

Santtu Saukkonen

# Johdatus turva-automaation ohjelmointiin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)  
Automaatiotekniikka

Insinööriytyö

4.4.2016

Tekijä Otsikko	Santtu Kalevi Saukkonen Johdatus turva-automaation ohjelmointiin
Sivumäärä Aika	40 sivua + 1 liite 4.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Automaatiotekniikka
Suuntautumisvaihtoehto	
Ohjaaja	Lehtori Jari Savolainen
<p>Insinööriyössä perehdyttiin turvallisuusajatteluun koneiden ja tuotantolaitosten suunnittelussa, käytössä ja kunnossapidossa. Erityistä huomiota kiinnitettiin turva-automaation ohjelmointiin ja ohjelmoinnin suunnitteluun.</p> <p>Teoriaosiossa esiteltiin voimassa olevien EU:n direktiivien ja EU:n direktiiveistä valtioneuvoston tekemien asetusten merkitys automaatio-suunnitteluun. Pohdittiin myös, miten standardit liittyvät turva-automaatio-suunnitteluun EU/ETA-alueella sekä kansainvälisesti. Tässä osiossa esiteltiin myös standardien mukaiset tärkeimmät menetelmät turvallisuuden eheystason (TET) laskentaan. Turva-automaation logiikkaohjelmointiin pääosin vaikuttavia standardeja ovat IEC 61311, IEC 61508 ja IEC 61511.</p> <p>Teoriaosiossa esiteltiin Beckhoffin TwinSAFE-turva-automaatiojärjestelmä ja se, miten Beckhoffin hajautettu turva-automaatiojärjestelmä toteutetaan. Tiedonsiirtoon Beckhoff käyttää standardisoitua turvaluokiteltua EtherCAT-väylää.</p> <p>Käytännön osiossa tehtiin ohjeistus TwinCAT3-ohjelmalla tehtävään turva-automaation ohjelmointiharjoitukseen.</p>	
Avainsanat	Turva-automaatio-ohjelmointi, TwinSAFE, standardi, koneturvallisuus.

Author(s) Title	Santtu Kalevi Saukkonen Guide to Safety Automation Programing
Number of Pages Date	40 pages + 1 appendices April 2016
Degree	Bachelor of Engineering
Degree Programme	Automation Engineering
Specialisation option	
Instructor(s)	Senior Lecturer, Mr Jari Savolainen
<p>In this Bachelor's thesis, the safety aspects in planning, use and maintenance of machines and production plans were analysed. The programing and the planning of the safety automation were considered in more detail.</p> <p>In the theoretical part of the study, the significance of EU directives regarding automation planning is analyzed, as well decrees based on them, set by the Finnish Council of State. How standards affect automation planning in the EU/EEA-area and internationality is also considered. Furthermore, the most common methods are introduced for the analysis of security integration level (SIL). Standards IEC 61311, IEC61508 and IEC61511 are some of the most significant standards for logic programming of safety automation.</p> <p>In the theoretical part of this Bachelor's thesis, the TwinSAFE safety automation system of Beckhoff is introduced as well as how the distributed safety automation system is implemented. An EthetCAT-field bus system by Beckhoff is used for the transfer of data. The EthetCAT is safety classified and standardized in accordance with the requirements of IEC 61508 SIL 3.</p> <p>As a result, a guide was created for a safety automation programing exercise with the TwinCAT3 software application.</p>	
Keywords	Safety automation programing, TwinSAFE, standards, machine safety, safety automation of proses industry.

# Sisällys

## Lyhenteet

1	Johdanto	1
1.1	Teoria	1
1.2	Käytännönosio	1
2	Yleistä turvallisuudesta	2
2.1	Turva-automaatio	3
2.2	Koneturvallisuus	6
2.2.1	Suoritustaso PL	7
2.2.1	Koneiden turvakomponentit	8
2.3	Prosessiteollisuus	8
2.3.1	HAZOP ja LOPA	9
2.3.2	Vikapuu	9
2.4	Standardeista	10
3	Logiikkaohjelmointi	11
4	Beckhoff	12
4.1	TwinCATin projektipuu	13
4.1.1	SYSTEM	13
4.1.2	PLC	14
4.1.3	SAFETY	16
4.1.4	I/O	16
4.2	TwinSAFE	16
4.2.1	EL 6900	17
4.2.2	TwinSAFE-ohjelman tasot	18
4.2.3	Tiedonsiirto	18
4.2.4	TwinSAFE EL 6900:n toimilohkot (function block)	19
4.3	Pohdintaa miten TwinSAFE täyttää standardien vaatimukset	35
5	Lopuksi	36
	Lähteet	38
	Liitteet	

Liite 1. Koneturvallisuus. Turva-automaation ohjelmointiharjoitus Bechhoffin TwinSafe-järjestelmällä.

## Lyhenteet

B10 <sub>d</sub>	Määrä ohjelmistokiertoja kun 10 % komponenteista on vaarallisesti tuhoutunut.
dop	Käyttöaika päiviä vuodessa
EU/ETA	Euroopan unioni / Euroopan talousalue
EC	European Community. Eurooppalainen talousjärjestö.
IEC	International Electrotechnical Commission. Kansainvälinen sähkötekniikan komissio.
ISO	International Organization for Standardization. Kansainvälinen standardisointijärjestö.
PFD	Probability of dangerous failure on demand. Vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä.
PFH	Probability of a dangerous failure per hour. Vaarallisten vikaantumisten todennäköisyys tunnissa.
PL	Performance Level. Suoritustaso.
PLC	Programmable logic controller. Ohjelmoitava logiikka.
SAT	Site Acceptance Test, Kokonaiskelpoistus
SFF	Safe failure fraction (ks. TVO )
SFS	Suomen Standardisointiliitto.
SIL	Safety Integrity Level (ks, TET).
SIS	Safety instrumented System (ks. TAJ).

TAJ	Turva-automaatiojärjestelmä.
TET	Turvallisuuden eheyden taso.
TLJ	Turvallisuuteen liittyvä järjestelmä.
TVO	Turvallisten vikaantumisten osuus.
VTT	Valtion teknillinen tutkimuslaitos.

# 1 Johdanto

Työ on kaksiosainen, jakaantuen teoria- ja käytännönsioon. Teoriaosiossa käsitellään yleisesti prosessien ja koneiden suunnittelussa huomioitavia näkökohtia painottuen turva-automaation ohjelmistosuunnitteluun. Käytännön osiossa toteutetaan ja tehdään ohjeistus Beckhoffin turva-automaatiojärjestelmän simulointi- ja harjoitusympäristöön Metropolian Myyrmäen kampuksen automaatiotekniikan laboratorioon.

## 1.1 Teoria

Teoriaosiossa syvennyttään turvallisuusajatteluun yleisellä tasolla koneiden ja prosessien automaatio suunnittelussa, sekä turva-automaation vaatimuksiin EU määräysten ja standardien valossa. Tavoitteena on antaa yleiskuva koneiden ja prosessien turvallisuussuunnittelun yhtäläisyyksistä ja eroavaisuuksista. Käsitellään yhtäläisyyksiä prosessi- ja kappaletavarateollisuuden turva-automaation välillä.

## 1.2 Käytännönsio

Insinööriyön käytännön osiossa tehtiin laboratorioharjoitukset PC-pohjaisen turva-automaatiojärjestelmän ohjelmointiharjoitukseen. Harjoituksessa käytetään ohjelmointiympäristönä Beckhoffin TwinCAT3 työkalua. Beckhoffin turva-automaatiojärjestelmä on nimeltään TwinSAFE. TwinSAFEin sovellusohjelmat tehdään TwinCAT-ympäristössä. Tehdyn turva-automaationohjelmoinnin perusteella laadittiin harjoitus-työohje turvapiirien ohjelmointiin. Harjoituksen tarkoituksena on kehittää turva-automaatiojärjestelmien ohjelmoinnin perustaitoja, sekä logiikoissa ja niiden ohjelmistoissa esiintyvien ongelmien ratkaisukykyä.

Käytännön työ alkoi komponenttien kokoamisella simulointiympäristöksi. Harjoituksessa käytettävä Logiikka on Beckhoff CX9020, jolle alkuun määriteltiin automaatiotekniikan laboratorion sisäverkon kiinteä IP-osoite, ja ohjelmoitiin se logiikalle USB-väylän kautta luodulla yhteydellä. Tämän jälkeen liitettiin asennuskiskoon tarvittavat I/O-kortit ja TwinSAFE-koodin sisältävä siltayksikkö turva-CPU EL6900. Järjestelmän ohjelmointi ja hallinnointi tapahtuu TwinCAT3-ympäristössä.



## 2 Yleistä turvallisuudesta

Turvallisuusajattelun on sisällyttävä kaikkeen automaatiosuunnitteluun ja kunnossapiinon. Koneiden ja prosessien turvallisuudella tarkoitetaan koko tuotteen elinkaaren aikaista turvallisuutta. Standardien mukaan laitteiden ja järjestelmien on oltava valmistettavissa, toimittava suunnitellussa käyttötarkoituksessaan sekä oltava poistettavissa käytöstä vaarantamatta ihmisiä, koneita tai ympäristöä. Koneet ja prosessit on suunniteltava niin että ne toimivat turvallisesti myös, mikäli käyttäjä käyttää niitä kuviteltavin tavoin kohtuullisesti väärin.

Koneiden ja prosessien suunnittelua tekevien henkilöiden on aina lähdettävä liikenteeseen ajatuksesta, jotta pahin mahdollinen kuviteltavissa oleva tilanne toteutuu. Tämän ajatuksen kautta saadaan järjestelmät suunniteltua mahdollisimman turvallisiksi. (1.)

Koneiden ja prosessien suunnittelussa tarvitsee heti projektin aluksi, sekä aika ajoin tuotteen suunnittelun ja valmistuksen edetessä laskea sen turvallisuuden eheydentaso (TET). Koneasetusten kuin myös sähköistä suunnittelua säätelevien standardien mukaan turvallisuuden eheydentaso vaikuttaa, millaiset turvallisuusjärjestelmät koneeseen tai prosessiin on luotava.

Koneiden ja teollisuuslaitosten suunnittelua, ja siten myös automaation suunnittelua, säätelevät EU/ETA-alueella direktiivit, sekä direktiiveissä määritellyt standardit. Direktiiveistä on valtioneuvosto tehnyt Suomen lainsäädäntöön suomenkieliset asetukset. Koko EU/ETA-alueella voimassa olevat standardit jakaantuvat yhdenmukaistettuihin, sekä standardeihin, jotka ovat kansallisia ja näin voimassa koko EU/ETA-alueella. Euroopan komissio julkaisee listaa yhdenmukaistetuista standardeista Euroopan komission virallisessa lehdessä. SFS:n mukaan mikäli tuotteen turvallisuuteen liittyvää standardia ei ole yhdenmukaistettu, on suunnittelija vastuussa siitä, että tuote täyttää EU:n konedirektiivin liitteen yksi mukaisen tason. Myös prosessiteollisuuden järjestelmissä suunnittelija on viime kädessä vastuussa turvallisuusmääräysten täyttymisestä.

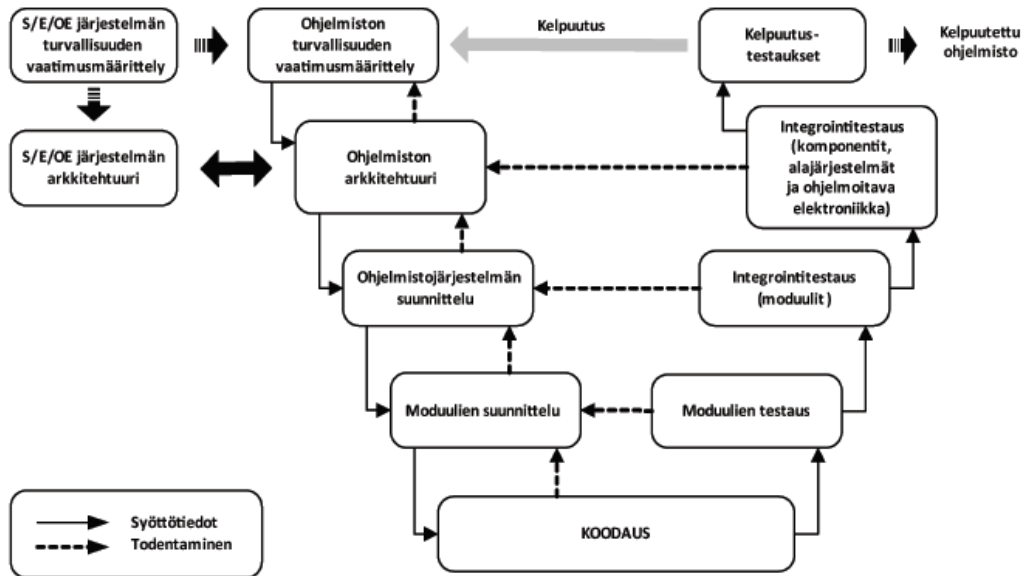
Automaatiosuunnittelussa on huomioitava, että koneet ja järjestelmät on suunniteltava sen alueen standardien mukaiseksi, jossa tuote otetaan käyttöön. Eri puolilla maailmaa on käytössä eri standardit, joissa etenkin automaatiota suunniteltaessa voi olla suuria eroavaisuuksia esimerkiksi teknisissä kaaviossa vaadittavien piirrosmerkkien, kaapelointien, logiikkaohjelmoinnin sekä dokumentoinnin suhteen.

## 2.1 Turva-automaatio

Turva-automaatiojärjestelmällä TAJ tarkoitetaan sitä prosessin tai koneen järjestelmää, joka on normaalista käyttöautomaatiojärjestelmästä erillinen järjestelmä. Turva-automaation on kaikissa tilanteissa, niin ennakoitavissa olevissa, ennakoimattomissa tilanteissa, kohtuudella kuviteltavissa olevissa koneen väärinkäyttö tilanteessa, kuin myös näiden kombinaation tapahtuessa, pystyttävä saattamaan prosessin tai koneen toiminta turvalliseen tilaan. Eli turva-automaatio suojaa viimeisenä ihmisiä, eläimiä, koneita, prosessia sekä ympäristöä vahingoilta.

Standardien hengen mukaisesti turva-automaatiojärjestelmien on pystyttävä toimimaan itsenäisesti, riippumatta siitä toimiiko perusautomaatiojärjestelmä.

Turva-automaatiojärjestelmiä suunniteltaessa kattostandardi on SFS-EN 61508 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Turva-automaatiojärjestelmien ohjelmistojen suunnittelua säätelee standardi IEC 61511 Functional safety - Safety instrumented systems for the process industry sector. SFS-EN 61508:n mukaan ohjelmistosuunnittelu toteutetaan ns. V-mallilla kuvan 1 mukaisesti. (2.) Seuraavat kuvat havainnollistavat mitä ohjelmistosuunnittelun V-mallilla tarkoitetaan. Kuvia luetaan vasemmalta ylhäältä alkaen. Standardin SFS-EN 61508-3 mukaan turva-automaatiojärjestelmän suunnittelu alkaa järjestelmän turvallisuuden sekä ohjelmiston turvallisuuden vaatimusmäärittelystä. Aina siirryttäessä V-mallissa vaiheesta seuraavaan on kyseinen vaihe testattava edeltävän kanssa ja todettava järjestelmä kyseiseen vaiheeseen asti toimivaksi. Mikäli johonkin vaiheeseen tarvitsee tehdä muutoksia, on se testattava edeltävän vaiheen kanssa ja todettava kokonaisuus toimivaksi. Viimeisimpänä järjestelmään tehdään kelpuutustestaus, mikäli järjestelmä ei läpäise kelpuutustestausta on koko V-malli käytävä uudelleen läpi. Kuva 1 on lainattu standardista SFS-EN 61508-3 ja kuva 2 on lainattu laadunohjauskurssin kurssimateriaalista.



Kuva 1. Standardin SFS-EN 61508-3 Kuva 6 Ohjelmiston systemaattisen kyvykkyyden ja kehittämisen elinkaarimalli (V-malli). (2.)

Automaation ohjelmistosuunnittelussa voi käyttää apuna myös ohjelmistotalojen ohjelmistojen suunnittelussa käyttämää kuvassa 2 olevaa v-mallia



Kuva 2. Ohjelmistosuunnittelussa käytetty V-malli. (3.)

Standardin SFS-EN 61508-1 kohdan 7.6.2.9 mukaan vaadittavaan TET-tasoon vaikuttaa, onko kyseessä harvojen vai tiheiden vaateiden toimintatapa, kohdassa 7.6.2.9 on määritelty vaadittavat turvallisuuden eheyden tasot niin harvojen kuin myös tiheiden vaateiden toimintatavalla. Mikäli turva-automaation vaatimustaso menee TET4-tasoon, on ensisijaisesti selvítettävä pystytäänkö muin toimin laskemaan TET-taso vaatimusta. Standardin hengenmukaista on suunnitella koneet sekä prosessit niin että päästään

mahdollisimman alhaiselle TET-tasolle. Aina on myös taloudellisesti edullisempaa, mitä pienimmän TET-tason turva-automaatiota tarvitaan.

Katsotaanko laitteiston olevan luokkaa A vai B, on määritelty standardissa SFS-EN 61508-2 kohdassa 7.4.4.1 Laitteiston turvallisuuden eheyden arkkitehtuuriset rajoitukset yleiset vaatimukset. Standardin mukaan laitteiston tyyppi vaikuttaa siihen, mikä on korkein sallittu turvallisuuden eheyden taso huomioiden laitteiston turvallisten vikaantumisten osuus, sekä vikasietoisuus.

Tarvittaessa SIL4-tason turva-automaattioratkaisua on laskettava myös yhteisten vikaantumisten osuus. Yhteisvikaantumisen osuuden arvo on mahdollista laskea käyttäen hyväksi Markovin metodia. (4.)

Turva-automaatiojärjestelmän elinkaari on määritelty standardissa SFS-EN 61508. Standardissa on määritelty vaatimuksia esimerkiksi testauksiin, joilla varmistetaan ohjelmistojen ja laitteiden toiminta.

Turva-automaatiojärjestelmät on suunnittelu- ja toimitusvaiheessa sekä käytön aikana määräajoin testattava. Kaikista testeistä tehdään vaaditut pöytäkirjat. Testeistä on tarkemmin standardissa SFS-EN 62381 Automation systems in the process industry - Factory acceptance test (FAT), site acceptance test (SAT) and site integration test (SIT). Testejä, joilla varmistetaan järjestelmän toiminta, ovat (5, s. 13–15) seuraavat:

- Tehdastestaus FAT (Factory Acceptance Test)  
Tämä testi tehdään yleensä virtuaaliympäristössä toimittajan tiloissa ja siinä pyritään varmistamaan ennen toimittamista, että automaatiojärjestelmä on oikein suunniteltu.
- Kylmätestaus. Tehdään tuotantolaitoksessa kun järjestelmä on asennettu paikalleen, ennen laitoksen käyttöönottoa. Tässä vaiheessa varmistetaan, että anturit ja toimilaitteet ovat oikein säädetyt.
- Viimeisenä TAJ:lle tehdään kokonaiskelpoistus SAT  
SAT-testi on osa koko prosessilaitoksen turvallisuuden kelpoistusta. Testissä testataan, että kaikki TAJ:n ohjelmistot ja komponentit ovat oikein asennetut ja toimivat oikein.

## Turvallisuuden eheyden taso TET

Standardeissa eri turvallisuuden eheyden tasojen määrittely on tehty suullisesti. Turvallisuuden eheydellä tarkoitetaan standardin SFS-EN 61508-4 kohdan 3.5.4 mukaan turvallisuuteen liittyvän järjestelmän kykyä suoriutua tehtävästään tyydyttävästi määrätyissä olosuhteissa määritellyn ajan. Turvallisuuden eheyden tasoja TET, eli englanniksi Security Integrity Level SIL, on standardin mukaan neljä. Tasolla TET4 on korkein turvallisuuden eheys, eli käytännössä tämä tarkoittaa sitä, että turvatekniikan on toimitava niin, jotta turvatoiminnot toteutuvat, vaikka osa turvajärjestelmistä olisi epäkunnossa niitä tarvittaessa. Matalin taso on TET1.

Käyttöautomaation TET/SIL-taso riippuu siitä onko kyseessä tiheiden vaateiden tai jatkuvan toiminnan, vai harvojen vaateiden toimintatapa. Turva-automaatiopuolelle löytyy useita menetelmiä TET-tason määrittelemiseen, esimerkiksi: ALARP-, kvantitatiivinen, riskigraafi-menetelmät ja LOPA. Menetelmät on kuvattu standardissa. Eri menetelmät on lueteltu standardin SFS-EN 61508-4 liitteessä B Menetelmien valinta turvallisuuden eheyden tason vaatimusten määrittämiseen.

Standardissa SFS-EN 61508 on yhtenäiset kaikkia tasoja koskevat määräykset turva-automaatiolle tasoille SIL1–SIL3, lisäksi on määritely vaatimukset SIL4-tasolle.

## 2.2 Koneturvallisuus

EU/ETA-alueella koneturvallisuuden kattodirektiivi on EU:n konedirektiivi 2006/42/EY, josta valtioneuvosto on Suomessa saattanut voimaan asetuksen 400/2008, Valtioneuvoston asetus koneiden turvallisuudesta.

Aina kun suunnitellaan koneita, sekä niiden modernisointia, on tiedettävä mitä standardeja on noudatettava suunnittelussa. Valtioneuvoston asetuksessa 2. 1Luku Yleiset säännökset 3§ Soveltamisalan rajaukset:

Jos koneeseen liittyvästä vaarasta säädetään jotakin toista direktiiviä vastavassa kansallisessa erityissäännöksessä, sovelletaan sitä tämän asetuksen sijasta. (6.)

Valtioneuvoston asetuksessa 400/2008 on selitetty varsin seikkaperäisesti koneiden suunnittelun vaatimukset. EU-direktiivit ja valtioneuvoston asetukset ovat pakottavaa lainsäädäntöä, sen sijaan standardien noudattaminen on vapaaehtoista. Koneita suunniteltaessa on suunnittelijan ja yrityksen kannalta suositeltavaa käyttää EU/ETA-määräysten mukaisia standardeja, sillä ne ovat voimassa koko talousalueella ja niissä on varsin yksityiskohtaisia vaatimuksia, sekä ne kertovat minimin turvallisuusratkaisuille. Asetuksen toisessa luvussa Markkinoille saattaminen ja käyttöön ottaminen 6§ Yhdenmukaistettujen standardien käyttö:

Jos kone on valmistettu yhdenmukaistetun standardin mukaisesti, jonka viite-numero on julkaistu Euroopan unionin virallisessa lehdessä, sen katsotaan täyttävän kyseisen yhdenmukaistetun standardin kattamat olennaiset terveys- ja turvallisuusvaatimukset. (6.)

Koneturvallisuusstandardit jakaantuvat A-, B- ja C-luokan standardeihin. A-luokan standardit ovat kattostandardeja jotka, määrittelevät SFS:n mukaan koneturvallisuuden perusfilosofian. B-luokan standardeissa on suunnittelijan tarvitsemaa perustietoa, ja C-luokan standardeissa on yksityiskohtaisia koneiden tai koneryhmien turvallisuusvaatimuksia. (7, s. 3.) Koneturvallisuuden A-luokan kattostandardi on SFS-EN ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. 2010.

Koneiden suunnittelua tekevien henkilöiden on aina varmistettava, onko olemassa kyseiseen suunnittelutyöhön liittyviä C-luokan standardeja. Mikäli asiasta on olemassa C- tai B-luokan standardeja, löytyy niistä viittaukset kyseisen laitteen suunnittelua sääteleviin ylemmän luokan standardeihin.

Yleensä konepuolella käytetään jatkuvien ja tiheiden vaateiden toimintatavan mukaista TET/SIL-tason laskentaa, sillä esimerkiksi koneen suojakatetta saatetaan avata useita kertoja tunnissa.

### 2.2.1 Suoritustaso PL

Standardissa SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1:Yleiset suunnitteluperiaatteet, 2008. on koneille määritelty suoritustaso PL (performance level), joka vastaa prosessiteollisuudessa ja muissa standardeissa määriteltyä SIL/TET-tasoa. Suoritustaso PL ymmärretään samoin kuin

SIL/TET-tason määritelmä. VTT:n tiedotteen 2485 mukaan standardissa SFS-EN 13849-1 PL-tasot ovat a–e. PL-tasolla a turvajärjestelmän pettämisen todennäköisyys ja mahdollisesti aiheutuvat vahingot ovat niin lieviä että SIL-luokituksessa ei ole vastaavaa tasoa. Korkein PL-taso e vastaa SIL-luokituksen tasoa SIL3. Koneturvallisuus standardissa ei tunneta SIL4 luokan tilannetta, sillä koneiden suunnittelua säätelevien määräysten piiriin kuuluvien laitteiden rikkoontuessa ei pahimmassakaan tilanteessa ole mahdollista kuolla useita ihmisiä ja aiheutua laajoja ympäristövahinkoja. (8, s. 18–26.)

### 2.2.1 Koneiden turvakomponentit

Turva-automaatiojärjestelmiin suoraan liittyvät komponentit on merkittävä selkeästi, yleensä keltaisella värillä. Standardissa SFS-EN ISO 13850 Koneturvallisuus. Häätäpysäytys. Suunnitteluperiaatteet kohdassa 4.3.1 sanotaan, että Hätäseis-painikkeiden on oltava helposti tunnistettavissa.

Turva-automaatioon liittyvät järjestelmät on suunniteltava niin, että niiden kuviteltavissa olevassa vikaantumistilanteessa koneen toiminta estyy, esimerkiksi häätäpysäytysjärjestelmät on suunniteltava niin että hätäseiskytkimen vioittuessa kone ei toimi. Käynnissä olevan koneen on hätäseiskytkimen vioittuessa pysähdyttävä. Häätäpysäytyksen suunnittelu määritellään Häätäpysäytys-standardissa SFS-EN ISO 13850. (9.)

### 2.3 Prosessiteollisuus

Turva-automaatiolla ymmärretään järjestelmää, jonka tehtävänä on saattaa prosessi turvalliseen tilaan siinä vaiheessa, kun perusautomaatiojärjestelmä ei pysty pitämään prosessia hallittavissa. Prosessiteollisuudessa prosessit ja järjestelmät on suunniteltava niin, että ensisijaisesti perusautomaatiojärjestelmä pystyy kontrolloimaan tuotantoa.

Prosessiteollisuudessa TET/SIL-tason laskentaan käytetään yleensä harvojen vaateiden toimintatapaa, sillä on oletettavaa turvatoimintoja tarvittavan harvemmin kuin keran vuodessa.

Suunniteltaessa uusia prosessiteollisuuden laitoksia, modernisointeja ja huoltoseisokkeja on aina tehtävä riskianalyysi suunnitelmasta. Tapoja riskianalyysin tekemiseen

ovat laitoksen laajoja osakokonaisuuksia huomioivat HAZOP- ja LOPA-menetelmät, sekä yksityiskohtaisempi vikapuumenetelmä. (1.) Riskianalyysia varten osien yhtäaikaisen vikaantumisen mahdollisuutta voidaan laskea esimerkiksi Markovin metodilla, jolloin saadaan huomioitua osien turvallisen eli ennakoitavissa olevan vikaantumisen ja vaarallisen eli täysin ennakoimattomissa olevan vikaantumisen todennäköisyys tapahtumiin. (4.)

### 2.3.1 HAZOP ja LOPA

HAZOP on poikkeamatarkistelu, joka VTT:n oppaan (10, s. 84) mukaan sopii käytettäväksi erityisesti kemianteollisuudessa. HAZOP- ja LOPA-menettelyissä perustetaan erillinen työryhmä, jonka jäsenenä on laitoksen suunnitteluun ja toimintaan osallistuvia asiantuntijoita. Kummassakin menetelmässä merkitsee kukin asiantuntija menetelmän mukaiseen riskimatriisiin arvioimiaan riskitekijöitä. Näin pystytään sekä vähentämään mahdollisia riskejä että luomaan edellytykset suunnitella niin prosessin normaalitoimintaan kuin myös poikkeustilan toimintaan tarvittava instrumentaatio ja automatiikka. Dokumentin The Layer of Protection Analysis (LOPA) method mukaan LOPA on Standardin IEC 61511 part 3 Annex F:n mukainen menettely.

### 2.3.2 Vikapuu

Vikapuuanalyysissä tarkistellaan prosessin yksittäisen osan turvatoimintoja. Lasketaan todennäköisyys sille, että prosessin turvatoiminnot pettävät niitä tarvittaessa. Turvatoimintojen osille määritellään todennäköisyys, millä ne eivät toimi niitä tarvittaessa Fractional dead Time (FDT). (11, s.167.) Laskettaessa vikapuun avulla yhteen kunkin yksittäisen toiminnon vikaantumisen todennäköisyys saadaan selville turvatoiminnon toimimattomuuden todennäköisyys sitä tarvittaessa.

FDT lasketaan kaavalla (12, s. 18):

$$FDT = 0,5 * f * T$$

jossa  $f$  on turvalaitteen vikaantumistaajuus ja  $T$  määräaikaistestausten väli. FDT on todennäköisyys ilman yksikköä, ja  $f$ :n sekä  $T$ :n yksikkö on kertaa vuodessa eli X tapahtumaa/vuosi.



Vikapuuanalyysistä on hyötyä määriteltäessä, onko kyseiseen prosessinosaan suunniteltu turvatoiminto riittävä. Konepuolella vikapuu eroaa hieman prosessipuolen vikapuusta, sillä koneet on mahdollista sammuttaa esimerkiksi hätäseis-toiminnolla, mutta käynnissä olevaa kemiallista prosessia ei saada pysäytettyä hetkessä, vaan se jatkaa etenemistään huonompaan suuntaan tai se saadaan vakautettua.

## 2.4 Standardeista

EU-direktiivien ja niistä tehtyjen kansallisten asetusten sekä näiden määrittelemien standardien päätehtävänä on yhtenäistää säännöstöä EU/ETA-talousalueella. Yhtenäisen säännöstön ansiosta on voitu luoda järjestelmä, jossa kun tuote on määräysten mukaisesti valmistettu ja se on CE-merkitty, voidaan konetta sekä sen CE-merkittyjä osia myydä koko talousalueella. On olemassa tuotekohtaisia eroja siinä, riittääkö CE-merkintään vain valmistajan ilmoitus vai vaaditaanko jonkin virallisen verifioijan testaus.

Kansainvälisten standardien pääasiallinen merkitys on saattaa hyväksi havaitut puitteet tuotteiden suunnittelulle maailmanlaajuiseen käyttöön. Yhtenäiset, yleisesti hyväksytyt kansainväliset standardit helpottavat uusien tekniikoiden ja ajatusten leviämistä sekä kansainvälistä kauppaa. Standardien ansiosta suunnittelijat sekä kunnossapidon puolen ihmiset pystyvät hankkimaan yhteen tuotantolaitokseen komponentteja useammalta eri laitevalmistajalta. Laite- ja ohjelmistovalmistajat voivat kuitenkin luoda standardien puitteissa toisistaan eroavia yksilöllisiä tuotteita, mikä mahdollistaa terveen taloudellisen kilpailun.

Standardeissa on paikoin ohjauksia toisiin standardeihin, sekä maininta että kyseisen asian kohdalla on syytä noudattaa viitatus standardin viitatus kohdan mukaista ohjeistusta.

Kansainvälisiä standardeja ovat esimerkiksi IEC (International Electrotechnical Commission) ja ISO (International Organization for Standardization).

### 3 Logiikkaohjelmointi

Logiikoiden ohjelmointikielet ja yleiset säännöt on määritelty kansainvälisen standardin IEC 61131 Programmable controllers osissa 1–9. IEC 61131 on standardi ohjelmoitavista logiikoista. Logiikoissa käytettävät ohjelmointikielet on määritelty standardissa IEC 61131-3, josta Suomen Standardisoimisliitto SFS ry on julkaissut englanninkielisen standardin SFS-EN 61131-3 Programmable controllers - Part 3: Programming languages. Kyseisessä standardissa määritellään logiikoiden ohjelmointikieliksi kaksi tekstimuotoista kieltä ja kolme graafista kieltä: (13.)

Standardin mukaiset tekstimuotoiset kielet ovat

- käskylista, Instruction List (IL)
- strukturoitu teksti, Structured Text (ST)

Standardin mukaiset graafiset kielet ovat

- tikapuukaavio, Ladder Diagram (LD)
- toimilohkokaavio, Function Block Diagram (FBD)
- sekventiaalinen toimintakaavio, Sequential Function Chart (SFC)

Standardisoitujen ohjelmointikielten- ja menetelmien käyttö helpottaa suunnittelijoiden siirtymistä ohjelmointiympäristöstä toiseen. (14, s. 9.) Kuitenkin standardien yleisen luonteen vuoksi on ohjelmoijan aina tutustuttava kunnolla käyttämäänsä ympäristöön, sillä eri valmistajien ohjelmointiympäristöt eroavat toisistaan.

Turva-automaation logiikkaohjelmointi

Prosessiteollisuudessa turva-automaation logiikkaohjelmointia ohjeistaa standardi IEC 61511 Functional safety - Safety instrumented systems for the process industry sector, kyseinen standardi on tarkoitettu ohjelmoijien, toteuttajien ja käyttäjien käyttöön. Turva-

automaatiojärjestelmiltä vaadittavasta reaaliaikaisuudesta, sekä turva-automaation logiikkojen ohjelmistojen standardin IEC 61511 mukaisesta turvallisuusvaatimuksesta johtuen, on käytettävä yksinkertaisempia ohjelmointikieliä. (15.)

