jamk

Toiminnallisen turvallisuuden eheyden todentaminen käyttäen laskentaohjelmistoa

Eero Kohtala

Opinnäytetyö, AMK

Huhtikuu 2023

Tekniikan ala

Insinööri (AMK), sähkö- ja automaatiotekniikan tutkinto-ohjelma
Automaatiotekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Kohtala, Eero

Toiminnallisen turvallisuuden eheyden todentaminen käyttäen laskentaohjelmistoa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Huhtikuu 2023, 109 sivua

Sähkö- ja automaatiotekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Turvallisuus on laaja käsite, joka pitää sisällään muun muassa toiminnallisen turvallisuuden. Vahinkojen välttämiseksi, koneiden on oltava turvallisia ihmisille, ympäristölle ja materiaaleille. Turvallisuuteen liittyvät toiminnot tulee toimia oikein ja riittävällä luotettavuudella. Luotettavuuden osoittaminen on nykyään suuremmassa roolissa, koneiden monimutkaisuuden, tehokkuuden ja automaatioasteen kasvaessa.

Opinnäytetyön tavoitteena oli selvittää markkinoilla olevat toiminnallisen turvallisuuden arviointiin ja todentamiseen tarkoitetut laskentaohjelmistot ja valita yksi ohjelmisto palvelemaan mahdollisimman hyvin A-Insinöörit Teollisuus ja talotekniikka Oy suunnittelijoiden käyttötarpeita asiakasprojekteissa. Toinen tavoite oli luoda suunnitteluohje toimeksiantajan sisäiseen käyttöön koskien turvatoimintojen suunnittelussa ja todentamisessa huomioitavia seikkoja. Suunnitteluohjeen tarkoitus oli ennen kaikkea dokumentoida opittuja asioita sekä osaamista, jolloin tieto on muuallakin kuin yhden ammattilaisen hallussa.

Opinnäytetyön teoriaosuus käsittelee aiheen taustalla olevaa lainsäädäntöä ja suunnittelua ohjaavia standardeja. Lisäksi teoriaosuus käsittelee turvatoimintojen luotettavuuden osoittamiseen tarvittavaa matematiikkaa, mikä on sisäistettävä käytettäessä laskentaohjelmistoja.

Opinnäytetyön tuloksena saatiin selvitettyä eri laskentaohjelmistojen ominaisuudet ja soveltuvuus A-Insinöörien tarpeisiin. Kolmesta tarkasteltavasta laskentaohjelmistosta toimeksiantajan käyttöön valittiin SISTEMA. Toiseen tavoitteeseen päästiin luomalla suunnitteluohje, joka palvelee aiheen kanssa vähemmän työskenteleviä suunnittelijoita.

Suunnitteluohjetta voidaan kehittää jatkuvasti vastaamaan eteen tulevien ongelmien ja kysymysten ratkaisussa. Suunnitteluohjeelle toinen jatkokehityksen suunta on laajentaa se käsittelemään prosessisektorilla yleisiä harvojen vaateiden turvatoimintoja.

Avainsanat

toiminnallinen turvallisuus, turvallisuuden eheys, laskentaohjelmisto, SIL, PL, turva-automaatio, turvatoiminto, turvakomponentti, koneturvallisuus, SISTEMA, ABB FSDT-01, Pilz PAScal, A-Insinöörit

Muut tiedot

Liite 1 on salassa pidettävä, ja se on poistettu julkisesta työstä. Salassapidon peruste on Julkisuuslain 621/1999 24§, kohta 17, yrityksen liike- tai ammattisalaisuus. Salassapitoaika on viisi (5) vuotta, salassapito päättyy 17.4.2028.

jamk

Description

Kohtala, Eero

Validation of the safety integrity level with calculation software

Jyväskylä: JAMK University of Applied Sciences, April 2023, 109 pages

Degree Programme in Electrical and Automation Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Safety is a broad concept that includes functional safety. To avoid risk and damage, machines must be safe for people, the environment, and materials. Safety-related functions must function correctly and with sufficient reliability. Proving reliability plays a bigger role today, as the complexity, efficiency, and degree of automation of machines increases.

The aim of the thesis was to find out the calculation software on the market for the evaluation and verification of functional safety and to choose one software to serve as well as possible the usage needs of A-Insinöörit Teollisuus ja talotekniikka Oy designers in customer projects. The second goal was to create design instructions for the client's internal use regarding issues to be considered in the design and verification of safety functions. The purpose of the design instructions was above all to document things learned and know-how, in which case the knowledge is other places than in the possession of one professional.

The theory part of the thesis deals with the legislation behind the topic and the standards guiding desing. In addition, the theory part deals with the mathematics needed to validate the reliability of safety functions, which is good to understand when using calculation software.

As a result of the thesis, the properties and suitability of different calculation software for the needs of A-Insinööries were clarified. From the three considered calculation software, SISTEMA was chosen for the client's use. The second goal was achieved by creating a design instruction that serves designers who work with the subject less.

The design instructions can be continuously developed to answer the problems and questions that come up. Another direction of further development for the design instructions is to expand it to deal with safety functions of low demand that are common in the process sector.

Keywords/tags (subjects)

functional safety, safety integrity, calculation software, SIL, PL, safety automation, safety function, safety component, machine safety, SISTEMA, ABB FSDT-01, Pilz PAScal, A-Insinöörit

Miscellaneous (Confidential information)

Attachment 1 is classified and has been removed from the public record. The basis for confidentiality is § 24, section 17 of the Act on the Openness of Government Activities 621/1999, the business or professional secret of the company. The confidentiality period is five (5) years, confidentiality ends on April 17, 2028.

Sisältö

Kuviot

Taulukot

Käsitteet ja lyhenteet

TLJ (SIS)	Turvallisuuteen liittyvä järjestelmä (Safety instrumented system)
Turvatoiminto (SF)	Toiminto, jonka vikaantuminen saattaa johtaa riskien kasvamiseen (Safety function)
Alajärjestelmä	Komponentti tai komponenttiryhmä, joka osallistuu turvatoiminnon suorittamiseen (esimerkiksi kaksi rajakytkintä tai kontaktoria)
TET(SIL)	Turvallisuuden eheyden taso (Safety integrity level)
$\mathrm{PFH_D}$	Probability of dangerous failure per hour (vaarallisen vikaantumisen todenäköisyys tunnissa), käytetään myös lyhennettä PFH
PL	Performance level (Suoritustaso)
$\mathrm{MTTF_D}$	Keskimääräinen aika vaaralliseen vikaantumiseen (Mean time to dangerous failure)
$\mathrm{B_{10D}}$	Sähkömekaanisien komponenttien käyttökertojen lukumäärä kunnes 10 % komponenteista on vikaantunut vaarallisesti
$\mathrm{N_{op}}$	Sähkömekaanisien komponenttien käyttökertojen lukumäärä vuodessa
DC	Diagnostic coverage (diagnostiikan kattavuus)
SFS	Merkintä, joka osoittaa standardin vahvistamisen Suomessa kansalliseksi standardiksi
EN	Merkintä, joka osoittaa standardin vahvistamisen Euroopalaiseksi standardiksi, mutta ei suoraan osoita harmonisointia
ISO	Merkintä, joka osoittaa standardin vahvistamisen kansainväliseksi standardiksi
IEC	Merkintä, joka osoittaa standardin vahvistamisen kansainväliseksi sähkö- ja elektroniikka-alan standardiksi
SISTEMA	Safety Integrated Software Tool for the Evaluation of Machine Applications
FSDT	Functional Safety Design Tool

1 Johdanto

1.1 Opinnäytetyön fokus

Vuonna 2022 yhteiskunnan yhä enemmän automatisoituessa ja vaatimustason kasvaessa tulee myös koneiden, prosessien ja muiden ensisijaisesti ihmisien turvallisuuteen vaikuttavien laitteistojen olla todennetusti turvallisia. Vaikeammaksi turvallisuuden saavuttamisen tekee monimutkaiset ohjausjärjestelmät, joiden vaarallisia vikaantumisia ei voida täydellisesti määrittää. Vaatimuksia turvallisuuteen tulee monesta eri lähteestä. Lainsäädäntö on yksi merkittävästi vaikuttava tekijä. Yhteiskunnan tahtotila on yksiselitteinen: koneiden on oltava turvallisia.

Tässä opinnäytetyössä käsitelty ohjausjärjestelmien toiminnallinen turvallisuus on vain osa kokonaisuuden turvallisuutta. Toiminnallisen turvallisuuden arviointiin on esitetty tapoja ja yksi osa arviointia on turvatoimintoihin osallistuvien ohjausjärjestelmien osien turvallisuuden eheyden todentaminen. Toiminnallisen turvallisuuden eheys on riippuvainen turvatoimintoon osallistuvien osien luotettavuudesta. Koko turvatoiminnon luotettavuus on osoitettava riittävällä todistusaineistolla. Velvoite koneen ohjausjärjestelmän toteuttamien turvatoimintojen turvallisuuden eheyden todentamiseen tulee konedirektiivin kohdasta 1.2.1 (Guide to application of the Machinery Directive 2006/42/EC 2019, §184.) Yleisesti käytetty keino on laskea matemaattisesti turvatoiminnon vikaantumisen todennäköisyys. Laskennan avuksi on olemassa maksuttomia sekä maksullisia tietokoneohjelmistoja.

Koska aihealueena toiminnallinen turvallisuus on varsin laaja kokonaisuus, oli opinnäytetyön aihe rajattava ajallisista syistä koskemaan vain automaation ja sähkön kenttäsuunnittelijan näkökulmasta merkittäviä asioita. Vaara- ja riskianalyysi on turvatoimintojen suunnittelua ja laitevalintaa edeltävä toimenpide ja täten se rajattiin pois. Turvallisuuteen liittyvä ohjelmointi on myös rajattu pois opinnäytetyöstä. Koska toiminnallinen turvallisuus jakautuu eri sovellussektoreille ja toimeksiantajan tarve oli enemmän konesektorilla, päätettiin rajata prosessisektoria koskevat asia pois.

Toimeksiantajalla oli tarve saada selvitettyä markkinoilla olevat laskentaohjelmistot sekä parantaa toiminnallisen turvallisuuden kanssa tekemisissä olevien henkilöstön tietämystä. Opinnäytetyön

tarkoituksena oli paneutua syvällisesti toiminnallisen turvallisuuden ja luoda yksinkertainen tietopaketiksi kutsuttu sisäinen suunnitteluohje toimeksiantajan henkilöstön käyttöön. Suunnitteluohje tehtiin salattuna liitetiedostona ja vain toimeksiantajan käyttöön. Toinen yhtä merkittävä tehtävä oli selvittää saatavilla olevat laskentaohjelmistot, niiden ominaisuudet ja valita toimeksiantajalle soveltuvin ohjelmisto. Laskentaohjelmistojen kartoitus ja valinta tehtiin toimeksiantajan sen hetkisiin tarpeisiin perustuen, ottaen huomioon mahdollisesti muuttuvat tarpeet.

1.2 A-Insinöörit

A-Insinöörit Oy on Tampereelta lähtöisin oleva suunnittelu- ja konsulttiyhtiö. Historia alkaa Tampereelta vuonna 1959 kahden paikallisen diplomi-insinöörin yrityksestä, joka kantoi nimeä Insinööritoimisto Ahonen-Palenius. Ahosen yhtiökumppanin vaihduttua vuonna 1964 yrityksen nimeksi vaihtui Ahonen-Ilveskoski. Nykyinen nimi tuli käyttöön vuonna 1984. Yhtiö on laajentunut vuosien aikana eri paikkakunnille sekä toimialoille orgaanisen ja epäorgaanisen kasvun myötä. (A-Insinöörien tarina n.d.)

A-Insinööreillä on viisi eri toimialaa, jotka jakautuvat omiin toimialayhtiöihin:

1. rakennuttaminen, (A-Insinöörit Rakennuttaminen ja A-Insinöörit Oy Lappi)
2. rakennesuunnittelu, (A-Insinöörit Suunnittelu Oy)
3. yhdyskunta- ja ympäristösuunnittelu, (A-Insinöörit Civil Oy)
4. teollisuus- ja talotekniikka, (A-Insinöörit Teollisuus- ja talotekniikka Oy)
5. arkkitehtisuunnittelu, (AW2 Architects Oy)

Toimipaikkoja on yhteensä 15, joista yksi Tallinnassa ja loput Suomessa Helsingistä aina Rovaniemelle saakka. Koko konsernin liikevaihto vuonna 2021 oli 106 miljoonaa euroa, ottaen huomioon uusien yritysten kaupat. Henkilöstömäärä vuonna 2022 on noin 1300. (Toimipaikkojen osoitteet n.d.)

Tämän opinnäytetyön toimeksiantaja on A-Insinöörit Teollisuus- ja talotekniikka Oy, joka on ennen vuoden 2021 yrityskauppoja tunnettu nimellä Insinööritoimisto AX-LVI Oy. Toimialayhtiön osaamisalueisiin kuuluu talotekninen LVI-, kylmä-, sähkö ja automaatiosuunnittelu ja konsultointi (Ax-Suunnittelu on nyt A-Insinöörit 2022). Teollisuuden puolelta mainittakoon prosessi-, LVI-, sähkö- ja automaatiosuunnittelu ja konsultointi (Ax-Suunnittelu on nyt A-Insinöörit 2022). Lisäksi osaamista

löytyy ympäristöpuolelta kattaen muun muassa teollisuuden päästömittaukset, työhygieeniset mittaukset ja päästömallintamien (Ax-Suunnittelu on nyt A-Insinöörit 2022).

1.3 Tutkimusasetelma

Työ toteutettiin tutkimuksellisena kehittämistyönä. Ensimmäisenä tutkimuksen ja kehittämisen kohteena oli toimeksiantajan suunnittelijoiden ymmärrys toiminnallisesta turvallisuudesta. Ensimmäisen kehittämiskohteita varten luotiin toiminnallisen turvallisuuden suunnitteluohje toimeksiantajan sisäiseen käyttöön. Ensimmäisestä aiheesta muodostui seuraava tutkimuskysymys:

> *Mitä täytyy tietää ollessaan tekemisissä toiminnalliseen turvallisuuteen liittyvien suunnittelutehtävien parissa ja mistä tämän tiedon löytää?*

Toinen tutkimuksen ja kehittämisen kohde oli turvatoimintojen todentamiseen tarkoitettujen laskentaohjelmistojen vertailu ja valinta toimeksiantajan käyttöön. Tässä tapauksessa tutkimuskysymys on yksinkertainen:

> *Mikä turvatoimintojen laskentaohjelmisto on soveltuvin toimeksiantajan käyttöön?*

Opinnäytetyön teoriaosuudessa perehdyttiin toiminnallisen turvallisuuden taustalla vaikuttavaan lainsäädäntöön ja suunnittelua ohjaaviin standardeihin. Teoriaosuudessa myös selitettiin toiminnallisen turvallisuuden todentamiseen käytettyjä termejä ja ominaisarvoja, jotka ovat relevantteja ymmärtää käytettäessä laskentaohjelmistoja. Lähdemateriaalina teoriaosuudelle suurimmassa roolissa oli alan standardit. Pienemmässä roolissa olivat standardien soveltamiseen tarkoitetut julkaisut. Siirilän ja Tytykosken kirjoittama massiivinen Koneturvallisuuden käsikirja oli oman oppimisen kannalta merkittävä lähde.

