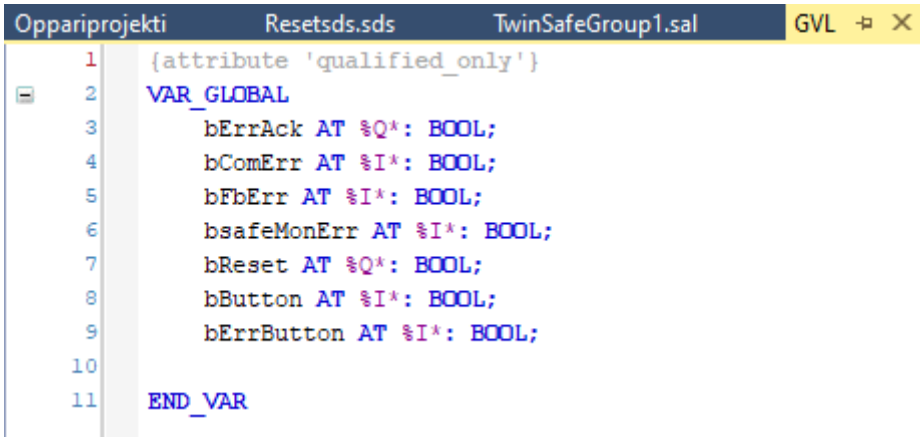
Ennen ohjelmointia kannattaa myös tarkistaa turvalogiikan ja I/O-moduulin kyljessä olevat DIP-kytkimet, joilla määritellään komponenttien turvaosoite. Turvalogiikan DIP-kytkimessä on 10 vipua ja I/O-moduulin DIP-kytkimenä toimii 3 pyöriteltävää kytkintä. DIP-kytkimillä määritetyt osoitteet eivät voi olla samat, työssä valittiin I/O-moduulille osoite 4 ja turvalogiikalle osoite 7, mikä voidaan nähdä Kuva 19, kohdasta Safe Address. Turvalogiikan ollessa yhdistettynä projektiin Hardware Address-kohdassa näytetään sama turvaosoite, jos kohdassa Safe Address on joku muu osoite, täytyy siihen korjata oikea.

Kuva 19. Turvalogiikan turvaosoite.



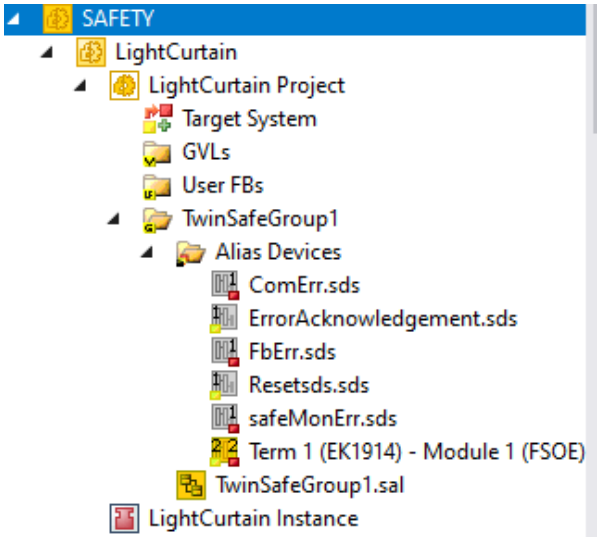
Seuraavaksi luodaan projektille Global Variable List (GVL), joka on Kuva 20. Projektissa tarvitaan 7 muuttujaa, joista 4 on virheiden tunnistukseen ja 3 kytkimien käyttöön. Muuttuja bErrAck on virheiden kuittausta varten, muuttuja bComErr ilmoittaa yhteysvirheistä, muuttuja bFbErr ilmoittaa virheistä turvatoimilohkossa ja muuttuja bsafeMonErr ilmoittaa virheistä turvatoimilohkon tuloissa.

Kuva 20. Global Variable List.