Turva-automaation ohjelmoinnissa sallitut ohjelmointikielet ovat standardin SFS-EN 61508-4 kohdan 3.2.14 Rajoitetun Muuntelun Kieli mukaan seuraavat:

- tikapuukaavio, ladder diagram
- Boolean algebra
- toimilohkokaavio, function block diagram
- sekventiaalinen toimintakaavio, sequential function chart

Standardissa on määritelty vaatimukset logiikkaohjelman luonnille sekä vaatimuksia turva-automaatiojärjestelmien kunnossapidolle. Kunnossapidon on esimerkiksi pystyttävä tekemään järjestelmään päivitykset ilman turva-automaatiojärjestelmän toiminnan häiriintymistä. Mainittuna tapana on esimerkiksi käyttöpaneelin erottaminen muusta järjestelmästä päivityksen ajaksi, ANSI/ISA-84.00.01-2004 Part 1 11.7.2 Maintenance/engineering interface requirements -kohdan mukaan. (16.)

#### **4 Beckhoff**

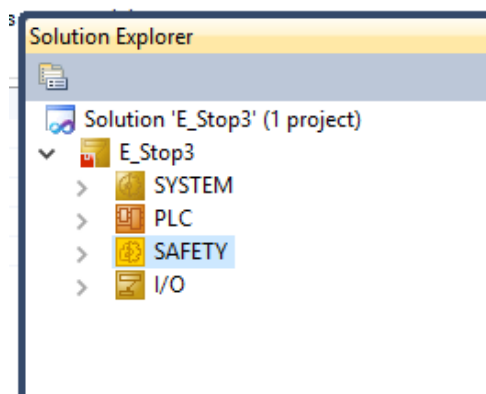
Beckhoffin automaatio-sovellukset ovat PC-pohjaisia. Tällä hetkellä uusien sovellusten kehitysympäristönä on TwinCat2:sta kehitetty TwinCAT3-ohjelmisto. Pohjimmiltaan TwinCAT-logiikkaohjelmistojen ohjelmointiympäristö on Codesys-ympäristö. (17, s. 13.) TwinCat2:ta käytetään, yhä vuonna 2016, niiden ohjelmistojen hallintaan ja päivittämiseen, jotka on tehty sillä. TwinCAT3 on integroitu Microsoft Visual Studioon. Myös TwinCAT3-ympäristössä pystytään tekemään muutoksia TwinCat2:lla luotuihin ohjelmiin.(18.) TwinCAT-ohjelmisto soveltuu lähes kaikkien reaaliaikaisten PC-pohjaisten automaatio ratkaisujen, kuten LC-, NC-, CNC- ja robottijärjestelmien ohjelmointiin. TwinCAT3:ssa on työkalut standardin IEC 61131-3 mukaisten ohjelmointikielten sekä C/C++ -kielten ohjelmointiin. TwinCAT3-ohjelmointiympäristö tukee myös säätötekni-

kassa tarvittavien parametrien ohjelmointia sisältäen Matlab ®/Simulink® -työkalut. (19.)

Beckhoffin logiikkaohjelmointi tapahtuu standardissa IEC 61131-3 määritellyin ohjelmin, ohjelmointi tehdään TwinCAT3-työkalulla. Insinööriyöhön kuuluneessa harjoitustyössä (liite1) logiikkana käytettiin logiikkaa CX9020, joka tukee kyseistä standardia.

#### 4.1 TwinCATin projektipuu

TwinCAT-ohjelman projektipuu löytyy solution explorerista. Projektipuun kautta ohjelmoija pystyy liikkumaan sovelluksen eri osien välillä, haluamaansa osioon. Kuvasta 3 on nähtävissä TwinCAT-ohjelman projektipuun päävalikot.



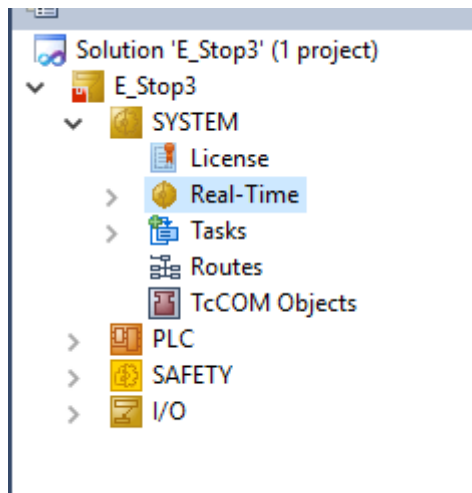
Kuva 3. TwinCATin projektipuu

Projektipuussa osiot ovat niin, että ylimpänä on yksittäisen projektin kannalta merkityksellisimmät osiot ja alimpana kaikille projekteille yhteiset osiot. Päällimmäisenä projektipuussa näkyy luodun projektin nimi. Projektipuun kansiot ovat alakansioita, joista kyseistä projektia hallinnoidaan. TwinCAT-projektipuuosion lähteenä käytettiin sivustolta [www.infosys.beckhof.com](http://www.infosys.beckhof.com) löytyvää materiaalia, sekä projektin käytännön osion tekoaihana kertynyttä tietotaitoa.

##### 4.1.1 SYSTEM

SYSTEM-osiossa hallinnoidaan projektin lisenssejä, projektin ajon ajastusasetuksia, sekä koko projektille yhteisiä reititysasetuksia. Kuvassa 4 on näkyvillä SYSTEM-valikot.

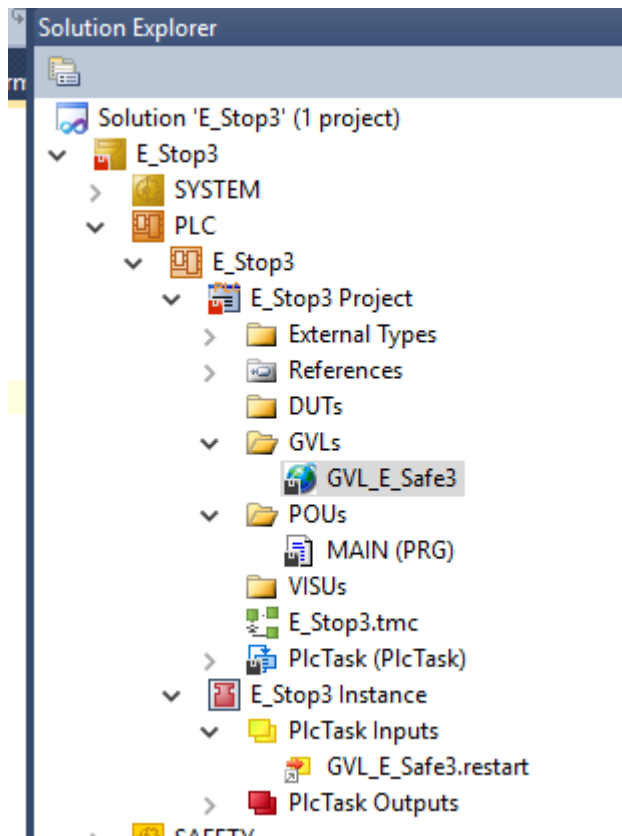
*Real-Time*-välilehdellä luodaan projektin sisäiset ajastukset, eli miten tiheästi projektin eri osat ottavat yhteyttä toisiinsa ja missä tärkeysjärjestyksessä logiikka käsittelee niitä. *Route*-välilehdellä määritellään yhteys projektista logiikkaan, eli mille logiikalle kyseinen sovellus on tehty. *License*-välilehdeltä nähdään ohjelman lisenssit ja päästään hallinnoimaan niitä.



Kuva 4. SYSTEM-valikko

#### 4.1.2 PLC

PLC-osiossa hallinnoidaan kyseisen projektin logiikalla olevia sovelluksia, eli tehtävä osioita, joita logiikalla ohjataan. Osiossa tehdään kaikki käyttöautomaation logiikkaohjelmointi ohjelmoijan haluamalla tai yrityksessä yhteisesti päätetyllä standardin mukaisella ohjelmointikielellä. TwinCAT-ohjelmisto osaa kääntää automaattisesti ohjelman koodin standardin mukaiselta kieleltä toiselle. Kuvassa 5 on nähtävissä *PLC*-osion välilehdet. Tässä kappaleessa kerrotaan tarkemmin vain insinööriyön käytännönsiossa (liite 1) tehdyssä turva-automaation ohjelmointiharjoituksessa tarvittavista *PLC*-osion välilehtien sisällöstä.



Kuva 5. PLC-valikko

GVLs-välilehdellä luodaan ohjelmaan haluttavat globaalit muuttujat ja määritellään, mitä tyyppiä ne ovat.

POU:hun luodaan projektin pääohjelma, sekä täällä tehdään muuttujien väliset reititykset. POU on yksinkertaisimmillaan lyhyt pääohjelman määrittely sekä tarvittavat reititykset globaalien muuttujien välille. Ohjelmointi Graafisilla logiikkaohjelmointikielillä tehdään POU:ssa, ja tekstimuotoisilla kielillä DUT:ssa.

PLC-valikon alimmassa osiossa tehdään globaalien muuttujien reititykset haluttujen I/O-korttien haluttuihin osoitepaikkoihin. Globaalien muuttujien reititykset turva-automaation siltakomponentteihin tehdään tässä osiossa.

Käyttöautomaation ohjelmiston simulointi eli kylmättestaus voidaan tehdä tässä osiossa. Ohjelmiston kylmättestaus on tärkeää, jotta nähdään, toimiiko tehty sovellus teoriassa niin kuin halutaan. On kustannustehokasta ohjelmiston suunnitteluvaiheessa tehdä tarvittavat muutokset.

#### 4.1.3 SAFETY

Projektin turva-automaatiota hallinnoidaan SAFETY-osiossa. Turva-automaatiolle on projektipuussa täysin oma valikkonsa, sillä koneiden ja prosessien turvajärjestelmien on toimittava täysin itsenäisesti riippumatta siitä, missä tilassa päälogiikan ohjelma on. Tässä osiossa ohjelmoidaan turva-automaation ohjelmisto sekä tehdään tarvittavat reititykset. Turva-automaation Application-tason ohjelmointi tehdään SAFETY-kansiosta löytyvissä työtiloissa, joissa tämän insinööriyön käytännönosion ohjelmointi on tehty. Jäljempänä oleva teoriaosa käsittelee tämän valikon funktioita.

#### 4.1.4 I/O

I/O eli input/output-valikko on perustason valikkona yksi TwinCATin tärkeimmistä osista. Täältä on löydettävä kaikki tarvittavat I/O-laitteet (I/O devices), jotta niitä ja niihin liitettjä laitteita voidaan ohjata projektista.

I/O-välilehdellä voidaan hallita kaikkien samassa aliverkossa olevien laitteiden input- ja outputliitäntöjä. Tässä valikossa saa tuotua projektiin tarvittavat saman aliverkon eri tietoliikenneprotokolliin yhdistetyt laitteet, sekä luotua täysin uudet I/O-yhteydet. Hallinnointityökalujen avulla voidaan määrittää I/O-osoitteet ja sekä toimintaa testattaessa että toiminnan aikana katsottua jokaisessa yksittäisessä I/O:ssa tapahtuvaa tietoliikennettä I/O:n omasta valikosta. TwinSAFE-järjestelmän Hardware-tasolla sijaitsevat komponentit löytyvät tästä valikosta.

#### 4.2 TwinSAFE

Beckhoffin turva-automaatiojärjestelmän nimi on TwinSAFE. Turvakomponentit on valmistettu standardien DIN EN ISO 13849-1:2008 (Cat4, PL e) ja IEC 61508:2010 (SIL3) määräykset täyttäväksi Beckhoff.com EL2902 ja EL1904 Technical data-sivujen mukaan. TwinSAFE-komponentit on suunniteltu niin että niitä voidaan käyttää myös ATEX-luokitelluissa tiloissa.(20.) Turvaominaisuudet tuodaan Beckhoffin automaatiojärjestelmiin siltakomponenteilla (EtherCAT Terminals), joissa sijaitsee järjestelmän turva-automaation CPU.

#### 4.2.1 EL 6900

Harjoitustyössä siltakomponentilla EL6900 tuodaan TwinSAFE-turva-automaatio-ominaisuus järjestelmään. Turva-automaatiologiikan EL6900 varmuuskopio-ohjelma pyörii yhtä aikaa myös tavallisella turvaluokittelemattomalla logiikalla, mistä järjestelmä osaa kopioida sen automaattisesti, mikäli EL6900 joudutaan vaihtamaan. EL6900 valvoo turvatuloilta inputeilta tulevaa dataa ja ohjaa turvalähtöjä outputeja. I/O:ilta tuleva data siirtyy reaaliaikaisesti myös logiikalle, jolla varmuusohjelma pyörii.

Yhteen EL6900:aan voidaan liittää 128 turvalaitetta ja ohjelmoida 256 toimilohkoa. Riippuen siitä millainen turva-automaatiojärjestelmä halutaan rakentaa, hankitaan tarvittava määrä komponentteja EL6900. Jokainen komponenteista toimii itsenäisesti niin kuin se on ohjelmoitu. Eli käytännössä turva-toiminnon redundanttisuus sitä vaadittaessa saadaan toteutettua.

Logiikoissa, jotka soveltuvat luokituksensa perusteella sekä turva-automaation että käyttöautomaation ohjaamiseen, on komponentin sisällä käytännössä vähintään kaksi erillistä logiikkaa. Standardien mukaan turva-automaation on toimittava itsenäisesti, sen on oltava riippumaton käyttöautomaation tilasta ja kyettävä saattamaan prosessi turvalliseen tilaan kaikissa tilanteissa. Turva-automaation logiikkojen toimintaa valvoo logiikan sisäinen watchdog-ohjelmisto.



#### 4.2.2 TwinSAFE-ohjelman tasot

TwinSAFE sovelluksessa turvaohjelmisto on jaettu kuvan 6 mukaisesti kolmeen eri tasoon, eli tasoihin *Application Level*, *Alias Level* ja *Hardware Level*.



Kuva 6. TwinSAFE:n eri tasot. (20.)

Hardware eli perustasolla sijaitsevat kaikki I/O:t eli myös ne jotka eivät ole osa turva-automaatiojärjestelmää. Alias tasolla reititetään hardware tasolla olevat I/O:t turva-automaation softalle eli Application Levelille.

Tasojen välillä on eroja siinä, miten paljon käyttäjä voi tehdä muutoksia itse softaan. Hardware-tasolle voidaan lisätä ohjelmallisesti I/O:ita standardissa IEC 61131-3 määritettyjen tekstikielten avulla. Alias-tasolla saadaan ilmoitettua eri tulot ja lähdöt sovellustasolle, tälle tasolle ohjelmoija pystyy luomaan eri I/O:t.

Syvin taso on niin sanottu Application Level. Tällä tasolla tehdään turva-automaatio-ohjelmointi standardin IEC 61511 mukaisin kielin. Application Levelillä olevien toimilohkojen sisältöä pääsevät muuttamaan vain Beckhoffin edustajat. TwinCATin TwinSAFE-turvaohjelma ohjelmoidaan toimilohkojen avulla.

#### 4.2.3 Tiedonsiirto

Beckhoffin järjestelmässä tietoliikenne tapahtuu EtherCAT-standardin mukaisesti. EtherCAT-tiedonsiirtostandardi on hyväksytty protokollaksi turva-automaatiojärjestelmien tiedonsiirtoon. Samaa väylää voidaan käyttää yhtä aikaa myös käyttöautomaation tiedonsiirtoon. EtherCAT täyttää standardin IEC 61784-3 Functional safety fieldbuses -

General rules and profile definition vaatimukset. EtherCAT-protokollan tiedonsiirtoon voidaan käyttää tunnettuja tiedonsiirtomenetelmiä. EtherCAT-tiedonkeruunopeus 1000 I/O:ta kohden on 30 µs. Kyseinen tiedonsiirtonopeus täyttää valmistajan mukaan turva-automaatiolta vaaditun reaaliaikaisuuden.

#### 4.2.4 TwinSAFE EL 6900:n toimilohkot (function block)

Kyseiset turva-automaation toimilohkot ovat käytävissä 7 päivän kokeilulisenssillä, ilmeisesti täysilisenssi sisältää enempi safeturvalohkoja. (21, s. 153.) Ainakin siltakomponentti EL 6910 sisältää muitakin lohkoja. (21, s. 16.)

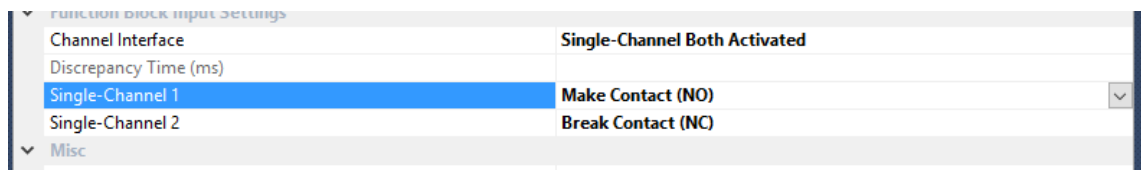
Turva-automaation input/In-tulot voidaan toteuttaa myös turvaluokittelemattomien inputtien kautta. (22, s.17.) Turva-output-lähdöt on toteutettava turva-outputien kautta. Tarkat englanninkieliset kuvaukset turvatoimilohkoista ja niiden toiminnasta löytyy lähteenä olevasta Beckhoffin dokumentista Documentation EL6900-FB, KL6904-FBTwinCAT function blocks for TwinSAFE logic terminals. (22.)

Lähdedokumentissa Documentation EL6900-FB, KL6904-FBTwinCAT function blocks for TwinSAFE logic terminals Version: 2.4.1 Date: 2015-03-11 esimerkit ovat TwinCAT2-ohjelmassa olevassa muodossa. Toimilohkojen toimintaperiaatteet sekä TwinCAT2:ssa että TwinCAT3:ssa ovat samat, mutta itse ohjelmoinnissa ja käytössä on hieman eroja.

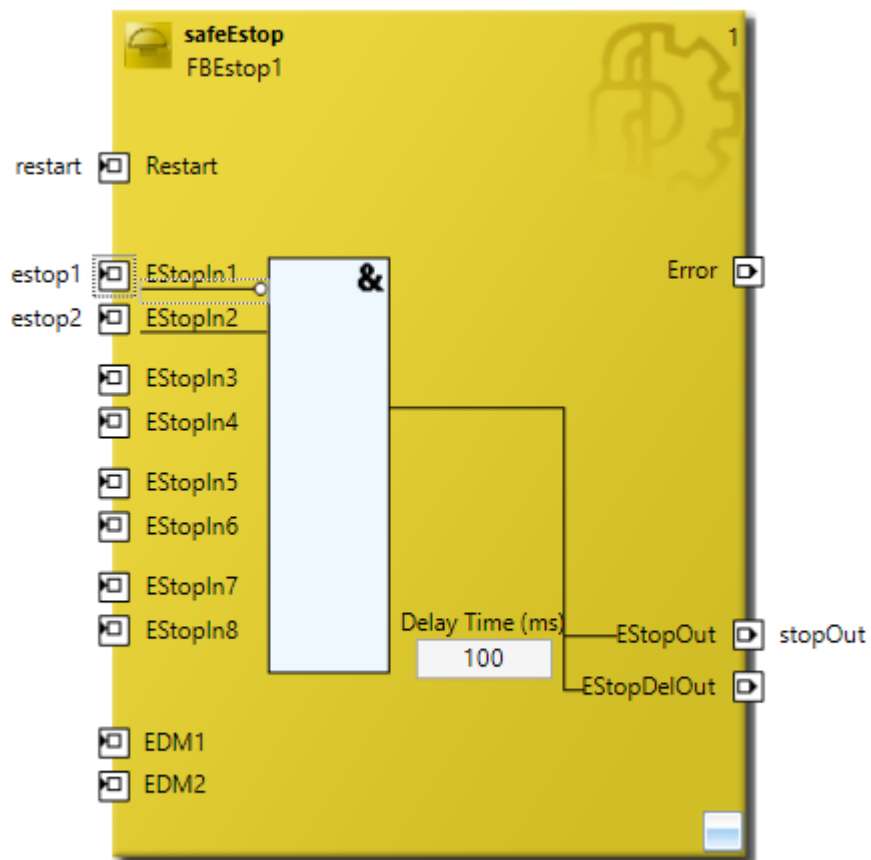
##### 4.2.4.1 Digitaalinen EI (negotiation)toiminto

TwinSAFE-tuloissa voidaan signaali myös kääntää, eli tulo voidaan toteuttaa niin että toimilohko tulkitsee viestin päinvastaiseksi kuin se on.

Operaatio toteutetaan klikkaamalla hiiren oikealla painikkeella ja valitsemalla aukeavasta valikosta *properties*. Tämän jälkeen painetaan halutun *Single-Channelin* päädysässä näkyvää pientä nuolta ja muuttamalla avautuvasta valikosta *Break Contact (NC)* muotoon *Make Contact (NO)*. Kuvassa 7 on nähtävissä valikko jossa tulosignaalin käännöstoiminto digitaalisesta ykkösestä nolllaksi, sekä digitaalisesta nolllasta ykköseksi toteutetaan. Viestin käännösoperaation merkiksi tulee kytkentään näkyviin pieni valkoinen pallo, kuten kuvasta 8 on signaalitulon *EStopIn1* kohdalla nähtävissä.



Kuva 7. Signaalitulon *EStopIn1* valikko.

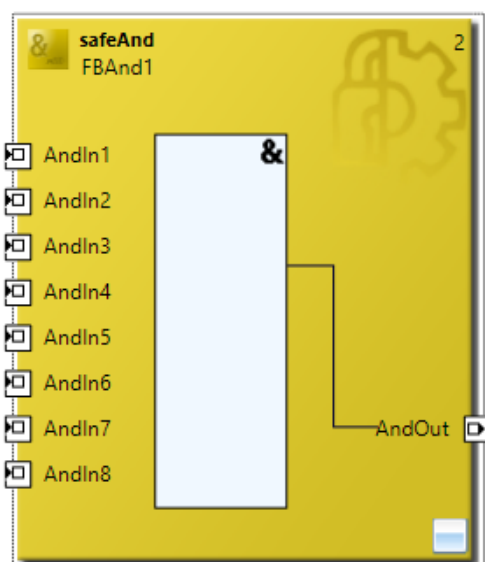


Kuva 8. *safeEstop*-toimilohko.

#### 4.2.4.2 safeAnd

Boolean algebran mukainen JA (AND) -funktio. Jotta informaatio menee AndOutiin, vaatii, että kaikki operaatioon kytketyt kanavat ovat yhtä aikaa aktiiviset. Mikäli esimerkiksi kanavat AndIn1, AndIn2 ja And3 ovat kytketyt, eli niistä menee kytkennän osoittava viiva &:lle, on kaikkien kanavien sallittava yhtä aikaa viestin meno AndOutille, eli niiden on oltava simulointitilanteessa vihreänä, jotta AndOut aktivoituu.

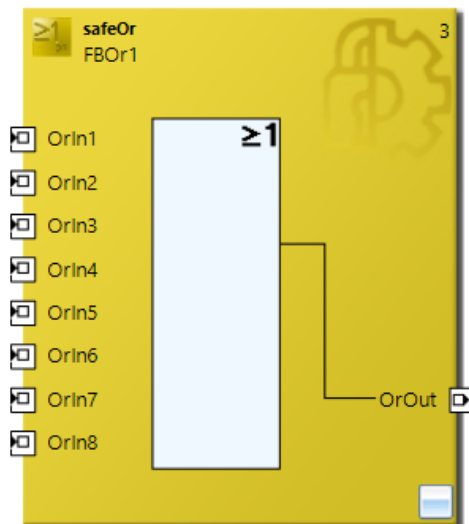
Käytettäessä safeAnd-lohkoa on vähintään kaksi andIn tuloa kytkettävä. (22, s. 17.) Kuvassa 9 nähtävään TwinCAT3:en TwinSAFE-sovelluksen *safeAnd*-lohkoon signaalit tuodaan toimilohkoon *AndIn*-liitännöihin ja toimilohkosta menee signaali eteenpäin *AndOut*-portin kautta.



Kuva 9. *SafeAnd*-toimilohko.

#### 4.2.4.3 safeOr

SafeOr toimii kuten tavallinen Boolean algebran TAI (OR) funktio. TAI (OR) -funktiossa vähintään yhden OrIn-kanavan on oltava aktiivinen, jotta viesti menee OrOutille. Kuvassa 10 nähtävään TwinCAT3:en TwinSAFE-sovelluksen *safeOr*-lohkoon signaalit tuodaan *OrIn*-porttien kautta ja signaali toimilohkosta ulos lähtee portin *OrOut* kautta.



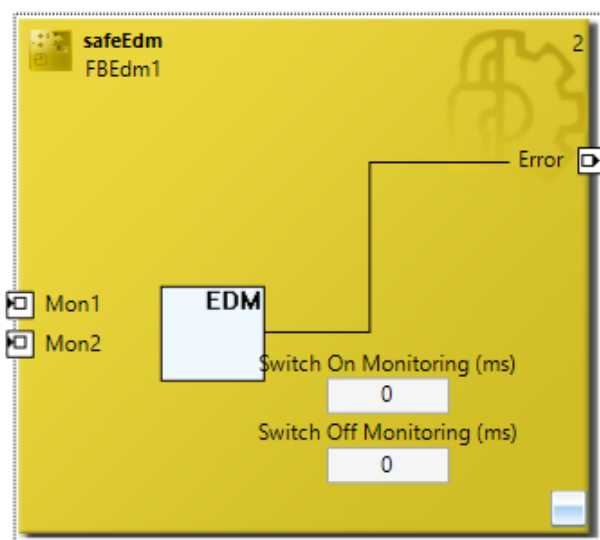
Kuva 10. *safeOr*-toimilohko.

#### 4.2.4.4 safeEDM

SafeEdm-funktiolla voidaan valvota, toteutuuko turvatoiminnon jälkeen sallittu tapahtuma tietyssä ajassa. Mikäli tapahtuma ei toteudu, lähtee Edm:ltä hälytys. Esimerkkinä kuva, jossa kaksi kytkintä on oltava yhtä aikaa kytkettynä. (21, s.77.)

Edm:ää käytetään myös muissa toimilohkoissa valvomaan, tapahtuuko sallittu toiminto. Muissa toimilohkoissa Edm on In puolella, kuten safeMon-toimilohkossa.

Kuvassa 11 olevaan TwinCAT3:en TwinSAFE-sovelluksen *safeEdm*-lohkoon signaalit tuodaan *Mon*-porttien kautta ja lohkoista ulos signaali lähtee *Error*-portin kautta.

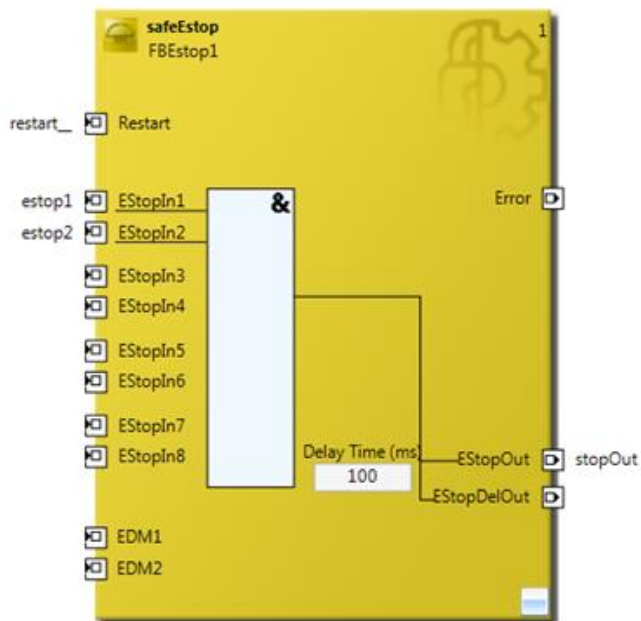


Kuva 11. *safeEdm*-toimilohko.

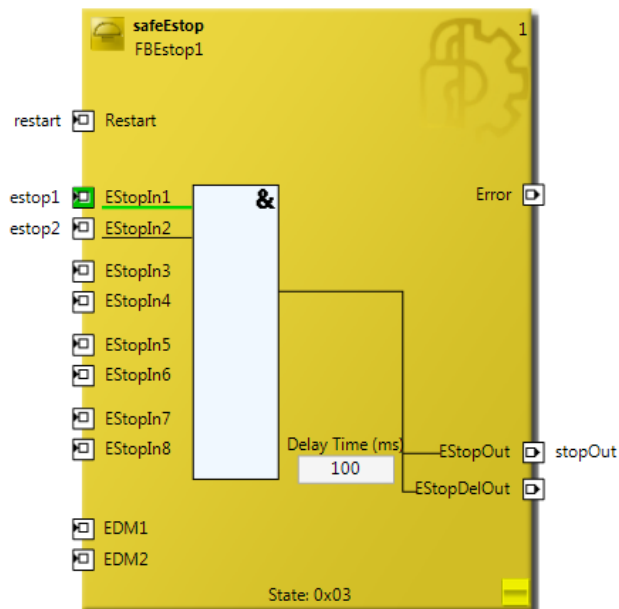
#### 4.2.4.5 safeEstop

SafeEstop-toimilohkoa käytetään hätäseis-toiminnon ohjelmointiin. Esimerkki toimineesta safeEstop-toimilohkosta on kuvassa 13. Funktiossa toinen hätäseis eli EStopIn2 on lauennut, joten viesti ei mene stopOutputille ja kone on pysähtynyt. Turvatoiminnot pitää saattaa jälleen sallittuun tilaan ja tämän jälkeen resetoida safeEstop, tuomalla viesti käynnistettäessä kone-Restart-tuloon. Kuvassa 12 nähtävään *safeEstop*-toimilohkoon koneen hätäseis turvatoiminnon laukaisevat signaalit tuodaan port-

tien *EStopIn* kautta ja koneen käynnistyksen salliva signaali portin *Restart* kautta. Signaali *safeEstop*-toimilohkosta ulos viedään yleisimmin portin *EStopOut* kautta.



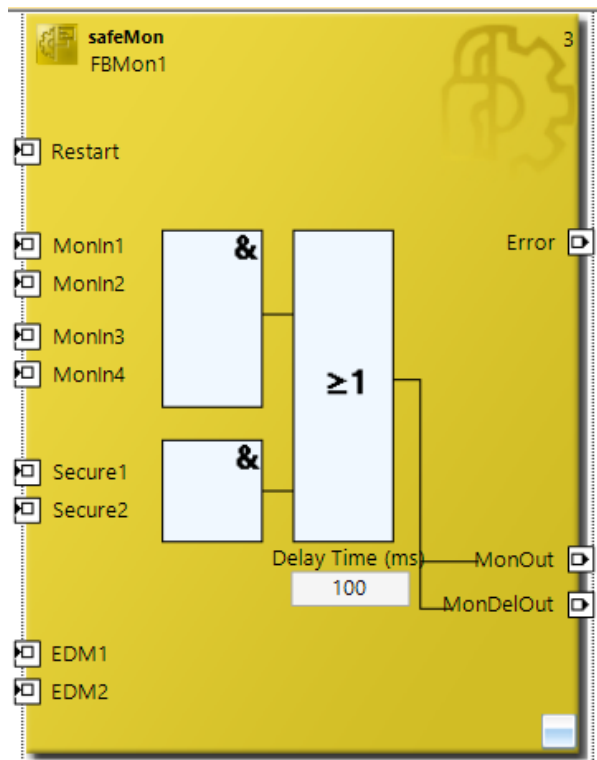
Kuva 12. *safeEstop*-toimilohko.



Kuva 13. Tarvittaessa toiminut *safeEstop*-toimilohko.

#### 4.2.4.6 safeMon

SafeMon toimilohkoa käytetään toimilohkon sisäisen Boolean algebran mukaiseen turvatoiminnon toteuttamiseen. Merkki TAI (OR)  $\geq 1$  tarkoittaa että joko kummankin tai vain toisen funktioista on toteuduttava, jotta turvatoiminto toteutuu. Kuvassa 14 on nähtävissä TwinCAT3:en TwinSAFE-sovelluksen safeMon-toimilohko. Esimerkit kuvassa 14 olevan *safeMon*-toimilohkon käytöstä on luettavissa Application Guide TwinSAFE oppaan sivuilta 57 ja 63. (21, s. 57 ja 63.)



Kuva 14. *safeMon*-toimilohko.

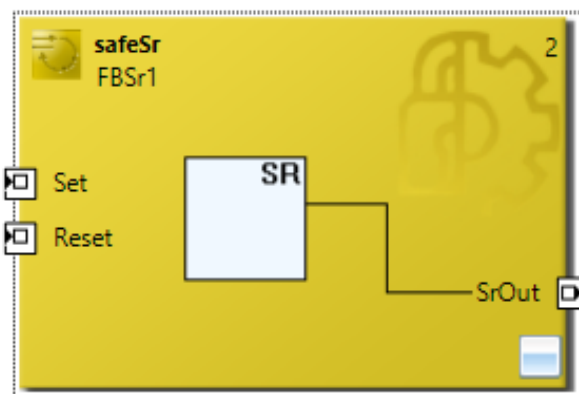


#### 4.2.4.7 safeSr

SafeSr ja safeRs toimilohkot ovat turvapuolen kiikkuja.