2 Toiminnallinen turvallisuus

Mitä on turvallisuus? Entä toiminnallinen turvallisuus? Nimensä mukaisesti toiminnallinen turvallisuus on suoraa verrannollinen oikeaan ja oikea-aikaiseen osien suunniteltuun toimintaan. Toiminnallisen turvallisuuden kattostandardissa IEC/TR 61508-0 (2011, 5) termit määritellään seuraavasti

> *Se on vapautta sellaisen fyysisen vamman tai ihmisten terveyteen kohdistuvan vahingon riskistä joko suoraan tai epäsuoraan omaisuuteen tai ympäristöön kohdistuvan vahingon seurauksena, jota ei voida sietää. Toiminnallinen turvallisuus on kokonaisuuden turvallisuuden osa, joka riippuu järjestelmän tai laitteiston oikeasta toiminnasta, vasteena sen tulojen tiloihin.*

Toiminnallisen turvallisuuden tunnettu historia alkaa 1960- luvulta, jolloin elektroniikka oli vielä kallista, joten ohjauksissa käytettiin sähkömekaanisia releitä ja kontaktoreita estämään pahimpia onnettomuuksia tapahtumasta. Ohjelmoitavat logiikat tulivat turvallisuuteen liittyvään käyttöön 1970–80-luvulla ja ohjattavuuden mahdollisuudet kasvoivat, mutta niin kasvoi myös monimutkaisuus. Lopulta 1990-luvulla käytössä oli varsinainen turvalogiikka, jonka suunnittelussa hyödynnettiin nykyäänkin käytössä olevia ominaisarvoja sekä analyysimenetelmiä. Vuosituhannen vaihtuessa kyberturvallisuus alkoi olla suuremmassa roolissa yhtenä osana kokonaisturvallisuudesta. (Yozallinas 2016.)

Toiminnallinen turvallisuus on nykyään yhä tärkeämpää, kun enenevissä määrin vaaroista aiheutuvan riskin pienentäminen toteutetaan monimutkaisella ja vaikeasti ymmärrettävällä tietokonetekнologialla. Tulevaisuudessa tekoäly tulee olemaan osa toiminallista turvallisuutta, muun muassa itseajavien ajoneuvojen ja tekoälyä sisältävien ihmisen tunnistamiseen tarkoitettujen laitteiden kehittyessä (Malm 2021). Tsutsumin ja van Gulijkin (2021, 31–33) mukaan tulevaisuudessa konsepti koneiden ja ihmisten välisestä yhteistyöturvallisuudesta tulee korvaamaan nykyisen konseptin, jossa vaarallinen kone pidetään erillään ihmisestä.

2.1 Lainsäädäntö

2.1.1 Konedirektiivi

Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY eli konedirektiivi on EU:n laatima lainsäädäntöohje jäsenmailleen. Kunkin jäsenmaan on ollut saatettava direktiivin sisältö osaksi kansallista lainsäädäntöä 29.6.2008 mennessä. Konedirektiivin tarkoitukseksi ja hyödyksi nähdään turvallisten koneiden vapaa liikkuvuus EU-talousalueella. Direktiivien soveltamisalaan kuuluvilta koneilta ja laitteilta edellytetään olennaisten terveys- ja turvallisuusvaatimusten täyttämistä. (Direktiivi 2006/42/EY. Tiivistelmä, 32006L0042.)

Nykyinen konedirektiivi ei ole ensimmäinen laatuaan, vaan perustuu direktiiviin 98/37/EY, joka oli voimassa 29.12.2009 saakka. Alkuperäinen konedirektiivi on annettu vuonna 1989, jota kuitenkin on päivitetty direktiiveillä 91/368/ETY, 93/44/ETY, 93/68/ETY ja 98/79/EY. Nykyisen konedirektiivin sisältöön on tullut muutoksia aina vuoteen 2019 asti. Viimeisin merkittävin muutos on asetettu voimaan direktiivillä 2014/33/EU (Guide to application of the Machinery Directive 2006/42/EC 2019, §4.)

Suppeassa merkityksessä kone on jotakin toimintoa varten kokoonpantu osien yhdistelmä, jossa ainakin yksi osa liikkuu (Guide to application of the Machinery Directive 2006/42/EC 2019, kohta §35). Konedirektiivissä 2006/42/EY (2. artikla, kohta a*)* koneella tarkoitetaan laajassa merkityksessä seuraavaa:

> *Toisiinsa liitettyjen osien tai komponenttien yhdistelmää, jossa on tai joka on tarkoitettu varustettavaksi muulla kuin välittömällä ihmis- tai eläinvoimalla toimivalla voimansiirtojärjestelmällä ja jossa ainakin yksi osa tai komponentti on liikkuva ja joka on kokoonpantu erityistä toimintoa varten,*
>
> *ensimmäisessä luetelmakohdassa tarkoitettua yhdistelmää, josta puuttuvat ainoastaan komponentit, joilla se liitetään paikan päällä tai kytketään voiman- tai käyntilähteisiin,*

> *ensimmäisessä tai toisessa luetelmakohdassa tarkoitettua yhdistelmää, joka on valmis asennettavaksi ja joka voi toimia vasta kun se on kiinnitetty liikennevälineeseen tai asennettu rakennukseen tai rakennelmaan,*
>
> *ensimmäisessä, toisessa tai kolmannessa luetelmakohdassa tarkoitettujen koneiden tai g alakohdassa tarkoitettujen puolivalmisteiden yhdistelmiä, jotka on tiettyjä toimintoja varten järjestetty ja ohjattu toimimaan yhtenä kokonaisuutena,*
>
> *toisiinsa liitettyjen osien tai komponenttien yhdistelmää, jossa ainakin yksi osa tai komponentti on liikkuva ja joka on kokoonpantu kuormien nostamista varten ja jonka ainoana voimanlähteenä on välitön ihmisvoima.*

Toinen merkityksellinen termi on valmistaja, joka määritellään konedirektiivissä 2006/42/EY (2. artikla, kohta i) seuraavasti:

> *Valmistajalla tarkoitetaan luonnollista tai oikeushenkilöä, joka suunnittelee ja/tai valmistaa tämän direktiivin soveltamisalaan kuuluvan koneen tai puolivalmisteen ja on vastuussa siitä, että kyseinen kone tai puolivalmiste on tämän direktiivin säännösten mukainen, jotta se voidaan saattaa markkinoille valmistajan omalla nimellä tai tuotemerkillä tai ottaa valmistajan omaan käyttöön. Edellä määritellyn valmistajan puuttuessa valmistajaksi katsotaan luonnollinen tai oikeushenkilö, joka saattaa markkinoille tai ottaa käyttöön tämän direktiivin soveltamisalaan kuuluvan koneen tai puolivalmisteen.*

Konedirektiivi velvoittaa koneiden valmistajia ja/tai markkinoille saattajaa. Soveltamisalaan kuuluu vain EU:n markkinoille valmistettavat ja tuotavat koneet (Introduction and Terminology for Functional Safety of Machines and Systems 2020, kohta 2.2.3). Tarkalleen ottaen konedirektiiviä (Direktiivi 2006/42/EY, 1. artikla, kohta 1) sovelletaan:

1. koneisiin
2. vaihdettaviin laitteisiin
3. turvakomponentteihin
4. nostoapuvälineisiin
5. ketjuihin, köysiin ja vöihin
6. nivelakseleihin
7. puolivalmisteisiin

Termillä kone voidaan käytännössä tarkoittaa pientä osakokonaisuutta eli osittain valmista konetta tai toisena ääripäänä kokonaista tuotantolinjaa/tehdasta. (Introduction and Terminology for Functional Safety of Machines and Systems 2020, kohta 2.2.3.)

Siirilän ja Tytykosken mukaan vaihdettava laite on jo olemassa olevaan traktoriin, kuorma-autoon tai muuhun koneeseen käyttäjän itse kiinnittämä kone, jolla saadaan uusi toiminto aikaiseksi. Kuitenkaan vaihdettavaksi laitteeksi ei katsota työkalua, joka tässä asiayhteydessä tarkoittaa laitetta, jossa itsessään ei ole liikkuvia osia. Siirilä ja Tytykosken havainnollistavassa esimerkissä traktoriin kiinnitettävä hydraulitoiminen harjakone on vaihdettava laite, mutta kiinteä tasauslevy on työkalu. (Siirilä ja Tytykoski 2016, 37.)

Puolivalmiste eli osittain valmis kone on aiheuttanut epäselvyyksiä ja eri tulkintoja. Osittain valmiilla koneella tarkoitetaan konetta, joka ei voi itsenään suorittaa erityistä toimintoaan, vaan vasta liitettynä muuhun koneeseen tai osittain valmiiseen koneeseen, kokonaisuudesta muodostuu konedirektiivin soveltamisalaan kuuluva varsinainen kone. Siirilän ja Tytykosken mukaan hyvä esimerkki osittain valmiiden koneiden yhdistelmästä on konelinja tai robottisolu. (Siirilä ja Tytykoski 2016, 39.)

2.1.2 Koneasetus

Nykyinen konedirektiivi on pantu täytäntöön Suomessa valtioneuvon asetuksella koneiden turvallisuudesta 400/2008 ja se on tullut voimaan 29.12.2009 (A 12.6.2008/400, 1 ja 12 §). Koneasetus on pitkälti samansisältöinen kuin konedirektiivi. Koneasetus koskee pääasiassa koneen valmistajaa, joka on vastuussa turvallisen koneen suunnittelusta ja markkinoille saattamisesta.

Koneasetusta edeltävä säädös on valtioneuvoston päätös koneiden turvallisuudesta 1413/1994 eli konepäätös (P 21.12.1994/1314, 1 §). Konepäätöksellä asetettiin sen aikainen direktiivi koneista 89/392/ETY täytäntöön (P 21.12.1994/1314, 1 §). Siirilä ja Tytykosken (2016, 31) mukaan koneasetuksessa on täsmennetty lakia 26.11.2004/1016 Laki eräiden teknisten laitteiden vaatimustenmukaisuudesta, joka tunnetaan konelakina.

2.1.3 Käyttöasetus

Nykyinen valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta (A 12.6.2008/403) velvoittaa työturvallisuuslain (L 23.8.2002/738) nojalla työnantajaa (L 23.8.2002/738, 2 §). Siirilä ja Tytykosken (2016, 44) mukaan käyttöasetuksen soveltamisala kattaa

kaikki työssä käytettävät välineet ja näin ollen myös koneasetuksen soveltamisalaan kuulumattomat koneet. Lisäksi Siirilä ja Tytykoski (2016, 46) painottaa käyttöasetuksen vaatimusten olevan samankaltaisia koneasetuksien vaatimusten kanssa, mutta koneasetuksessa ne ovat tarkemmin esitetty.

2.1.4 Muita säädöksiä

Konelaki (L 26.11.2004/1016, 2 ja 10 §) koskee teknisien laitteiden valmistajaa ja muun muassa edelleen luovuttajia eli käytetyn teknisen laitteen myyjää. Konelain (L 26.11.2004/1016, 9 §) mukaan käytetyn koneen tai teknisen laitteen myyjällä on velvollisuus huolehtia vaatimustenmukaisuudesta sekä ohjeiden toimittamisesta koneen mukana. Käytännössä käytetyn koneen on oltava vähintään käyttöönottoajankohdan aikaisten vaatimusten mukainen.

2.2 Standardit

Standardi tarkoittaa yhteisien hyvien tapojen, käytäntöjen, vaatimusten ja menetelmien laatimista kirjalliseen julkaisuun. Standardisointi on hyödyksi kuluttajille, yrityksille ja viranomaisille. Standardin mukaisuus takaa kuluttajalle laadukkaat, yhteensopivat ja turvalliset palvelut tai tuotteet. Kuluttajien on turvallista ostaa kaupasta tuote, joka on standardin mukainen. Yritysten on helpompi viedä tuotteita toiselle puolelle maailmaa, kun käytössä on kansainväliset standardit. Viranomaisten on helpompaa valvoa lakien noudattamista, kun käytössä on standardit. (Mitä standardi tarkoittaa n.d.)

Harmonisoituja eli yhdenmukaistettuja EN-standardeja noudattamalla tuote tai palvelu katsotaan olevan EU:n lainsäädännön vaatimusten mukainen. Harmonisoidut standardit ovat useimmiten Euroopan komission aloitteesta luotuja direktiivien jatkoksi. Harmonisoidut standardien viitetiedot tulee löytyä Euroopan unionin virallisesta lehdestä (EUVL), jotta harmonisointi on virallista. Vaikka standardien noudattaminen ei ole pakollista, tekee se vaatimustenmukaisuuden osoittamisesta helpompaa. Harmonisoidut EN-standardit tulee vahvistaa ja julkaista identtisinä kansallisen standardisoimiselimen toimesta kussakin EU-jäsenmaassa. EN-standardien kanssa ristiriidassa olevat kansalliset standardit tulee kumota. (EU ja standardisointi n.d.)

Siirilän ja Tytykosken mukaan vielä 1980-luvulla EU:n direktiivit olivat sisällöltään yhtä yksityiskohtaisia kuin nykyiset standardit. Direktiivien päivittämisen kankeus oli syy uuden lähestymistavan (New Approach) käyttöön ottamiseen. Uuden lähestymistavan tavoite oli linjata direktiiveissä vain yleisiä periaatteita, jotka eivät muutu yhtä nopeasti kuin yksityiskohtaiset tekniset ratkaisut. Uuden lähestymistavan myötä direktiiviä täsmentävät edellä mainitut harmonisoidut EN-standardit. Kuten aiemmin mainittu, harmonisoituja standardeja ei ole pakko noudattaa, mutta mikäli poiketaan standardista, on saavutettava vähintäänkin sama turvallisuustaso (Siirilä & Tytykoski 2016, 87–89.)

Koneturvallisuuden standardit jakautuvat hierarkkisesti kolmeen eri tasoon: A, B ja C. B-taso jakautuu vielä kahteen eri tyyppiin. (CEN ISO/TR 22100-1:2021, kohta 4.)

- A: turvallisuuden perusstandardi, joka soveltuu kaiken tyyppisille koneille ja ottaa kantaa turvallisuuteen yleisesti. Esimerkiksi: (SFS-EN ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen).
- B1: turvallisuuden ryhmästandardi, joka esittää tietyn turvallisuusnäkökohdan, joka voi olla esimerkiksi turvallisuuteen liittyvä ohjausjärjestelmä (SFS-EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet).
- B2: turvallisuuden ryhmästandardi, joka esittää tietyn turvallisuusteknisen toimenpiteen tai lait-teen, joka voi olla esimerkiksi koneen toimintaan kytketyt suojukset (SFS-EN ISO 14119 Koneturvallisuus. Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta).
- C: koneturvallisuusstandardi, joka esittää tietyn koneen tai koneryhmän yksityiskohtaisia turvallisuusvaatimuksia ja näkökohtia. Esimerkiksi teollisuusroboteille on oma C-tyypin standardi (SFS-EN ISO 10218-1 Robotit ja robotiikkalaitteet. Turvallisuusvaatimukset. Osa 1: Teollisuus-robotit).