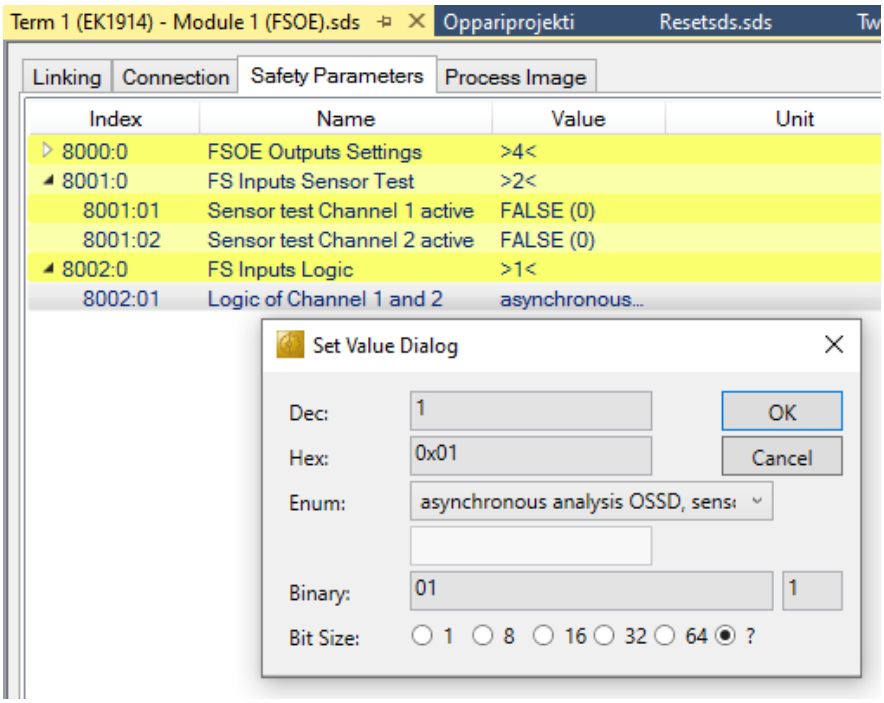
Turvaohjelman luonti onnistuu Solution Explorer-palkin kohdasta SAFETY, luodaan uusi turvaprojekti. TwinSAFE luo automaattisesti uuden TwinSAFE-ryhmän TwinSafeGroup1, jossa voidaan tehdä turvatoimintojen ohjaus. Seuraavaksi luodaan 5 Alias-laitetta, näiden kautta voidaan kommunikoida turvaohjelman kanssa. Alias-laitteista 2 on digitaalitulo-laitteita ja 3 digitaalilähtö-laitetta. Uudet Alias-laitteet luodaan klikkaamalla hiiren oikealla kohdasta Alias Devices ja valitsemalla Add new item, eteen tulee valikko, mistä halutun Alias-laitteen voi luoda. Jokainen luotu Alias-laite yhdistetään nimeänsä vastaavaan GVL-muuttujaan, tämä voidaan tehdä Alias-laitteen valikon kohdasta Linked to. Projektissa on valmiina myös yksi Alias-laite, joka sisältää I/O-moduulin EK1914 turvatulot ja -lähdöt. Kuva 21 nähdään koko turvaprojekti ja luodut Alias-laitteet, kohdasta Target System päästään tarkistamaan turvalogiikan DIP-kytkimen osoite.

Kuva 21. Turvaprojekti.



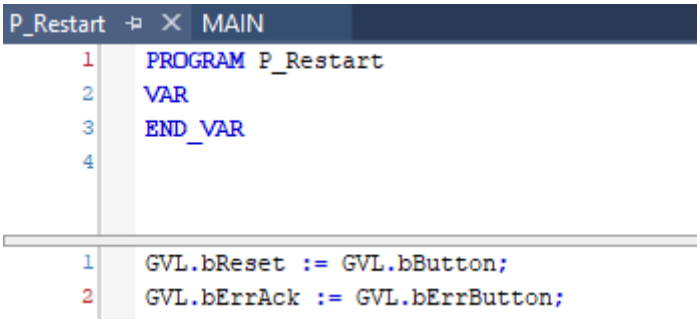
EK1914 I/O-moduulin Alias-laite kohdasta päästään tarkistamaan DIP-kytkimen osoite ja tarvittaessa vaihtamaan se. Saman valikon turvaparametrit-osiosta käydään vaihtamassa FS Inputs Sensor Test-kohtaan molemmille kanaville FALSE ja FS Inputs Logic-kohtaan asynchronous analysis OSSD, sensor test deactivated. Näillä muutoksilla otetaan logiikan testipulssit pois päältä ja käytetään turvavalopuomin omia testipulsseja. Kuva 22 nähdään EK1914-moduuliin tehdyt muutokset.

Kuva 22. EK1914 testisignaalit.



Seuraavaksi luodaan projektille Program eli ohjelma PLC-valikon POUs-kohdasta, valitaan ohjelmointi kieleksi rakenteellinen teksti (ST). Ohjelmassa yhdistetään muuttujat bReset ja bErrAck, jo aiemmin luotuihin kytkimien muuttujiin. Kuva 23 nähdään ohjelman koodi.

Kuva 23. Ohjelman koodi.



MAIN-ohjelmalla kutsutaan äsken luotua ohjelmaa, mikä nähdään Kuva 24.

Kuva 24. Ohjelman kutsu.