SafeSr-toimilohkoa voidaan käyttää turva-automaatioon liitettyjen kytkinten lukitsemi-  
seen. (21, s. 70.)

SR-kiikuissa, kun Set on aktivoitu, aktivoituu myös lähtö-SrOut. SrOut resetoituu vasta  
kun Reset-tulo aktivoituu riippumatta siitä, mikä on Set-tulon tila. Mikäli molemmat tulot  
ovat aktiivisia, on Set määräävä, ja SrOut aktivoituu.

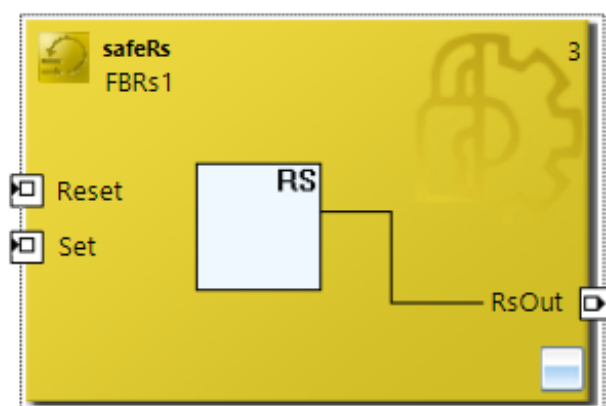


Kuva 15. *safeSr*-toimilohko.

Kuvassa 15 olevaa *SafeSr*-toimilohkoa käytetään esimerkiksi komponentin *safeMon*  
kanssa lukitsemaan suoja-alueen ovet, kun laite käynnistetään. Kun *safeMonOut* saa  
aktivoitumisviestin eli turvaovet ovat kiinni, tulee asetusviesti *safeSr*-toimilohkon *Set*-  
tuloon ja *SrOut*-lähdestä lähtee viesti magneettikytkimelle. Kun jokin turvakytkin ava-  
taan, eli kone ei saa toimia, tulee *safeSr*:n *Reset*-tuloon viesti ja turva-alueen ovet voi-  
daan avata. Kaavio tapahtumasta on lähdemateriaalissa. (21, s. 70.)

#### 4.2.4.8 safeRs

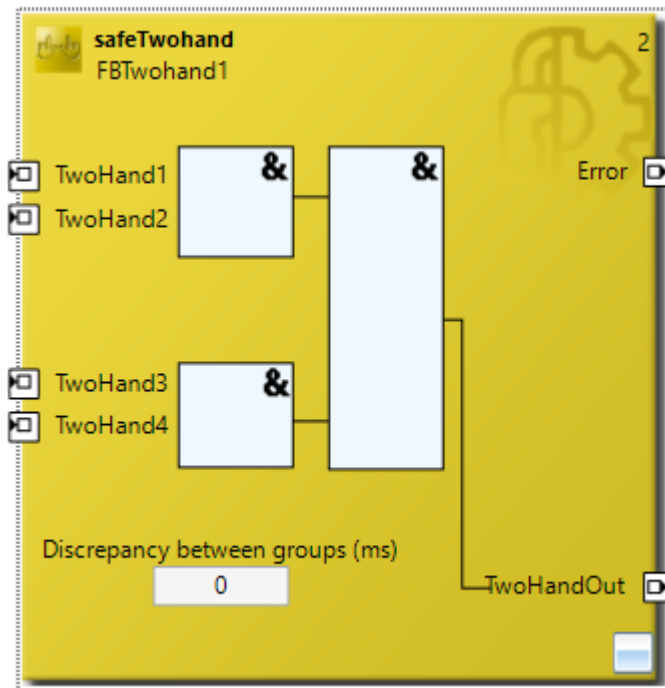
Rs-kiikuissa, kun *Set* on aktivoitu, aktivoituu myös *RsOut*-lähtö. *RsOut* resetoituu vasta kun *Reset*-tulo aktivoituu riippumatta siitä, mikä on *Set*-tulon tila. Mikäli molemmat tulot ovat aktiivisia, on *Reset* määräävä, ja *RsOut* ei saa viestiä. Kuvassa 16 olevaan Twin-CAT3 TwinSAFE-sovelluksen *safeRs*-lohkoon signaalit tuodaan porttien *Reset* ja *Set* kautta. Signaali toimilohkosta *ulos* vietään portin *RsOut* kautta.



Kuva 16. *safeRS*-toimilohko.

#### 4.2.4.9 safeTwohand

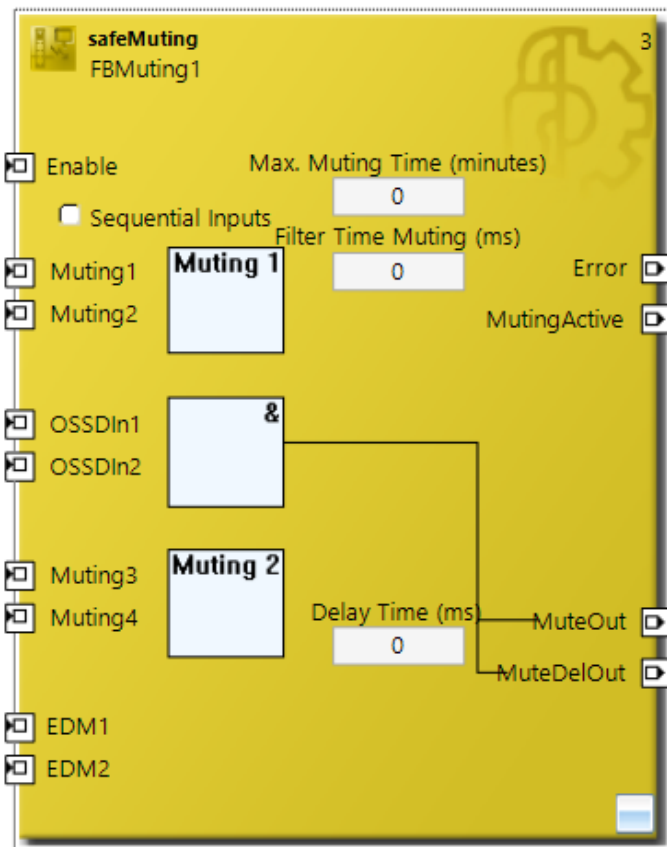
SafeTwohand toimilohkoa käytetään sisäisten funktioidensa mukaiseen JA (AND) ohjelmointiin. Funktiossa on kaikkien kytkentöjen oltava aktiivisena, jotta kone voi toimia. Nimensä mukaisesti käyttökohteena ovat kahdenkädenohjaimet, eli koneenkäyttäjän käsien on kytkettävä samanaikaisesti kytkimet jotta konetta voi käyttää. Kuvassa 17 olevaan TwinCAT3:en TwinSAFE-sovelluksen *safeTwohand*-lohkoon tuodaan signaalit porttien *TwoHand* kautta ja koneen toiminnan salliva signaali portin *TwoHandOut* kautta. .



Kuva 17. *safeTwohand*-toimilohko.

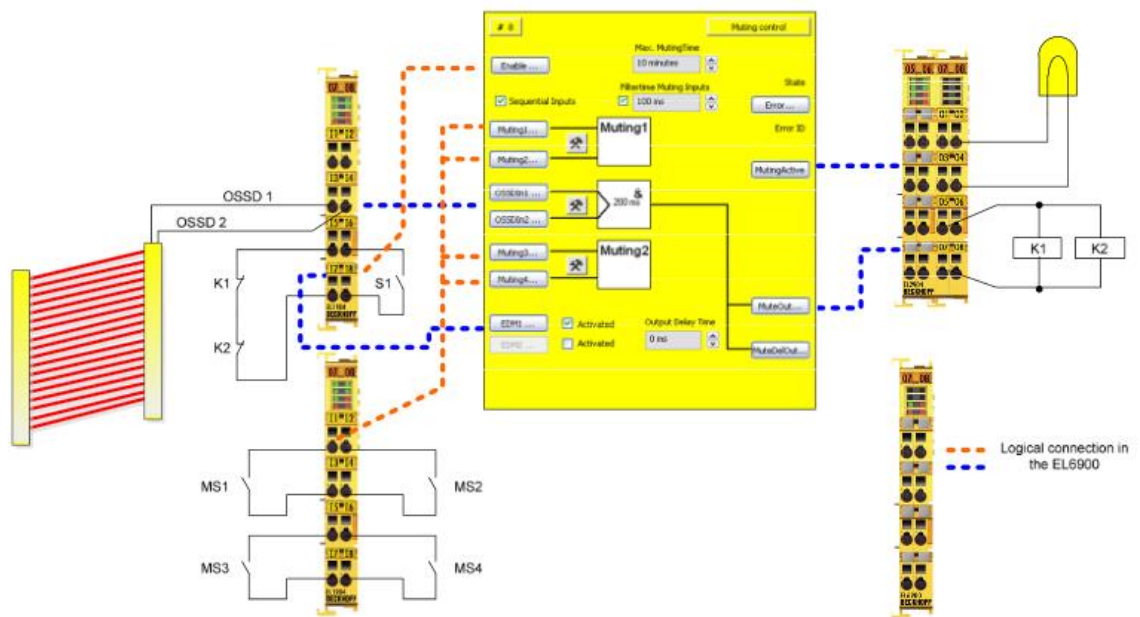
#### 4.2.4.10 safeMuting

Muting on suomeksi kohinanpoisto. Komponenttia voidaan käyttää esimerkiksi kappaletavara-teollisuudessa turvaloverhojen kytkemiseen pois päältä, tuotannossa olevan sallitun esineen ohittamisajaksi. (21, s. 97.) Kuvassa 18 on nähtävissä TwinCAT3:en TwinSAFE-sovelluksen *safeMuting*-lohko.



Kuva 18. *safeMuting*-toimilohko.

Kuvista 19 ja 20 on nähtävissä esimerkki *safeMuting*-toimilohkon käytöstä kappaletavara-teollisuudessa. Esimerkissä turvaloverho kytkeytyy pois päältä ajastetuksi ajaksi, sallitun esineen siirtyessä ihmisille vaaralliselle alueelle turvaloverhon ohi.



Kuva 19. SafeMuting-lohkon käyttö. (21, s. 97.)

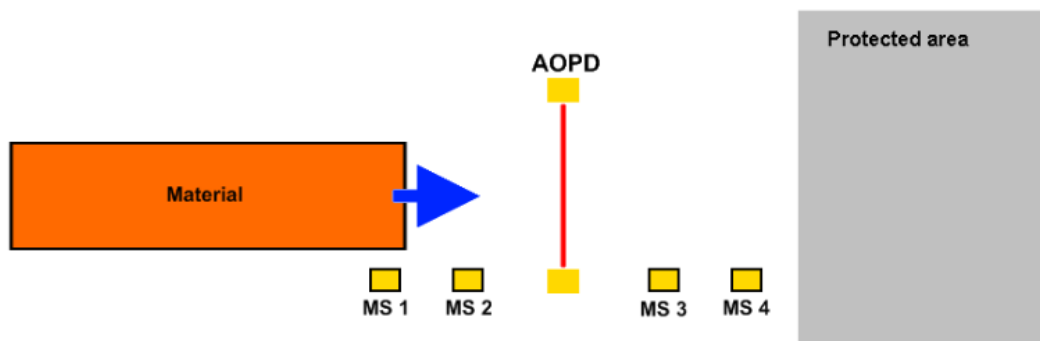
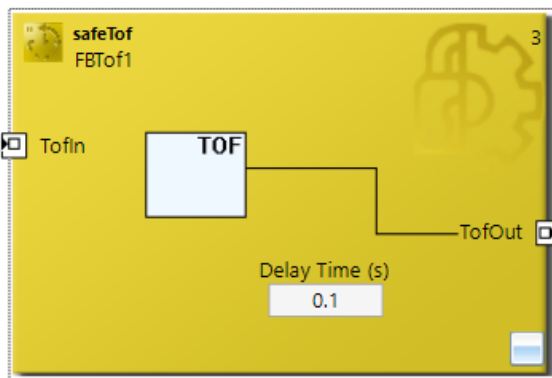


Figure 3-19: Configuration example with FB MUTING

Kuva 20. Sallittu esine lähestymässä turvavaloverhoa. (21, s. 97.)

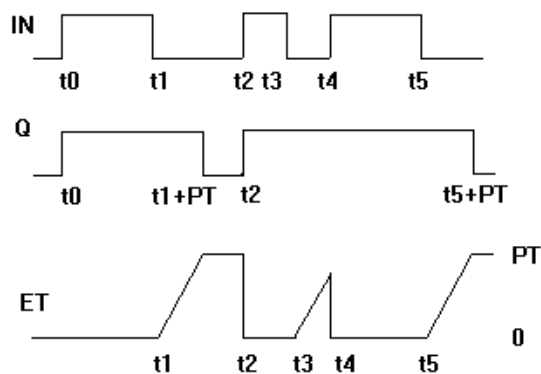
## 4.2.4.11 safeTof

TOF (timer off-delay)-toimilohkoa käytetään viiveen luontiin siitä, kun Tofin resetoituu siihen, kun TofOut resetoituu. TwinCAT3 PLC Lib: Tc2\_Standard sivulla TOF olevan aikakaavion esimerkin mukaisesti. Esimerkissä Q = Out, ET on TOF:illa toteutettu viive. Kuvassa 21 olevaan TwinCAT3 TwinSAFE-sovelluksen *safeTof*-lohkoon signaali tuodaan portin *TofIn* kautta ja signaali lähtee toimilohkosta eteenpäin portin *TofOut* kautta.



Kuva 21. *safeTof*-toimilohko.

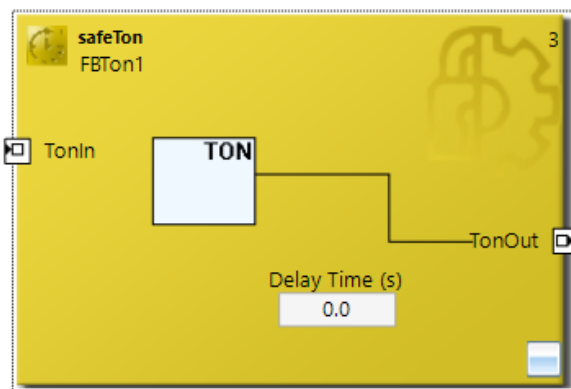
TOF (timer off-delay)-toimilohkoa käytetään viiveen luontiin siitä, kun Tofin saa resetoitumis signaalin siihen, kun TofOut resetoituu. TwinCAT3 PLC Lib: Tc2\_Standard sivulla TOF olevan aikakaavion esimerkin mukaisesti. Esimerkissä Q = Out, ET on TOF:illa toteutettu viive.



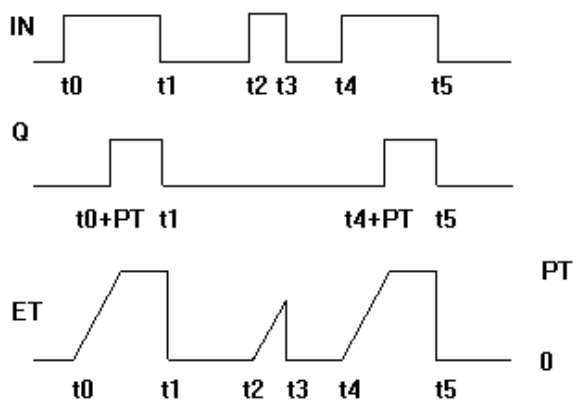
Kuva 22. Tof-lohkon toiminta. IN Tofille tuleva signaali. Q Tofilta lähtevä signaali. ET viiveen luonti ajastus. (23.)

## 4.2.4.12 safeTon

TON (Timer on-delay) toimilohkoa käytetään viiveen luontiin siitä, kun Tofin aktivoituu siihen, kun TofOut aktivoituu. Toiminnolla saadaan ehkäistyä virheellisiä turvatoiminnon laukeamisia. TwinCAT3 PLC Lib: Tc2\_Standard sivulla TON olevan aikakaavion esimerkin mukaisesti. Esimerkissä  $Q = \text{Out}$ , ET on TON:in viive. Kuvassa 23 olevaan TwinCAT3 TwinSAFE-sovelluksen *safeTon*-lohkoon signaali tuodaan portin *TonIn* kautta ja signaali lähtee toimilohkosta eteenpäin portin *TonOut* kautta.



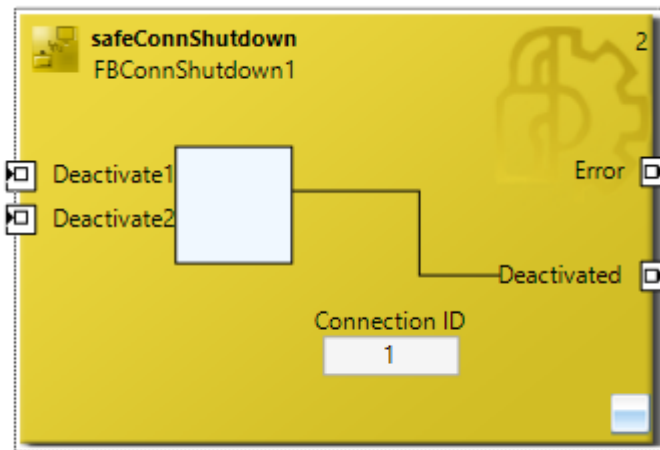
Kuva 23. *safeTon*-toimilohko.



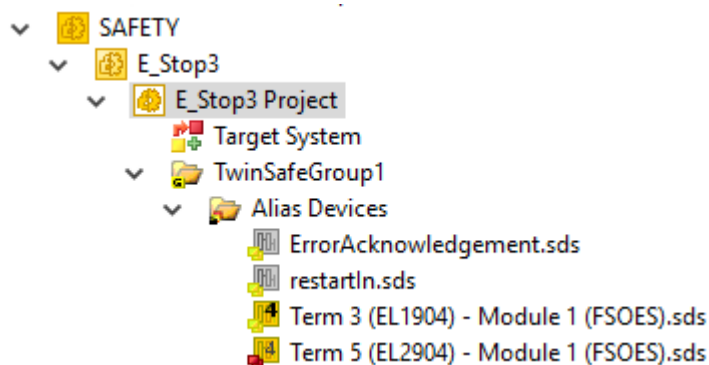
Kuva 24. Ton-lohkon toiminta. Tof lohkon toiminta. IN Tofille tuleva signaali. Q Tofilta lähtevä signaali. ET-viiveen ajastus. (24.)

#### 4.2.4.13 safeConnShutdown

ConnShutdown-toimilohkoa käytetään kytkemään TwinSAFE-turvalohko FSoE device (turva-automaatiojärjestelmän yksittäinen laite) pois päältä, esimerkiksi huollon ajaksi. (20, s. 76.) Toimilohkon uudelleenaktivointi tapahtuu Microsoft Visual Studioon kautta TwinCAT3-ohjelmalla *Solution Explorer Alias Devices*-valikon kautta laittamalla FSoE partner DATA-tilaan. Kuvassa 26 olevassa valikossa näkyvät sovelluksessa olevat FSoE-laitteet. Todennäköisesti kunnossapito saa tehtyä uudelleen aktivoinnin myös kyseisen käytössä olevan sovelluksen huoltotilavalikon kautta. Kuvassa 25 olevaan TwinCAT3 TwinSAFE-sovelluksen *safeConnShutdown* -lohkoon signaalit tuodaan *porttienDeactivate* kautta ja signaali vietään toimilohkosta ulos portin *Deactivated* kautta.



Kuva 25. *safeConnShutdown*-toimilohko.

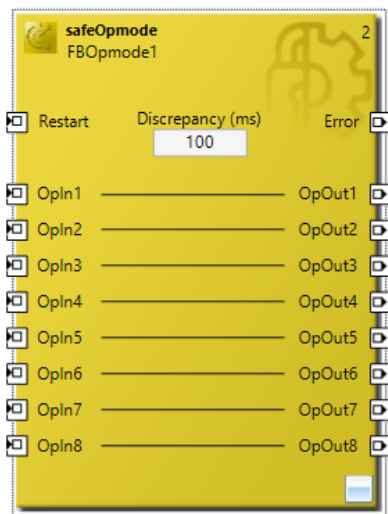


Kuva 26. FSoE-laitteet.



#### 4.2.4.14 safeOpmode

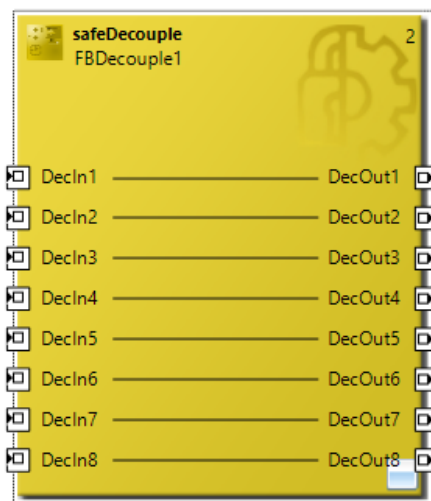
SafeOpmode-toimilohkossa mikäli ei yksikään OpIn ole aktiivinen tai useampi OpIn-tulo on aktiivinen, saavat kaikki OpOut-lähdöt tilan tosi, eli ovat kytkettyinä. Toimilohkoa käytetään vain koneen käynnistysvaiheessa. safeOpmode:ssa on oltava vähintään kaksi OpIn-tuloa reititettyinä. (22, s. 25.) Kuvassa 27 on nähtävissä TwinCAT3 TwinSAFE-sovelluksen safeOpmode-lohko.



Kuva 27. *safeOpmode*-toimilohko.

#### 4.2.4.15 safeDecouple

SafeDecouple-toimilohkoa käytetään tarvittaessa useamman TwinSAFE-ryhmän järjestelmässä estämään halutun turvallisuusdatan pääsy halutulle ryhmälle. Kaikki toimilohkoon liitetyt DecOut output-signaalit kytkeytyvät tietoliikennehäiriötilanteessa (a connection communication error) (22, s. 41.) pois päältä eli niihin liitetyt turvatoiminnot aktivoituvat, mikäli edempänä ohjelmaan ei ole muuta ohjelmoitu. Kuvassa 28 on nähtävissä TwinCAT3:en TwinSAFE-sovelluksen *safeDecouple*-lohko.



Kuva 28. *safeDecouple*-toimilohko.

### 4.3 Pohdintaa miten TwinSAFE täyttää standardien vaatimukset

TwinSAFE turva-automaatiosovelluksessa toteutuu standardin vaatimus eri käyttäjätasosta. TwinCAT-sovellus on suunniteltu kaikkien prosessi- ja koneautomaatiota suunnittelevien henkilöiden työvälineeksi. TwinCATstä löytyy työvälineet esimerkiksi logiikkaohjelmointiin, automaatiojärjestelmäohjelmointiin, PI-suunnitteluun ja prosessista kerättävän tiedon analysointiin. TwinCAT-sovelluksessa pystyy ohjelmoimaan turva-automaatiota sallittujen turva-automaation ohjelmointikielten avulla, mutta esimerkiksi turva-automaation toimilohkojen sisäistä rakennetta ei ohjelmoija pääse muuttamaan. Ohjelmoija saa TwinCATillä luotua järjestelmään tason, jolla käyttäjät eivät pääse muuttamaan itse järjestelmän logiikkojen ohjelmistoa, mutta pääsevät operoimaan konetta sekä prosessia, eli pystyvät muuttamaan tarvitsemiaan parametreja.

Ohjelmiston toimittaja saa järjestelmässä ohjelmoitua sovellukseen kunnossapidolle oman tason, jolla pääsee muokkaamaan tiettyjä ennalta määriteltyjä säätöparametreja. TwinSAFE-softassa on myös ohjelman suunnittelijoille kaksi eri tasoa: taso jolla ohjelmoija pääsee luomaan turva-automaatio-ohjelmiston standardin IEC 61511 mukaisilla ohjelmointikielillä ja turva-automaatio-ohjelmiston aivan ydintaso, jolle muutoksia pääsee tekemään vain Beckhoffin tuotekehitys. TwinSAFE-järjestelmässä toteutuu standardeissa oleva vaatimus, jonka mukaan turva-automaatioon on suunniteltava omat tasonsa eri ryhmille.

TwinCAT-ohjelmistossa olevan simulointiominaisuuden ansiosta saadaan ohjelmaa suunniteltaessa noudatettua standardin SFS-EN 61508-3 mukaista ohjelmiston systemaattisen kyvykkyyden ja kehittämisen elinkaarimallia. Käytännössä ohjelman toimivuus pystytään suunnittelun joka vaiheessa testaamaan simuloimalla, ennen kylmätestausta.

TwinCAT-ohjelmointiympäristöstä löytyvät työkalut myös SIL-tasojen laskentaan, joten kyseinen sovellus sopii työkaluksi niin käyttöautomaatiojärjestelmiä ohjelmoiville kuin myös turva-automaatiota valmistaville ja huoltaville henkilöille.

Standardien vaatimus turva-automaatiojärjestelmien huollettavuudesta ilman että turvatoiminnon toteutuminen tarvittaessa vaarantuu, toteutuu. Vioittuneen komponentin EL 6900 voi vaihtaa tarvittaessa uuteen, vaihdon aikana käsittääkseni logiikka valvoo turvatoimintoja, ja TwinCAT-järjestelmä pystyy lataamaan logiikalta varmuustiedostosta ohjelmiston automaattisesti uudelle EL6900-komponentille. Myös softan päivitys voidaan suunnitella ja simuloida TwinCAT-ohjelmalla ja ajaa vasta huoltoseisokin aikaan tai muuten sopivaksi katsottuna ajankohtana käytössä olevaan järjestelmään.

## **5 Lopuksi**

Koneiden ja teollisuuslaitosten turvallisuusjärjestelmistä on saatavissa niin ilmaista kuin maksullistakin materiaalia huomattavasti enemmän kuin tämän insinööriyön lähdeluetteloon on laitettu. Suunnittelijoiden, käyttäjien sekä kunnossapidon puolen henkilökunnan on hyvä käyttää työssään tukena alakohtaisia teoksia. Lähes jokatyypiseen laitteeseen ja teollisuuden alaan on saatavissa materiaalia, josta löytyy selkeiden alaotsikoiden alla suurin osa kyseiseen sektoriin vaikuttavista standardeista ja määräyksistä.

Jokaisen yrityksen on hyvä hankkia luku- ja käyttöoikeudet viralliselta taholta tarvitsemiinsa standardeihin, jotta pystyy olemaan varma siitä, että käytössä on standardeista uusimmat, voimassa olevat versiot.

TwinCAT-sovellusohjelmisto on huomattavasti laajempi, kuin tässä insinööriyössä on aiheen rajauksen puolesta käsitelty. Ohjelmisto soveltuu kaikkien tehtaan automaatiosta vastaavien henkilöiden käyttöön.

Insinööriyön käytännönosiossa tehdyn turva-automaation ohjelmointiharjoituksen toimivuuden ovat testanneet myöhempien vuosikurssien opiskelijat keväällä 2016 olleissa automaatiotekniikan laboratorioissa. Harjoitusta on automaatiotekniikan laboratoriossa tehnyt yhtä aikaa useampi ryhmä. Tähän insinööriyöhön kuuluva turva-automaation ohjelmointiharjoituksen ohje on tehty harjoitustyöohjeessa mainitulle kokonaisuudelle (liite1). Automaatiotekniikan laboratoriotunneilla ryhmillä on ollut käytössään omat komponenttikokonaisuudet, joten harjoitus on kehittänyt myös insinöörin työhön kuuluvaa ongelman ratkaisukykyä. Jokaisella turva-automaation siltakomponentilla on oma sarjanumeronsa, joka ryhmien on täytynyt selvittää.

## Lähteet

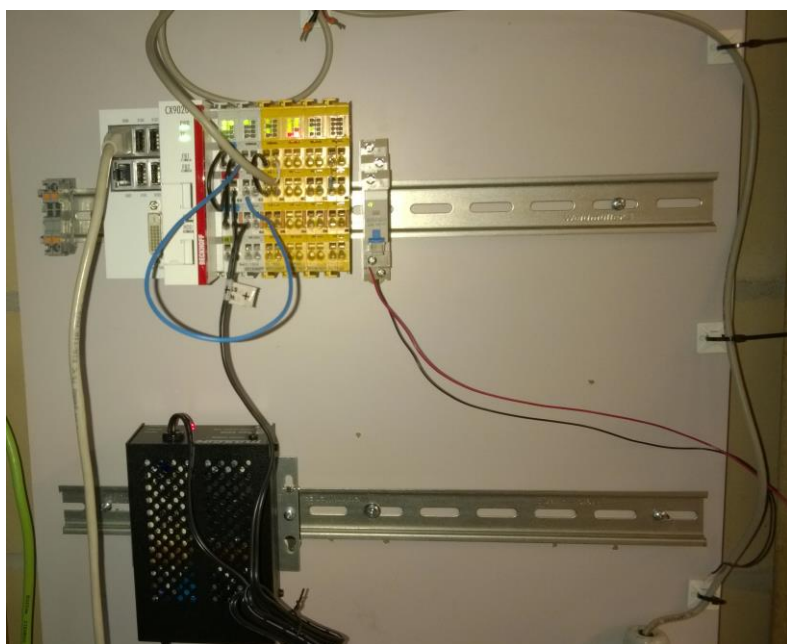
- 1 Pakarinen, Jussi. 2013. Turva-automaatio, luentomateriaali. Metropolia ammattikorkeakoulu.
- 2 Standardi SFS-EN 61508-3 SÄHKÖITEN/ELEKTRONISTEN/OHJELMOITAVIEN ELEKTRONISTEN TURVALLISUUTEEN LIITTYVIEN JÄRJESTELMIEN TOIMINNALLINEN TURVALLISUUS. OSA 3: OHJELMISTOVAATIMUKSET.
- 3 Saari, Juha. 2015. LAADUNOHJAUS Luento7. PDF-dokumentti. Metropolia ammattikorkeakoulu.
- 4 Dr.-Ing. Konnov, Alexei. 2015. Courses: Reliability Engineering Basic and Advance concept. Hochschule Karlsruhe – Technik und Wirtschaft.
- 5 Pakarinen, Jussi. 2013. TAJ elinkaari, PDF-dokumentti. Metropolia ammattikorkeakoulu.
- 6 Valtioneuvoston asetus 400/2008, valtioneuvoston asetus koneiden turvallisuudesta. Verkkodokumentti. <http://www.finlex.fi/fi/laki/smur/2008/20080400>. Luettu 3.1.2016
- 7 Suomen standardisoimisliitto SFS. Koneturvallisuuden standardit. Verkkodokumentti, <http://www.sfs.fi/files/63/Koneturvallisuusesite2015web.pdf>. Luettu 3.1.2016.
- 8 Hietikko, Marita. Malm, Timo ja Alanen, Jarmo. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen, VTT TIEDOTTEITA 2485. [http://www.vtt.fi/Documents/2009\\_T2485.pdf](http://www.vtt.fi/Documents/2009_T2485.pdf). Luettu 20.1.2016.
- 9 Standardi SFS-EN ISO 13850 Koneturvallisuus. Häätöpysäytys. Suunnitteluperiaatteet. Luettu tammikuussa 2016.
- 10 Suunnittelijan rooli prosessilaitoksen turvallisuuden varmistamisessa, Opas suunnittelijoille ja suunnittelun tilaajille. VTT 2012. [http://www.vtt.fi/sites/usva/Documents/usva\\_opas\\_helmikuu\\_v2\\_2012.pdf#search=Hazop](http://www.vtt.fi/sites/usva/Documents/usva_opas_helmikuu_v2_2012.pdf#search=Hazop) Luettu 6.1.2016.
- 11 Tweeddale, Mark. 2003. Managing Risk and Reliability of Process Plants, Gulf Professional Pub.
- 12 Pakarinen, Jussi. 2013. Turva-automaatio HAZOP, LOPA ja vikapuu analyysi. PDF-dokumentti. Metropolia ammattikorkeakoulu.