C-tyypin standardeissa annetaan vaatimuksia tietyille koneille, joiden erityispiirteet ovat hyvin tiedossa. Näin ollen vaatimukset voivat olla tiukempia tai löysempiä, kuin ylemmän luokan standardeilla. (Hietikko, Malm & Alanen 2009, 23.)

2.2.1 SFS-EN 61508

SFS-EN 61508- sarja on toiminnallisen turvallisuuden ns. kattostandardi eli perusturvallisuusjulkaisu. Sektorikohtaiset standardit pohjautuvat kattostandardiin (Toiminnallinen turvallisuus n.d). Taulukon 1 mukaisesti SFS-EN 61508- sarja sisältää 6 julkaisua suomeksi käännettynä sekä 2 englanniksi (Toiminnallinen turvallisuus n.d).

Kattostandardin merkittävät hyödyntäjät ovat sovellus- ja sektorikohtaisten standardien kehittäjät eli käytännössä teknilliset komiteat. Kattostandardia tulee käyttää, kun sovellus- tai sektori kohtaista standardia ei ole olemassa. (SFS-EN 61508-1:2011, 7–10.)

Taulukko 1. IEC 61508- sarjan sisältö

Standardi	Nimike
SFS-EN 61508-0	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0: Toiminnallinen turvallisuus ja IEC 61508
SFS-EN 61508-1	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset
SFS-EN 61508-2	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille
SFS-EN 61508-3	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 3: Ohjelmistovaatimukset
SFS-EN 61508-4	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 4: Määritelmät ja lyhenteet
SFS-EN 61508-5	Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi
SFS-EN 61508-6	Functional safety of electrical/electronic /programmable electronic safety-related systems – Part 6: Guidelines on application of IEC 61508-2 and IEC 61508-3
SFS-EN 61508-7	Functional safety of electrical/electronic /programmable electronic safety-related systems – Part 7: Overview of techniques and measures

2.2.2 SFS-EN IEC 62061

Konesektorin standardi SFS-EN IEC 62061 kuuluu aiemmin mainitun kattostandardin viitekehykseen. Tämän standardin soveltamisalaan kuulu koneiden turvallisuuteen liittyvien ohjausjärjestelmien (Safety related Control System (SCS)) suunnittelu ja etukäteen suunnittelujen alajärjestelmien yhdistämien SCS:ään. Sovellusalaan ei kuulu monimutkaisten alajärjestelmien suunnittelu, mikä tarkoittaa käytännössä ohjelmoitavia elektronisia turvakomponentteja. Standardin hyödyntäjiksi luetaan koneensuunnittelijat, integraattorit (yhdistäjät) ja ohjausjärjestelmien valmistajat (SFS-EN IEC 62061:2021, 9–11)

Poiketen toisesta konesektorin standardista SFS-EN ISO 13849-1:2015, tässä standardissa turvatoimintojen kykyä suorittaa suunniteltu toimintansa, mitataan turvallisuuden eheyden tasoilla (SFS-EN IEC 62061:2021, 9). Standardissa myös annetaan ohjeet, miten etukäteen suunnitellut alajärjestelmät yhdistetään niiden ollessa suunniteltu eri standardien mukaisesti (SFS-EN IEC 62061:2021, kohta 6.3.4).

2.2.3 SFS-EN ISO 13849

Toinen yleisesti konesektorin käytössä oleva standardi on SFS-EN ISO 13849-1:2015. Kyseinen standardin soveltamisalaan kuuluu yleispätevästi koneiden turvallisuuteen liittyvien ohjausjärjestelmien osien (Safety Retaled Parts of Control Systems, SRP/CS) suunnittelun ja integroinnin turvallisuusvaatimukset, oli käytetty teknologia sitten sähköistä, pneumaattista tai hydraulista. Turvallisuuteen liittyvällä ohjausjärjestelmän osalla standardissa tarkoitetaan käytännössä koko ohjausketjua lähtien tulosignaalin syntymisestä aina lähtölaitteeseen. Tämän standardin merkityksellisempinä hyödyntäjinä ovat konevalmistajat ja valvovat viranomaiset. (SFS-EN ISO 13849-1:2015, kohta 1)

Koneturvallisuuden standardin toinen osa SFS-EN ISO 13849-2:2012 keskittyy ensimmäisen osan mukaisesti suunnitellun turvallisuuteen liittyvän järjestelmän kelpuutukseen (SFS-EN ISO 13849-

2:2012, johdanto). Standardin toisen osan opastavat liitteet A-D sisältävät eri teknologioille turvallisuuden perusperiaatteita, hyvin koeteltuja turvallisuusperiaatteita, hyvin koeteltuja komponentteja, komponenttien vikoja ja vikojen poissulkemisien tiedot (SFS-EN ISO 13849-2:2012, liite A-D).

Verrattuna toiseen konesektorin standardiin SFS-EN IEC 62061:2021, on tämä yksinkertaisempi. Yksinkertaisuus johtaa kuitenkin epätarkempaan lopputulokseen, jolloin laskennallisesti sama riskinpienennys saadaan aikaiseksi vähemmällä, sovellettaessa standardia SFS-EN IEC 62061. Standardin SFS-EN ISO 13849-1:2015 epätarkkuus aiheutuu yksinkertaistetuista arviointimenetelmästä, joka perustuu nimettyihin rakenteisiin.

2.3 Riskin pienentämisen strategia

2.3.1 Koneiden riskit

Vaikka tässä opinnäytetyössä ei käsitellä vaara- ja riskiarviota, on siitä mainittava yleisiä asioita. Siirilän ja Tytykosken mukaan (2016, 162) vaara- ja riskiarviointi velvoite tulee monesta eri säädöksestä ja koskee useita tahoja. Muun muassa työturvallisuuslaki (L 23.8.2002/738, 10 §) velvoittaa työnantajan tunnistamaan ja poistamaan vaarat sekä arvioimaan jäljelle jäävien vaarojen merkitys. Konedirektiivi ja näin ollen myös koneasetus (A 12.6.2008/400, liite 1, 1. kappale) velvoittaa tekemään riskin arvioinnin.

Jotta riskien suuruutta ja merkitystä voidaan arvioida, täytyy ensin tunnistaa vaarat. Riski arvioidaan vahingon vakavuuden ja esiintymistodennäköisyyden perusteella. Tämän standardin mukaan vahingon esiintymistodennäköisyys on vaaralle altistuneet henkilöiden, tapahtuman todennäköisyyden ja vahingon välttämisen mahdollisuuden funktio. (SFS-EN ISO 12100: 2010, kohta 5.5.2.1.)

Mikäli riski ei ole riskin arvioinnin jälkeen siedettävällä tasolla, on riskiä pienennettävä. Ensisijainen toimenpide on riskin pienentäminen luontaisesti turvallisella suunnittelulla, jonka tavoitteena on poistaa vaara kokonaan. Mikäli ensimmäinen toimenpide ei saa aikaan riskin pienentymistä siedettävälle tasolle on tehtävä suojausteknisiä ja/tai täydentäviä suojaustoimenpiteitä. Kolmas vaihe on jäljellejäävistä riskeistä tiedotettava koneen käyttäjää esimerkiksi turvallisista työmenetelmistä, henkilösuojaimista ja varoituksilla. (SFS-EN ISO 12100: 2010, kohta 6.1.)

Luontaisesti turvallisella suunnittelulla voidaan rakenteellisesti vaikuttaa koneen turvallisuuteen esimerkiksi vaarallisten liikkeiden nopeuden tai voiman rajoittamisella, vaarallisten osien sijoittamisella ihmisen ulottumattomiin, sijoittamalla liikkuvat osat riittävän etäälle kiinteistä osista tai koneen huoltokohteiden sijoittaminen turvalliseen tilaan. (Guide to application of the Machinery Directive 2006/42/EC 2019, kohta §173.)

Suojausteknisellä toimenpiteellä tarkoitetaan käytännössä henkilön vaaravyöhykkeelle pääsyn estämiseksi asetettujen kiinteiden suojusten tai avattavaan suojukseen toimintaan kytketyn turvalaitteiden käyttämistä osana riskin pienentämistä. (SFS-EN ISO 12100: 2010, kohta 6.3.2.1.)

Täydentävänä suojaustoimenpiteenä voidaan pitää esimerkiksi hätäpysäytyslaitteita, tehonsyötössä olevia lukittavia energian syötönerotuskytkimiä (huoltokytkimiä), turvallisia kulkuteitä, poistumisteitä ja kulkutasoja. (SFS-EN ISO 12100: 2010, kohta 6.3.5.)

Viimeisenä riskinpienennystoimenpiteenä käyttöä koskevien tietojen välittäminen koneen hyödyntäjille tarkoittaa käytännössä esimerkiksi käyttäjien ymmärrettävissä olevilla tekstillä ja symboleilla esitettyä tietoa jäännösriskeistä koneeseen kiinnitettynä ja/tai käyttöohjekirjassa. Riskiä pienennetään myös esimerkiksi kouluttamalla koneen hyödyntäjät riittävästi. (SFS-EN ISO 12100: 2010, kohta 6.4.)

Mikäli riskiä joudutaan pienentämään käyttö koskevilla tiedoilla, on olemassa mahdollisuus, ettei koneen käyttäjä (ihminen) tietoisesti noudata annettuja turvallisuusohjeita. Tämän vuoksi riskiä kuuluisi pienentää luontaisesti turvallisella suunnittelulla ja käyttäjästä riippumattomilla teknisillä toimenpiteillä. (Käyttöasetuksen soveltamissuosituksia 2009, 54–55.)

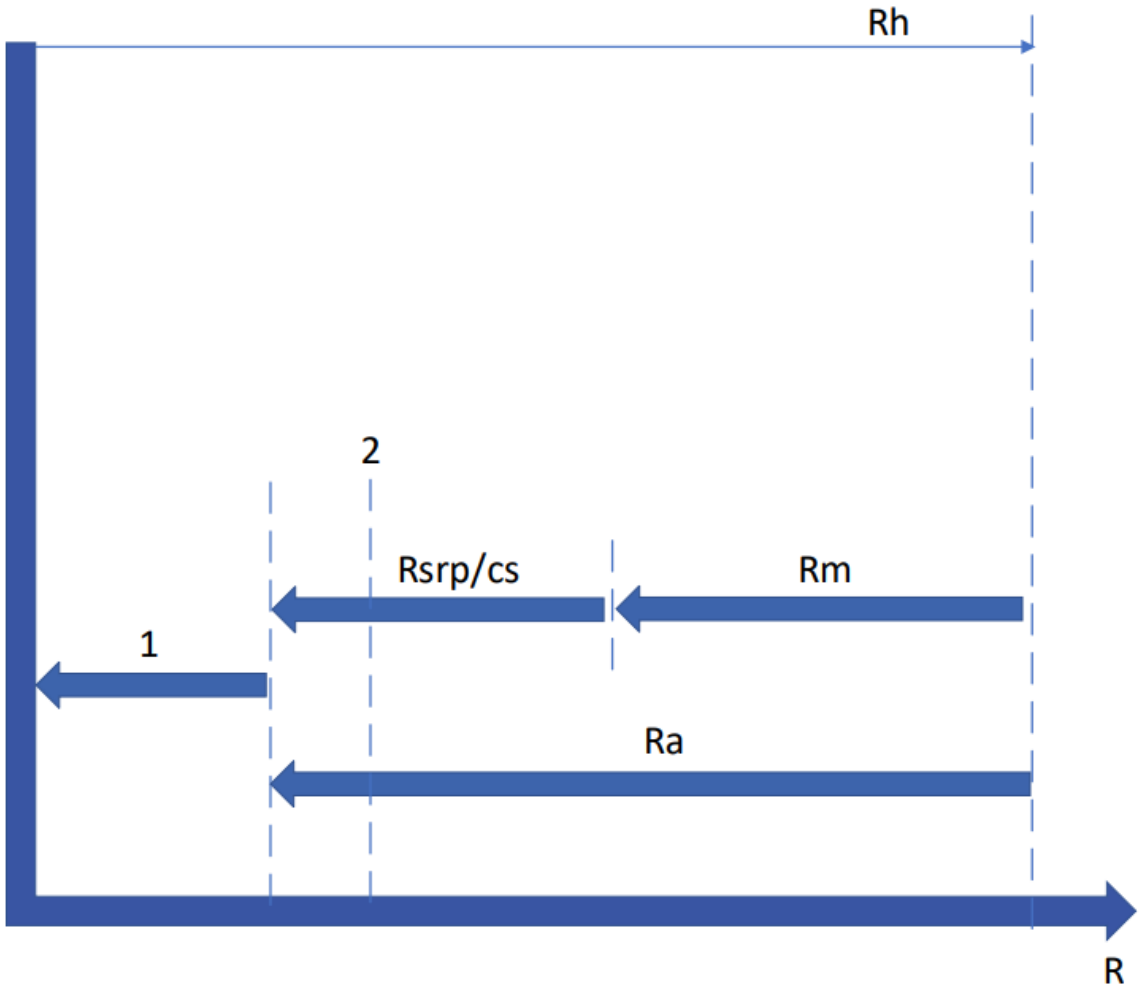
Siirilän ja Tytykosken (2016, 222–243) merkittävä asia riskien arvioinnin oikeellisuuden kannalta on valita sopiva arviointimenetelmä, koska eri menetelmillä saadaan huomattavasti toisistaan eroavia tuloksia, mikä johtaa riskien yli- tai aliarvioimiseen. Malm, Venho-Ahonen, Hietikko, Stålhane, de Bésche, ja Hedberg (2015, 42) osoittavat VTT:n julkaisussa kahden eri standardin riskiarviomenetelmien antavan eri tuloksia turvatoimintojen turvallisuuden eheyden- ja suoritustasojen välillä.

Ylimitoitetut turvatoiminnot ovat turvallisuuden kannalta hyväksi, mutta kustannukset saattavat olla huomattavasti suuremmat varsinkin laajoissa laitteistossa.

2.3.2 Riskin pienentäminen ja kohdennus turvatoiminnalle

Riskin pienentäminen perustuu eri menetelmiin ja on tärkeä kohdentaa oikea osuus oikeille toimenpiteille. Riskianalyysin tuloksena saadaan jokaiselle turvatoiminnolle vaadittu suoritustaso (SFS-EN ISO 13849-1:2015, kohta 4.3). Kuviossa 1 havainnollistetaan riskin pienentämisen osuuksia eri suojaustoimenpiteillä. Käytännössä jäljellejäävää jäännösriskiä tulisi kuviosta poiketen pienentää käyttöä koskevilla tiedoilla. Eri sovelluksissa turvatoiminnon ja muiden riskinpienennystoimenpiteiden välinen suhde saattaa vaihdella hyvinkin paljon.