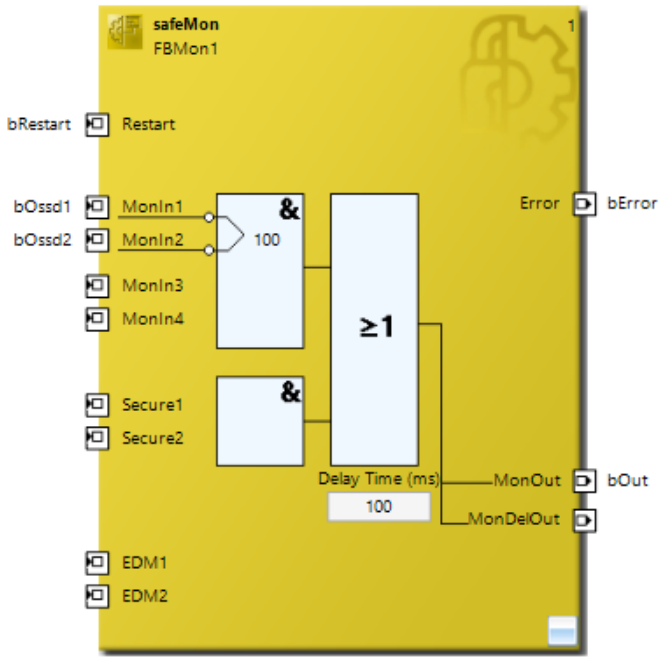
```
P_Restart        MAIN
1   PROGRAM MAIN
2   VAR
3
4   END_VAR
5

1   P_Restart();
```

Kytkinten muuttujat bButton ja bErrButton, linkitetään I/O-moduulin tuloihin 1 ja 2. Muuttujien linkitys onnistuu Solution Explorer-palkin DIO Inputs-kohdasta ja valitsemalla halutut tulot.

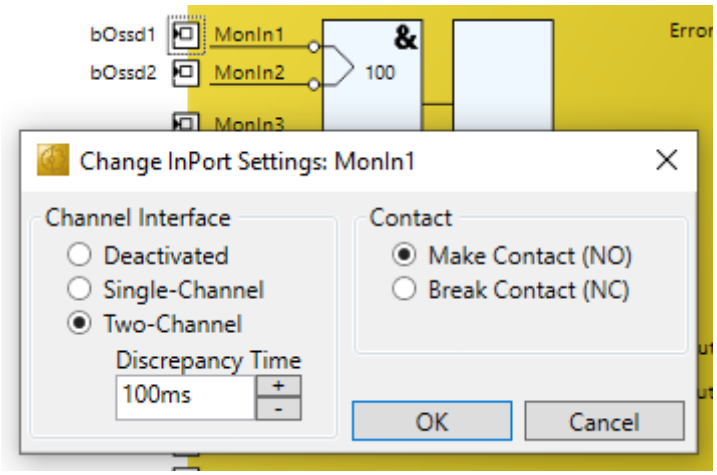
TwinSAFE-ryhmään TwinSafeGroup1, lisätään turvatoimilohko nimeltä safeMon, toimilohkon avulla saadaan turvavalopuomit toimintaan. Toimilohkon Restart-, MonIn1- ja MonIn2-tulot, sekä Error- ja MonOut-lähdöt voidaan nimetä Kuva 25 mukaisesti.

Kuva 25. Turvavalopuomin toimilohko.



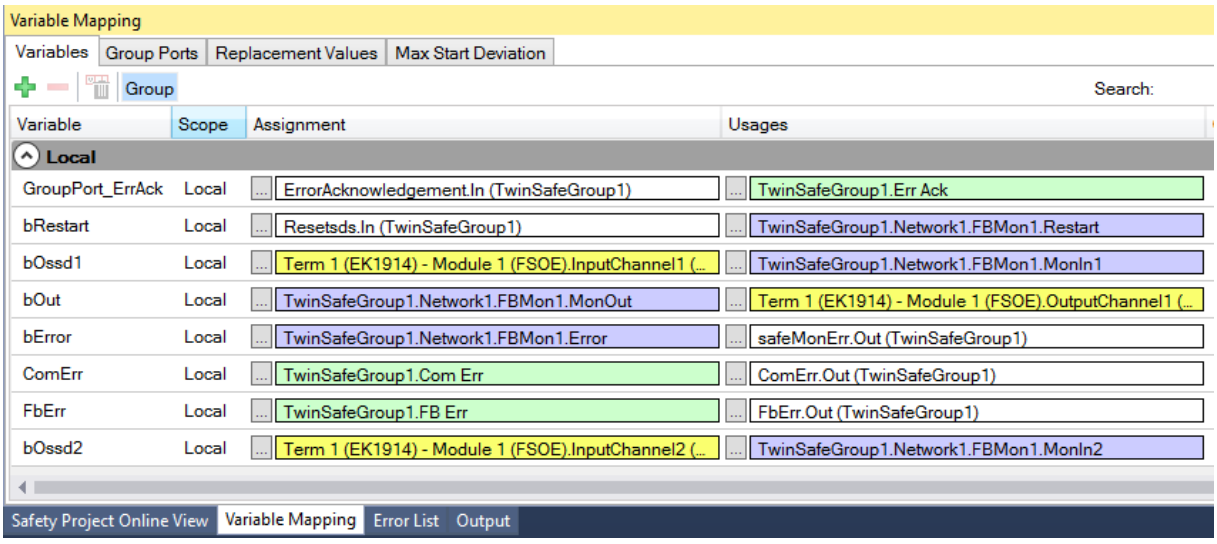
Toimilohkon MonIn1- ja MonIn2-tuloista tehdään kaksikanavaiset ja invertoidaan tulot, muutokset päästään tekemään klikkaamalla hiiren oikealla laatikosta ennen MonIn-tuloa ja valitsemalla Change InPort Settings. Kuva 26 nähdään MonIn-tulojen muutokset.