- 13 EN 61311. Wikipedia. [https://de.wikipedia.org/wiki/EN\\_61131](https://de.wikipedia.org/wiki/EN_61131). Luettu 7.1.2016
- 14 Kääriäinen, Jarkko. 2008. Ohjelma hyödyntäminen automaatiojärjestelmässä, Diplomityö. Teknillinen korkeakoulu Elektroniikan, tietoliikenteen ja automaation tiedekunta. <http://lib.tkk.fi/Dipl/2008/urn012791.pdf>. Luettu 7.1.2016.
- 15 Holmström, Kalevi. IEC 61511 Mukaiset vaatimukset turva-automaation ohjelmistoille. <https://wiki.metropolia.fi/display/alykas/IEC+61511+mukaiset+vaatimukset+turva-automaation+ohjelmistoille> Luettu 6.1.2016.
- 16 AMERICAN NATIONAL STANDARD. ANSI/ISA-84.00.01-2004 Part 1 11.7.2 Maintenance/engineering interface requirements. PDF dokumentti. Luettu internetistä tammikuussa 2016.
- 17 TwinCAT Safety Editor. Operating instructions for EL6900 TwinSAFE Logic Terminal. Version 1.5.2 Date: 2015-10-02 <http://download.beckhoff.com/download/document/automation/twinsafe/el6900en.pdf>. Luettu 24.1.2016.
- 18 TwinCAT Safety Editor. [http://www.beckhoff.com/presentation/default.php?media=http://multimedia.beckhoff.com/presentation/en/Beckhoff\\_MMP\\_SafetyEditor\\_EN\\_final.swf&title=TwinCAT+Safety+Editor&preload=1](http://www.beckhoff.com/presentation/default.php?media=http://multimedia.beckhoff.com/presentation/en/Beckhoff_MMP_SafetyEditor_EN_final.swf&title=TwinCAT+Safety+Editor&preload=1). Luettu 23.1.2016.
- 19 TwinCAT3 | eXtended Automation (XA) Motion. Beckhoff. [http://download.beckhoff.com/download/Document/catalog/Beckhoff\\_TwinCAT3\\_042012\\_e.pdf](http://download.beckhoff.com/download/Document/catalog/Beckhoff_TwinCAT3_042012_e.pdf). Luettu 8.1.2016
- 20 [www.beckhoff.com](http://www.beckhoff.com) . Automation, TwinSAFE. Luettu 23.1.2016.
- 21 Application Guide TwinSAFE. Version 1.6.2 Date 2015-10-02. <https://download.beckhoff.com/download/Document/automation/twinsafe/applicationguidetwinsafeen.pdf>. Luettu 24.1.2016.
- 22 Documentation EL6900-FB, KL6904-FBTwinCAT function blocks for TwinSAFE logic terminals. Version: 2.4.1 Date: 2015-03-11. [https://download.beckhoff.com/download/Document/automation/twinsafe/el6900\\_kl6904-fben.pdf](https://download.beckhoff.com/download/Document/automation/twinsafe/el6900_kl6904-fben.pdf). Luettu 27.1.2016.
- 23 TwinCAT3 PLC Lib: Tc2\_Standard. TOF. [http://infosys.beckhoff.com/english.php?content=../content/1033/tcplclib\\_tc2\\_standard/74403595.html&id](http://infosys.beckhoff.com/english.php?content=../content/1033/tcplclib_tc2_standard/74403595.html&id). Luettu 24.1.2016.
- 24 TwinCAT3 PLC Lib: Tc2\_Standard. TON. [http://infosys.beckhoff.com/english.php?content=../content/1033/tcplclib\\_tc2\\_standard/74403595.html&id](http://infosys.beckhoff.com/english.php?content=../content/1033/tcplclib_tc2_standard/74403595.html&id) Luettu 25.1.2016.

- 25 EUR-LEX – EU:n lakitietokanta. <http://eur-lex.europa.eu/homepage.html?locale=fi>. Luettu 8.1.2016.
- 26 SFS / IEC / ISO standardit.
- 27 Malm, Timo & Kivipuro, Maarit. 2004. Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa, VTT tiedotteita 2264. <http://www.vtt.fi/inf/pdf/tiedotteet/2004/T2264.pdf>. Luettu 4.1.2016.
- 28 Dr.-Ing. Stripf, Wolfgang. 2015. Funktionale Sicherheit in der Automatisierung, Teil 1, Hochschule Karlsruhe – Technik und Wirtschaft. PowerPoint luento.
- 29 Dr.-Ing. Stripf, Wolfgang. 2015. Funktionale Sicherheit in der Automatisierung, Teil 2, Hochschule Karlsruhe – Technik und Wirtschaft. PowerPoint luento.
- 30 Hazard and operability study. Wikipedia. [https://en.wikipedia.org/wiki/Hazard\\_and\\_operability\\_study](https://en.wikipedia.org/wiki/Hazard_and_operability_study). Luettu 7.1.2016.
- 31 Anton A. Frederickson. 2012. The Layer of Protection Analysis (LOPA) method, Safety Users Grup. <https://www.jlab.org/eng/ssg/safety/lopa.pdf>. Luettu 10.3.2016.
- 32 SFS-EDU. Oppilaitoskäsikirjat, Automaatio, 631-2. <http://sfs.multiedition.fi/www/fi/oppilaitoskasikirjat/Automaatio/631-2.php>. Luettu 7.1.2016.
- 33 Operating instructions for EL1904 TwinSAFE input terminal with 4 fail-safe inputs. Version 1.5.2 Date2015-10-02. <http://download.beckhoff.com/download/document/automation/twinsafe/el1904en.pdf>. Luettu 23.1.2016.

## Koneturvallisuus. Turva-automaation ohjelmointiharjoitus Bechhoffin TwinSafe-järjestelmällä.

Tehdään koneturvallisuuden turva-automaation ohjelmointiharjoitus. Harjoituksessa työvälineenä logiikan Bechhoff CX9020-ohjelmointiin käytetään TwinCat-ohjelmistoa, joka löytyy automaatiotekniikan laboratorion sisäverkkoon liitetyiltä PC-koneilta. Ympäristönä johon tehtävä ohjelma ladataan ja jossa se testataan, käytetään automaatiotekniikan laboratorion seinältä löytyvää Bechhoffin TwinSAFE-simulointiympäristöä.



Kuva Simulointiympäristö

Simulointiympäristön komponentit:

- Logiikka Beckhoff CX 9020
- Input kortti: EL1004
- TwinSAFE Input EL1904
- TwinSAFE Output EL2904



- TwinSAFE Communication EL6900
- Virtalähde
- Koneita simuloiva tuuletin (FUN)
- Häätäseis

Harjoitus on kaksiosainen. Ensin luodaan TwinCAT3-ohjelmalla toimiva häätäseisohjelma projektin luonnista lähtien. Seuraavassa vaiheessa lisätään luotuun ohjelmaan komponentti, joka voi olla koneissa, esimerkiksi koneen suojuksien ovikytkimet, valoverho tai niin sanottu kahdenkäden ohjaus. Kahdenkäden ohjauksessa koneen käyttäjän molempien käsien on yhtä aikaa oltava ohjaimilla, jotta kone saa toimia.

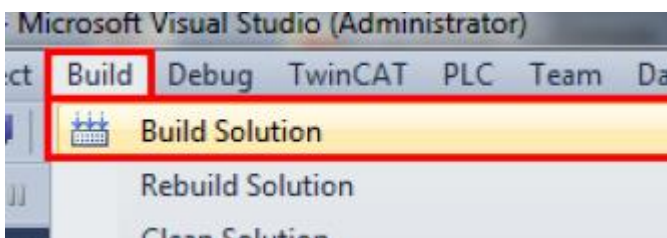
Harjoitus: osa 1

1. Tehdessäsi projektia muista tekemiesi vaiheiden jälkeen tallentaa projekti. Projektin luonnin jälkeen tallennus onnistuu painamalla näytön oikeassa yläkulmassa näkyvää symbolia.



Voit tehdä myös *Build*-valikosta löytyvän *Build Solution*in aina kun olet tehnyt seuraavan vaiheen, tallentaaksesi tekemäsi.

Klikkaa hiiren vasemmalla *Build*, sieltä *Build Solution* tai paina näppäintä F6.



## 2. Vaihe 1: Sovelluksen tarkistus.

TwinSAFE-harjoitustyöt ohjelmoidaan TwinCAT3-sovelluksella. Kun aloitat harjoitustyön tekemisen, tarkista ensin näyttöruudun alaosan tehtäväpalkin oikeasta alareunasta, kumpi TwinCATin sovellus 2 vai 3 kyseisellä tietokoneella on käytössä. Mikäli tietokoneella on käytössä TwinCAT2, on se vaihdettava TwinCAT3:een.



Kuvassa TwinCAT2-symboli

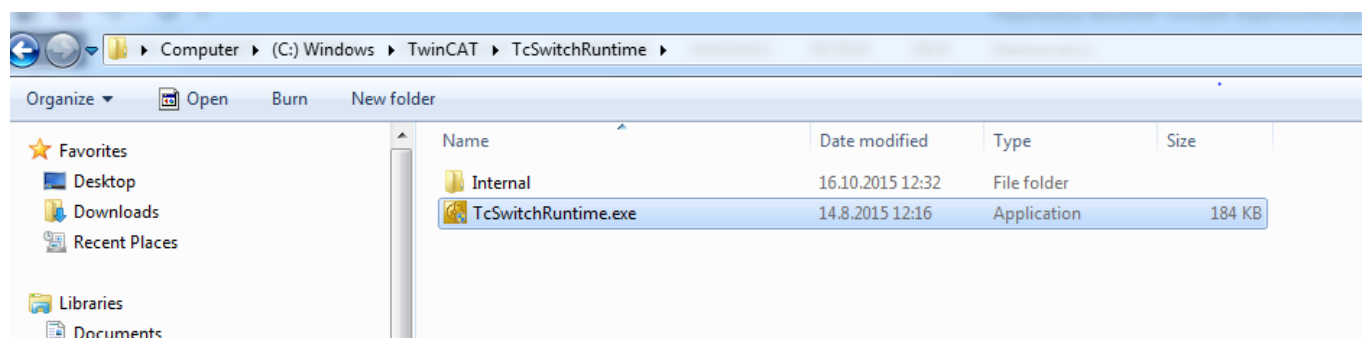


Kuvassa TwinCAT3-symboli.

## Ohjeet

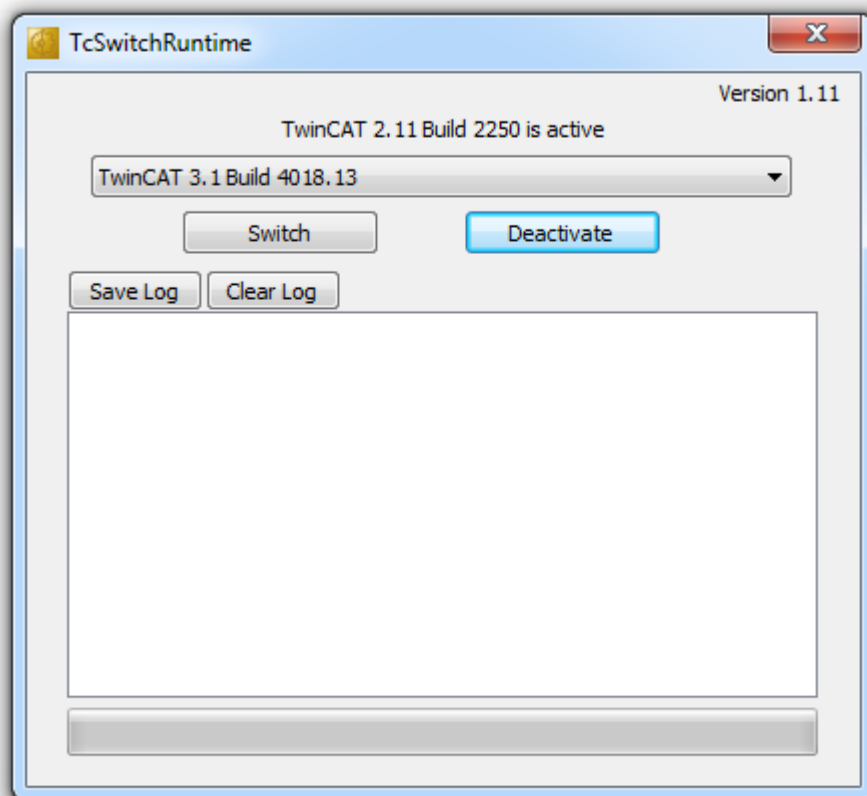
### 1.1 Sovelluksen vaihto.

- Mene C-juureen
- Hae sieltä TwinCAT
- *TwinCat*in alta *TcSwitschRuntime*
- Sieltä valitse:



- Tämän jälkeen näytölle tulee ikkuna, jossa *User Account Control* kysyy:  
*Do you want to allow the following program to make Changes to this computer.*  
Vastaa kysymykseen *YES*.

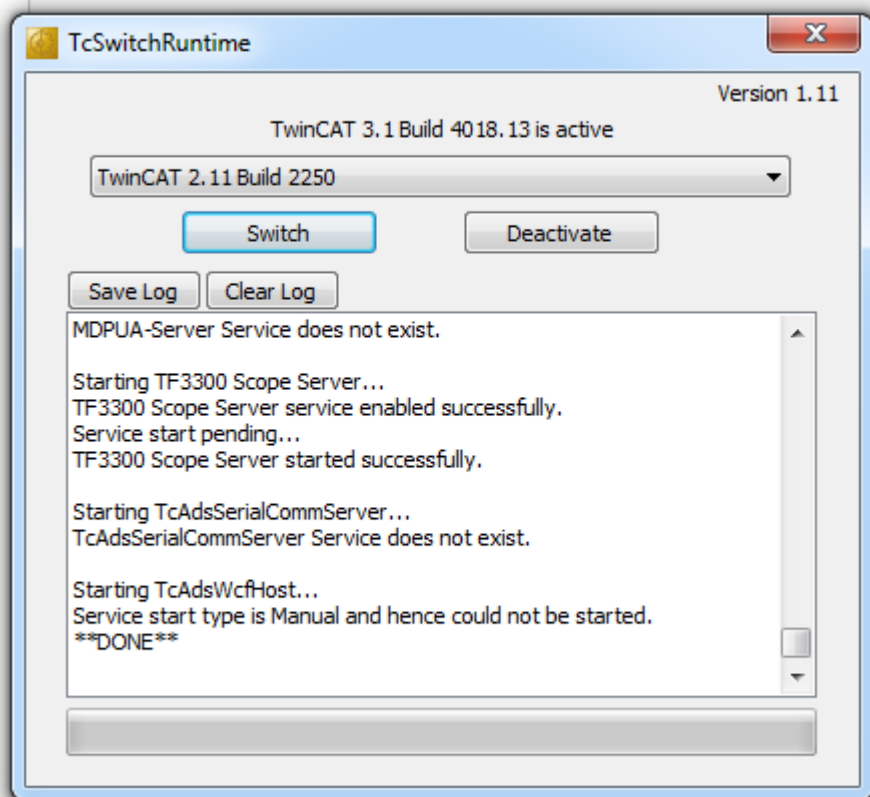
- Tämän jälkeen näytölle ilmestyy ikkuna:



Vastaa *Switch*.

- Seuraavaksi sovellus alkaa ajaa versionvaihto-ohjelmaa läpi.

- Kun vaihto on valmis, tulee näkyviin:



Sulje ikkuna oikeassa yläkulmassa olevasta punaisesta rastista x.

- Näet näytön oikeasta alakulmasta, onko ohjelma vaihtunut.



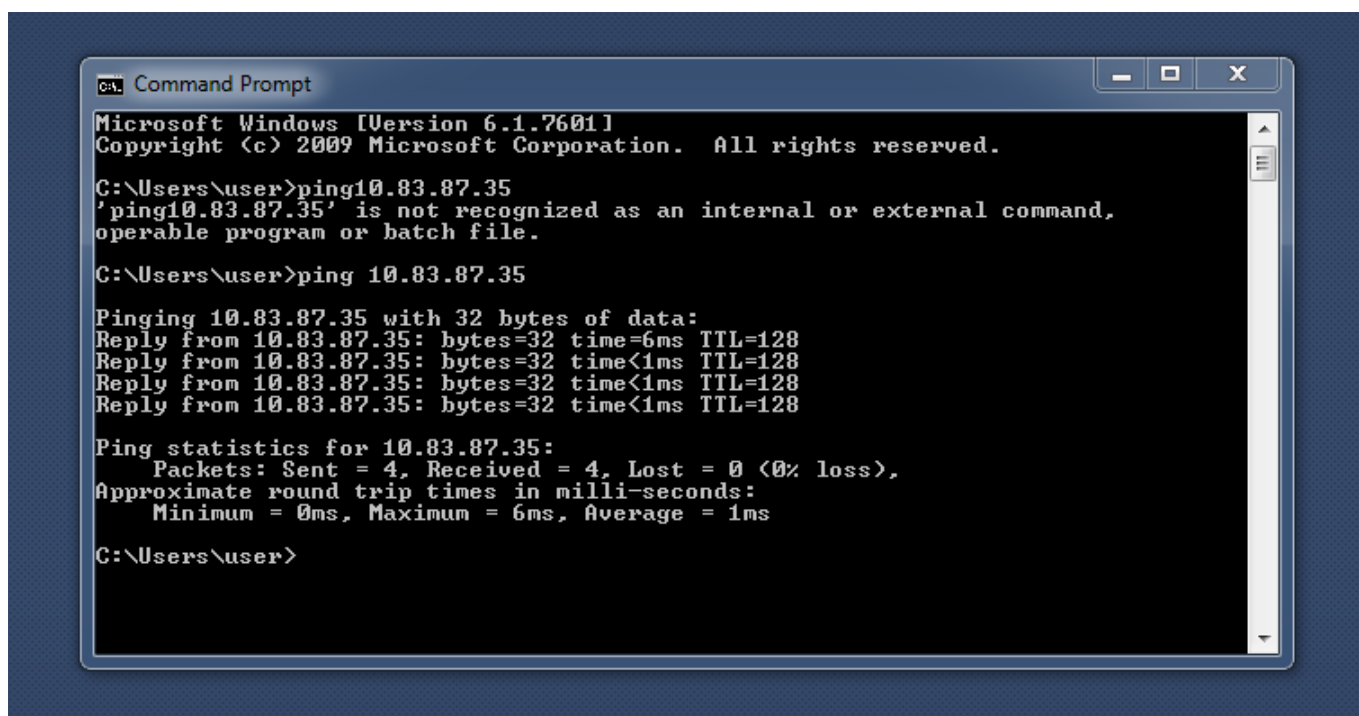
Kuvassa TwinCAT3

- Toiseen suuntaan vaihto tehdään päinvastaisessa järjestyksessä.

3. Tarkista käytettävän logiikan olevan päällä ja verkkojohdon kiinni.

Alkuvuodesta 2016 harjoituksessa käytettävä logiikka on Beckhoff CX9020, jonka ip-osoite on 10.83.87.35 ja maski 255.255.254.0.

1. Saat tarkistettua asian pingaamalla.
2. Hae sovellusten hakutoiminnolla Command Prompt.
3. Kirjoita kohtaan C:\user> komento ping 10.83.87.35.
4. Mikäli tietokone löytää logiikan tulee näkyviin:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>ping10.83.87.35
'ping10.83.87.35' is not recognized as an internal or external command,
operable program or batch file.

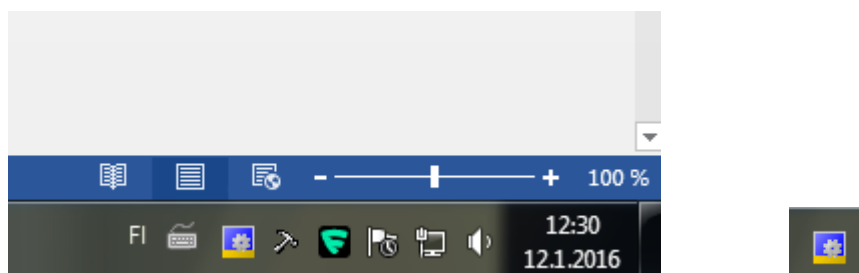
C:\Users\user>ping 10.83.87.35

Pinging 10.83.87.35 with 32 bytes of data:
Reply from 10.83.87.35: bytes=32 time=6ms TTL=128
Reply from 10.83.87.35: bytes=32 time<1ms TTL=128
Reply from 10.83.87.35: bytes=32 time<1ms TTL=128
Reply from 10.83.87.35: bytes=32 time<1ms TTL=128