Riskien kohdentamisessa tulee olla tarkka. Konesektorilla voidaan miettiä, kuinka suuri riski olisi esimerkiksi sorvissa ilman avattavaa suojaovea ja vaarallista liikettä pysäyttävää oven rajakytkintä. Robottisolu ilman turvavaloverhoja hihnakuljettimen sisääntuloaukossa tai hydraulinen purisin ilman toimintaan kytkettyä valoverhoa tai pakkokäyttöisiä kahdenkäden hallintalaitetta? Prosessiteollisuudessa voidaan miettiä esimerkiksi paineistetun säiliön repeämistä, kuinka suuri riski olisi ilman murtolevyä, hätäpaineenpurkua tai säiliötä ympäröiviä suojavalleja.



Kuvio 1. Riskinpienentämisen yleinen periaate (SFS-EN ISO 13849-1:2015, kohta 4.2.2, muokattu)

missä 1 = Jäännösriski

2 = Siedettävä riski

Rsrp/cp = Turvatoiminnon aikaansaama riskinpienennys

Rm = Muiden toimenpiteiden aikaansaama riskinpienennys

Ra = Kokonaisuuden riskinpienennys

Rh = Kokonaisriski tietylle vaaralliselle tilanteelle ennen suojaustoimenpiteitä

R = Riskin määrä

2.4 Turvatoiminto

Turvatoiminto (Safety Function) on nimitys turvallisuuteen liittyvän järjestelmän (TLJ) toteuttamalle toiminnalle. Turvatoiminnon tarkoitus on saattaa ohjattava järjestelmä turvalliseen tilaan tai ylläpidettävä turvallinen tila (SFS-EN 61508-4:2010, 18). Koneturvallisuuden standardi SFS-EN ISO 12100 (2010, 11) määrittelee turvatoiminnon olevan ”koneen toiminto, jonka vikaantuminen voi aiheuttaa välittömän riskin (riskien) kasvamisen”.

Turvatoiminto koneiden ohjausjärjestelmissä standardin SFS-EN ISO 13849-1:2015 (kohta 5.1, muokattu) mukaan voi olla esimerkiksi seuraavaa:

- Turvalaitteen käynnistämä turvallisuuteen liittyvä pysäytystoiminto
- Odottamattoman käynnistymisen estäminen
- Hätäsulku, -avaus, -pysäytys, -käynnistys tai -poiskytkentä
- Kahdenkäden hallintalaite
- Pakkotoiminen ohjaus

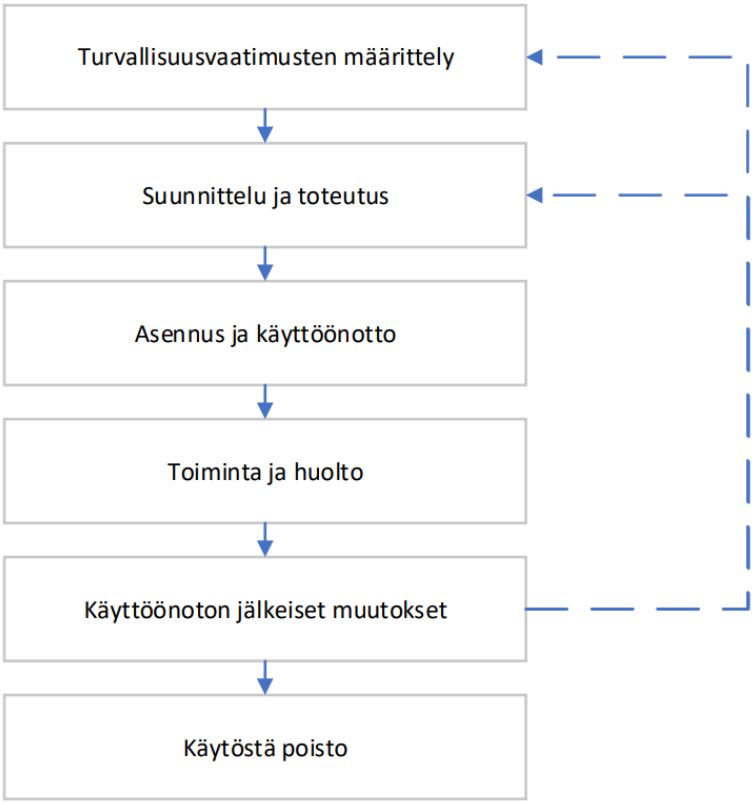
Siirilän ja Tytykosken mukaan koneissa tyypillinen turvatoiminto on avattavaan suojukseen toimintaan kytketyn turvalaitteen aikaan saama vaarallisen liikkeen pysäytys. Toinen suojuksen avaamisen aikaansaama turvatoiminto on odottamattoman käynnistyksen estäminen. Useimmiten vaarallisen liikkeen käynnistäminen on mahdollista vasta käsikäyttöisen kuittauksen jälkeen, joka myös on turvatoiminto. (Siirilä ja Tytykoski 2016, 488 ja 495–496.)

Siirilä ja Tytykoski (2016, 717–718) antavat koneturvallisuuden käsikirjassaan useita esimerkkejä tapaturmista, jotka ovat sattuneet turvatoimintojen vikaantuessa. Esimerkiksi pakkokäyttöisen liikkeen ohjauspainikkeen vikaantuminen on ollut yksi vaikuttava tekijä lentomekaanikon kuolemaan johtaneessa tapaturmassa (Lentokonemekaanikko puristui lentokoneen rahtiruuman luukun väliin 2005).

2.4.1 Turvatoiminnan vaatimusmäärittely

Kattostandardi määrittelee kokonaisuuden turvallisuuden elinkaaren vaiheet. Konesektorilla elinkaari on pääpiirteittäin sama. Myös prosessisektorin standardissa SFS-EN 61511-1: 2017 on sama

elinkaarikonsepti käytössä. Kuviossa 2 on yksinkertaistettu versio turvallisuuden elinkaaren eri vaiheista, missä katkoviivalla tarkoitetaan muutoksien jälkeen paluuta sopivaan elinkaaren vaiheeseen.

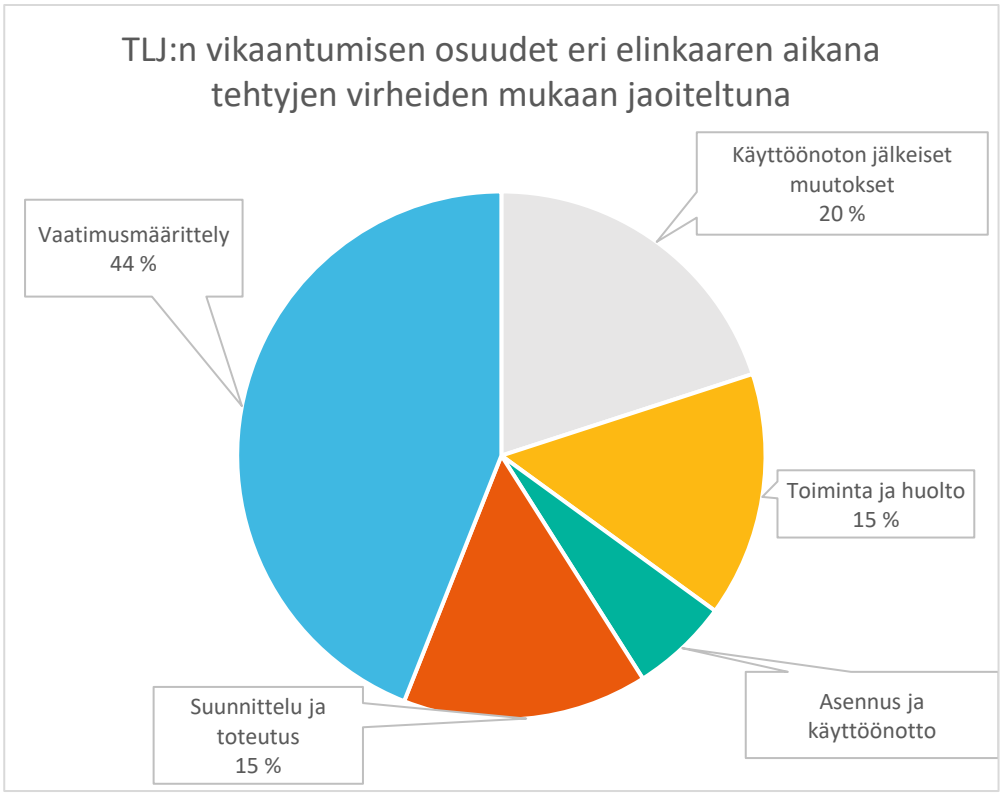


Kuvio 2. Turvallisuuden elinkaaren vaiheet (SFS-EN 61508-1:2010, 176, muokattu)

Turvatoiminnoille ja myös koko turvallisuuteen liittyvälle järjestelmälle sopivat Hietikon, Malmin ja Alasen (2009, 12) mukaan tavanomaiset vaatimusmäärittelyprosessit. Turvallisuusvaatimusten määrittely on merkittävässä roolissa elinkaaren vaiheista, sillä Iso-Britannian terveys- ja turvallisuusviranomaisen (HSE) tutkimuksen mukaan jopa 44 % turvallisuuteen liittyvien ohjausjärjestelmien vikaantumiset johtuvat vaatimusmäärittelyvaiheessa tehdyistä virheistä (Out of control

2003, 31). Kuviossa 3 ilmenee HSE:n tutkimuksen muidenkin elinkaaren vaiheiden aikana tehtyjen juurisyiden osuudet.

Siirilä ja Tytykoski painottavat koneturvallisuuden käsikirjassaan käyttöönotto- ja koekäyttövaiheen olevan riskialtista. Varsinkin suurien kokonaisuuksien, kuten paperikoneen tai pakkauslinjaston käyttöönotto ennen lopullisten suojusten ja turvalaitteiden toimintaan kytkentää altistaa henkilöstön riskeille. Yksinkertaisimmillaan koneen käyttöönotto on pistotulpan liittäminen pistorasiaan, mutta monimutkaisien koneyhdistelmien käyttöönottoon osallistuu useiden eri tahojen työntekijöitä ja käyttöönotto kestää pitkään. (Siirilä ja Tytykoski 2016, 71–72.)



Kuvio 3. HSE:n tutkimuksen mukaiset TLJ:n vikaantumiset (Out of control 2003, 31, muokattu)

Turvallisuuteen liittyvillä ohjausjärjestelmillä turvallisuusvaatimuksia tulee useasta lähteestä, joista Hietikko ja kumppanit painottaa erityisesti lakien ja säädösten määräämiä vaatimuksia, kuten konedirektiivi, harmonisoidut standardit ja viranomaiset. Vaatimusten tullessa laeista ja säädöksistä,

on kiinnitettävä erityistä huomiota vaatimusten jäljitettävyyteen ja versionhallintaan. Muita turvallisuusvaatimusten lähteitä ovat muun muassa riskinarvio, asiakas, laitevalmistaja tai esimerkiksi kunnossapito-organisaatiot. (Hietikko, Malm & Alanen 2009, 13.)

2.5 Turvatoimintojen vikaantumiset

Turvallisuudesta puhuttaessa eri vikaantumisten käsitteet, syyt ja merkitykset ovat tärkeää ymmärtää, koska vikaantumisia ensisijaisesti täytyy välttää ja hallita. Vikaantumisella tarkoitetaan standardissa SFS-EN 61508-4:2010 (kohta 3.6.4): ”toiminnallisen yksikön kyvyn loppuminen vaaditun toiminnan tuottamiseen tai toiminnallisen yksikön toiminta millä muulla tavalla tahansa kuin vaadittu”. On tärkeä sisäistää, että ennen vikaantumista laitteistossa on vika, jota seuraa vikaantuminen. Varsinkin systemaattisissa vikaantumisissa, vika saattaa olla pitkään olemassa ennen kuin tapahtuu vikaantuminen.

Vikaantuminen jaetaan toiminnallisen turvallisuuden kontekstissa usealla eri tavalla. Yksi jaottelu on satunnainen laitteistovikaantuminen ja systemaattinen vikaantuminen. Toinen tapa jaotella vikaantumiset turvallisiin, vaarallisiin, paljastumattomiin ja paljastuviin, kuten kohdassa 2.6.1 kerrotaan. Perustavan laatuinen ero näissä vikaantumisissa on vikaantumismitan ennustettavuus.

Satunnainen laitteistovikaantuminen ilmenee ajansuhteen satunnaisesti, mutta odotettavissa olevalla nopeudella. Laitteistossa on useita erityyppisiä komponentteja, joiden valmistustoleranssit ja useat erilaiset huononemismekanismit vaikuttavat vikaantumismittaan. (SFS-EN 61508-4:2010, kohta 3.6.5.)

Systemaattisella vikaantumisella tarkoitetaan vikaantumista, joka aiheutuu tietystä syystä ja voitaisiin välttää ainoastaan oikealla ihmisen toiminnalla eri elinkaaren vaiheissa, kuten vaatimusmäärittelyssä tai suunnittelussa. Systemaattisia vikaantumisia ei pystytä luotettavasti ennustamaan, johtuen vaikeasti määriteltävistä tapahtumien juurisyistä. (SFS-EN 61508-4:2010, kohta 3.6.6.)

Standardissa SFS-EN 61508-2:2011 luokitellaan vikaantumiset elinkaaren vaiheiden mukaan: ennen järjestelmän valmistumista tai järjestelmän valmistumisen jälkeen syntyneiden vikojen aikaan-

saamien vikaantumisten mukaisesti. Tyypillisesti järjestelmän valmistumisen jälkeen tapahtuu satunnaisia laitteistovikaantumisia tai virheellisen käytön ja kunnossapidon aiheuttamia systemaattisia vikaantumisia. Ennen valmistumista syntyneet viat ovat tyypillisimmin vaatimusmäärittelyyn tai suunnitteluun liittyviä. (SFS-EN 61508-2:2011, liite B.)

Standardin liitteissä A ja B esitetään käytännön toimia eri elinkaaren vaiheille, mitä noudattamalla voidaan välttää tai hallita vikaantumisia (SFS-EN 61508-2:2011, liite B). Vaikka kattostandardin soveltamisalaan kuuluvat monimutkaiset laitteistot, on periaatteet hyvä sisäistää yksinkertaisimmillakin laitteistoilla. Konesektorilla systemaattisen vikaantumisen hallintaan ja välttämiseen esitetään keinoja standardissa SFS-EN ISO 13849-1 ja 2, joissa myös viitataan kattostandardiin (SFS-EN ISO 13849-1:2015, liite G).

Turvallisuuden eheyden ja suoritustason määrittämiseen käytettävien vikaantumismitoissa (PFH_D, $MTTF_D$, jne.), on huomioitu ainoastaan tässä osiossa mainitut satunnaiset laitteistovikaantumiset. Systemaattisia vikaantumisia ei kuulu ottaa huomioon laskennassa, sillä ensinnäkin niitä ei pitäisi standardin mukaisen suunnittelun ja toteutuksen myötä olla olemassa ja toiseksi niitä on vaikea arvioida.