Kuva 26. Turvavalopuomin signaalien yhdistäminen.



TwinSAFE-ryhmä välilehdellä valitaan ikkunan alaosasta Variable Mapping ja Variables-valikko. Tässä valikossa tehdään linkitykset Alias-laitteiden ja ohjelman välille, sekä määritellään mikä turvatuloja ohjaa ja mitä turvalähdöt ohjaavat. Muuttuja bOSSD1 yhdistetään turvatuloon 1 ja bOSSD2 yhdistetään turvatuloon 2. Jokaiselle muuttujalle pitää valita Assignment ja Usage, valinnat on helppo suorittaa klikkaamalla laatikkoa, missä on kolme pistettä. Kuva 27 Assignment- ja Usages-laatikoiden väreistä voidaan päätellä mihin ne on liitetty, valkoinen on Alias-laite, keltainen turvatulo tai -lähtö, sininen kuuluu toimilohkoon ja vihreä linkitys tehdään kuvasta nähtävällä Group Ports-välilehdellä.

Kuva 27. Muuttujien kartoitus.



Turvavalopuomien kohdistus tehdään heti kun järjestelmä käynnistetään. Kohdistuksen tarkkuutta voidaan seurata vastaanotin puomin näytöstä, jos näyttö näyttää lukua 0, niin kohdistus on silloin erittäin huono. Näytön näyttäessä lukua 1, silloin kaikki säteet eivät ole vielä kohdillaan, jos näyttö näyttää lukua 2, niin kaikki säteet osuvat jo hyvin lähelle optimaalista paikkaa ja kun näyttö on tyhjänä, niin optimaalinen paikka on löytynyt. Kohdistustila kytkeytyy automaattisesti pois päältä, kun optimaalinen paikka on pysynyt 2 minuuttia ja kohdistuksen voi aloittaa uudestaan käynnistämällä järjestelmän uudestaan. (SICK, 2015b, s. 244)

Turvatoimilohkojen tilaa voi seurata lohkon alakulmassa olevasta neliöstä, mikä nähdään Kuva 28. Toimilohkon näyttäessä tilaa 0x03 ja neliö on keltainen, niin se on turvallisessa-tilassa. Tilan ollessa 0x02 ja neliö on punainen, niin toimilohko on pysäytys/virhetilassa. Toimilohkon näyttäessä tilaa 0x01 ja neliö on vihreä, niin toimilohko on käynnissä.

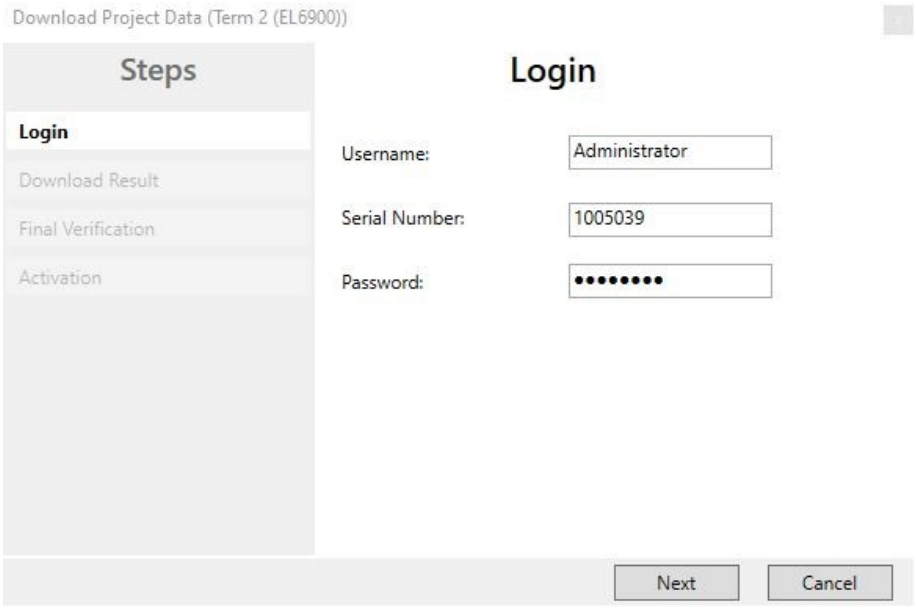
Kuva 28. Toimilohkon tila.

Ennen kuin turvaohjelma ladataan turvalogiikalle, aktivoidaan konfiguraatio ja suoritetaan Build Solution TwinCATin yläpalkin kohdasta Build, tällä tavoin varmistetaan, ettei koodauksessa tullut virheitä. Seuraavaksi verifioidaan turvaprojekti, verifiointi tehdään TwinCATin yläpalkin kohdasta TwinSAFE ja valitsemalla Verify Safety Project, jos turvaprojektin verifiointi menee läpi, tehdään seuraavaksi samasta valikosta Verify Complete Safety Project, millä tarkistetaan myös fyysiset komponentit. Koko turvaprojektin verifioinnin tulos nähdään TwinCATin alareunasta, jossa sinisellä pohjalla pitäisi lukea Verification Completed. Verifiointien jälkeen voidaan ryhtyä lataamaan turvaohjelmaa logiikalle.