Ping statistics for 10.83.87.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Users\user>
```

3. Avaa TwinCAT3 näytön oikeasta alakulmasta painamalla kerran hiiren vasenta näppäintä TwinCAT3-symbolin päällä.

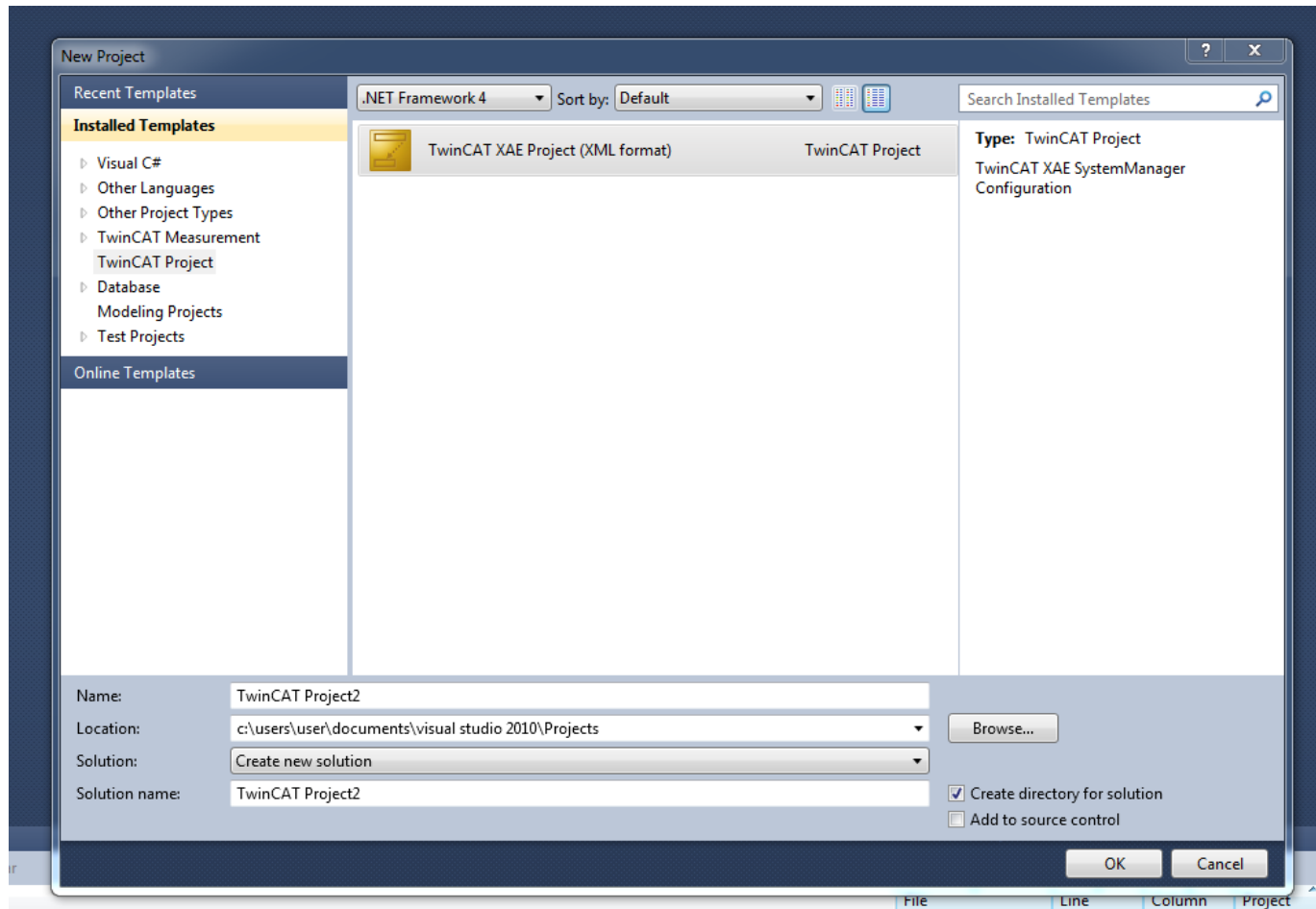


jolloin aukeavasta ikkunasta paina kerran hiiren vasemmalla näppäimellä TwinCAT XAE (VS2010).

4. Tarkista että käyttämäsi koneen TwinCatissä on näkyvillä View-valikosta Toolbars-palkit: *Build, Debug, Standard, TwinCat PLC, TwinCAT, TwinCAT safety Toolbar* ja *TwinCAT XAE Base*.

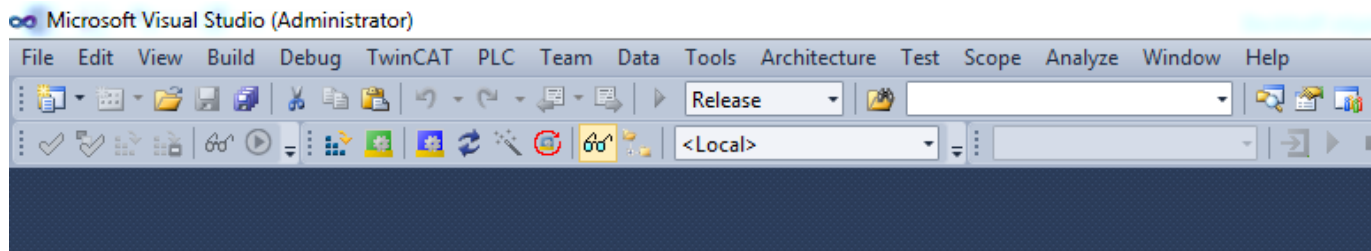
## 5. Luo uusi projekti.

- Luo C-juureen: C:\users\user ryhmäsi nimellä uusi kansio, johon jatkossa tallennat työn versiot.
- Seuraavaksi mene näytön yläreunan työkalujen *file*-valikkoon.
- Sieltä valitse *New -> Project*.
- Valitse *twinCAT Project*.

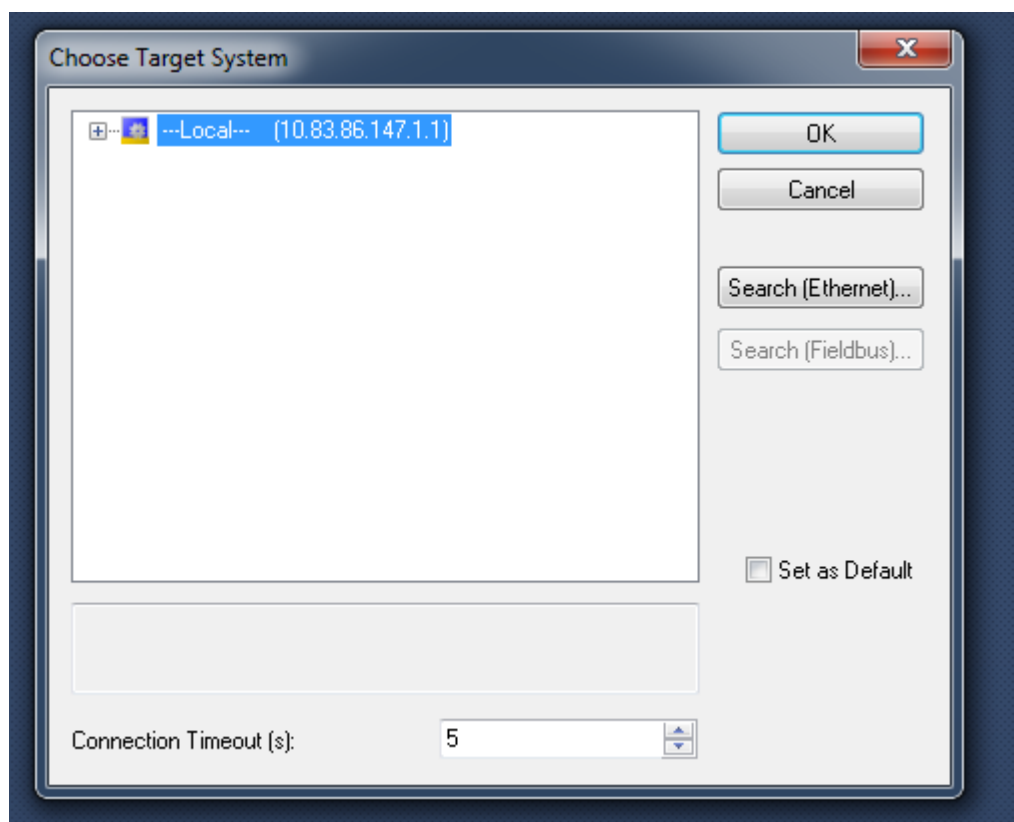


- Nimeä projekti jollain työtä kuvaavalla nimellä jonka muistat.
- Katso *Location*-kohdasta, mihin ohjelma tallentaa uuden projektin, ja merkitse polku ylös, jotta löydät myöhemmin projektisi.

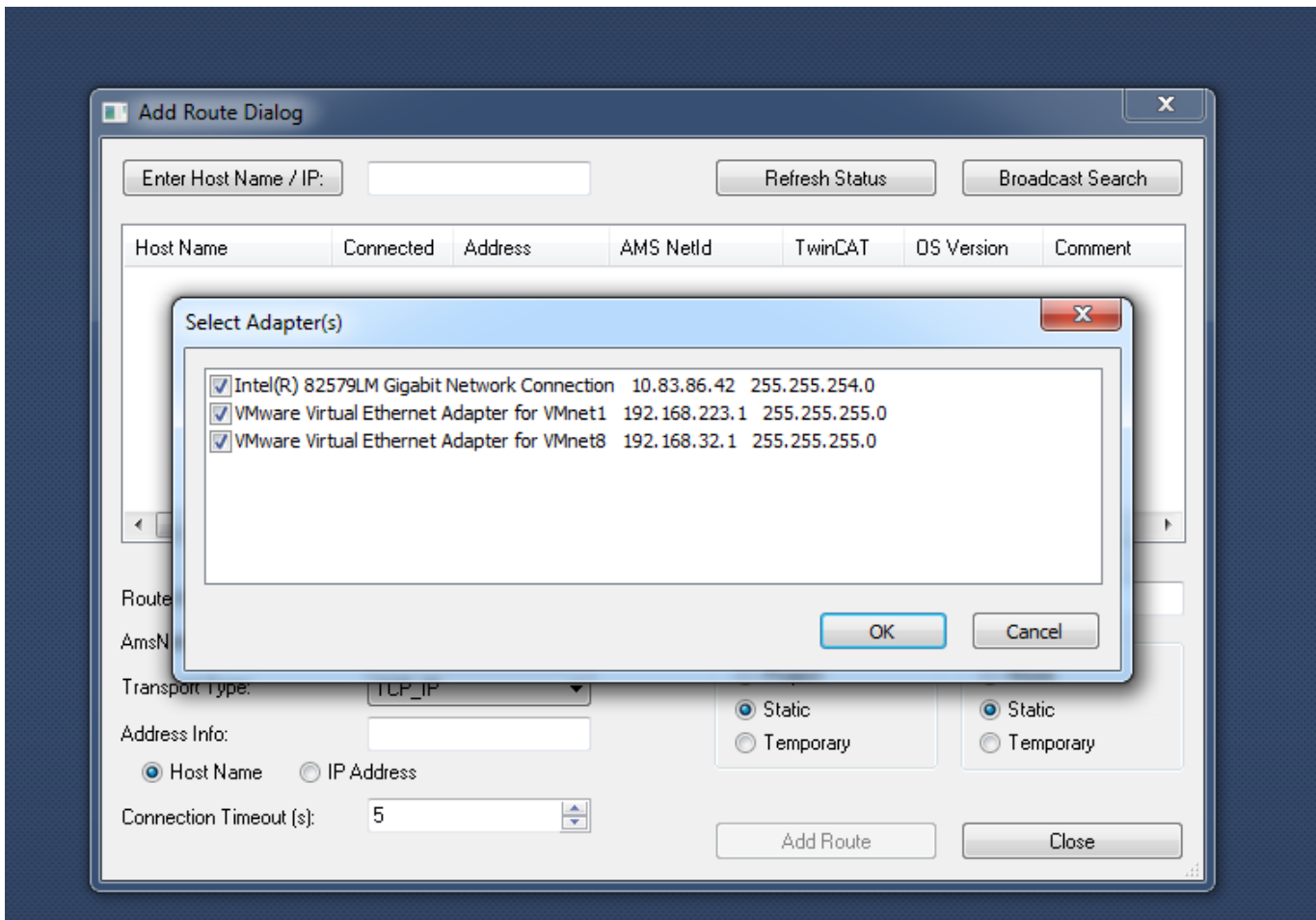
6. Katso TwinCATin ylätyöpalkista, löydätkö harjoituksessa käytettävän logiikan. Logiikka löytyy valikosta, jossa lukee *<Local>*. Logiikan nimi MAC osoitteen mukaisesti on CX-1984ED. Mikäli logiikkaa ei löydy valitse: *Choose target system*.



- Avautuvasta ikkunasta *Search (Ethernet)*.

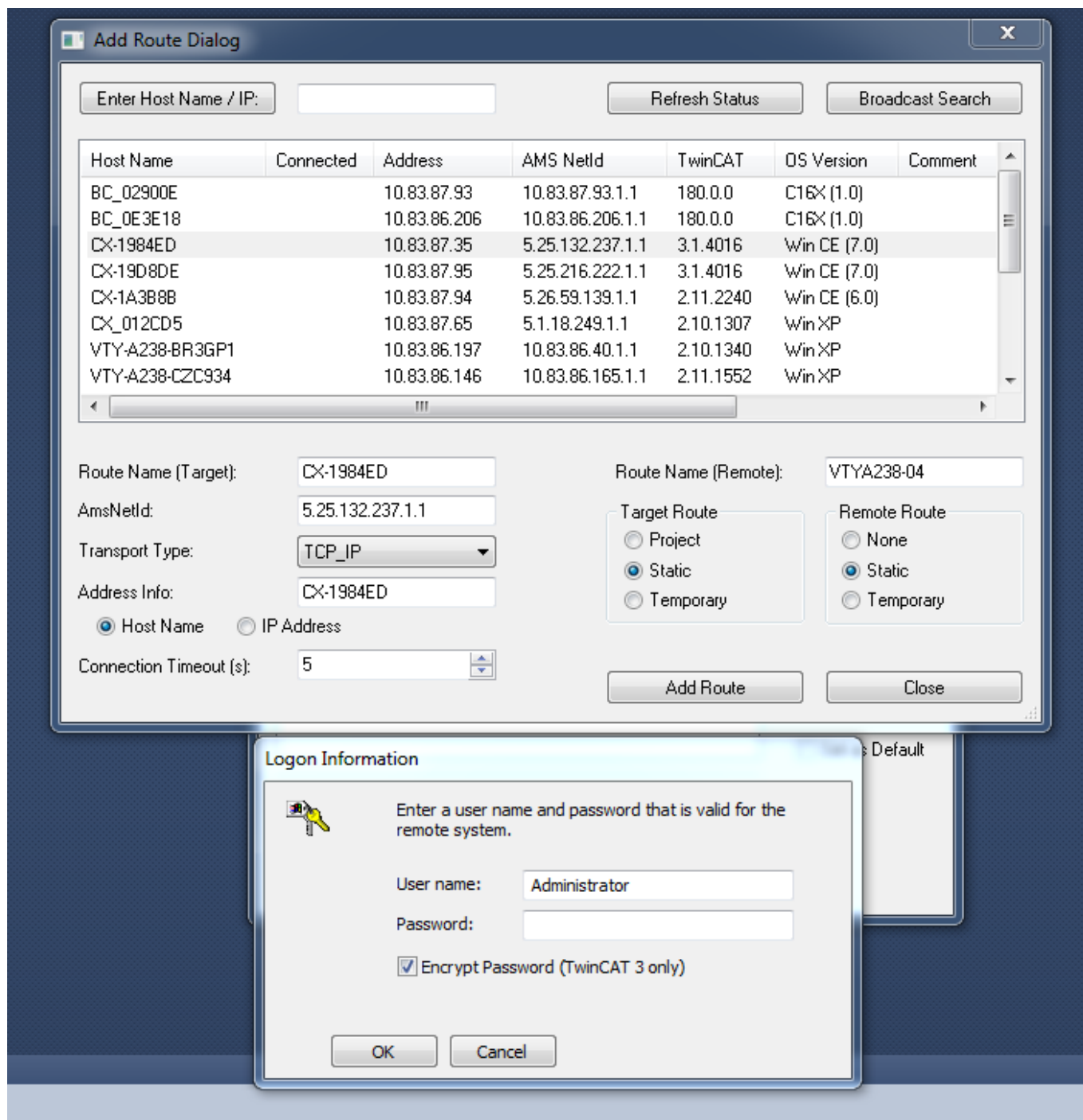


- Seuraavaksi avautuvasta ikkunasta valitse *Broadcast Search*, jonka jälkeen avautuu ikkuna *Select Adapter(s)*. Anna rastin olla kaikissa, ja paina *OK*.



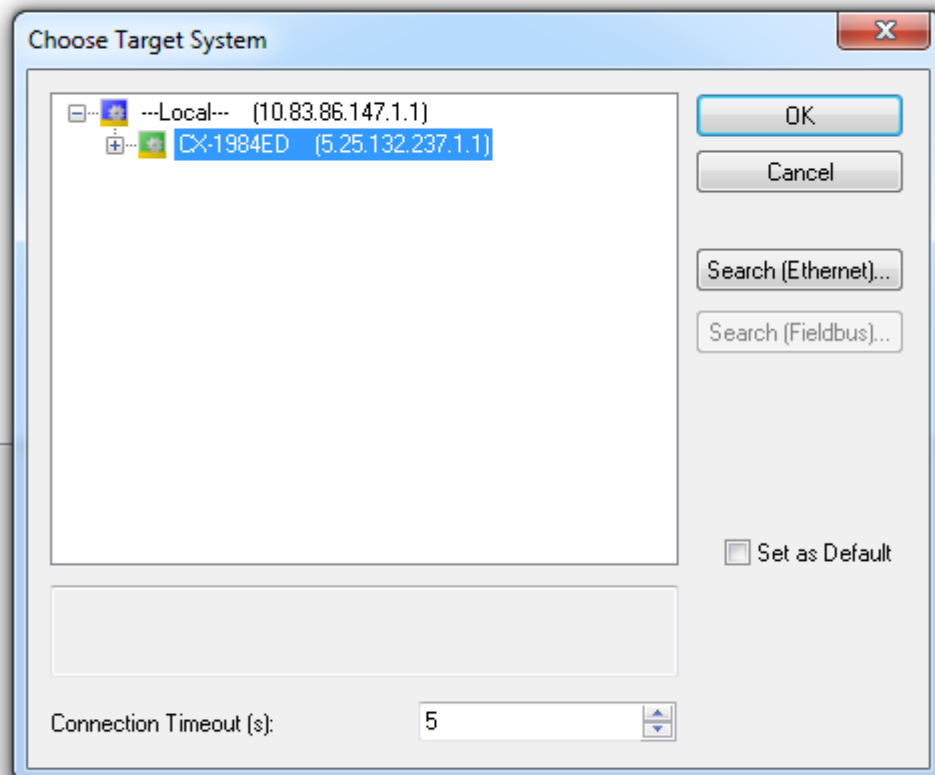
- Näkyviin tulevat ohjelman löytämät logiikat. Valitse harjoituksessa käytettävä logiikka ja paina *Add Route*. TwinSAFE-harjoituksessa käytettävä logiikan *Host Name*: CX-1984ED, *Adress* 10.83.87.35.



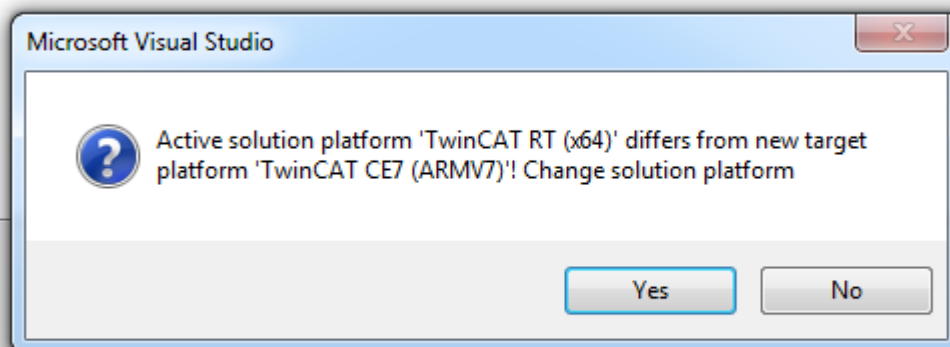


- Tämän jälkeen kone pyytää salasanaa: *User name*: Administrator ja *Password*: 1
- Kun logiikka on yhdistetty, ilmestyy *Connected*-kohtaan rasti.

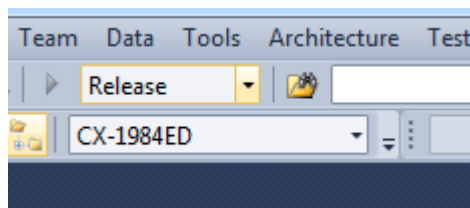
- Suljettuasi ikkunan tulee näkyviin:



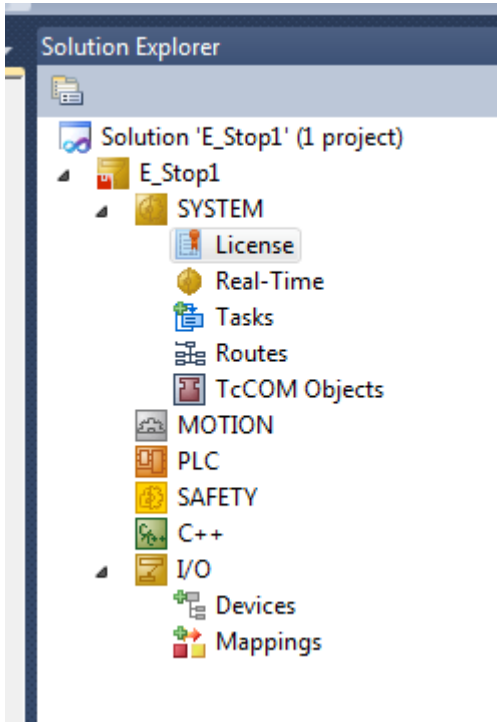
- Paina OK.



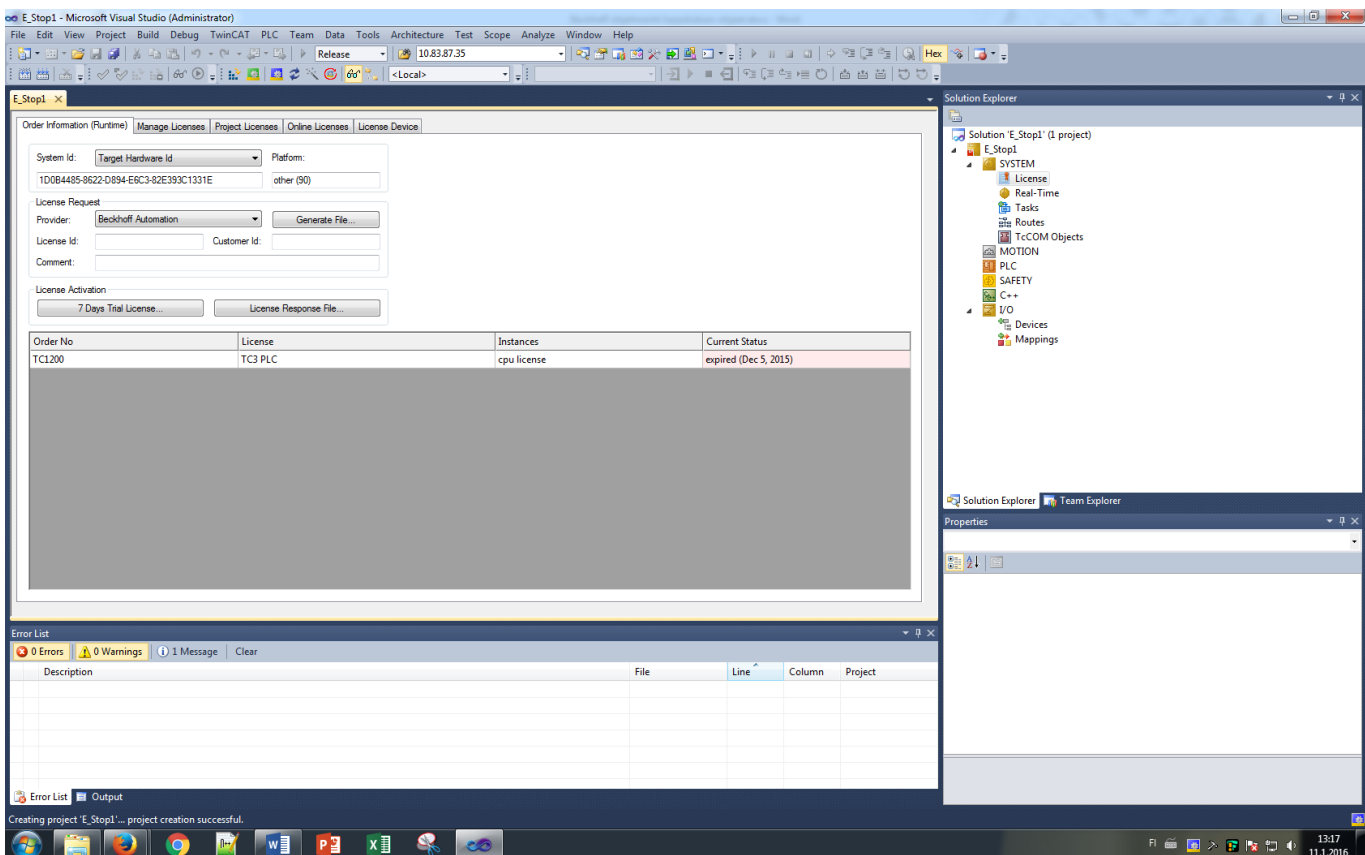
- Valitse Yes.
- Mene yläpalkin kohtaan *Release*, valitse *Configuration Manager*.





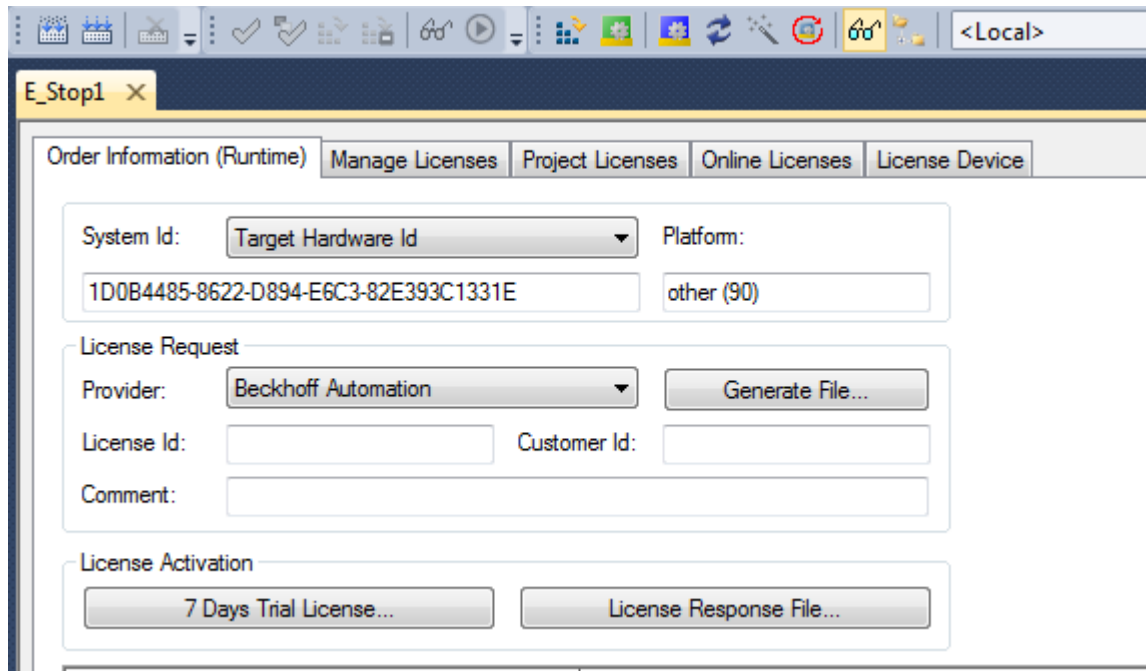


Kaksoisklikkaa hiiren oikealla välilehteä *License*, jolloin näkymäksi tulee:



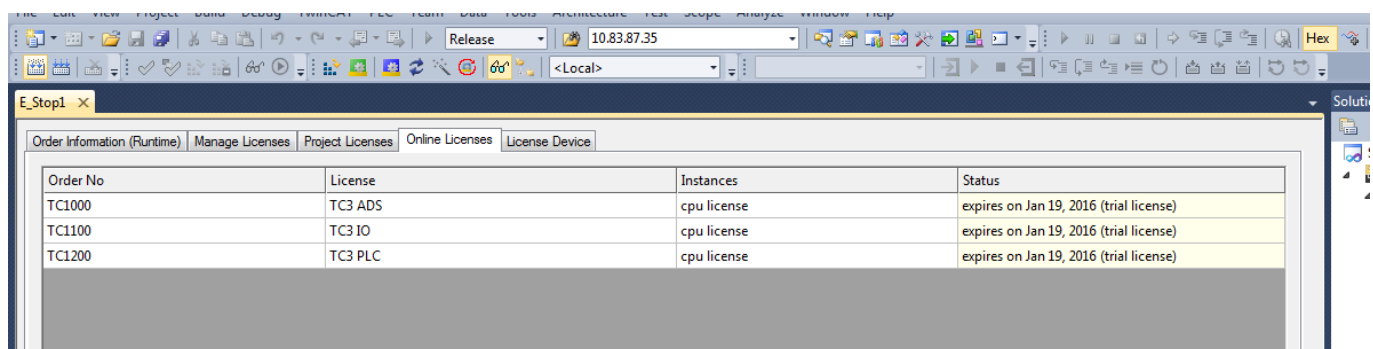
Mene välilehdelle *Manage Licenses*. Laita rasti *Add License*-kohdassa tarvitsemiisi lisensseihin.

Seuraavaksi mene:

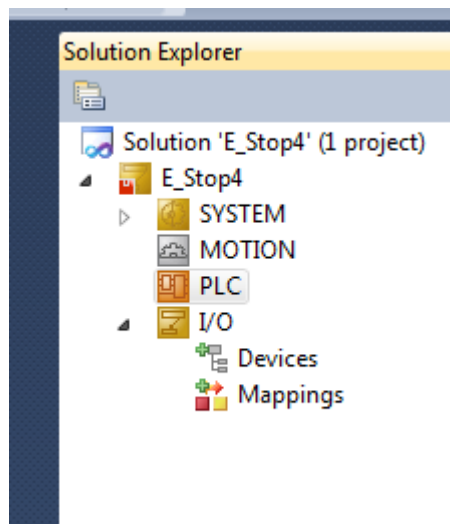


Valitse *7 Days Trial License* (7 päivän kokeilulisenssi), jolloin esiin tulee koodi. Näppäile koodi annettuun kenttään.

Saat tarkistettua sivulta *Online Licences*, mitkä lisenssit ovat voimassa ja kuinka kauan. Voimassa olevat lisenssit näkyvät vihreällä ja eräntyneet punaisella värillä.

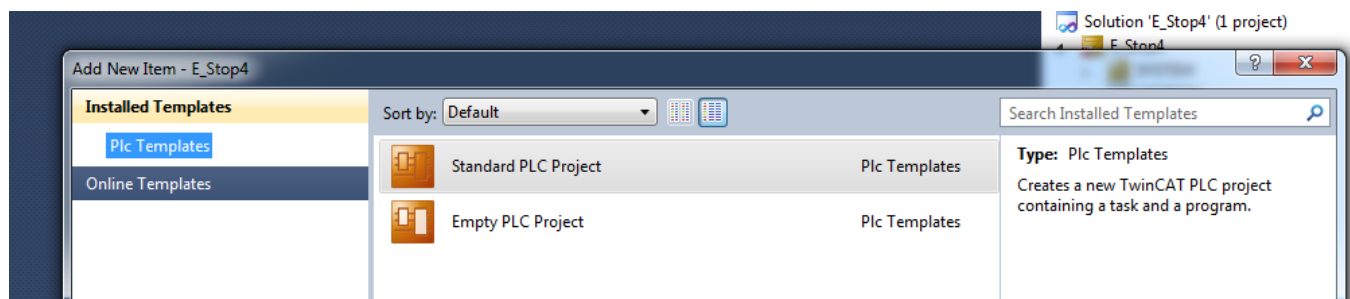


Kun lisenssit ovat voimassa, luo uusi PLC samalla nimellä kuin luomasi projekti *Solution Explorer PLC*-valikkoon.



## 8. PLC:n luonti.

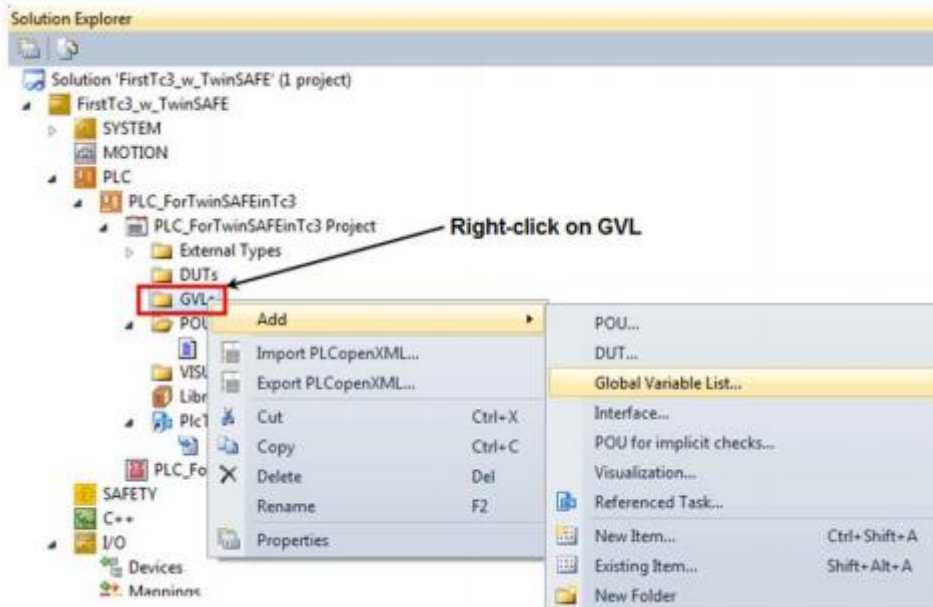
- Tee tämä vaihe *Local*ina.
- Klikkaa *PLC* aktiivisena kerran hiiren oikeaa.
- Valitse *Add New Item*. Avautuu ikkuna:



- Valitse *Standard PLC Project*.
- Anna sama nimi kuin projektillasi on.
- Seuraavaksi luo GVL (Global variable List).

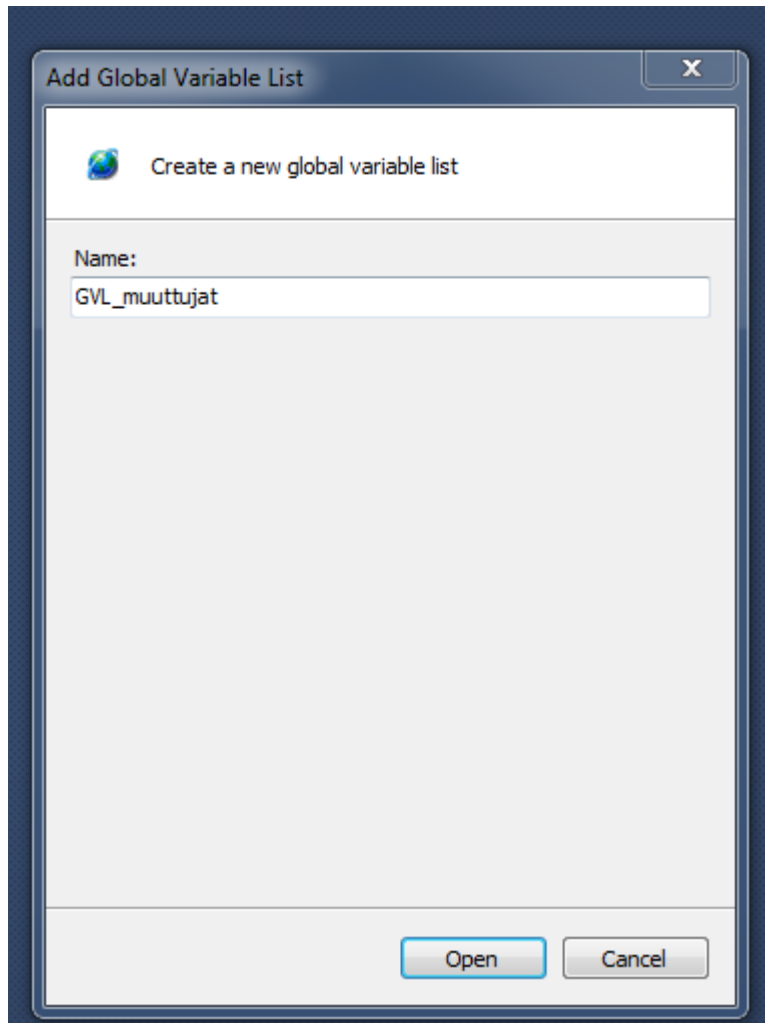
## 9. GVL:n luonti:

- Mene *PLC*:alta projektisi nimiseen *PLC*-valikkoon. Esimerkkikuvassa nimeltään *PLC\_ForTwinSAFEinTC3*, sieltä paina hiiren oikealla *GVLs*, jonka jälkeen aukeaa *Add*. Valitse *Add*-valikoista *Global Variable List*.





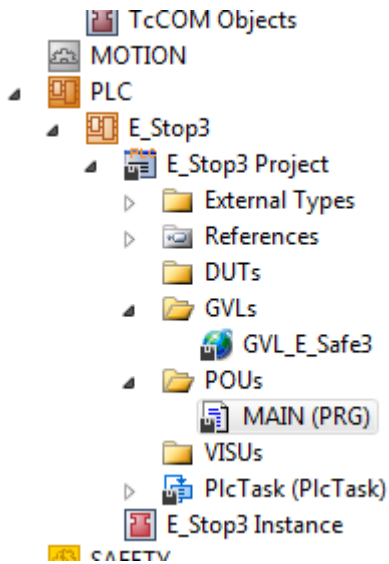
- Nimeä *Name*: GVL\_muuttujat.



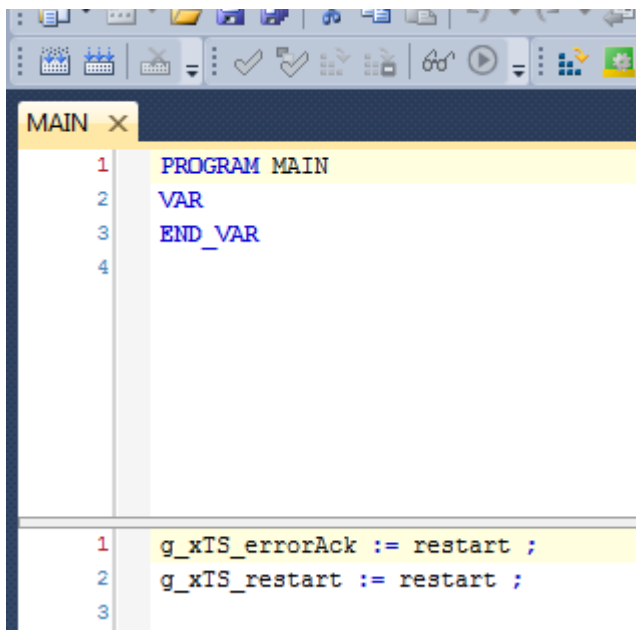
- Paina *Open*.
- Kirjoita GVL\_ kenttään kuvassa näkyvät käskyt:

```
GVL_E_Safe3 x E_Stop3
1  VAR_GLOBAL
2
3  //Commands to TwinSAFE controller's safety group
4  g_xTS_restart AT %Q* : BOOL ;
5  g_xTS_errorAck AT %Q* : BOOL ;
6
7  // Feedback from TwinSAFE controller's safety group
8  restart AT %I* : BOOL ;
9
10 END_VAR
```

10. Seuraavaksi luo pääohjelmaan HÄTÄSEIS-ohjelman resetointi.
- Mene *POUs MAIN (PRG)*.

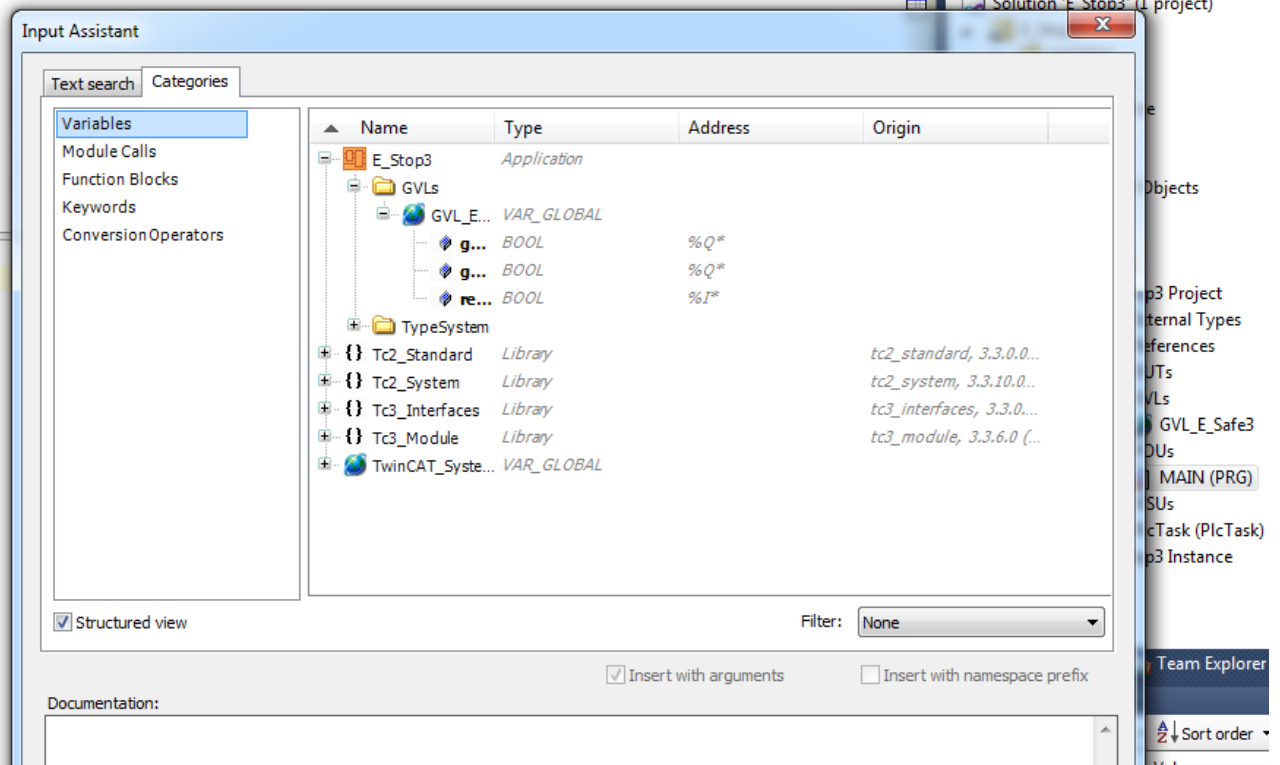


- Luo yhteydet.



Kuva: valmis *MAIN*-käskytyiskohta.

- Luo alimmaisen osan rivillä 1 näkyvä komento.
- Paina näppäimistöstä F2, aukeaa:

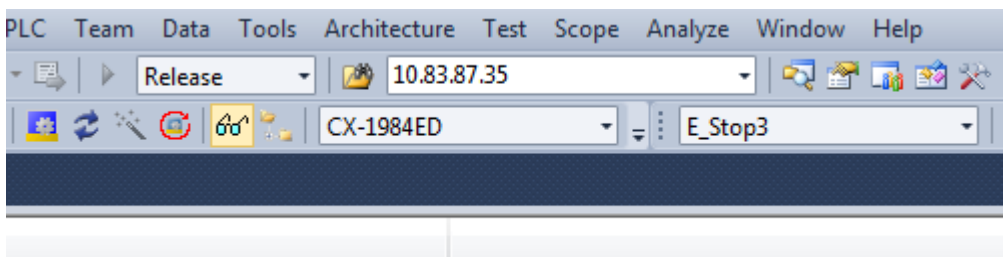


Valitse sieltä *GVL\_E ...VAR\_GLOBAL*-valikon alta *g\_xTS\_errorAck BOOL %Q\** kaksoisklikkaamalla hiiren vasenta näppäintä, jolloin se ilmestyy kenttään. Kirjoita perään komento `:=` ja lisää perään `restart`. Lisää `restart` samoin, mutta valitse *restart BOOL %I\**.

- Anna seuraava komento.

11. Lisää harjoitukseen seuraavaksi I/O:t.

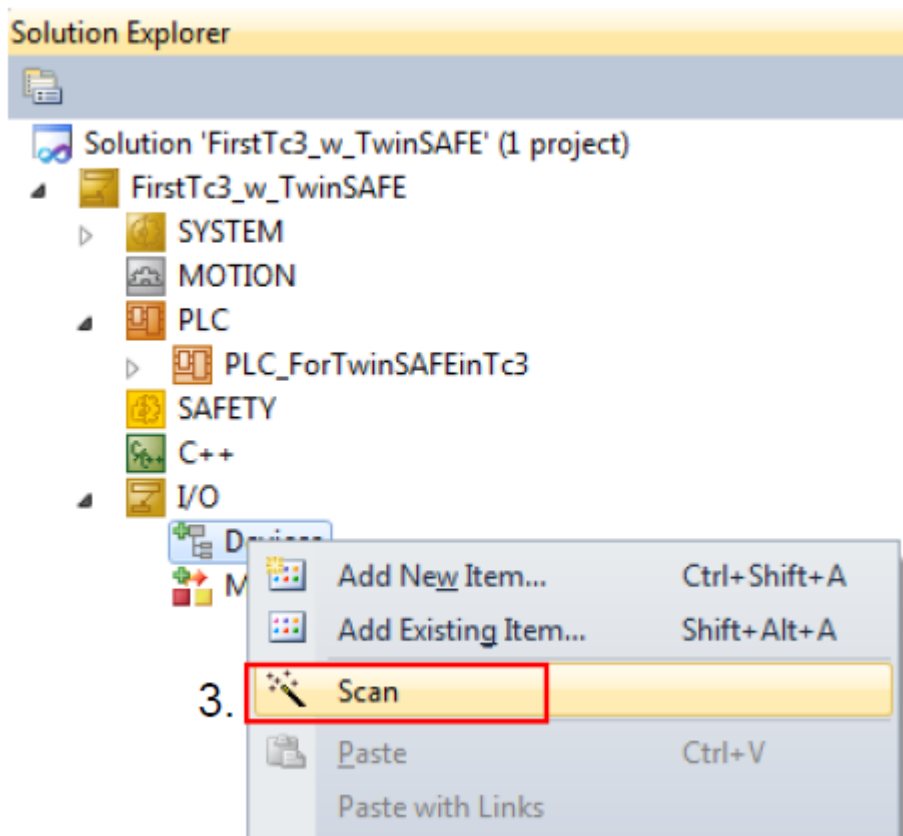
- Lisätessäsi I/O:t on oltava valittuna kyseinen logiikka:



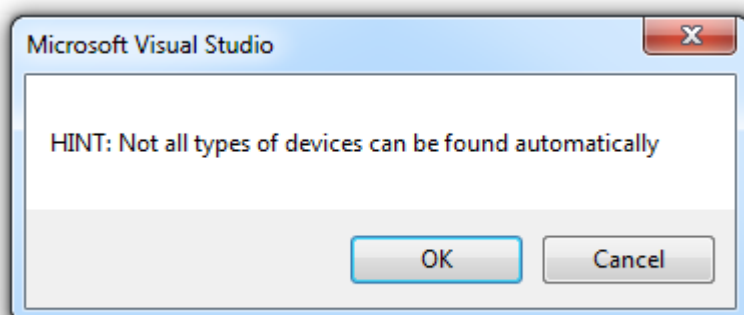
- Katso, että TwinCAT on tilassa Config Mode.



- Mene I/O Devices -> Scan.

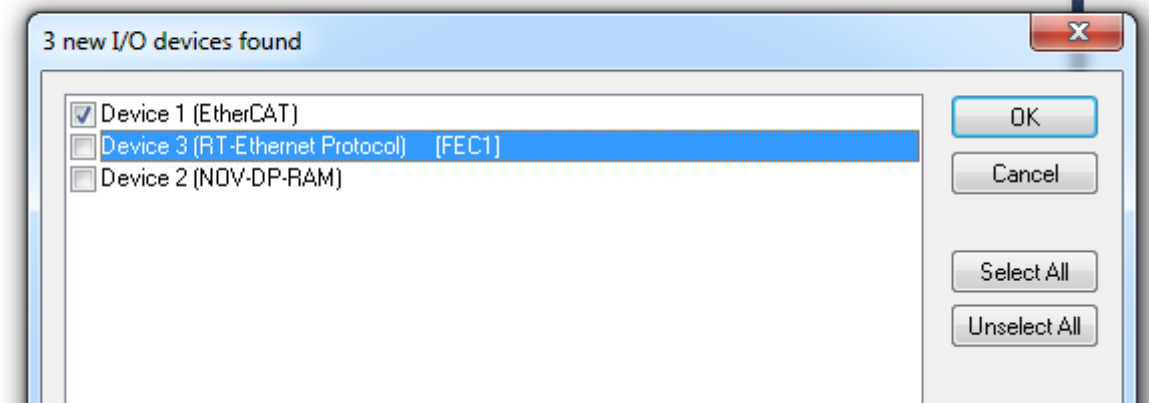


- Ohjelma huomauttaa:

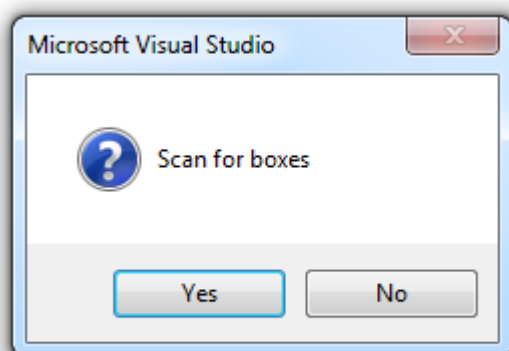


Paina OK.

- Valitse näkyviin avautuvasta ikkunasta *Device 1 (EtherCAT)*.

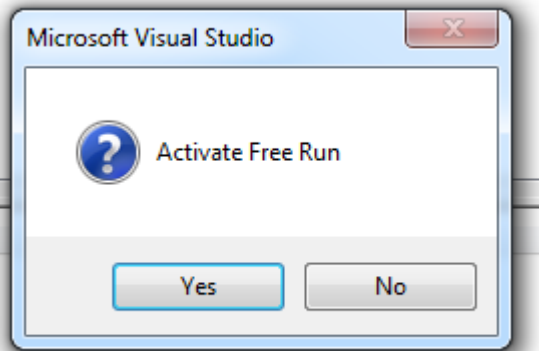


- Kysyy:



Vastaa Yes.

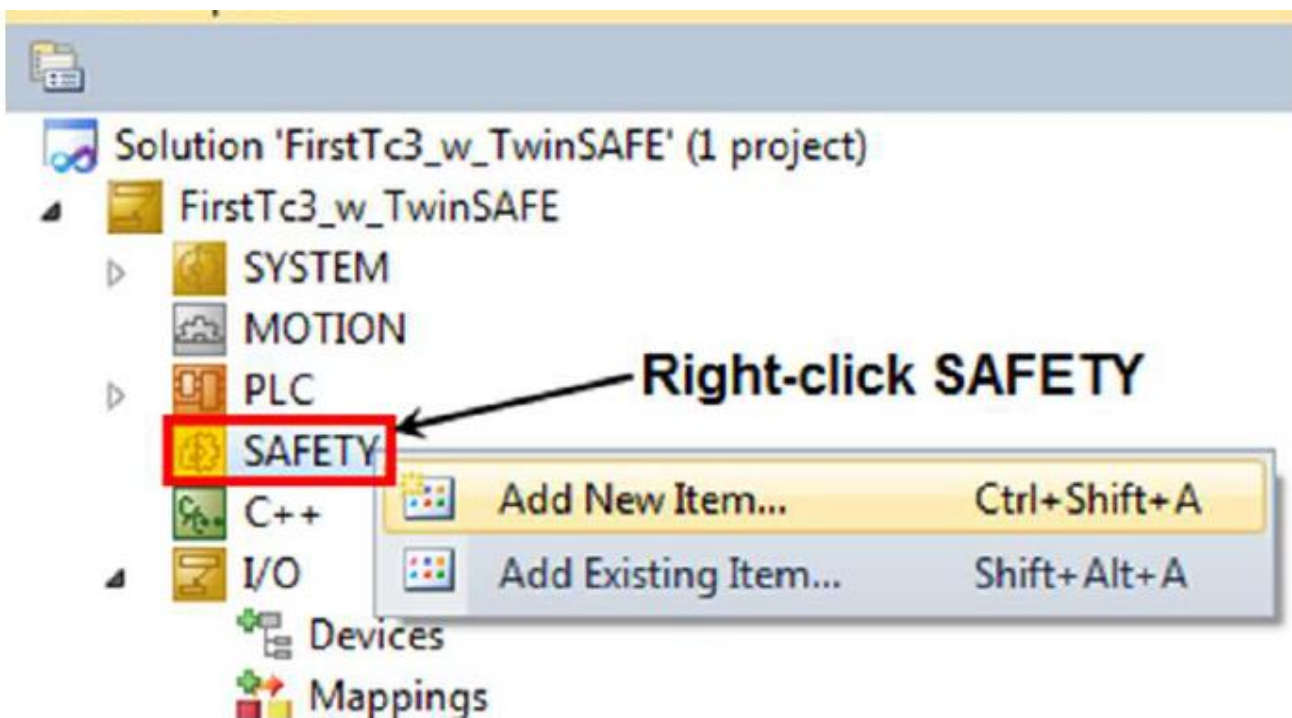
- Kysyy:



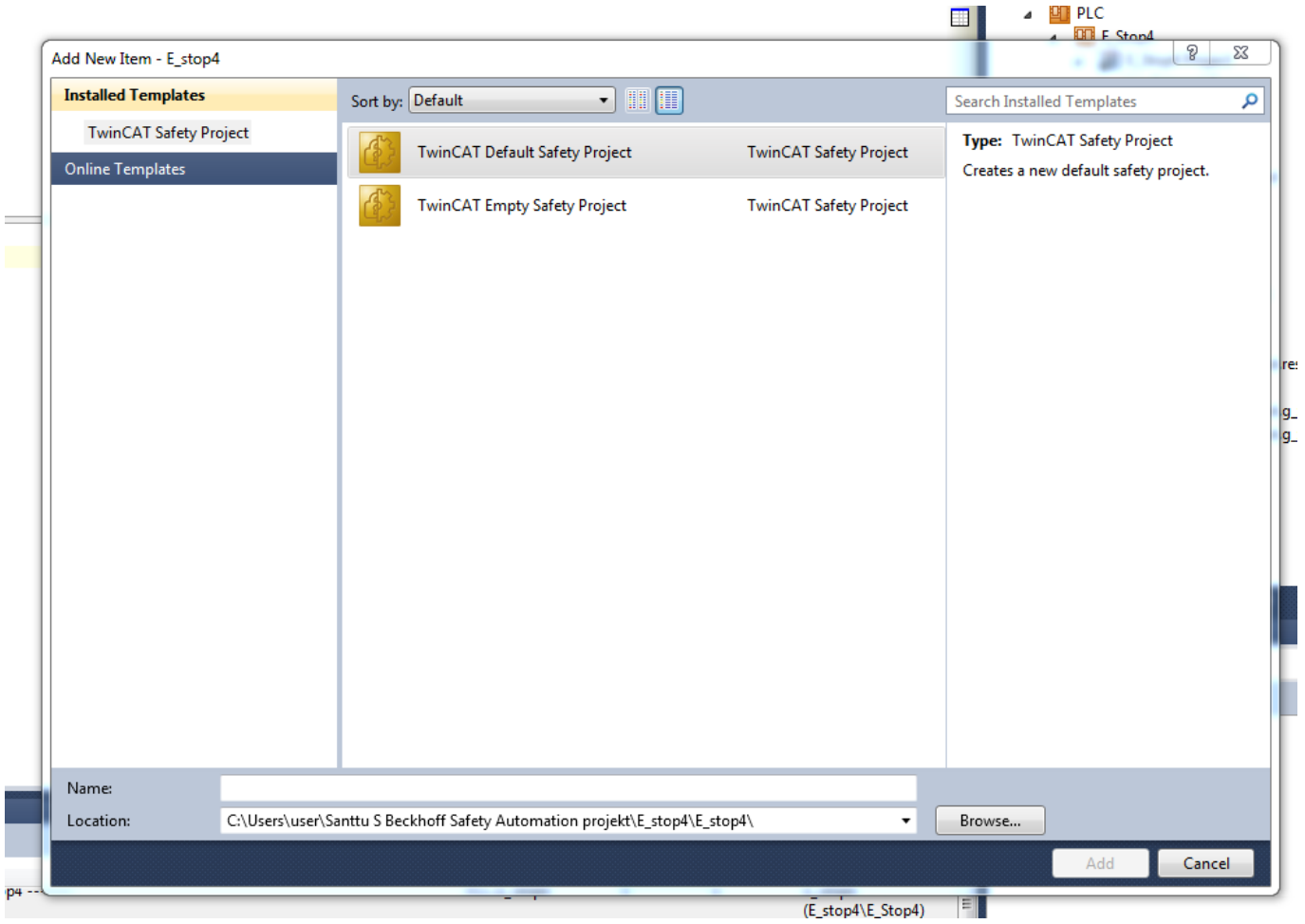
- Vastaa No.

12. Luo turva projekti Safety Projekt.

- Mene *Solution Explorerin*-valikkoon *SAFETY*.
- Klikkaa hiiren oikealla.



- Valitse *Installed Templates* valikosta ohjelman ehdottama *TwinCAT Safety Project*.
- Projektiksi *TwinCAT Default Safety Project*.
- Kirjoita kenttään *Name* luomasi projektin nimi.
- Paina *Add*.



- Tulee näkyviin kenttä:



TwinCAT Safety Project Wizard

TwinCAT 3 Safety Wizard

Target System: EL69XX

Programming Language: Graphical Editor

Author: user

Internal Project Name:

Ok Cancel

- Kirjoita *Internal Project Name* -kenttään projektisi nimi ja paina *Ok*.

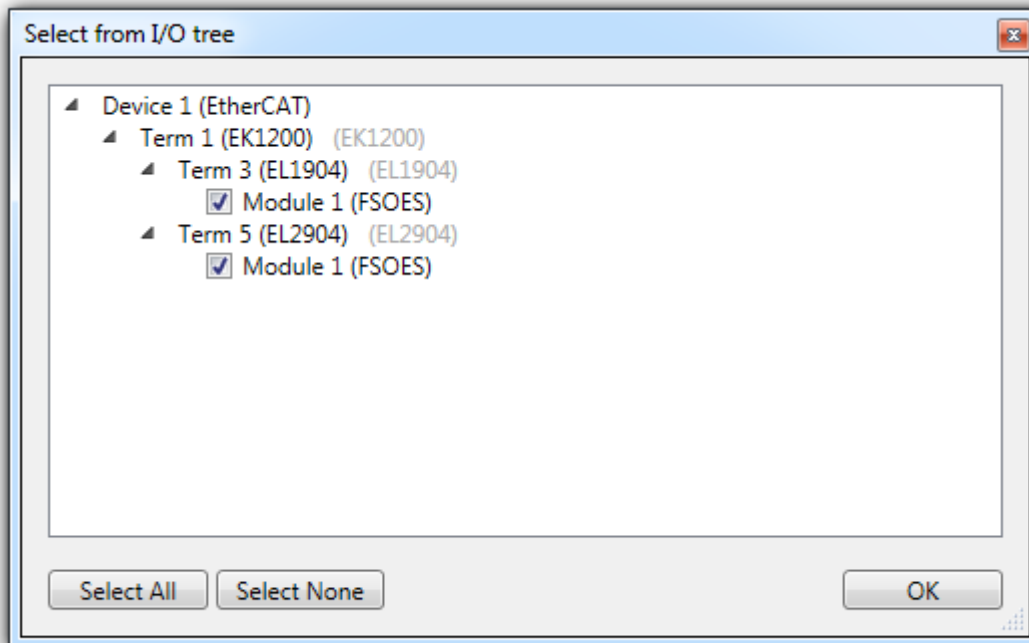


### 13. Seuraavaksi tuodaan I/O:t turva-automaatiolle

- Mene kohtaan *Alias Devices*, klikkaa hiiren oikealla ja valitse *Import Alias-Device(s) from I/O-configuration*.

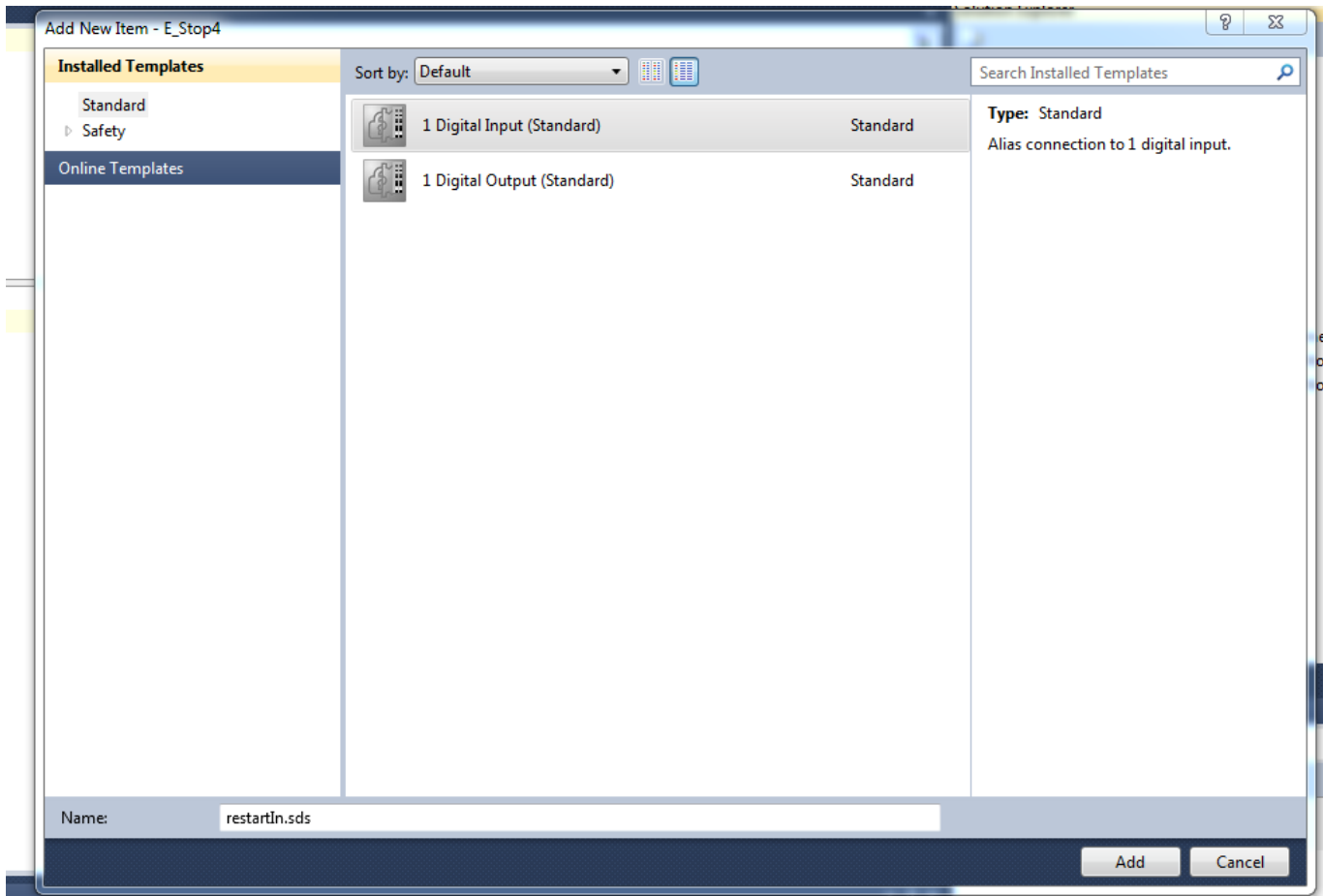


- Valitse haluamasi I/O:t ja paina OK. Tässä harjoituksessa kuvassa näkyvät:



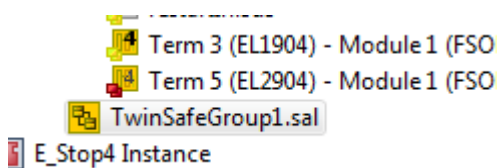
### 14. Seuraavaksi luo uusi alias Devices: restartIn.sds.

- Klikkaa hiiren oikealla *Alias Devices*.
- Valitse *Add* sieltä *New Item*,
- Aukeavasta ikkunasta valitse *Installed Templates, Standard*.
- Luo *Digital Input (Standard)*.
- Anna nimeksi *restartIn.sds*.
- paina *Add*.

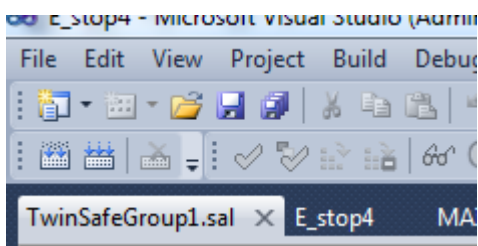


#### 15. Luodaan Hätäseis.

- Mene turva-automaatiosovelluksen ohjelmointitasolle.
- Kaksoisklikkaa hiirellä *TwinSafeGroup1.sal*.

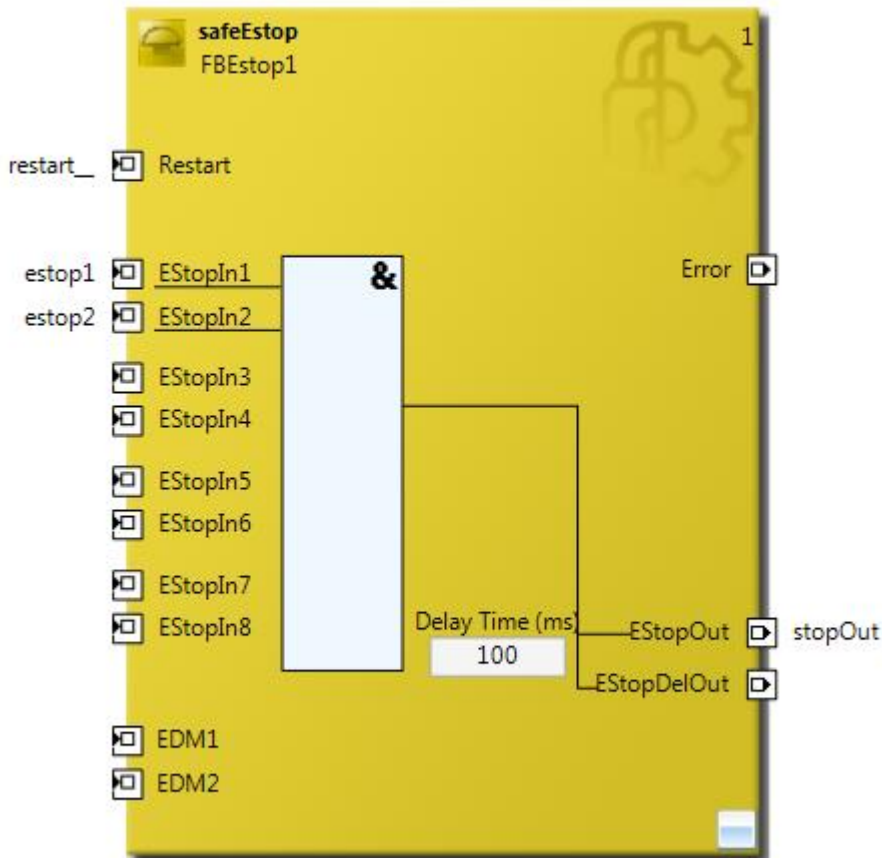


- Avaa *View* valikosta *Toolbox*.

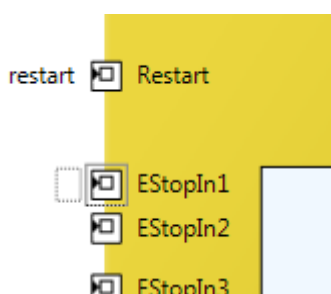


- Valitse *toolbox*sta *safeEstop* ja vie se työpöydälle.

- Nimeä safeEstopin tulot ja lähtö. Näin luot kytkennän komponentin kyseiseen paikkaan.

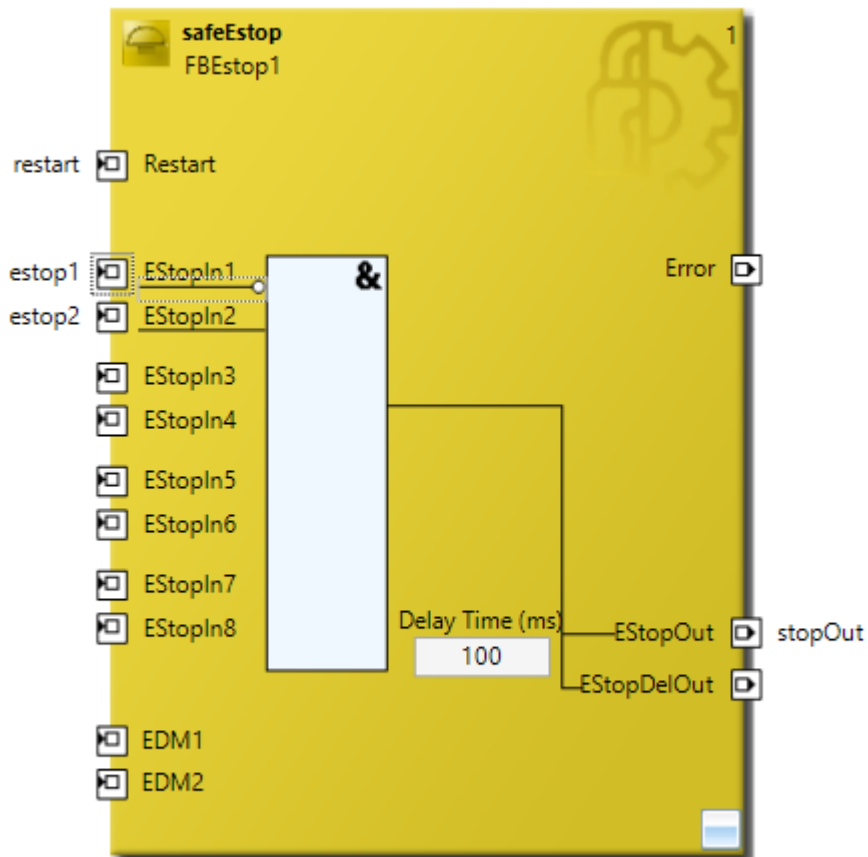


- Klikkaa kohdan pienen vaalean laatikon päältä niin että katkoviivoin oleva pienempi laatikko tulee näkyviin. Kirjoita nimi siihen.



- Mikäli tarpeen tee In-tuloon tulosignaalinkäyntö eli boolean algebran EI-toiminto.
- Operaatio toteutetaan klikkaamalla hiiren oikealla painikkeella ja valitsemalla aukeavasta luettelosta *properties*, sekä painamalla halutun *Single-Channelin* päädyssä näkyvää pientä nuolta.
- Muuttamalla avautuvasta valikosta *Break Contact (NC)* muotoon *Make Contact (NO)*.

Function Block Input Settings	
Channel Interface	Single-Channel Both Activated
Discrepancy Time (ms)	
Single-Channel 1	Make Contact (NO)
Single-Channel 2	Break Contact (NC)
Misc	

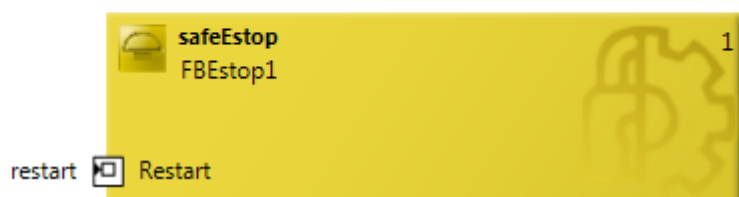


- Kaksoisklikkaa hiiren oikealla työpöydän yläreunassa näkyvää *Network*.
- Viestin käänösoperaation merkiksi tulee kytkentään näkyviin valkoinen pallo.
- Sulje *Toolbox*.

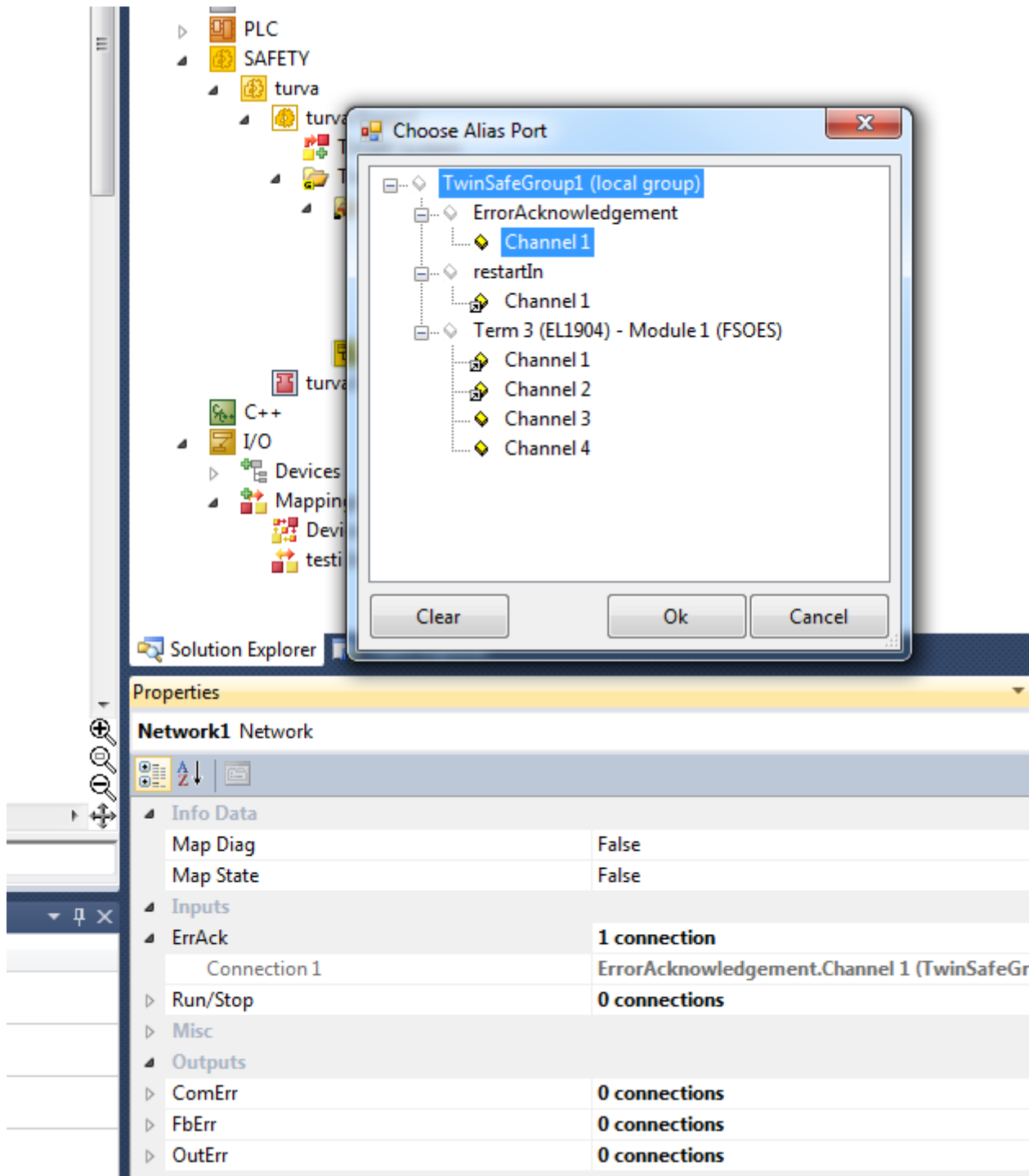
- Kaksoisklikkaa hiiren oikealla työpöydän yläreunassa näkyvää *Network1*.

---

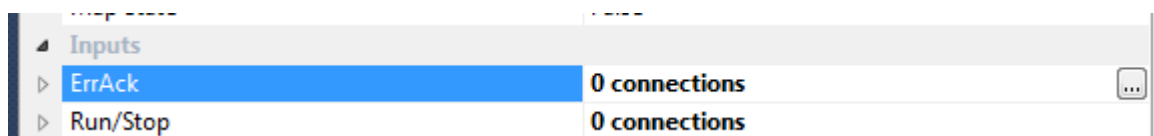