2.6 Turvallisuuden eheyden taso (SIL)

Turvallisuuden eheyden taso (TET) eli SIL (Safety Integrity Level) on turvatoiminnan turvallisuuden eheyden numeerinen taso 1, 2, 3 tai 4. Jako tasoihin on tehty vikaantumismitan perusteella. Mitä isompi TET on, sitä harvemmin turvatoiminto vikaantuu vaarallisesti. (SFS-EN 61508-4:2010, kohta 3.5.8.)

Turvatoimintojen toimintatapa jaetaan seuraavalla tavalla (SFS-EN 61508-4:2010, kohta 3.5.16.):

> Harvojen vaateiden toimintatapa, vaadetaajuus < 1 vuodessa
> Tiheiden vaateiden toimintatapa, vaadetaajuus >= 1 vuodessa
> Jatkuva toiminnan toimintatapa, jolloin turvallista tilaa ylläpidetään jatkuvasti turva toiminnolla

Turvatoiminnan tavoitteellinen vikaantumismitta eli todennäköisyys vaaralliselle vikaantumiselle määritellään harvojen vaateiden toimintatavan mukaan: turvatoiminnan vaarallisen vikaantumisen

keskimääräinen todennäköisyys vaadittaessa (Probability of Failure on Demand average, $\mathrm{PFD}_{\mathrm{avg}}$). Kun toimintatapa on tiheiden vaateiden tai jatkuva, vikaantumismitta on vaarallisten vikaantumisten keskimääräinen taajuus tunnissa (The Probability of Failure on Demand per Hour, PFH). (SFS-EN 61508-4:2010, kohta 3.5.17.) Vikaantumismitan ja turvallisuuden eheyden tason välinen yhteys on esitetty taulukossa 2 ja 3.

Taulukko 2. TET:n suhde vikaantumismittaan harvojen vaateiden toimintatavalla (SFS-EN 61508-1: 2010, kohta 7.6.2.9, muokattu).

Turvallisuuden eheyden taso (TET)	Keskimääräinen vaarallisten vikaantumisten todennäköisyys turvatoiminnan vaateesta ($\mathrm{PFD}_{\mathrm{avg}}$)
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Taulukko 3. TET:n suhde vikaantumismittaan tiheiden tai jatkuvien vaateiden toimintatavalla (SFS-EN 61508-4:2010, kohta 7.6.2.9, muokattu).

Turvallisuuden eheyden taso (TET)	Keskimääräinen turvatoiminnan vaarallisten vikaantumisten taajuus [h^{-1}] (PFH)
4	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-6} \ldots < 10^{-5}$

Koneturvallisuuden standardissa SFS-EN IEC 62061 ei käsitellä harvojen vaateiden toimintatapaa eikä täten myöskään $\mathrm{PFD}_{\mathrm{avg}}$- arvoa. Harvojen vaateiden turvatoiminto voidaan olettaa tiheiden vaateiden turvatoiminnaksi aktivoimalla se vähintään kerran vuodessa. Aina turvatoiminnan manuaalinen aktivointi ei ole järkevää prosessin luonteen vuoksi. (SFS-EN IEC 62061: 2021, kohta 5.2.4.)

2.6.1 Arkkitehtuuri

Arkkitehtuuri määritellään standardissa SFS-EN 61508-4:2010 olevan laitteiston ja ohjelmiston osien tietyn lainen kokoonpano, eli rakenne (SFS-EN 61508-4:2010, kohta 3.3.4). Tässä vaiheessa on syytä selventää muutamaa tekstissä esiintyvää termiä, jotka ovat spesifejä puhuttaessa niistä toiminnallisen turvallisuuden kontekstissa.

Turvallisuuteen liittyvä järjestelmä (TLJ) on ylin taso hierarkiassa ja siihen sisältyy kaikki turvatoiminnon suorittamiseksi tarpeellinen laitteisto, ohjelmisto ja mahdollisesti myös ihminen. TLJ koostuu ainakin yhdestä itsenäisestä ja hierarkkisesti alempana olevasta alajärjestelmästä, jonka vaarallinen vikaantuminen saattaa johtaa turvatoiminnan menettämiseen. Elementillä tarkoitetaan alajärjestelmän hierarkkisesti alenevaa osaa, joka koostuu ainakin yhdestä komponentista. (SFS-EN 61508-4:2010, kohta 3.4.)

Käytännössä elementti voisi olla esimerkiksi rajakytkin tai rajakytkimen sähkömekaaninen kosketin. Jos samaan turvatoimintoon käytetään kahta eri rajakytkintä, katsotaan rajakytkinten yhdessä muodostavan alajärjestelmän. Etukäteen suunnitellulla alajärjestelmällä voidaan tarkoittaa esimerkiksi turvalogiikkaa tai turvarelettä.

Arkkitehtuuriin liittyy vahvasti termi: laitteiston vikasietoisuus (Hardware Fault Tolerance, HFT), joka tarkoittaa turvatoiminnon sietämien vikojen lukumäärää, ennen kuin turvatoiminto menetetään. Mikäli HFT = 0, yksikin vika saattaa johtaa turvatoiminnon menettämiseen ja järjestelmän ollessa kahdennettu, HFT = 1. Vikasietoisuutta määritellessä ei tule ottaa huomioon diagnostiikan tai muiden toimenpiteiden vaikutusta vikojen seurauksiin. (SFS-EN IEC 62061:2021, kohta 7.4.1.)

Jotta turvatoiminnon turvallisuuden eheys pysyisi luotettavalla tasolla, on rajoitettava laitteiston korkeinta turvallisuuden eheyden tasoa. Rakenteellisilla rajoituksilla ehkäistään alhaisen vikasietoisuuden laitteiston rakentaminen korkeille turvallisuuden eheyden tason turvatoiminnoille. Jotkin turvatoimintoon osallistuvat komponenttien yhdistelmät saattaisivat luotettavuutensa puolesta saavuttaa korkean turvallisuuden eheyden tason, mutta TET rajoitetaan vikasietoisuuden ja turvallisten vikaantumisten osuuden (Safe Failure Fraction, SFF) perusteella. (SFS-EN 61508-2:2011, kohta 7.4.4.1.1.)

Turvallisten vikaantumisten osuudella tarkoitetaan turvatoimintoon osallistuvan alajärjestelmän tai elementin turvallisten vikaantumisten taajuuden suhdetta paljastumattomien vaarallisiin vikaantumisien taajuuteen kaavan 1 mukaisesti. (SFS-EN IEC 62061:2021, kohta 7.4.2, muokattu.)

$$SFF = \frac{(\sum \lambda_S + \sum \lambda_{DD})}{(\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU})} \quad (1)$$

missä SFF = Turvallisten vikaantumisten osuus

λ_S= turvallisten vikaantumisten taajuus

λ_{DD}= diagnostiikan paljastamien vaarallisten vikaantumisten taajuus

λ_{DU}= paljastumattomien vaarallisten vikaantumisten taajuus

Yksikanavaisen alajärjestelmän tapauksessa, vikasietoisuuden ollessa 0, SFF on suoraan verrannollinen diagnostiikan kattavuuden kanssa kaavan 2 mukaisesti. (SFS-EN IEC 62061:2021, kohta 7.4.2, muokattu.)

$$SFF = DC \quad (2)$$

Kaavat 1 ja 2 perustuvat vakiovikaantumistiheyksiin. Mikäli vikaantumistiheydet eivät ole vakioita, on laskennassa käytettävä keskimääräisiä vikaantumistiheyksiä. Vaikutuksettomia- eikä turvatoimintoon osallistumattomien osien vikoja tule huomioida laskettaessa turvallisten vikaantumisten osuutta (SFS-EN 61508-2:2011, Liite C).

Vaikutuksettomana vikaantumisena voidaan pitää esimerkiksi sorvin oven rajakytkimen sulkeutuvan koskettimen jäämistä tarkoituksettomasti auki. Tällöin ovea avatessa ja sulkeutuvan koskettimen ollessa auki, ei sillä ole vaikutusta turvatoiminnon toteuttamiseen. (SFS-EN IEC 62061:2021, kohta 7.4.2.)

Arkkitehtuuriset rajoitukset esitetään standardissa SFS-EN 61508-2:2011 kahdella eri taulukolla. Taulukko 4 esittää TET rajoituksen tyypin A ja taulukko 5 tyypin B elementille tai alajärjestelmälle.

Tyypin A elementissä:

1. kaikkien osakomponenttien vikaantumismuodot ovat selkeästi tiedossa ja
2. elementin reaktio vikatilanteessa tiedetään täydellisesti ja
3. luotettavaa vikaantumistietoa on riittävästi vaarallisien vikaantumistiheyksien määrittämiseksi

Tyypin B elementissä:

1. osakomponenttien vikaantumismuodot ei ole tiedossa tai
2. elementin reaktiota vikatilanteessa ei täydellisesti tiedetä tai
3. ei ole luotettavaa vikaantumistietoa riittävästi vaarallisten vikaantumistiheyksien määrittämiseksi

Käytännössä, jos yksikin tyypin B ehto täyttyy, luokitellaan elementin tai alajärjestelmän tyypiksi B. (SFS-EN 61508-2:2011, kohta 7.4.4.1.)

Taulukko 4. Turvallisuuden eheden tason arkkitehtuuriset rajoitukset tyypin A elementille tai alajärjestelmälle (SFS-EN 61508-2:2011, kohta 7.4.4.2, muokattu).

Elementin tai alajärjestelmän turvallisten vikaantumisten osuus (SFF)	Laitteiston vikasietoisuus (HFT)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Taulukko 5. Turvallisuuden eheden tason arkkitehtuuriset rajoitukset tyypin B elementille tai alajärjestelmälle (SFS-EN 61508-2:2011, kohta 7.4.4.2, muokattu).

Elementin tai alajärjestelmän turvallisten vikaantumisten osuus (SFF)	Laitteiston vikasietoisuus (HFT)		
	0	1	2
< 60 %	Ei sallittu	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Toinen arkkitehtuurinen rajoite liittyy alajärjestelmän sarjaan kytkettyihin elementteihin. Näissä tapauksissa koko alajärjestelmän TET määräytyy sen elementin perusteella, jolla on matalin TET taulukkojen 4 ja/tai 5 mukaan. (SFS-EN 61508-2:2011, kohta 7.4.4.2.3.)

Standardissa SFS-EN IEC 62061:2021 rakenteelliset rajoitukset esitetään ainoastaan taulukon 5 mukaisesti, koska konesektorilla ei yleisesti ole harvojen vaateiden turvatoimintoja.

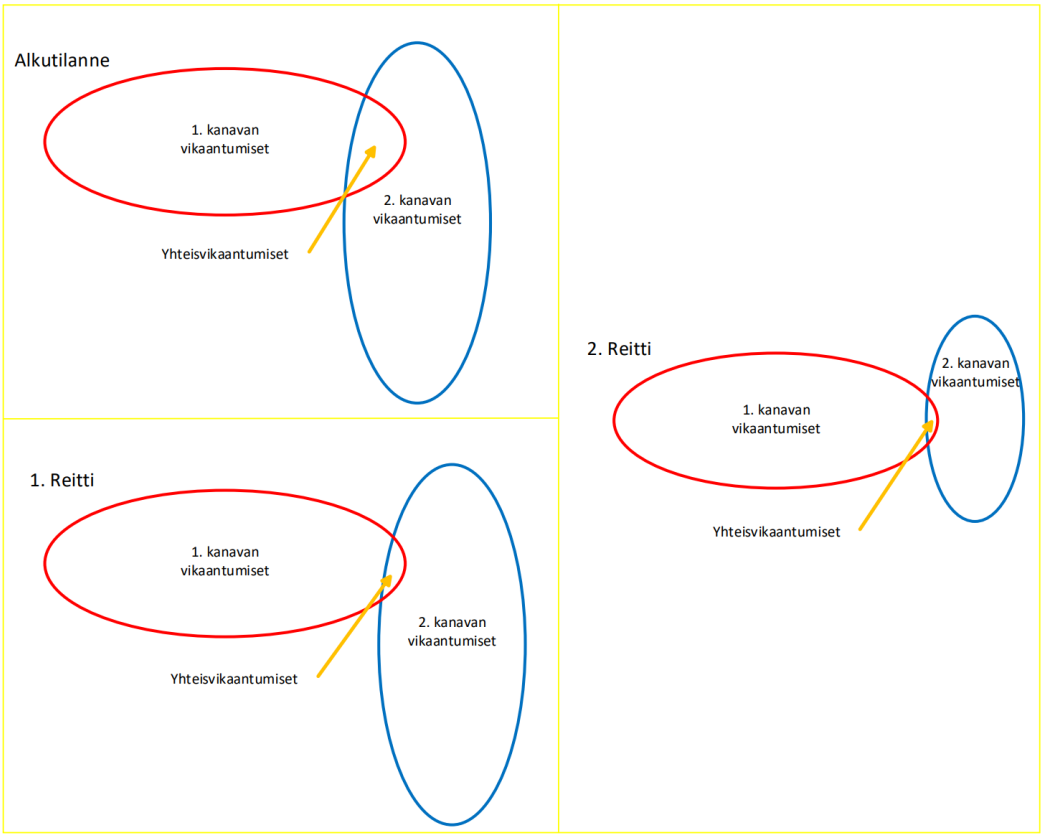
2.6.2 Yhteisvikaantuminen

Standardin SFS-EN 61508-6: 2010 (kohta D.1) mukaan riippuvat vikaantumiset yleisesti jaetaan kolmeen eri kategoriaan:

- Yhteisvikaantuminen (Common Cause Failure, CCF) tarkoittaa nimensä mukaisesti yhteisen syyn aiheuttamaa vikaa useammalle, kuin yhdelle komponentille.
- Yhteisen toimintatavan vikaantuminen (Common Mode Failure, CMF) tarkoittaa usean komponentin vikaantumista saman toimintatavan (Mode), ollessa käytössä.
- Kaskadi vikaantuminen (Cascade failure) tarkoittaa yhden vikaantumisen aloittamasta itse itseään ruokkivasta ketjureaktiosta, joka johtaa useiden komponenttien vikaantumiseen.

Yhteisvikaantumisen estämiseksi esitellään kolme eri reittiä, joista kahta ensimmäistä havainnollistetaan kuviossa 4:

1. Käyttämällä redundanttisissa järjestelmissä kullakin kanavalla mahdollisimman suurta riippumattomuutta toisiinsa nähden. Riippumattomuutta parannetaan kanavien erilaisuudella ja erottelulla. (1. Reitti)
2. Vähennetään kanavien ja tai komponenttien systemaattisia ja satunnaisia vikaantumista kokonaisuutena. (2. Reitti)
3. Paljastamalla yhteisvikaantuminen diagnostiikalla, ennen kuin toinenkin kanava on vikaantunut.