Turvaohjelman lataus aloitetaan TwinSAFE-valikosta, missä valitaan Download Safety Project. Ennen latausta tarvitaan tunnukset kirjautumista varten. TwinSAFEn oletus käyttäjätunnus on Administrator ja oletus salasana on TwinSAFE. Turvalogiikan sarjanumeron löytää Solutien Explorer-palkin SAFETY osiosta ja valitsemalla Target System. Kirjautumisen jälkeen näytetään vielä lataus tulokset ja viimeisen verifioinnin tulokset, jonka

jälkeen järjestelmä aktivoidaan laittamalla salasana vielä kerran. Turvaohjelman lataus on valmis, kun TwinCAT ilmoittaa ikkunan alareunassa Download Process succeeded. Kuva 29 on turvaohjelman lataus prosessin kirjautumisosio.

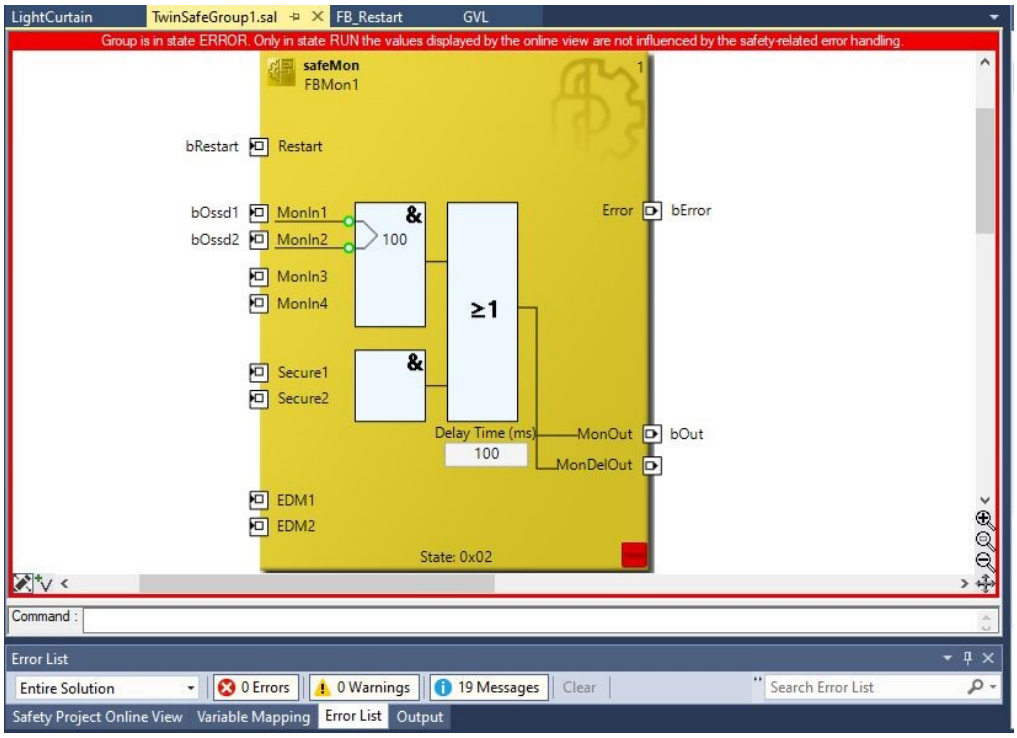
Kuva 29. TwinSAFE kirjautuminen.