Network1



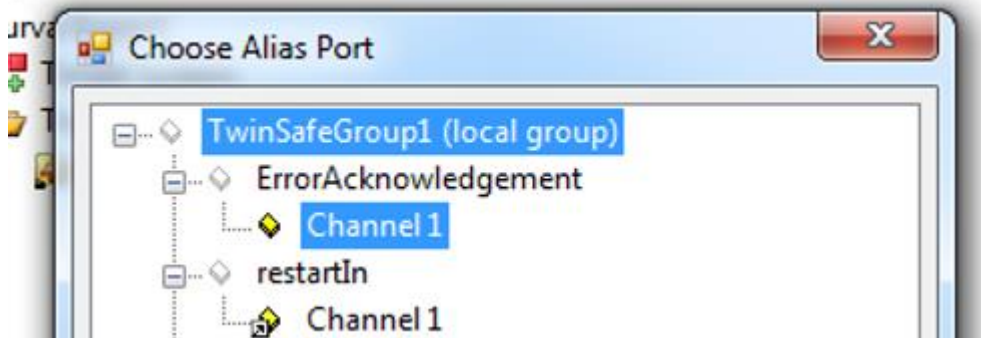
- Näytön vasempaan alareunaan aukeaa: *Properties*.



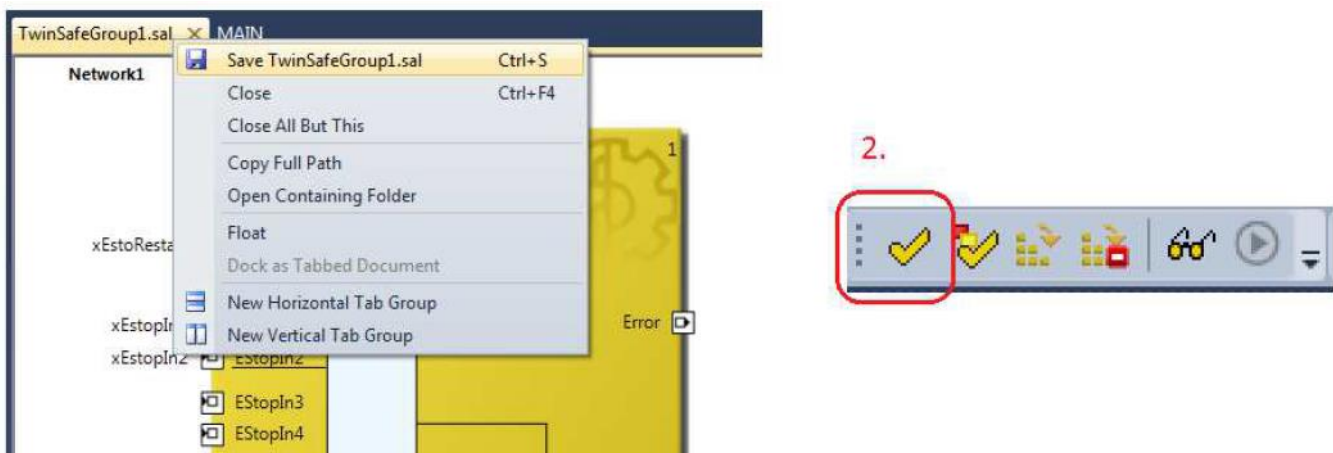
- reitit sieltä *ErrAck* kaksoisklikkaamalla oikealla näkyvää pientä laatikkoa vasemmalla.



- Määrittele:



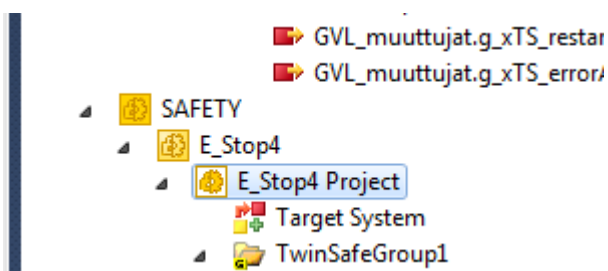
- Tallenna tekemäsi sovellus TwinSAFE ohjelman projektitasolle.



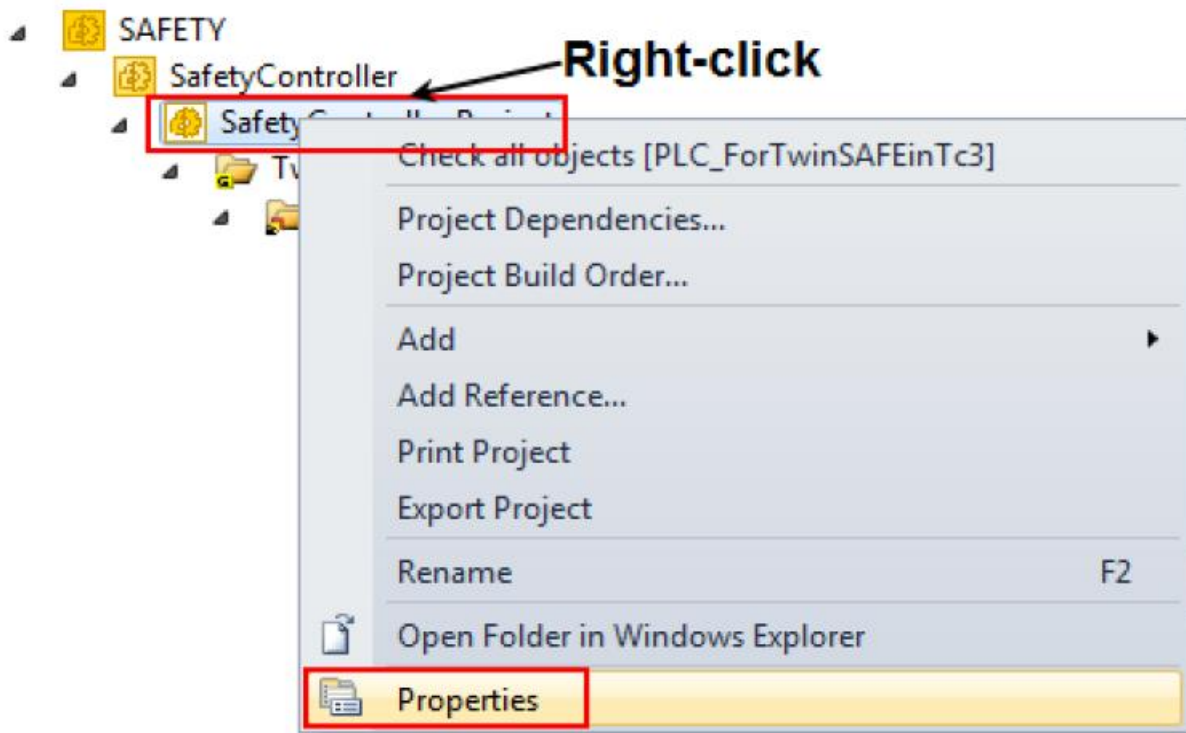
- Ensin painamalla yläkulmassa näkyvää tallenna symbolia: *Safe TwinSafeGroup1.sal*.
- Seuraavaksi klikkaa turvaohjelman työkaluista keltaista V-merkkiä.
- Älä tässä vaiheessa välitä näytön vasempaan alareunaan tulevista varoituksista ja virheistä; Ohjelman luonti on vielä kesken!!!

16. Seuraavaksi kytketään SAL (Safety Application Layer) logiikkaan. I/O korttirivistössä on kortti EL6900. Tuodaan tämä projektiin.

- Mene kohtaan:



- Kaksoisklikkaa hiiren oikealla nimeämäsi projektin päätä. Valitse sieltä *Properties*.

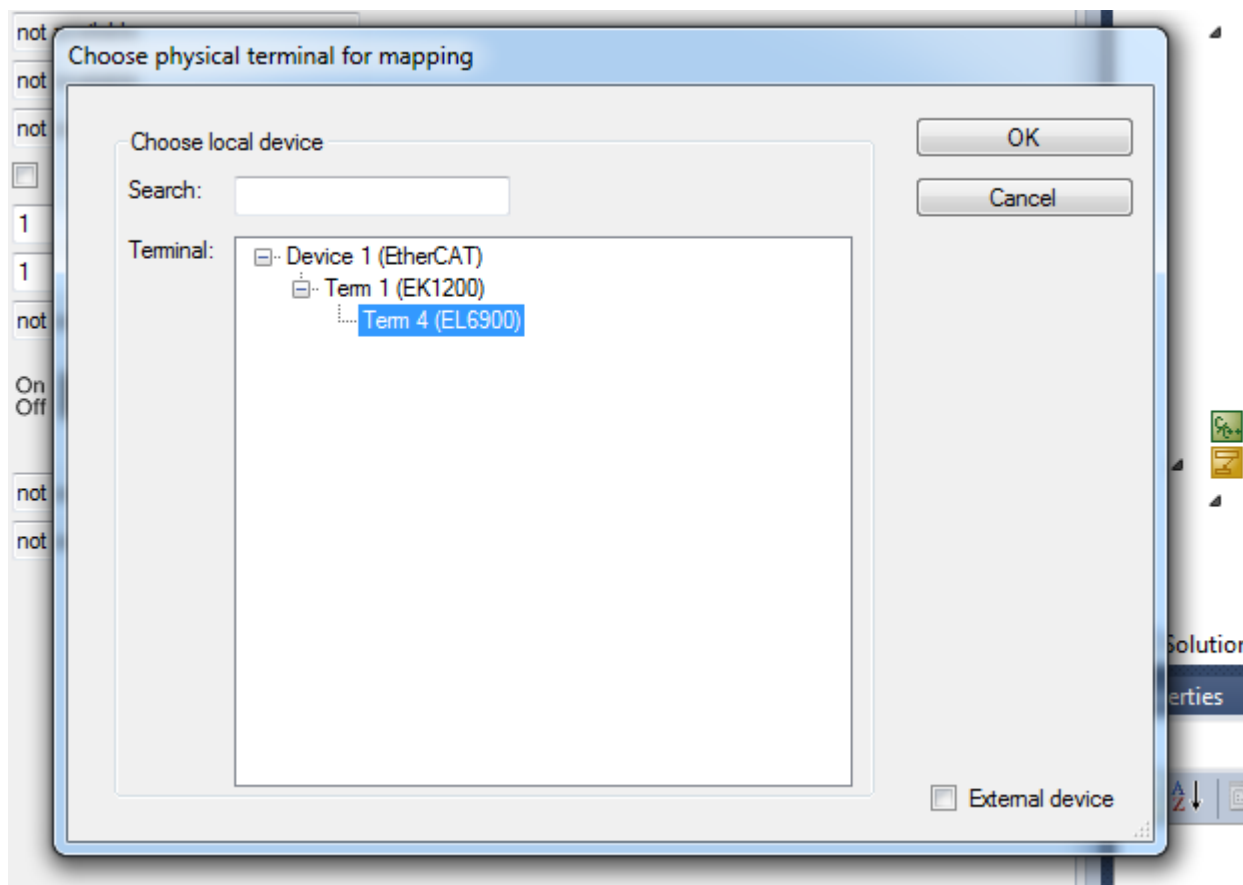


- Näkyviin tulevasta ikkunasta klikkaa värikästä neliötä.



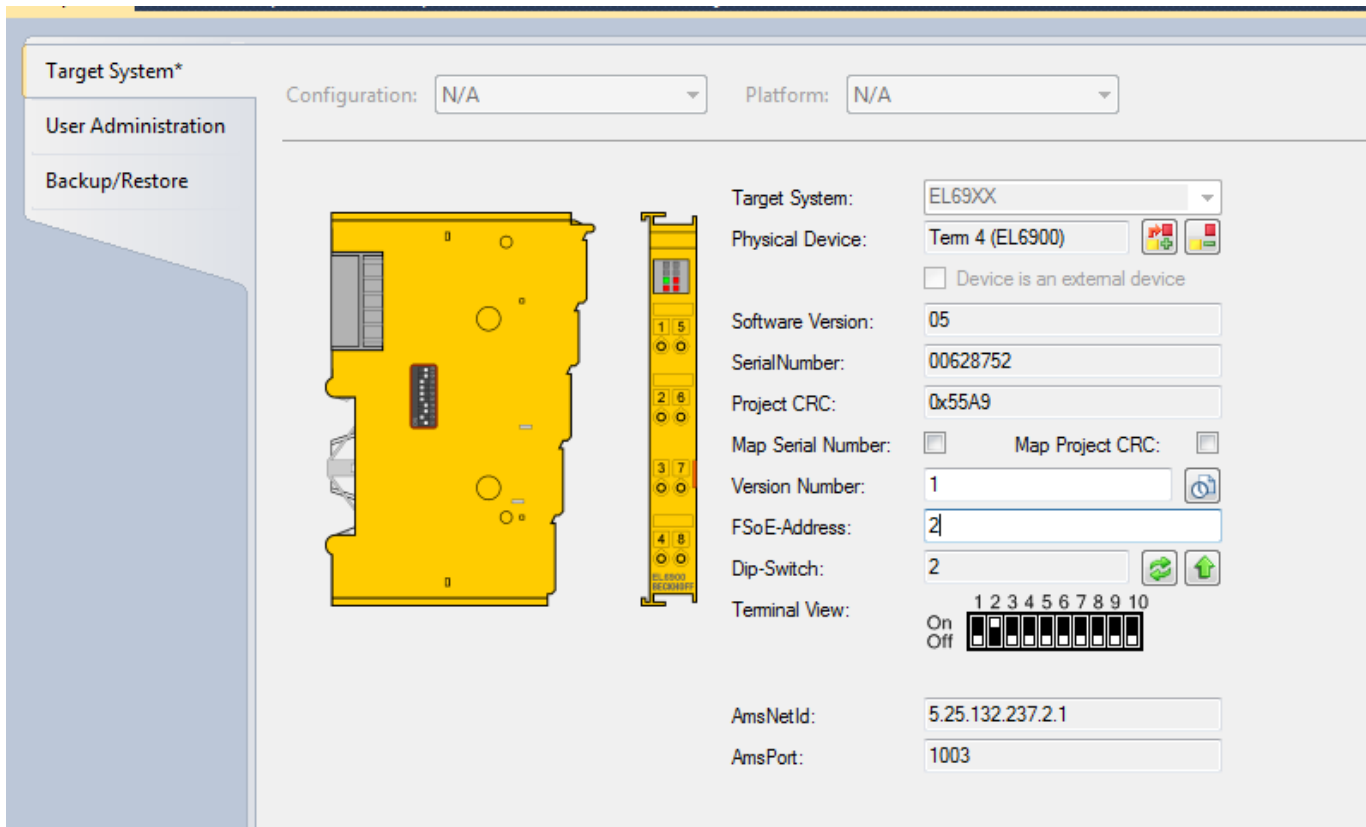
- Valitse *Term\_* (EL6900) ja paina OK.



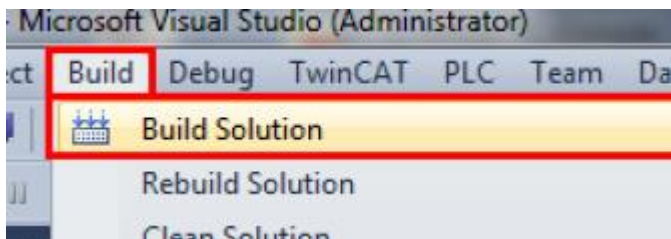


- Ohjelman pitäisi löytää kortin tiedot.
- Muuta *FSoE-Address*: 2

- Alla olevassa kuvassa on oikeat tiedot.

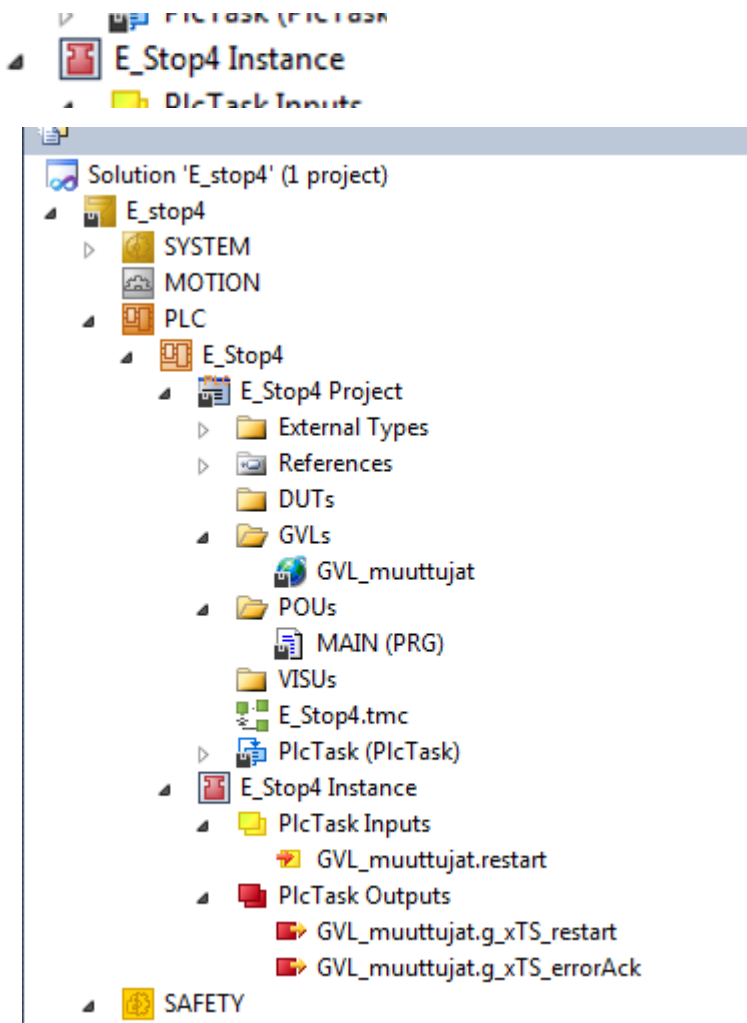


- Mene ylävalikkoon *Build* ja tee sieltä *Build Solution*, voit tehdä sen myös näppäimellä F6.

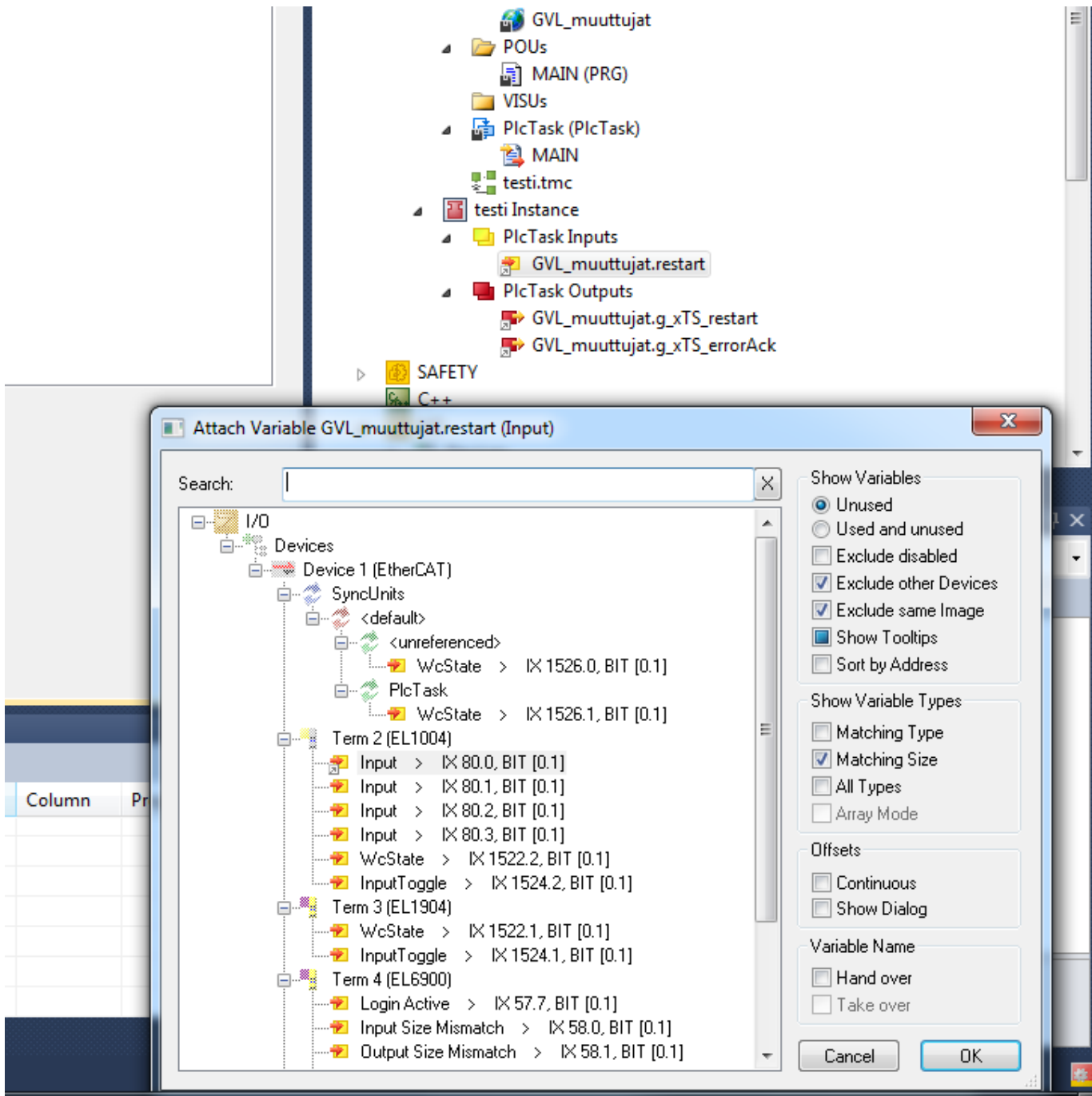


- Jätä ikkuna työpöydälle auki.

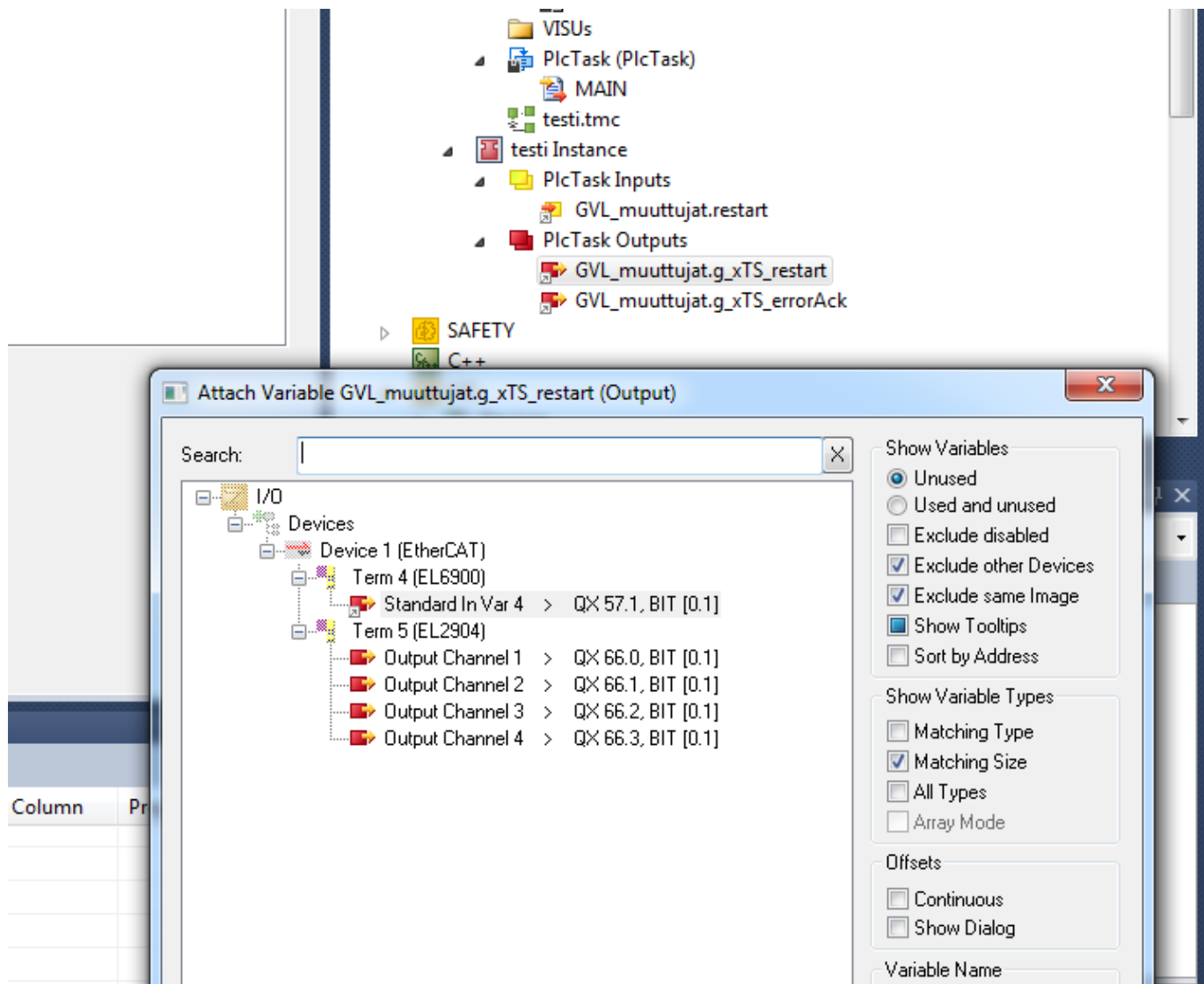
17. Tee reititykset *Instans* -kohdan Inputseille ja Outputseille.



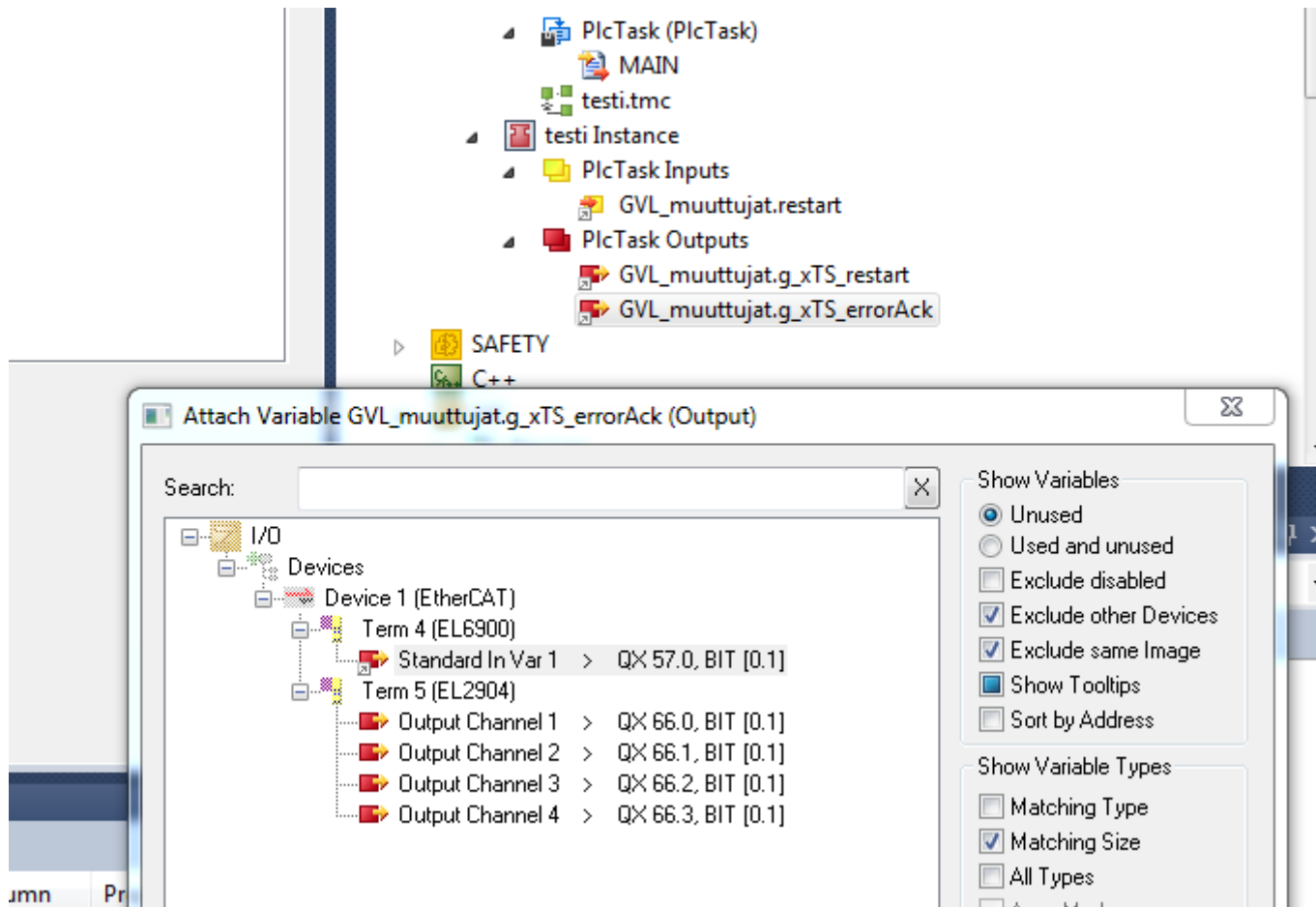
- Klikkaa vasemmalla *GVL\_muuttujat.restart* päältä.
- paina *Change Link*.
- Valitse Inputiksi *TERM2 (EL1004)*, *input > IX 80.0, BIT [0,1]*
- Paina *OK* vahvistaaksesi valinnan.



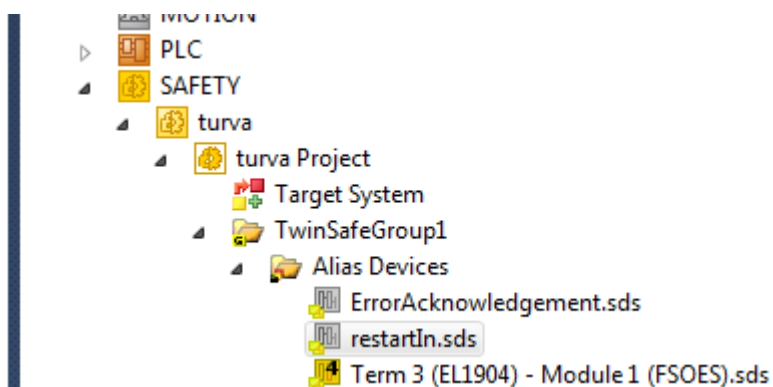
- Klikkaa vasemalla *GVL\_muuttujat.g\_xTS\_restart* päältä.
- paina *Change Link*.
- Valitse Inputiksi *TERM4 (EL6900), standardIn Var 4 > QX 57.1, BIT [0,1]*
- Paina *OK* vahvistaaksesi valinnan.



- Klikkaa vasemmalla *GVL\_muuttujat.g\_xTS\_errorAck* päältä.
- paina *Change Link*.
- Valitse Inputiksi *TERM4 (EL6900), standardIn Var 1 > QX 57.0, BIT [0,1]*
- Paina *OK* vahvistaaksesi valinnan



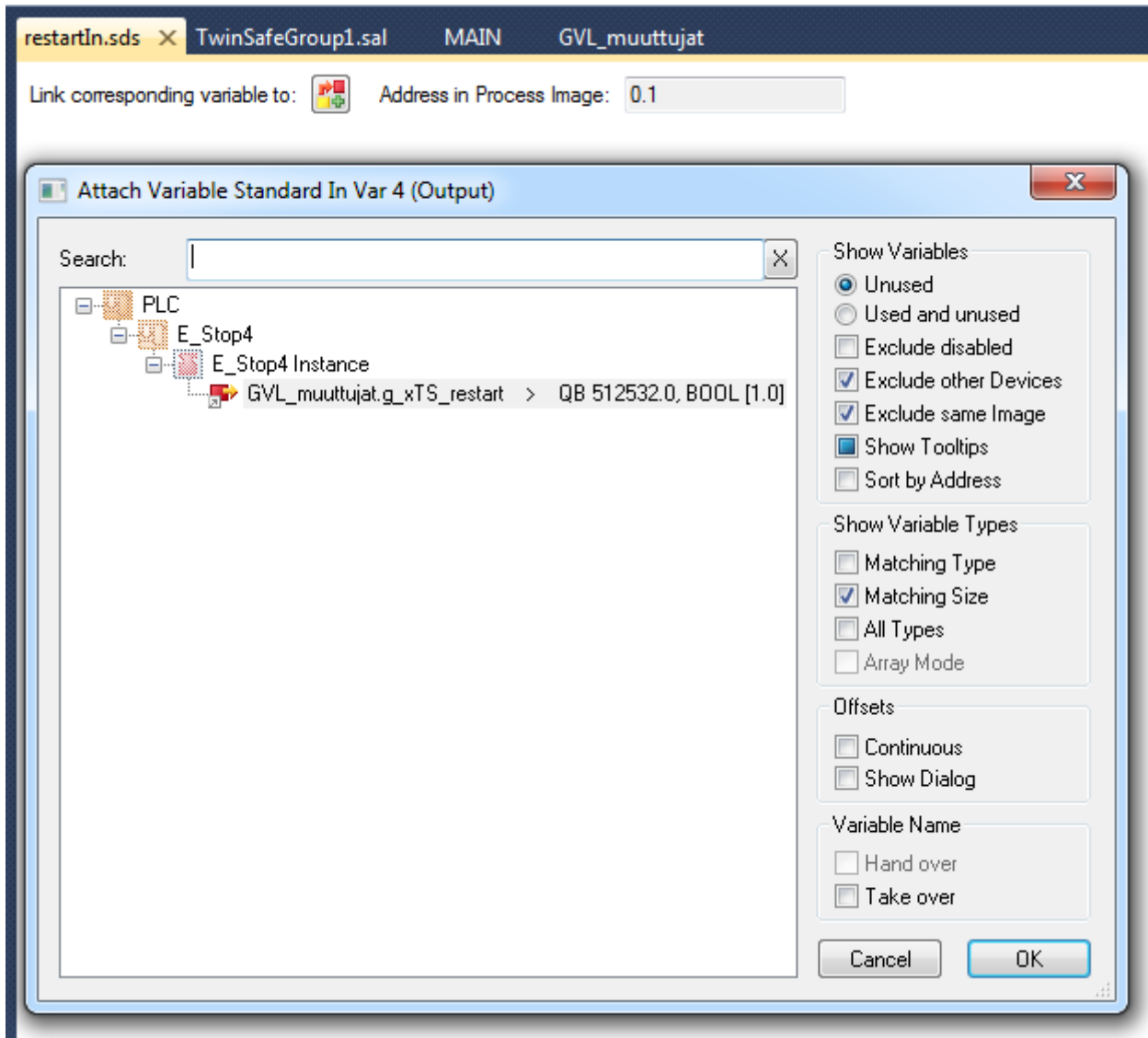
#### 18. SAFETYssä olevan *Alias Devices restartIn.sds*:n reititys



- Tuplaklikkaa hiiren vasemmalla *restartIn.sds*:n päältä.
- Työpöydälle aukeaa välilehti *restartIn.sds*
- Klikkaa hiiren vasemmalla siinä näkyvää ikkunaa:

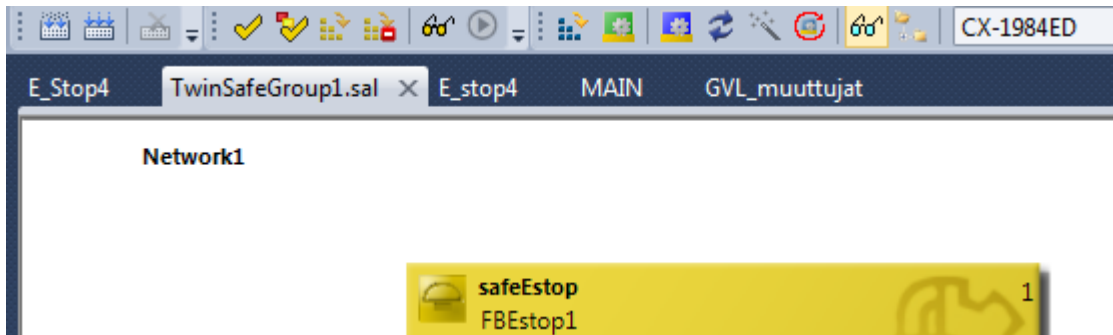


- Tulee näkyviin *Attach Variable Standard in Var 4 (Output)*.
- Valitse sieltä *PLC* -> projektisi nimi (kuvassa *E\_Stop4 Instance* -> *GVL\_muuttujat.g\_xTS\_restart* < *QB 512532.0,BOOL[1.0]*)
- Paina *OK*.

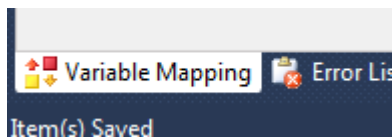


## 19. safeEstopin tulojen ja lähtöjen reititys.

- Mene työpöydälle tilaan:



- Avaa joko näytön alakulmasta:



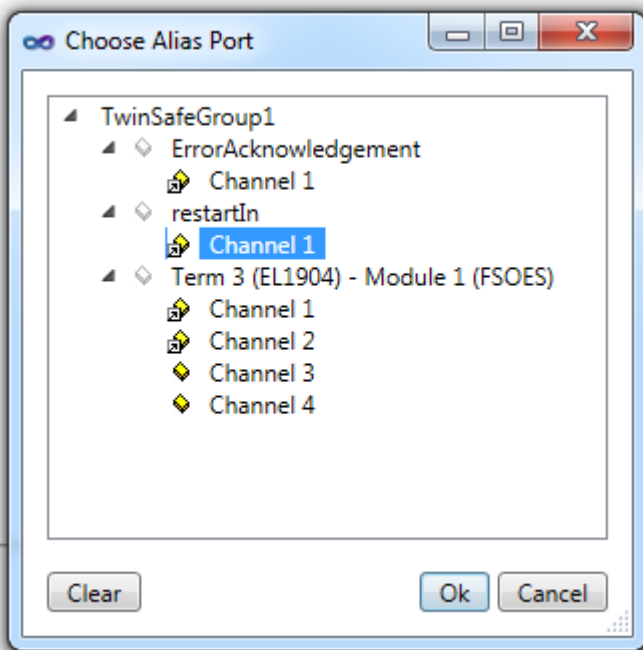
- tai mikäli täällä ei näy mitään, mene *View -> Other Window -> Variable Mapping*.

- Seuraavaksi aukeaa ikkuna:

Variable Mapping						
Function Name	Instance Name	Port Name	Direction	Assigned Variable	Data Type	Alias Port
safeEstop	FBEstop1	Restart	input	restart	safeBool	-
safeEstop	FBEstop1	EStopIn1	input	estop1	safeBool	-
safeEstop	FBEstop1	EStopIn2	input	estop2	safeBool	-
safeEstop	FBEstop1	EStopOut	output	stopOut	safeBool	-

- Tee reititys täällä.
- Muuta *Data Typessä safeEstop port name: restartin* data tyyppiä *Bool* ja *Alias Port* ikkunassa. *TwinSafeGroup1-> restartIn-> Channel 1*.





Command :

Variable Mapping						
Function Name	Instance Name	Port Name	Direction	Assigned Variable	Data Type	Alias Port
safeEstop	FBESop1	Restart	input	restart_	Bool	restartIn.Channel 1 (TwinSafeGroup1)
safeEstop	FBESop1	EStopIn1	input	estop1	safeBool	Term 3 (EL1904) - Module 1 (FSOES).Channel 1 (TwinSafeGroup1)
safeEstop	FBESop1	EStopIn2	input	estop2	safeBool	Term 3 (EL1904) - Module 1 (FSOES).Channel 2 (TwinSafeGroup1)
safeEstop	FBESop1	EStopOut	output	stopOut	safeBool	Term 5 (EL2904) - Module 1 (FSOES).Channel 1 (TwinSafeGroup1)

Variable Mapping | Error List | Output

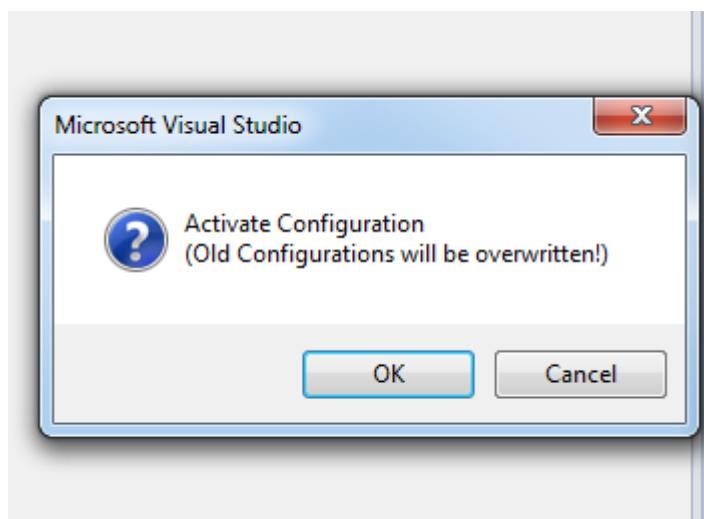
- Määrittele kaikkien muidenkin porttien kytkentä, kuten *restartin* yllä olevan kuvan mukaisiksi.