Kuvio 4. Yhteisvikaantumisten pienentämisen eri reitit (SFS-EN 61508-6: 2010, kohta D.1, muokattu)

Toisin kuin konesektorin standardissa SFS-EN ISO 13849-1:2015, kattostandardi esittää tavan laskea matemaattisesti vaarallisen yhteisvikaantumistaajuuden 1oo2 -rakenteiselle järjestelmälle kaavan 3 mukaisesti (SFS-EN 61508-6: 2010, liite D). Tämä tapa vaikuttaa koko turvatoiminnon vaaralliseen vikaantumismittaan. Perusperiaate on kuitenkin sama, kuin konestandardissa: suoritettujen toimien perusteella lasketaan pisteitä ja pisteiden perusteella määräytyy yhteisvikaantumiskerroin.

$$\lambda_{DU} * \beta + \lambda_{DD} * \beta_D \qquad (3)$$

missä λ_{DD}= yhden kanavan diagnostiikan paljastamien vaarallisten vikaantumisten taajuus

λ_{DU}= yhden kanavan paljastumattomien vaarallisten vikaantumisten taajuus

β= yhteisvikaantumiskerroin (%) paljastumattomille vaarallisille vikaantumisille

β_D= yhteisvikaantumiskerroin (%) paljastuneille vaarallisille vikaantumisille

2.7 Suoritustaso (PL)

Koneturvallisuuden standardissa SFS-EN ISO 13849-1:2015 määritellään termin suoritustaso tarkoittavan: tasoa, jolla ilmaistaan turvallisuuteen liittyvien ohjausjärjestelmien kyky suorittaa turvatoiminto. Suoritustasoja (Performance Level, PL) on yhteensä viisi ja vastaavat turvallisuuden eheyden tasoja taulukon 6 mukaisesti. Suoritustasoista ei löydy vastaavuutta turvallisuuden eheyden tasolle 4, koska niin suuria riskejä ei pääsääntöisesti konesektorilla pitäisi esiintyä. Taulukosta myös havaitaan, että suoritustasot b ja c vastaavat tasoa 1 eikä tasolle a löydy vastaavuutta. (SFS-EN ISO 13849-1:2015, kohta 4.5.1.)

Keskimääräinen aika vaaralliseen vikaantumiseen (Mean Time To Dangerous Failure, $\mathrm{MTTF_D}$), jota standardissa SFS-EN ISO 13849-1:2015 käytetään, on käytännössä käänteisluku PFH- arvosta. Muunnettaessa $\mathrm{MTTF_D}$-arvoa PFH-arvoksi on huomioitava muutos vuosista tunneiksi.

Taulukko 6. Suoritustasojen ja turvallisuuden eheyden tasojen vastaavuus. (SFS-EN ISO 13849-1:2015, kohta 4.5.1, muokattu.)

PL	SIL (Tiheiden tai jatkuvien vaateiden toimintatapa)
a	Ei vastaavuutta
b	1
c	1
d	2
e	3
Ei vastaavuutta	4

Standardissa SFS-EN ISO 13849-1:2015 $\mathrm{MTTF_D}$ jokaiselle kanavalle jaetaan kolmeen eri tasoon taulukon 7 mukaisesti. Nimettyjen rakenteiden kanavien suurin $\mathrm{MTTF_D}$ on rajoitettu 100 vuoteen, sillä turvatoiminto ei saisi olla riippuvainen pelkästään komponenttien luotettavuudesta. Poikkeuksena luokassa 4 kanavien $\mathrm{MTTF_D}$ on rajoitettu 2500 vuoteen. (SFS-EN ISO 13849-1:2015, kohta 4.5.2)

Taulukko 7. Kanavien $\mathrm{MTTF_D}$ (SFS-EN ISO 13849-1:2015, kohta 4.5.2, muokattu.)

Verbaalinen $MTTF_D$- taso	Kunkin kanavan vaihteluväli
Matala	3 vuotta ≤ $\mathrm{MTTF_D}$ < 10 vuotta
Keskitaso	10 vuotta ≤ $\mathrm{MTTF_D}$ < 30 vuotta
Korkea	30 vuotta ≤ $\mathrm{MTTF_D}$ < 100 vuotta

2.7.1 Arkkitehtuuri

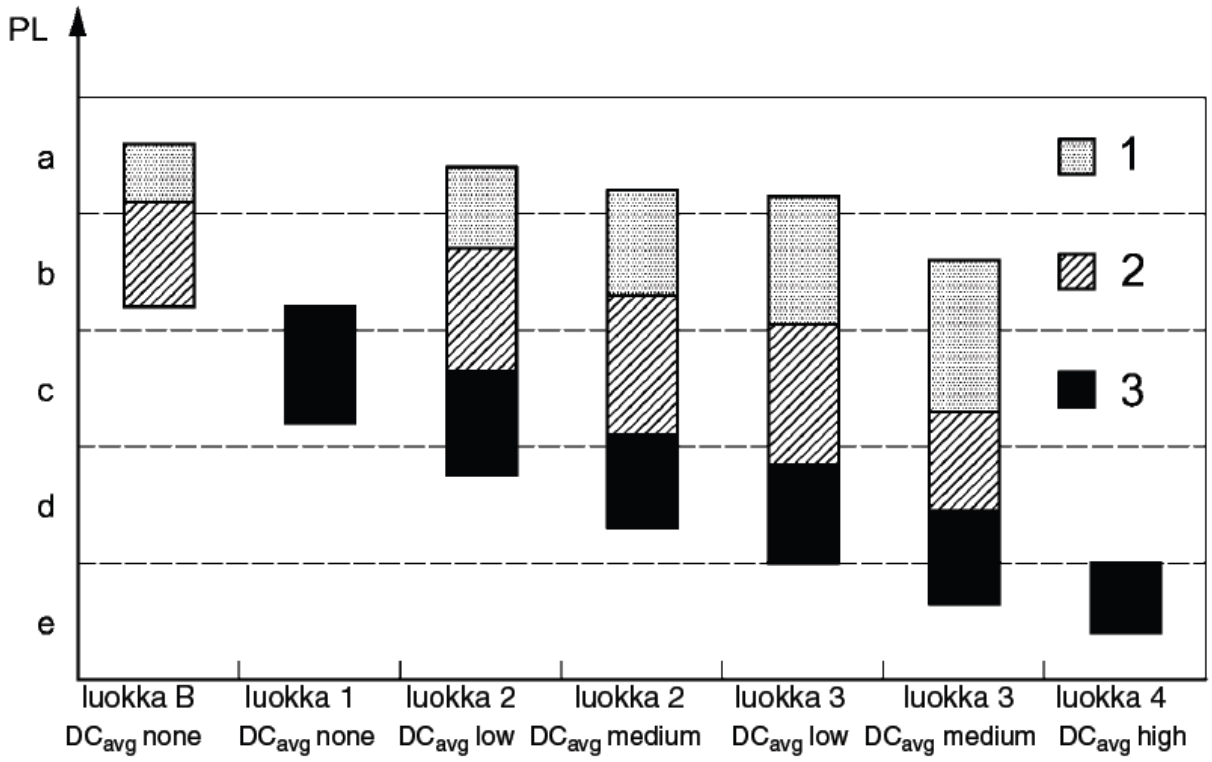
Standardissa SFS-EN ISO 13849-1:2015 ei ole tarkoituksena käyttää turvatoimintojen suunnitteluun ja todennukseen monimutkaisia matemaattisia malleja ja laskutoimituksia, vaan arviointi perustuu viiteen nimettyyn rakenteeseen, joita noudattamalla turvatoiminto on standardin vaatimusten mukainen. (SFS-EN ISO 13849-1:2015, kohta 4.5.1.) Nimettyjä rakenteita voidaan nimittää lähteestä riippuen kategorioiksi tai luokiksi.

Nimetyt rakenteet jakautuvat redundanttisiin ja ei redundanttisiin. Luokat B, 1 ja 2 eivät ole redundanttisia, kun taas luokat 3 ja 4 ovat. Kaksikanavaisissa rakenteissa tulee ottaa huomioon yhteisvikaantuminen (Common Cause Failure, CCF). Kuviosta 5 voidaan nähdä kullakin nimetyllä rakenteella saavutettavat suoritustasot, missä

väritys 1: $\mathrm{MTTF_D}$ = matala,

väritys 2: $\mathrm{MTTF_D}$ = keskitaso,

väritys 3: $\mathrm{MTTF_D}$ = korkea. (SFS-EN ISO 13849-1:2015, kohta 4.5.5.)



Kuvio 5. Luokilla saavutettavat suoritustasot. (SFS-EN ISO 13849-1:2015, kohta 4.5.4.)

Luokka b on perusluokka, jonka vaatimukset ylempienkin luokkien on täytettävä (Apfeld, Hauke & Otto 2015, 49). Vaatimuksena b-luokkaan on muun muassa asiaankuuluvien standardien mukainen suunnittelu, rakentaminen, yhdistäminen sekä turvallisuuden perusperiaatteiden käyttäminen (SFS-EN ISO 13849-1:2015, kohta 6.2.3).

Luokassa 1 on käytettävä hyvin koeteltuja komponentteja ja noudatettava hyvin koeteltuja turvallisuusperiaatteita. Luokka 1 on pääsääntöisesti 1 kanavainen ja kanavan $\mathrm{MTTF_D}$ on oltava korkea. (SFS-EN ISO 13849-1:2015, kohta 6.2.4.)

Luokassa 2 noudatetaan hyvin koeteltuja turvallisuusperiaatteita. Ohjausjärjestelmässä on yksi toiminnallinen kanava sekä yksi valvontakanava, joka tarkistaa turvatoiminnon vikojen varalta. Tarkistus on tehtävä käynnistyksen yhteydessä ja ennen vaaratilanteiden alkamista. Vikojen paljastuttua on testauslaitteiston saatava aikaan turvallinen tila, mikäli se on käytännöllistä. Luokan 2 toiminnallinen kanava sisältää diagnostiikkaa, jonka taso on oltava vähintään matala. Kanavien $\mathrm{MTTF_D}$ on oltava vähintään matala. Yhteisvikaantuminen (CCF) on huomioitava. (SFS-EN ISO 13849-1:2015, kohta 6.2.5.)

Luokassa 3 noudatetaan hyvin koeteltuja turvallisuusperiaatteita. Ohjausjärjestelmän on siedettävä yksi vika missä tahansa osassa menettämättä turvatoimintoa. Käytännössä vikasietoisuus tarkoittaa redundanttista ohjausjärjestelmää. $\mathrm{DC_{avg}}$ on oltava vähintään matala. Yhteisvikaantuminen (CCF) on huomioitava. (SFS-EN ISO 13849-1:2015, kohta 6.2.6.)

Myös luokassa 4 noudatetaan hyvin koeteltuja turvallisuusperiaatteita. Yksi vika on siedettävä menettämättä turvatoimintoa ja vian on paljastuttava seuraavan vaateen yhteydessä. Mikäli vikojen paljastuminen ei ole mahdollista, ei vikojen kerääntyminen ei saa aiheuttaa turvatoiminnon menettämistä. $\mathrm{DC_{avg}}$ on oltava korkea. $\mathrm{MTTF_D}$kullekin kanavalle on oltava korkea ja yhteisvikaantuminen täytyy huomioida. (SFS-EN ISO 13849-1:2015, kohta 6.2.7.)

Aiemmin mainitut turvallisuuden perusperiaatteet sekä hyvin koetellut turvallisuusperiaatteet ovat lueteltuna koneturvallisuus standardissa SFS-EN ISO 13849-2:2012. Standardin liitteissä on lueteltu periaatteet mekaaniselle pneumaattiselle, hydrauliselle ja sähköiselle teknologialle. Taulukossa 8 on lueteltu sähköiselle teknologialle yleisimpiä turvallisuuden perusperiaatteita. Taulukossa 9 on lueteltu muutamia hyvin koeteltuja turvallisuusperiaatteita. (SFS-EN ISO 13849-2:2012, 6)

Taulukko 8. Yleisimpiä turvallisuuden perusperiaatteita. (SFS-EN ISO 13849-2:2012, liite D, muokattu)

Turvallisuuden perusperiaate	Lisätieto
Oikea mitoitus ja muotoilu	Otetaan huomioon esim. kuormitus, jännitys, väsyminen, pinnankarheus, toleranssit ja valmistus.
Komponenttien ja /tai järjestelmän oikea valinta, yhdistely, järjestelyt, kokoonpano ja asennus	Sovelletaan valmistajan antamia käyttöön soveltamista koskevia ohjeita esim. tuoteluettelo, asennusohjeet, määrittelyt, ja noudatetaan hyvää insinöörikäytäntöä.
Oikeanlainen suojamaadoitus	Ohjauspiirin yksi puoli, kunkin sähkömagneettisen laitteen ohjauskelan tai muun sähkölaitteen yksi liitin yhdistetään suojamaadoituspiiriin (IEC 60204-1:2005 kohta 9.4.3.1).
Energiattomaksi tekemisen soveltaminen	Turvallinen tila saavutetaan kytkemällä kaikki asianomaiset laitteet jännitteettömiksi, ellei sähkön syötön katkeaminen aiheuta lisävaaraa. Esim. käyttämällä tuloissa avautuvia koskettimia ja käyttämällä releissä sulkeutuvia koskettimia (ks ISO12100:2010 kohta 6.2.11.3).
Ympäristöolosuhteiden sieto	Laite suunnitellaan siten, että se kykenee toimimaan kaikissa odotettavissa olevissa ympäristöissä ja missä tahansa ennakoitavissa olevissa epäsuotuisissa olosuhteissa, esim. lämpötila, kosteus, tärinä ja sähkömagneettinen häiriö.

Taulukko 9. Hyvin koetellut turvallisuusperiaatteet. (SFS-EN ISO 13849-2:2012, liite D, muokattu)

Hyvin koeteltu turvallisuusperiaate	Lisätieto
Koskettimet ovat mekaanisesti pakkotoimisia	Käytetään mekaanisesti pakkotoimisia koskettimia, esim. valvontatoiminnoissa luokkien 2, 3 ja 4 järjestelmissä (ks. IEC 60947-4-1:2001, liite F ja IEC 60947-5-1:2003 + A1:2009, liite L).
Kaapelivikojen välttäminen	Käytetään kahden vierekkäisen johtimen välisen oikosulun välttämiseksi suojavaipallista kaapelia, jossa jokaisen johtimen suojavaippa on maadoitettu.
Pakkotoimisuus	Ohjaus suoraan mekaanisen voiman vaikutuksella ilman joustavia elementtejä, esim. ilman jousta ohjauskappaleen ja koskettimien välissä (ks. ISO 14199:1998 kohta 5.1).
Vikaantumistavan suuntautuminen	Aina kun mahdollista, laitteen ja/tai piirin olisi vikaannuttava turvalliseen tilaan tai olosuhteeseen.
Ylimitoittaminen	Komponenttien kuormitusta pienennetään esimerkiksi puolittamalla koskettimien läpi kulkevan virran nimellisarvosta, kytkentätaajuus mitoitusarvosta.
Minimoidaan vikaantumisen mahdollisuus	Turvallisuuteen liittyvät toiminnot erotetaan muista toiminnoista.