3.5 Turvajärjestelmän toiminta

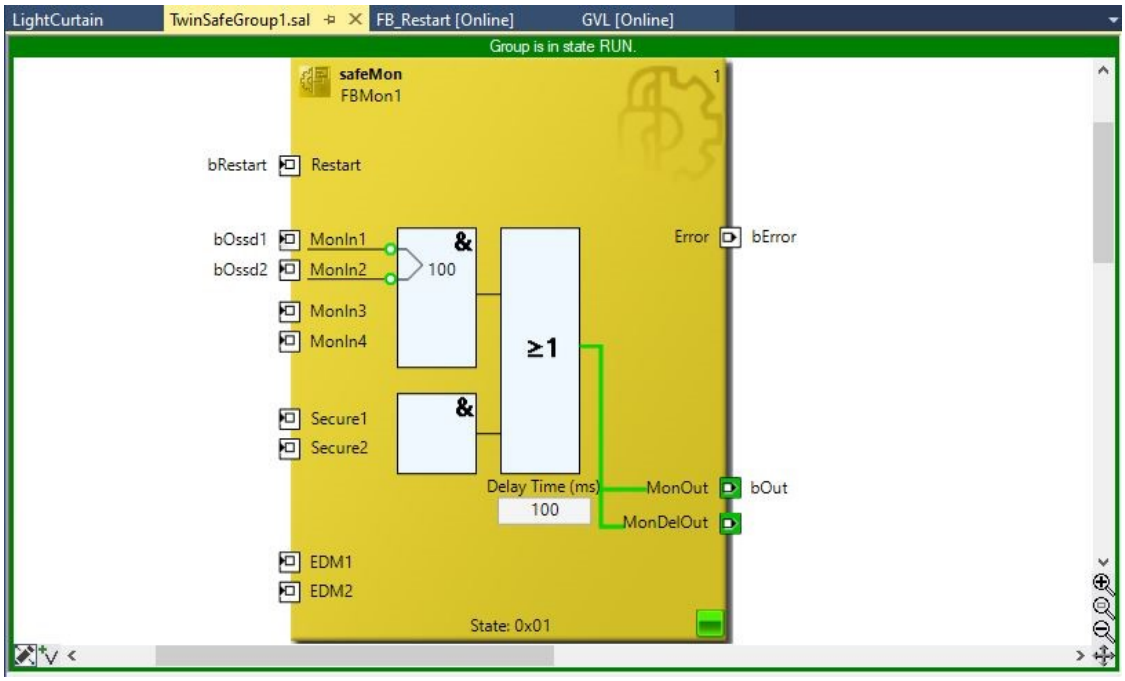
Turvaohjelman latauksen jälkeen, mennään ohjelmassa Online-tilaan klikkaamalla yläpalkista Login ja laitetaan ohjelma käymään painamalla play-nappia. Turvaohjelman tilaa ja toimintaa voidaan seurata, valitsemalla TwinSAFE-valikosta Show Online Data. Turvaohjelma näyttää aina virhetilaa, kun ohjelma käynnistetään, kuten Kuva 30 nähdään. Virheet saadaan poistettua, kun Error Acknowledgement-signaali huomaa nousevan- ja laskevan-pulssin. Ohjelmassa ErrAck-signaalia ohjaa muuttuja bErrButton, mikä on linkitetty I/O-moduulin tuloon 2, johon on liitetty kytkin.

Kuva 30. Turvaohjelman käynnistystila.



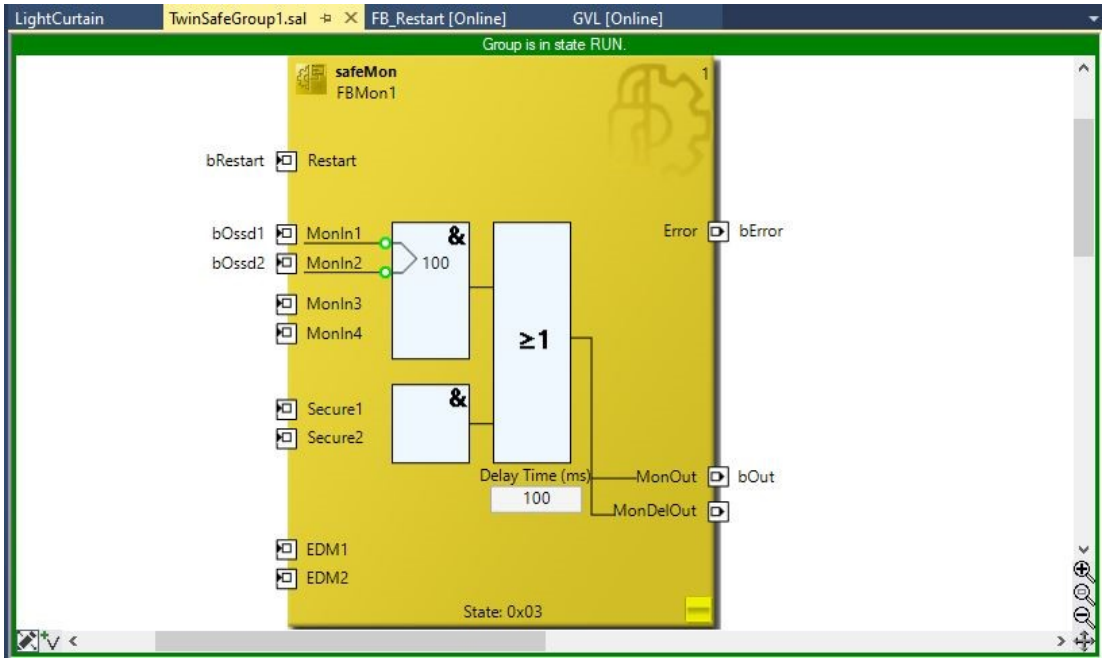
Virheiden kuittausten jälkeen resetoidaan toimilohko painamalla muuttujan bButton kytkintä, joka on työssä linkitetty I/O-moduulin tuloon 1. Resetointi pitää tehdä aina virheiden kuittausten jälkeen. Resetoinnin jälkeen toimilohko on käyntitilassa, eli turvatoiminnot ovat toiminnassa. Toimilohko näyttää Kuva 31 mukaiselta, kun resetointi on tehty. Turvaohjelman toiminnan voi tarkastaa bOut-muuttujan avulla, joka saa signaalin, mikä aktivoi turvalähdön 1, minne merkkivalo on kytketty.