20. Tallenna ja aktivoi konfigurointi, eli lataa se ohjelmasi logiikalle.

- Paina kuvan mukaista symbolia.

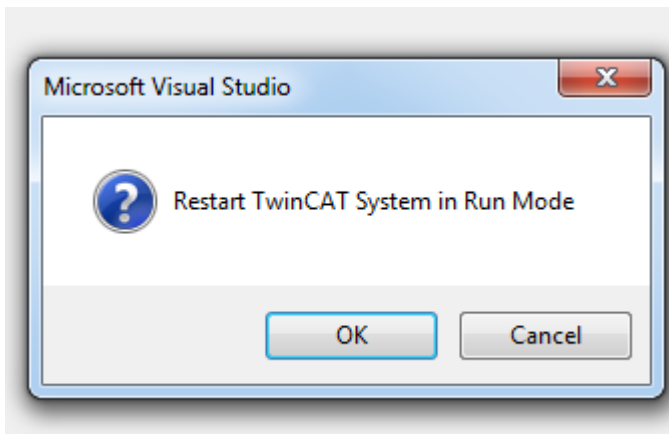


- Ohjelma kysyy:



- Vastaa OK.

- Seuraavaksi:



Myös tähän vastaa *OK*.

- Tarkista oikeasta alareunasta ohjelman olevan konfiguraation suoritusilassa. Alakulmassa näkyvä neliö on vihreänä.



- Käynnistä PLC, paina *Login*:



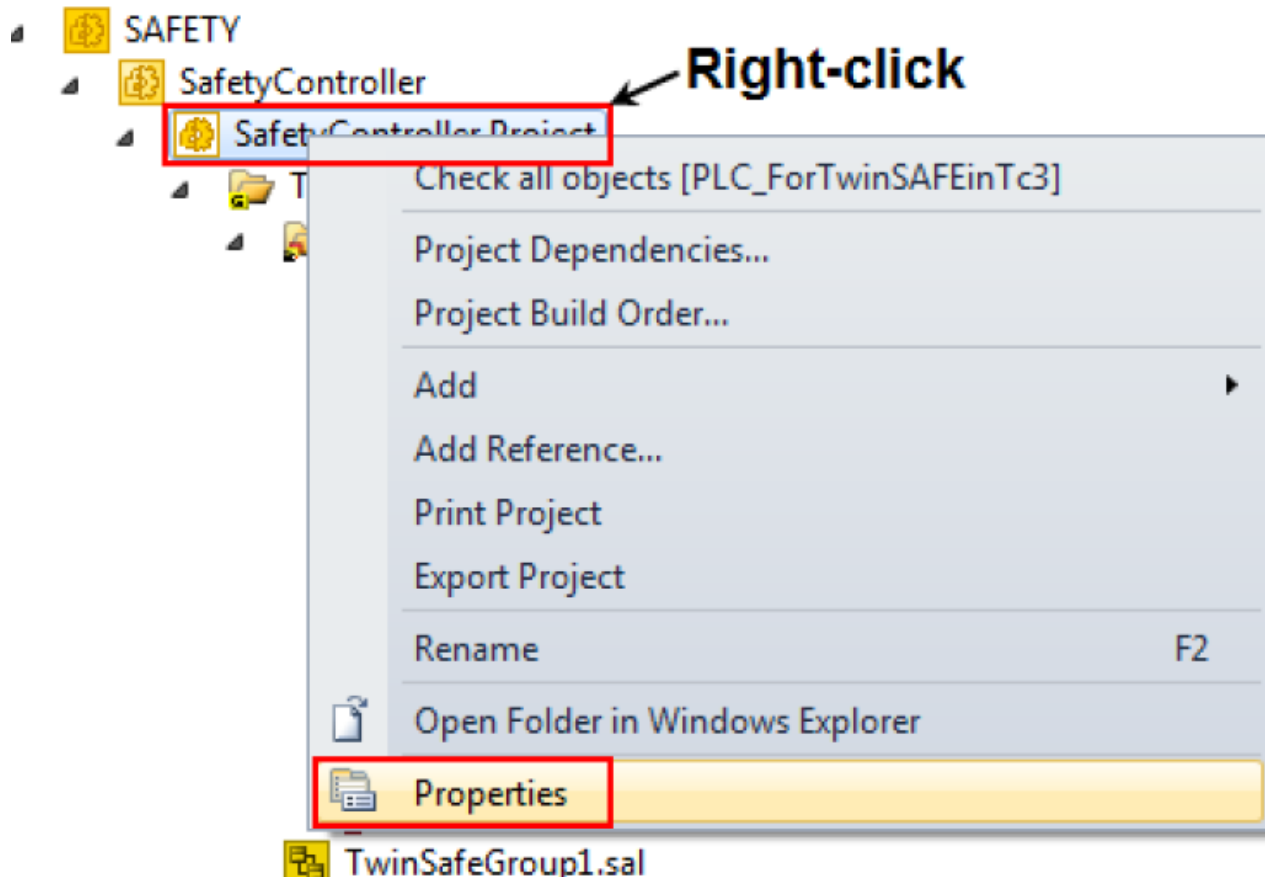
- seuraavaksi ohjelma kysyy:



- Vastaa Yes.
- Seuraavaksi paina.



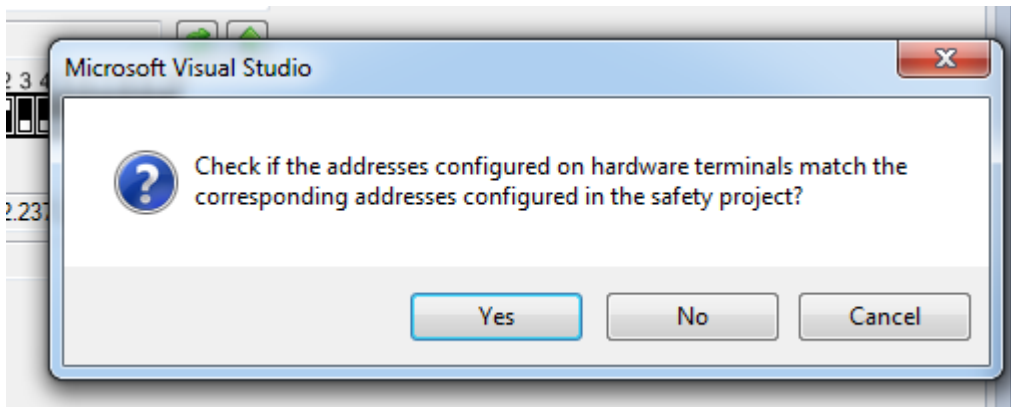
- Seuraavaksi paina hiiren oikealla *SafetyControllerProject* ja valitse *properties*.



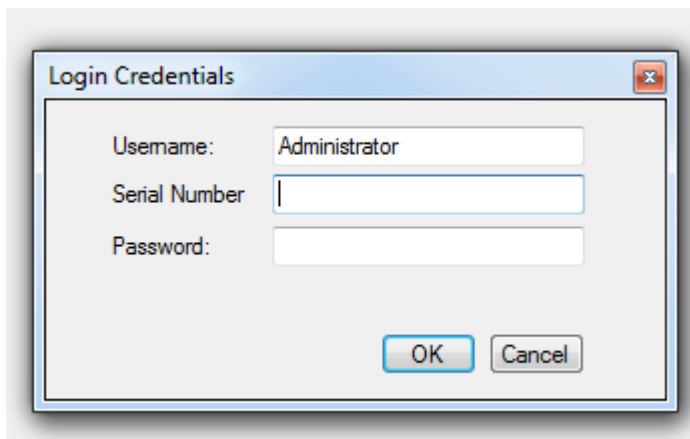
- Kopioi EL 6900 sarjanumero.
- Lataa Safety Controller painamalla kuvan symbolia:



- Ohjelma kysyy:

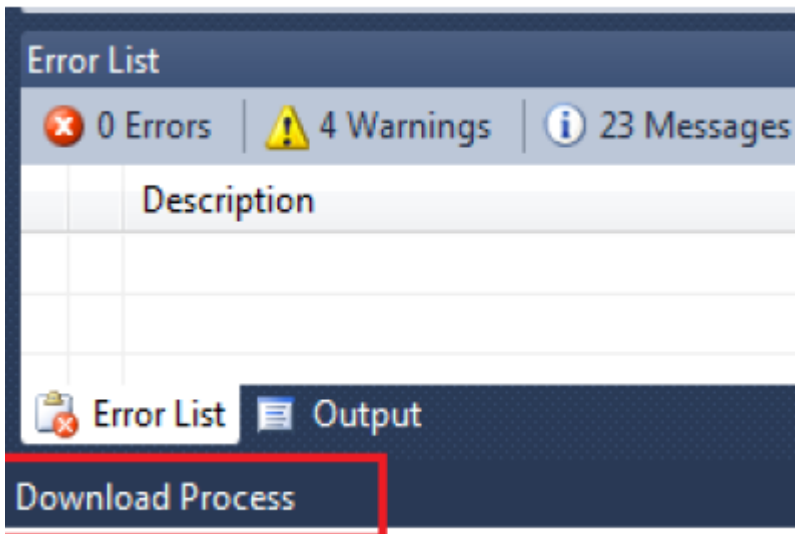


- Vastaa Yes
- Tulee näkyviin:

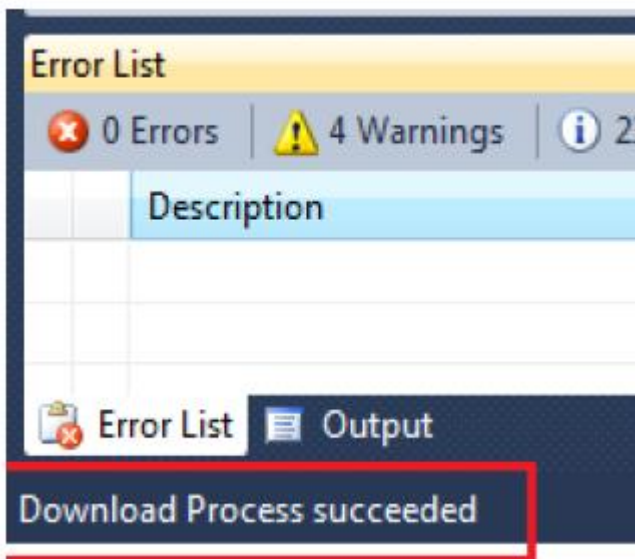


- Anna *Username*: Administrator; sarjanumeroksi (*Serial Number*) EL6900 sarjanumero, tässä 00628752; Salasanaksi (*Password*): TwinSAFE
- Seuraavaan kenttään anna myös salasanaksi TwinSAFE

- Latauksen aikana alakulmassa näkyy *Download Process*:



- Kun lataus on valmis, tulee näkyviin *Download Process succeeded*:



## 21. Testaa ohjelman toimivuus.

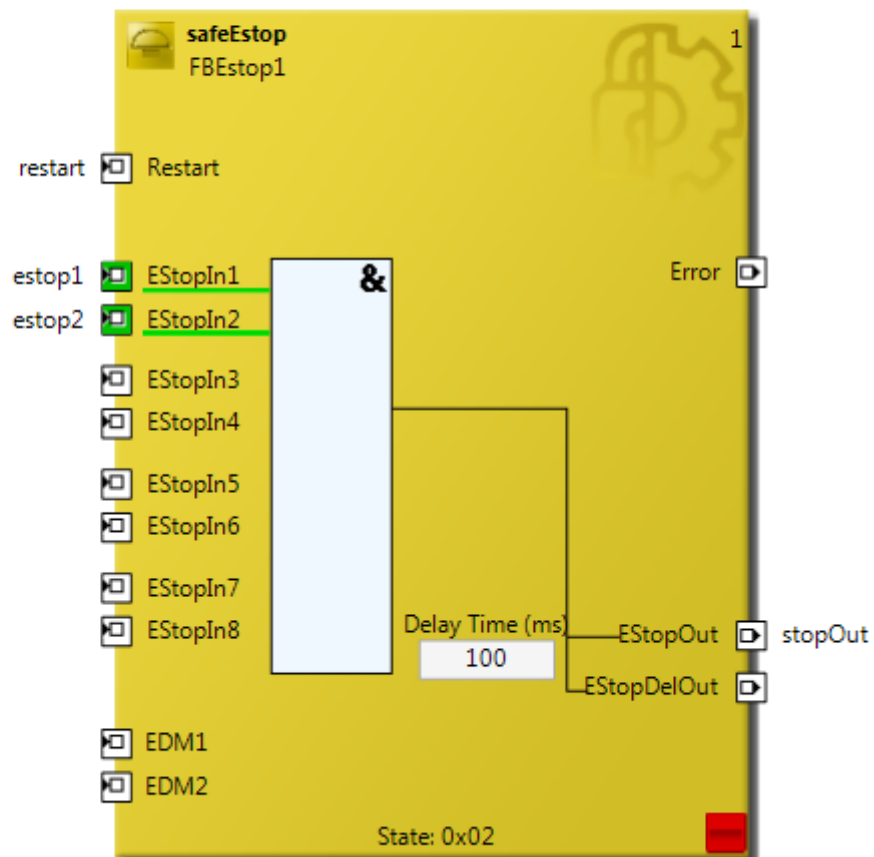
- Käynnistä sovelluksen ajo painamalla pientä vihreää nuolta.
- Tarkista, että hätäseis ei ole kytketty. Tällöin hätäseiskytkimen punainen painonappi on ylhäällä.



- Näet sovelluksen tilan aktivoimalla ohjelmointityöpöytä tilassa turva-automaation "silmläsit".

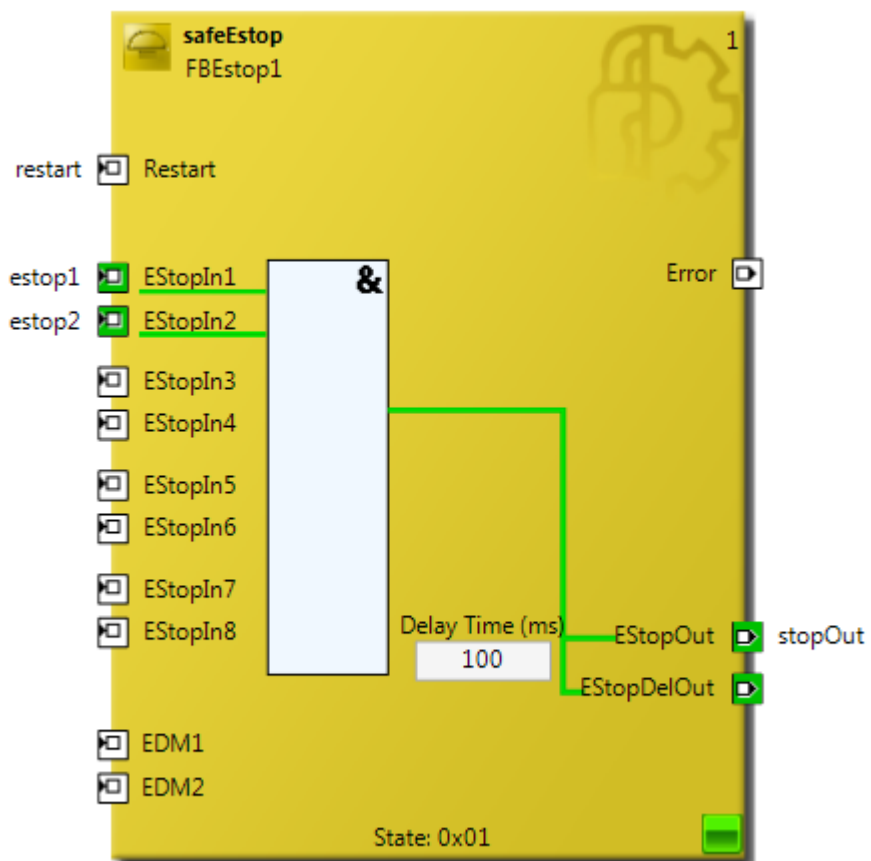


Network1

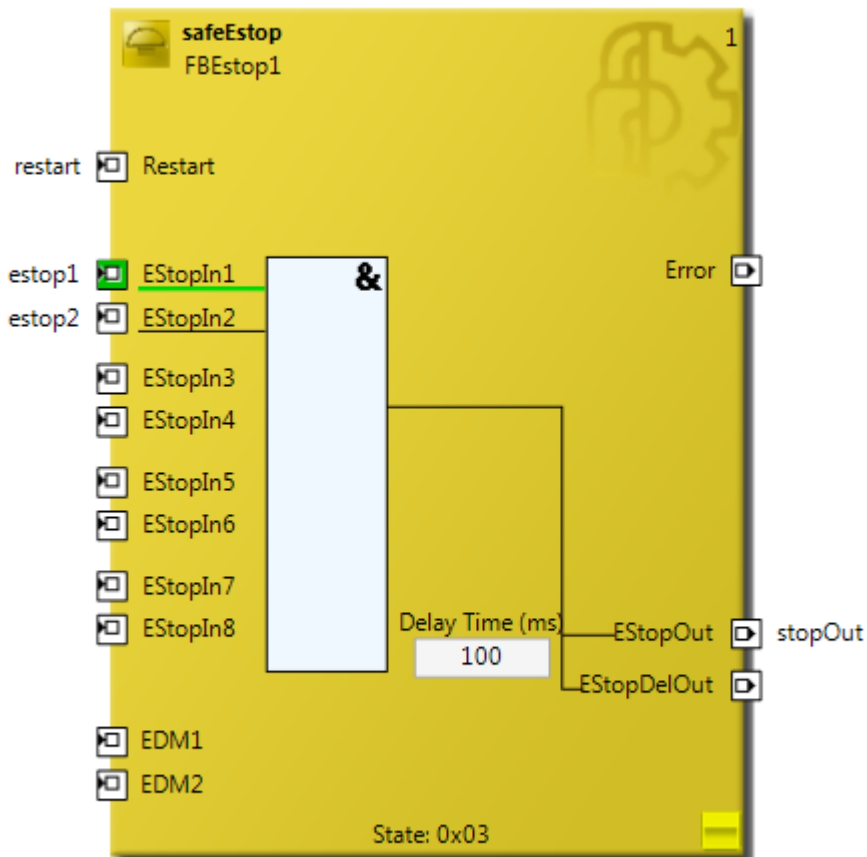


- Kuvassa lähtötilanne ohjelman käynnistämisen jälkeen, ennen kuin ohjelmaa on ajettu.
- Tee resetointi restart-kytkimellä.
- Mikäli ohjelma toimii 16.1.2016 olleessa tilanteessa, alkaa turva-automaation output-kortissa out1 oleva vastus lämpenemään.
- Tilanne muuttuu alla olevan kuvan mukaiseksi.





- Paina hätäseis, jolloin safeEstop katkaisee laitteelta virran.



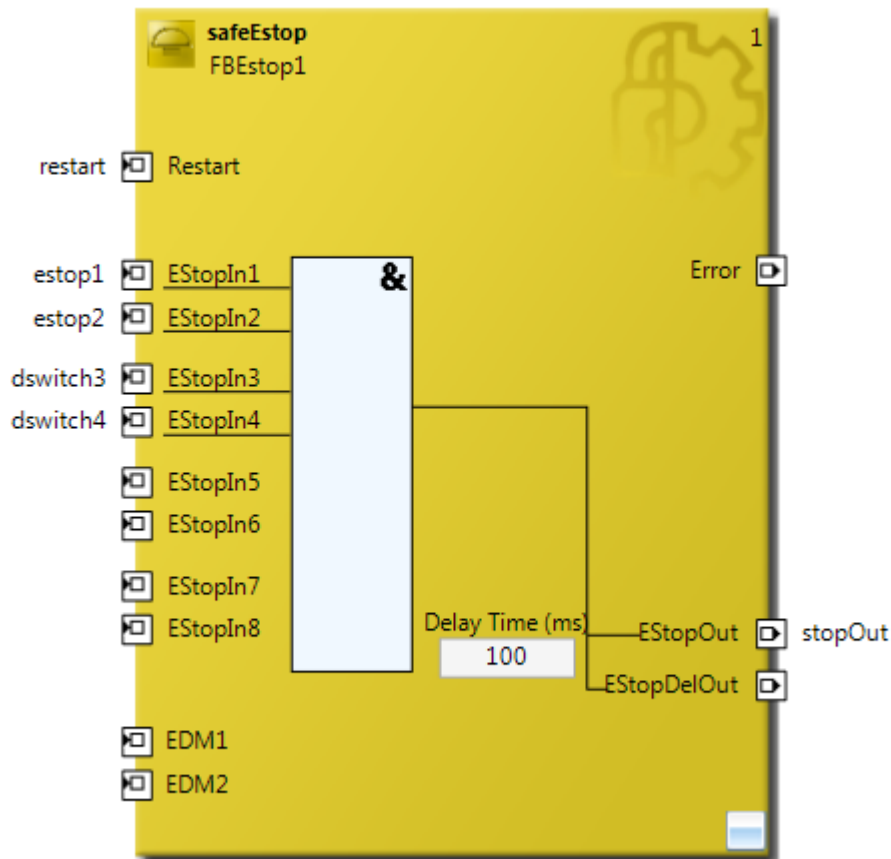
Harjoituksen toinen osa: Lisää edelliseen harjoitukseen turva-automaatio-ohjelmaan koneen suoja-alueen ovien turvakytkimet. Turvajärjestelmään liittyvät komponentit on yleensä merkitty punaisella.

22. Mikäli olet simulointitilassa, mene takaisin Config Modeen. Paina yläosan työkalupalkissa näkyvää



Lilaa neliötä Restart TwinCAT (Config Mode)

23. Kytke TwinSafeGroup1.sal-ikkunassa portit EStopIn3 ja EStopIn4 käyttöön, nimeä dswitch3 ja dswitch2 ( door switch)




24. Reitit uudet kytkimet *Variable Mappingissa* samoin kuin teit hätäseisohjelmointivaiheessa reitityksen. Liitä *TwinSafeGroup1 -> dswitch3 -> Term 3 (EL1904)-Module1 (FSOES) Channel 3*:een ja *TwinSafeGroup1 -> dswitch3 -> Term 3 (EL1904)-Module1 (FSOES) Channel 4*:ään

Variable Mapping

Function Name	Instance Name	Port Name	Direction	Assigned Variable	Data Type	Alias Port
safeEstop	FB_Estop1	EStopIn2	input	estop2	safeBool	Term 3 (EL1904) - Module 1 (FSOES).Channel 2 (TwinSafeGroup1)
safeEstop	FB_Estop1	EStopOut	output	stopOut	safeBool	Term 5 (EL2904) - Module 1 (FSOES).Channel 1 (TwinSafeGroup1)
safeEstop	FB_Estop1	EStopIn3	input	dswitch3	safeBool	
safeEstop	FB_Estop1	EStopIn4	input	dswitch4	safeBool	

Choose Alias Port dialog box showing the tree structure:

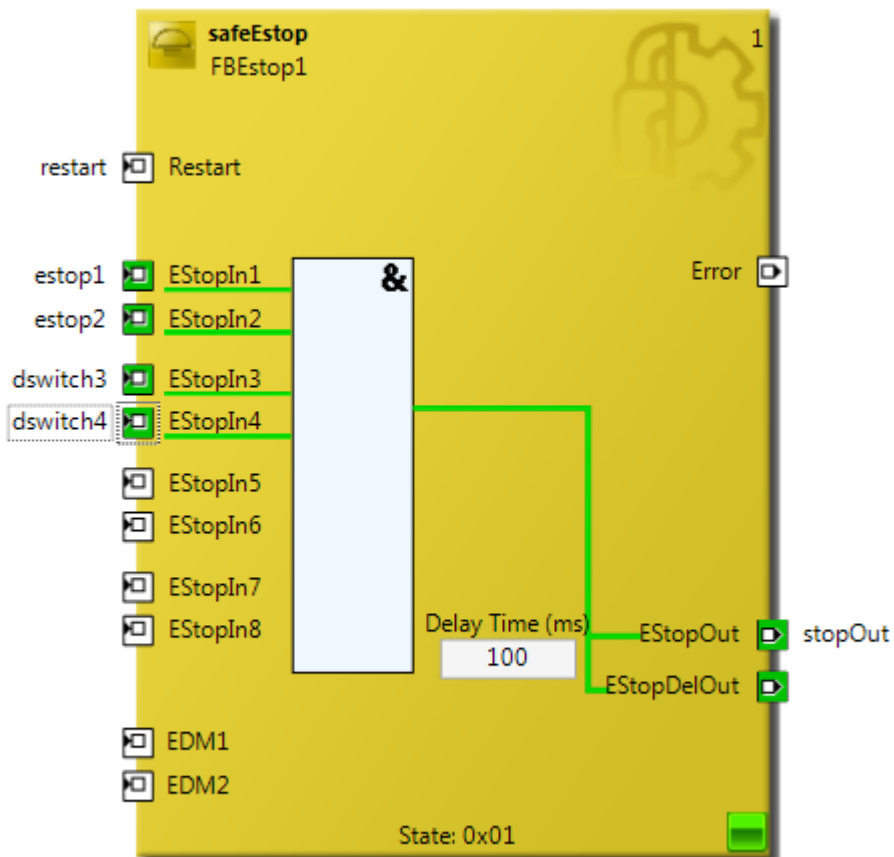
- TwinSafeGroup1
  - Term 3 (EL1904) - Module 1 (FSOES)
    - Channel 1
    - Channel 2
    - Channel 3
    - Channel 4

25. Seuraavaksi paina yläkulmasta *Build* vaihkosta *Build solution* ja tallenna tekemäsi sovellus painamalla  *Save All*

26. Seuraavaksi kytke ovikytkimet TwinSAFE input-kortin EL1904 tuloihin 3 ja 4

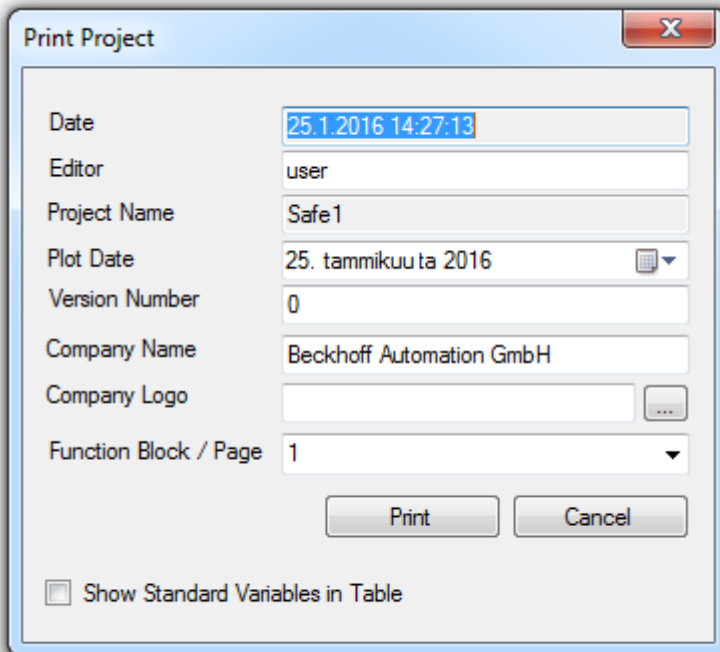
27. Tee uudelleen kohdassa 20 tekemäsi toimenpiteet.

28. Kun viesti menee simuloitaessa turvalogiikan läpi eli kaikki on tilassa, jossa koneen toiminta on sallittu, on näkyvä simulointiajossa seuraavanlainen:

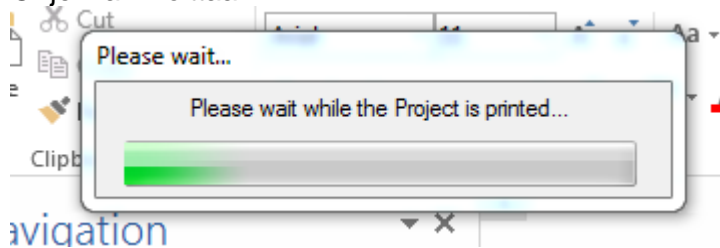


## 29. Tee harjoitustyöstäsi PDF-raportti:

- Mene *SAFETY*- kansiossa olevaan paikkaan, jossa lukee projektisi nimi,
- Klikkaa hiiren oikeaa ja valitse *Generate Documentation*:



- Paina *Print*
- Ohjelma ilmoittaa



## 30. Kun dokumentaatio on valmis, tallenna se haluamaasi kansioon ja palauta kurssin opettajalle.