Hyvin koettelulla komponentilla voidaan tarkoittaa aikaisemmin laajasti käytettyä komponenttia, jonka kokemukset ovat osoittanut hyväksi tietyissä sovelluksissa. Valmistamalla ja todentamalla komponentin luotettavuus ja toimivuus voidaan myös uudentyyppisiä komponentteja pitää hyvin koeteltuna. Monimutkaisia komponentteja, jotka sisältävät elektroniikkaa ei voida olettaa hyvin koetelluiksi. Hyvin koeteltuja komponentteja ovat muun muassa hätäpysäytyslaite, pakkotoiminen kosketin, lämpökytkin ja painekytkin. (SFS-EN ISO 13849-2:2012, liite D, muokattu) Hyvin koeteltujen komponenttien oikea käyttö ja toimintaympäristö on oltava huomioitava, sillä eri ympäristöissä voi sama komponentti voi olla hyvin koeteltu tai systemaattinen suunnitteluvirhe.

$\mathrm{MTTF_D}$- arvo arvioidaan ensisijaisesti ohjausjärjestelmien osien valmistajalta saatujen parametrien perusteella. Mikäli tietoa valmistajalta ei ole, noudatetaan standardin SFS-EN ISO 13849-1: 2015 liitteitä C ja D. Kyseisissä liitteissä esitetään yleisiä $\mathrm{MTTF_D}$- ja $\mathrm{B_{10D}}$-arvoja tietyille komponenteille tietyissä olosuhteissa. Mikäli tietoa ei löydy liitteistä valitaan komponenteille $\mathrm{MTTF_D}$-arvoksi 10 vuotta. (SFS-EN ISO 13849-1:2015, kohta 4.5.2.)

Sähkömekaanisille komponenteille, joiden $\mathrm{MTTF_D}$ riippuu käyttökertojen määrästä valmistajat ilmoittavat usein pelkän $\mathrm{B_{10D}}$-arvon. $\mathrm{B_{10D}}$ tarkoittaa käyttökertojen lukumäärää, kunnes 10 % komponenteista on vikaantunut vaarallisesti. Pelkkä $\mathrm{B_{10}}$-arvo tarkoittaa käyttökertojen lukumäärää, kunnes 10 % komponenteista vikaantuu ottamatta huomioon vikaantumisen vaarallisuutta. (SFS-EN ISO 13849-1:2015, kohta C.4.2.)

Komponenttivalmistajat selvittävät $\mathrm{B_{10D}}$-arvon useimmiten laboratorio- tai kenttätutkimuksilla. Esimerkki: laboratoriossa testataan 1000 kpl NC- koskettimia. Kun 100 kpl koskettimista on vikaantunut vaarallisesti, on sen hetkinen käyttökertojen lukumäärä kyseisen koskettimen $\mathrm{B_{10D}}$-arvo. (Hauke, Schaefer, Apfeld, Werner, Bömer, Huelke, Steimers, Borowski, Büllesbach, Dorra, Foermer-Schaefer, Uppenkamp, Lohmaier, Heimann, Köhler, Zilligen, Otto, Rempel & Reuß 2019, kohta D.2.4.1.)

Ellei tarkempaa tietoa ole, voidaan konservatiivisesti olettaa vaarallisia vikaantumisia olevan 50 % kaikista vikaantumisista, jolloin $B_{10D} = 2 * B_{10}$. Toinen parametri laskettaessa $MTTF_D$- arvoa on n_{op} eli keskimääräinen toimintajaksojen määrä vuodessa. Standardissa esitetään n_{op}:n laskettavan kaavan 4 mukaisesti:

$$n_{op} = \frac{d_{op} * h_{op} * 3600 s/h}{t_{toimintajakso}} \quad (4)$$

missä n_{op} = keskimääräinen toimintajaksojen määrä vuodessa

d_{op} = keskimääräinen toiminta-aika, päivää vuodessa

h_{op} = keskimääräinen toiminta-aika, tuntia päivässä

$t_{toimintajakso}$ = keskimääräinen aika peräkkäisten toimintajaksojen välillä, sekuntia

Keskimääräinen aika kunnes 10 % komponenteista vikaantuu vaarallisesti (T_{10D}) on yleisesti ottaen komponenttien toiminta-aika, jolloin vaarallisten vikaantumisten taajuus (λ_D) voidaan olettaa pysyvän vakiona. Näin ollen T_{10D}-aika rajoittaa komponentin ja myös koko turvatoiminnon elinikää. Kaavan 5 mukaisesti saadaan laskettua $MTTF_D$:

$$MTTF_D = \frac{T_{10D}}{0{,}1} = \frac{B_{10D}}{0{,}1 * n_{op}} = \frac{1}{\lambda_D} \quad (5)$$

missä $MTTF_D$= keskimääräinen aika vaaralliseen vikaantumiseen, vuotta

T_{10D}= keskimääräinen aika kunnes 10 % komponenteista vikaantuu vaarallisesti

B_{10D} = käyttökertojen lukumäärä kunnes 10% komponenteista vikaantuu vaarallisesti

n_{op} = keskimääräinen toimintajaksojen määrä vuodessa

λ_D = vaarallinen vikaantumistaajuus, tunnissa

On huomioitavaa käytettäessä parametria λ_D yksikkönä on tunnit, joten muunnos vuosiin vaaditaan. Laskettaessa $MTTF_D$- arvoa on syytä huomioida, ettei T_{10D}- ajan ylittyessä ja λ_D- arvon samalla kasvaessa, lasku ole enää pätevä. (SFS-EN ISO 13849-1:2015, kohta C.4.2.)

2.7.2 Yhteisvikaantuminen

Yhteisvikaantuminen tarkoittaa turvallisuuteen liittyvän ohjausjärjestelmän kaikkien toiminnallisten kanavien ja/tai testauskanavan vikaantumista yksittäisen tapahtuman takia (SFS-EN ISO 13849-1:2015, kohta 3.6.10). Yhteisvikaantumisen syynä voi olla ympäristön olosuhteet kuten lämpötila tai voimakas elektromagneettinen kenttä, kun taas systemaattiset yhteisvikaantumiset saattavat johtua tietyissä tilanteissa ilmenevien ohjelmointivirheiden vuoksi (Apfeld & muut 2015, 239).

Yhteisvikaantumista vastaan vaaditaan toimenpiteitä luokan 2, 3 ja 4 turvallisuuteen liittyvissä ohjausjärjestelmissä, kuten opinnäytetyön kohdassa 2.7.1 kerrotaan. Näin ollen yhteisvikaantumista on tarkasteltava, kun on käytössä useampi kuin 1 kanava.

Standardissa SFS-EN ISO 13849-1:2015 (liite F) opastetaan käyttämään laadullista arviointimenetelmää, jossa esitetään yhteisvikaantumista estäviä toimenpiteitä sovellettuna erityisesti koneisiin. Jokaisesta kokonaan suoritetusta toimenpiteestä saadaan tietty määrä pisteitä ja lopuksi pisteet lasketaan yhteen. Maksimipisteet ovat 100, joista vähintään 65 on saatava täyttääkseen vaatimukset yhteisvikaantumisen estämisestä.

Erottelulla suojataan kukin kanava yhteisvikaantumisella. Voidaan käyttää fyysistä erottelua esim. erilleen sijoitetuilla johtoreiteillä/instrumenteilla. Merkittävä toimi on diversiteetti, joka käytännössä tarkoittaa erilaisten teknologioiden tai mitattavien suureiden käyttämistä kummallakin kanavalla. (SFS-EN ISO 13849-1:2015, liite F)

2.7.3 Diagnostiikka

Standardissa SFS-EN ISO 13849-1:2015 diagnostiikan kattavuus (Diagnostic Coverage, DC) määritellään olevan diagnostiikalla paljastuvien vaarallisten vikojen ja kaikkien vaarallisten vikojen suhde, joka kuvaa kuinka tehokkaasti diagnostiikka paljastaa vaarallisia vikoja. Standardissa esitetään yksinkertainen tapa arvioida diagnostiikan kattavuutta, eikä näin ollen tarvitse tehdä työläitä vika- ja vaikutusanalyyseja. (SFS-EN ISO 13849-1:2015, kohta 3.1.26 ja 4.5.3)

Suoritustasoa arvioidessa tarvitaan kuitenkin keskimääräinen diagnostiikan kattavuus ($\mathrm{DC_{avg}}$), joka lasketaan kunkin turvatoimintoon osallistuvan osien diagnostiikan kattavuuksien keskiarvo kaavan 6 mukaisesti (SFS-EN ISO 13849-1:2015, kohta E.2.) Taulukossa 10 esitetään diagnostiikan kattavuuksien jakautuminen neljään verbaaliseen tasoon standardin SFS-EN ISO 13849-1:2015 mukaisesti.

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \quad (6)$$

missä DC_{avg} = turvatoiminnon keskimääräinen diagnostiikan kattavuus

DC_1 = ohjausjärjestelmän osan 1 diagnostiikan kattavuus

DC_2 = ohjausjärjestelmän osan 2 diagnostiikan kattavuus

DC_N = ohjausjärjestelmän osan N diagnostiikan kattavuus

$MTTF_{D1}$ = ohjausjärjestelmän osan 1 keskimääräinen aika vaaralliseen vikaantumiseen

$MTTF_{D2}$ = ohjausjärjestelmän osan 2 keskimääräinen aika vaaralliseen vikaantumiseen

$MTTF_{DN}$ = ohjausjärjestelmän osan N keskimääräinen aika vaaralliseen vikaantumiseen

Taulukko 10. Diagnostiikan kattavuuden tasot (SFS-EN ISO 13849-1:2015, kohta 4.5.3, muokattu)

Verbaalinen DC- taso	Vaihteluväli
Ei lainkaan	DC < 60 %
Matala	60 % ≤ DC < 90 %
Keskitaso	90 % ≤ DC < 99 %
Korkea	99 % ≤ DC

3 Laskentaohjelmistojen vertailu ja valinta

Tarkoitus oli selvittää saatavilla olevat toiminnallisen turvallisuuden SIL- ja PL- tasojen laskentaan tarkoitetut tietokoneohjelmistot. Ohjelmistoja vertailtaessa huomioitavia asioita oli muun muassa:

1. Standardituki:
   Minkä standardin tai standardien mukaan ohjelmistolla pystyy suorittamaan laskennan?

2. Käyttöliittymä:
   Onko käyttöliittymä selkeä ja käyttäjäystävällinen?

3. Ohjeet ja tukipalvelut:
   Onko ohjelmistossa saatavilla hyvät käyttöohjeet ja teknistä tukea?

4. Kustannukset:
   Mitä hankinta- ja ylläpitokustannuksia ohjelmistoon liittyy?

5. Raportointi:
   Onko ohjelmiston generoima raportti asianmukainen ja tarvittavassa formaatissa?

6. Mukautuvuus.
   Soveltuuko ohjelmisto useille soveltamisalueille (Kone- ja prosessisektori)?

Laskentaohjelmistoja ei vuonna 2023 ollut runsain määrin saatavilla. Uskoisin kuitenkin tarjonnan vastaavan kysyntään. Tässä opinnäytetyössä esitellyt laskentaohjelmistot ovat yleisesti käytössä olevia. Vuonna 2023 ohjelmistoversiot olivat seuraavat:

1. SISTEMA Versio 2.0.8 Build 4
2. ABB FSDT-01 Versio 1.2.0.2
3. Pilz PAScal Versio 1.9.1

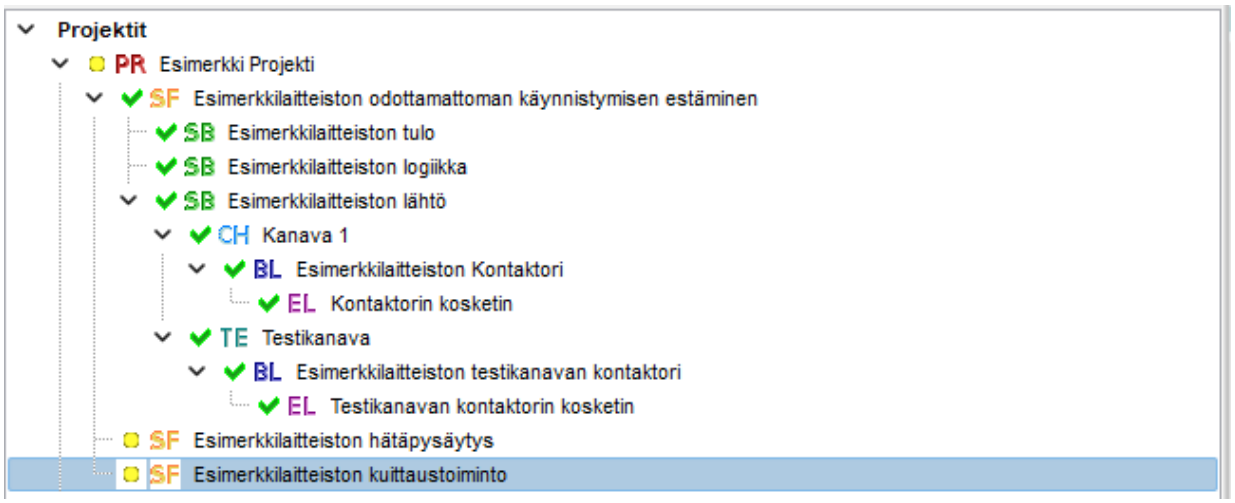
3.1 SISTEMA

Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA) on Saksan työturvallisuuden ja työterveyden vakuutusinstituution (IFA) toimeksiannosta kehitetty sovellus koneturvallisuuden riskiarviointiprosessista aina toiminnallisen turvallisuuden todentamisprosessiin. Sovellusta voi käyttää maksuttomasti kaupallisiin tarkoituksiin ja se noudattaa standardin SFS-EN ISO 13849-1 mukaista toiminnallisen turvallisuuden arviointia. (Software-Assistent SISTEMA n.d.)