Kuva 31. Turvaohjelma käynnissä.



Turvavalopuomeista läpi mentäessä, menee toimilohko turvatilaan ja merkkivalo sammuu. Ohjelma saadaan takaisin käyntiin resetoinnin kautta. Ohjelma on taas toiminnassa, jos merkkivalo on päällä. Kuva 32 nähdään, miltä toimilohko näyttää, kun turvavalopuomien läpi on kuljettu.

Kuva 32. Ohjelman turvatila.



4 Pohdinta

Opinnäytetyön tavoitteena oli suunnitella ja rakentaa turvajärjestelmä opetuskäyttöön, käyttäen standardien mukaisia ohjeita. Opinnäytetyö onnistui mielestäni hyvin ja aihe oli mielenkiintoinen. Työssä käytettiin standardin mukaisia menetelmiä riskinarvioinnissa ja turvatoimintojen määrittelyssä, sekä turvajärjestelmän komponentit olivat standardin mukaisia.

Opinnäytetyön aikana ymmärsin, miksi standardien mukainen suunnittelu ja järjestelmän rakennus ovat tärkeitä. Standardien avulla varmistetaan, ettei työympäristöihin tule vaarallisia järjestelmiä ja laitteita, mitkä voivat aiheuttaa pahimmillaan henkilövahinkoja. Uskon, että työn avulla saadaan käsitys standardien merkityksestä.

En ollut ennen opinnäytetyötä kokeillut turvajärjestelmien rakentamista tai ohjelmointia. Turvajärjestelmän ohjelmointi oli työn mieluisin, sekä haastavin osuus. TwinSAFE-ohjelmoinnista piti etsiä paljon tietoa, ennen kuin ohjelmoinnista sai niin sanotusti ¨kopin¨ ja kun ohjelmoinnin eri asioiden merkitykset alkoivat jäädä muistiin, oli ohjelmointi mieluista. Työssä oli myös haastavaa kertoa ohjelmoinnista ja ohjelmointiin valmistautumisesta ilman runsasta kuvien käyttöä.

Toivon, että opinnäytetyön avulla voidaan harjoitella ja tutustua turvajärjestelmien suunnitteluun ja rakentamiseen oikeaoppisesti. Isot kiitokset Hämeen ammattikorkeakoululle mieluisasta opinnäytetyöaiheesta. Opinnäytetyö tehtiin korona-aikana, joten olosuhteet työn tekoon olivat hieman haastavat. Haluan kiittää vielä opinnäytetyön ohjaajia ja koulun henkilökuntaa, jotka mahdollistivat mahdollisimman normaalin opinnäytetyö prosessin.

Lähteet

Alanen, J., Hietikko, M. & Malm, T. (2009). *Koneiden ohjausjärjestelmien toiminnallinen turvallisuus.* s. 20 – 21. Haettu osoitteesta https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2009/T2485.pdf

Arrow. (2018). Safety Light Curtains - How Do Light Curtains Work? Haettu osoitteesta https://www.arrow.com/en/research-and-events/articles/safety-light-curtains-principles-and-applications

Auma. (n.d.). Functional safety – SIL. s. 10. Haettu osoitteesta https://www.auma.com/index.php?eID=ix_product_ajax&action=download&fileUID=1662

Automation.com. (2018). A beginners PLC overview. Haettu osoitteesta https://www.automation.com/en-us/articles/2018/a-beginners-plc-overview-part-3-of-4-plc-inputs-an

Beckhoff. (2020). *CX9020 | Embedded PC ARM Cortex A8 CPU Manual.* s. 8 – 27. Haettu osoitteesta https://download.beckhoff.com/download/document/ipc/embedded-pc/embedded-pc-cx/cx9020_en.pdf

Beckhoff. (2019a). TwinCAT | eXtended Automation. s. 2 – 7. Haettu osoitteesta https://download.beckhoff.com/download/document/catalog/Beckhoff_TwinCAT3_e.pdf

Beckhoff. (2019b). EL6900. Haettu osoitteesta https://www.beckhoff.com/EL6900/

Beckhoff. (2019b). EL6900 | TwinSAFE Logic. Haettu osoitteesta https://www.beckhoff.com/EL6900/

Beckhoff. (2019c). CX9020. Haettu osoitteesta https://www.beckhoff.com/english.asp?embedded_pc/cx9020.htm

Beckhoff. (2019d). *TwinSAFE Logic FB.* s. 13. Haettu osoitteesta https://download.beckhoff.com/download/Document/automation/twinsafe/TwinSAFE-Logic-FBen.pdf

Beckhoff. (2019e). EK1914. Haettu 5.4.2020 osoitteesta https://www.beckhoff.com/EK1914/

Beckhoff. (2017a). *Operating instructions for EL6900.* s. 17. Haettu osoitteesta https://download.beckhoff.com/download/Document/automation/twinsafe/el6900en.pdf

Beckhoff. (2017b). *Operating instructions for EK1914.* s. 12 – 17. Haettu osoitteesta https://download.beckhoff.com/download/Document/automation/twinsafe/ek1914en.pdf

Beckhoff. (2015). TwinSAFE: Safety and I/O technology in one system. Haettu osoitteesta https://www.beckhoff.com/english.asp?bus_terminal/twinsafe.htm

Contact and Coil. (n.d.). *TwinCAT 3 Tutorial: Introduction to TwinSAFE.* Haettu osoitteesta http://www.contactandcoil.com/twincat-3-tutorial/introduction-to-twinsafe/

Control design. (2009). *What controls safety?* Haettu osoitteesta https://www.controldesign.com/articles/2009/safety0908/

Keyence. (n.d.). Understanding Safety Laser Scanners. Haettu osoitteesta https://www.keyence.com/landing/safety/pr_sz-v_safetyscanner.jsp

Konedirektiivi 42/EY/2006. Haettu osoitteesta https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0042:FI:HTML#d1e32-35-1

Phoenix Contact. (n.d.). *Standardit ja direktiivit.* Haettu osoitteesta https://www.phoenixcontact.com/online/portal/fi?1dmy&urile=wcm%3Apath%3A/fifi/web/main/products/technology_pages/subcategory_pages/Safety_Standards_and_directives/12aba7c3-a904-4cd5-9aea-791540c7fc6b

Pilz. (2014). *Safe Camera System SafetyEYE.* s. 8 – 12. Haettu osoitteesta https://www.pilz.com/download/open/Leaf_SafetyEYE_1003954-ENU-01.pdf

Pilz. (n.d.a). Turvallisuuden eheystaso (SIL). Haettu osoitteesta https://www.pilz.com/fi-FI/knowhow/law-standards-norms/functional-safety/en-iec-62061

Pilz. (n.d.b). EN ISO 13849-1: Suorituskykytaso (PL). Haettu osoitteesta https://www.pilz.com/fi-FI/knowhow/law-standards-norms/functional-safety/en-iso-13849-1

Pilz. (n.d.c). SafetyEYE-turvakamerajärjestelmä. Haettu osoitteesta https://www.pilz.com/fi-FI/eshop/00106002207042/SafetyEYE-Safe-camera-system

Realpars. (n.d.). What is a Safety PLC. Haettu osoitteesta https://realpars.com/safety-plc/

SICK. (2015a). *Guide for Safe Machinery.* s. 8 – 137. Haettu osoitteesta https://cdn.sick.com/media/docs/8/78/678/Special_information_Guide_for_Safe_Machinery_en_IM0014678.PDF

SICK. (2015b). *Operating instructions C2000/M2000.* s. 213 – 244. Haettu osoitteesta https://cdn.sick.com/media/docs/8/48/848/operating_instructions_c2000_m2000_da_de_en_fi_fr_el_it_nl_no_pt_sv_es_im0013848.pdf

SICK. (n.d.a). Turvavalopuomi toiminta-alueella. Haettu osoitteesta https://www.sick.com/fi/fi/toimialat/tyoestoekoneet/muovaavat-koneet/levyleikkuri/levyleikkurin-vaarakohtien-valvonta/c/p346604

SICK. (n.d.b). Kuljetuskone. Haettu osoitteesta https://www.sick.com/ag/en/small-agvs-carts/personnel-detection-and-machine-safety/protecting-a-automated-guided-cart-agc-with-a-safety-laser-scanner/c/p613550

SICK. (n.d.c). Monisäteiset turvavalopuomit M2000 sarjaan kytkettävä. Haettu osoitteesta https://www.sick.com/fi/fi/valosaehkoeiset-turvalaitteet/monisaeteiset-turvavalopuomit/m2000-sarjaankytkettaevae/c/g187283#selection

SICK. (n.d.d). M2000-Turvavalopuomi. Haettu osoitteesta https://www.sick.com/fi/fi/valosaehkoeiset-turvalaitteet/monisaeteiset-turvavalopuomit/m2000-standard/m20s-03140a122/p/p36723

Sundquist, M. (2011). *Toiminnallinen turvallisuus: periaatteet.* s. 13 – 18. Haettu osoitteesta https://www.automaatioseura.fi/site/assets/files/1431/asaf_teema_1_2011_jestelmsuunnittelu_171011.pdf

Tukes. (2014). CE-merkintä. Haettu osoitteesta https://tukes.fi/-/tuotteiden-ce-merkinnat-kunto-1

Tukes. (2007). *Turva-automaatio prosessiteollisuudessa.* Haettu osoitteesta https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0

Tukes. (2007). Riskin vähennys: yleiset periaatteet. Haettu osoitteesta https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0

Unitronics. (n.d.). What is the definition of ”PLC”? Haettu osoitteesta https://www.unitronicsplc.com/what-is-plc-programmable-logic-controller/

VTT. (2009). Suoritustason PL ja eheystason SIL vastaavuus. Haettu osoitteesta https://www.vtt.fi/inf/pdf/tiedotteet/2009/T2485.pdf