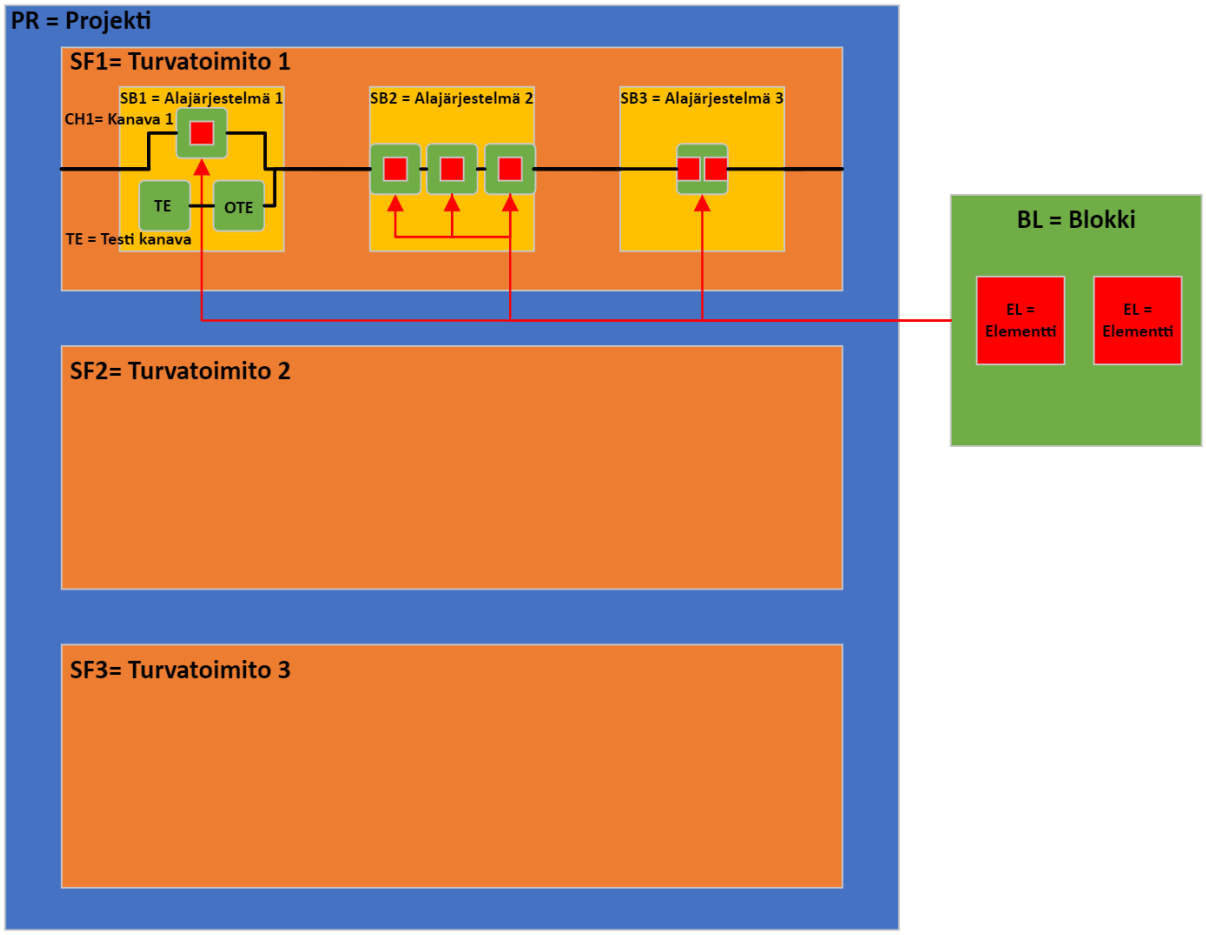
SISTEMAn on hyödyksi turvallisuuteen liittyvien ohjausjärjestelmien suunnittelijoille. SISTEMAlla saadaan tulostettua raportti koko turvallisuuteen liittyvästä ohjausjärjestelmästä. Kuten aiemmin mainittu, ohjelmisto perustuu standardiin SFS-EN ISO 13849-1, joten siinä myös käytetään nimettyjä rakenteita (luokkia). SISTEMAssa tiedot voi syöttää ohjelmaan hyvinkin spesifisti elementin tarkkuudella tai etukäteen suunnitellun alajärjestelmän tiedot, silloin kun komponenttivalmistaja ilmoittaa turvallisuuteenliittyvät parametrit sekä vastaa niiden täyttymisestä.

Suurena aikaa säästävänä ominaisuutena on tietenkin automaattinen ja jatkuvatoimiminen laskenta monimutkaisista matemaattisista malleista ja kaavoista. SISTEMA esittää muokattaessa ja lisätessä TLJ:n osia koko turvatoiminnon saavutetun suoritustason sekä $\mathrm{PFH_D}$- arvon. Muihin laskentasovelluksiin verrattuna SISTEMAssa on ohjelmiston sisällä hyvät ohjeet, kullekin projektin vaiheelle. Ohjeet esitetään ruudulla syötettäessä tulotietoja, kuten esimerkiksi $MTTF_D$- tai DC-arvoja. Ennen kaikkea SISTEMAn ohjelmisto on käännetty suomen kielelle.

SISTEMAssa turvatoiminnon osat esitetään kuvion 6 näköisessä projektipuussa. Ohjelmistossa on yhteensä 6 eri hierarkkisella tasolla olevaa osaa, joita havainnollistetaan kuviossa 7. Ylimmäinen taso on projekti (PR). Projektin sisällä voi olla useita turvatoimintoja (SF). Turvatoiminto koostuu vähintään yhdestä alajärjestelmästä (SB). Alajärjestelmän sisällä voi olla joko yksi tai kaksi kanavaa (CH), jotka koostuvat blokeista (BL). Blokit voivat taas sisältää useita elementtejä (EL). Jos suunniteltu arkkitehtuuri sisältää testikanavan, kutsutaan testauslaitteistoa (TE) ja testauslaitteiston lähtöjä (OTE).



Kuvio 6. Näkymä SISTEMAn projektipuusta



Kuvio 7. SISTEMAn osien hierarkiset rakenteet

SISTEMAssa voi luoda ja tallentaa omia alajärjestelmiä, joka on hyödyllistä etenkin projektien ollessa samankaltaisia. Toinen vaihtoehto on ladata komponenttivalmistajien omia kirjastoja, joissa komponentteihin on sisällytetty kaikki oleelliset turvallisuuteen liittyvät parametrit. Valmistajien kirjastot sisältävät komponentin mukaan joko valmiita alajärjestelmiä, blokkeja tai elementtejä. Virheen mahdollisuus syöttäessä manuaalisesti tietoja SISTEMAan on suuri verrattuna kopioidessa projektiin valmiita komponentteja kirjastosta. SISTEMAn omien kirjastojen tiedostoformaatti on ”.slb”, mutta on mahdollista käyttää maailmanlaajuisen VDMA 66413-spesifikaation mukaisia kirjastoja. (Huelke, Hauke & Lungfiel 2016, kohta 1 ja 3.)

VDMA 66413-spesifikaatio on kehitetty maailmanlaajuiseksi tavaksi tallentaa toiminnalliseen turvallisuuteen liittyvien komponenttien, laitteiden ja muiden asiaan liittyvien osien ominaisarvoja. Tietoformaatti soveltuu muun muassa konevalmistajien, komponenttivalmistajien ja laskentasovellusten toimittajien käyttöön. Tietokanta on XML-formaatissa. (VDMA 66413 2012.)

3.2 ABB FSDT-01

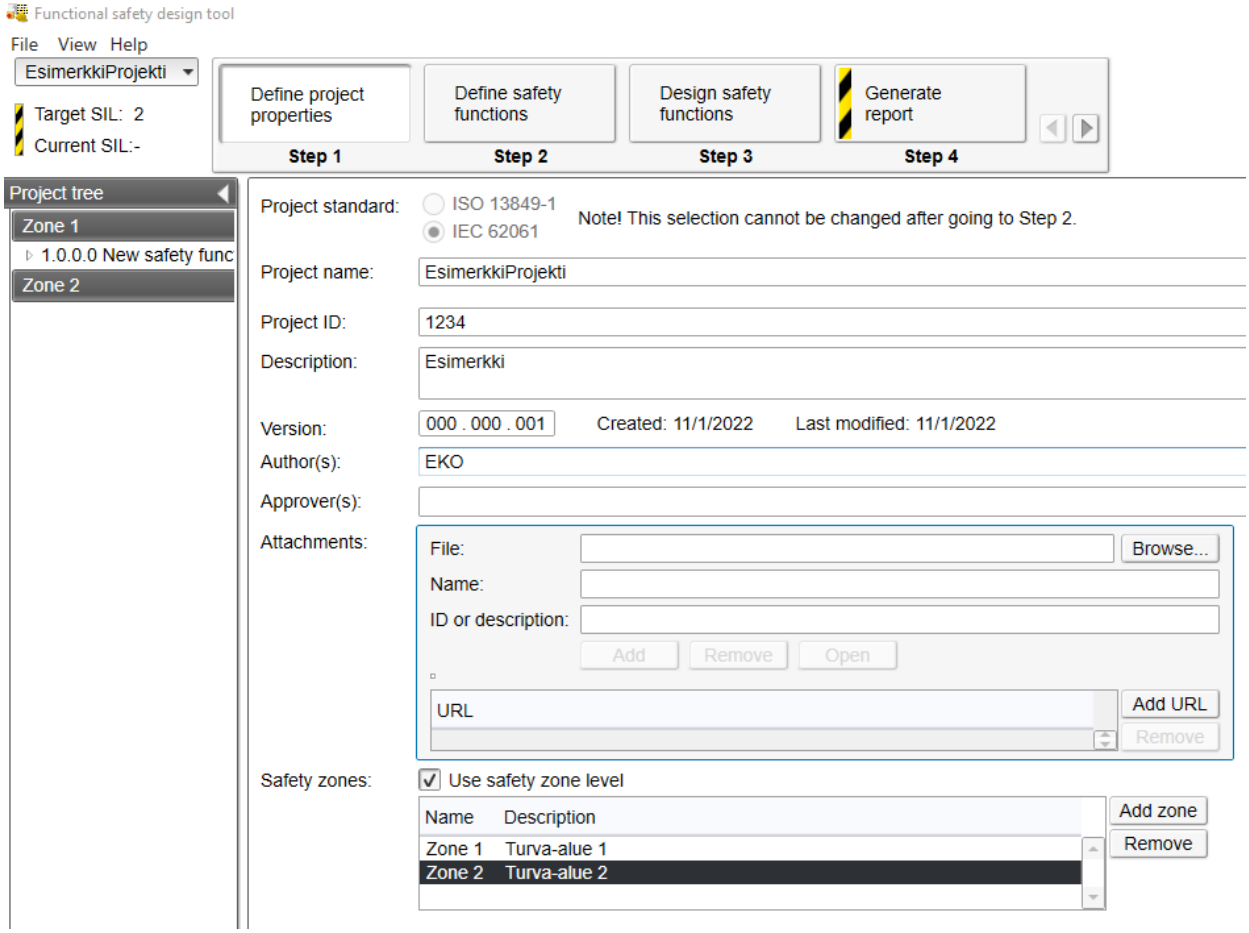
ABB:n sovellus koneiden toiminnallisen turvallisuuden mallintamiseen, suunnitteluun, laskemiseen ja todentamiseen on Functional safety desing tool (FSDT-01). Ohjelmisto perustuu molempiin koneturvallisuuden standardeihin: SFS-EN ISO 13849-1 ja SFS EN IEC 62061. Ohjelmisto on TÜV Nordlaitoksen sertifioima standardin SFS-EN IEC 61508-3: 2011 kohdan 7.4.4 ja T2-luokan mukainen ”ohjelmiston ei käytön aikainen tukityökalu” ylimmillään PLe- tai SIL3-tasoon saakka. (User’s manual Functional safety design tool 2019, 10–12.)

Suunnitteluprosessi tällä ohjelmistolla jakautuu neljään eri vaiheeseen:

1. Projektin tietojen määrittäminen
2. Turvatoimintojen määrittäminen
3. Turvatoimintojen suunnittelu
4. Raportin generoiminen ja tulostaminen

Kuvion 8 mukaisessa ensimmäisessä vaiheessa luodaan projekti, valitaan noudatettavaksi standardiksi joko SFS-EN ISO 13849-1 tai SFS EN IEC 62061 ja annetaan mahdollisesti valinnaisia tietoja.

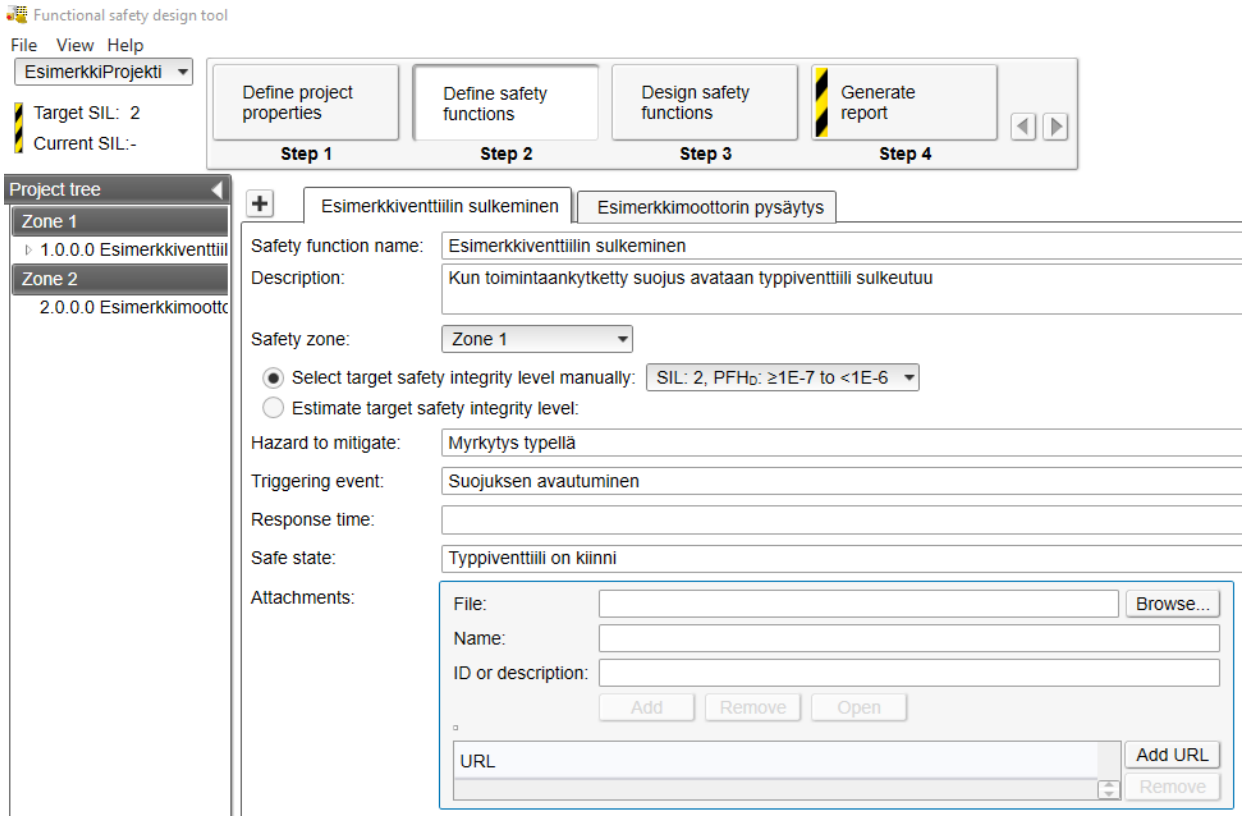
Valinnaisiin tietoihin lukeutuu muun muassa turva-alueet, joihin turvatoiminnot voidaan kohdentaa. Ensimmäinen eroavaisuus verrattuna SISTEMAan on mahdollisuus edetä käyttäen standardia SFS EN IEC 62061.



Kuvio 8. ABB FSDT-01-projektin tiedot

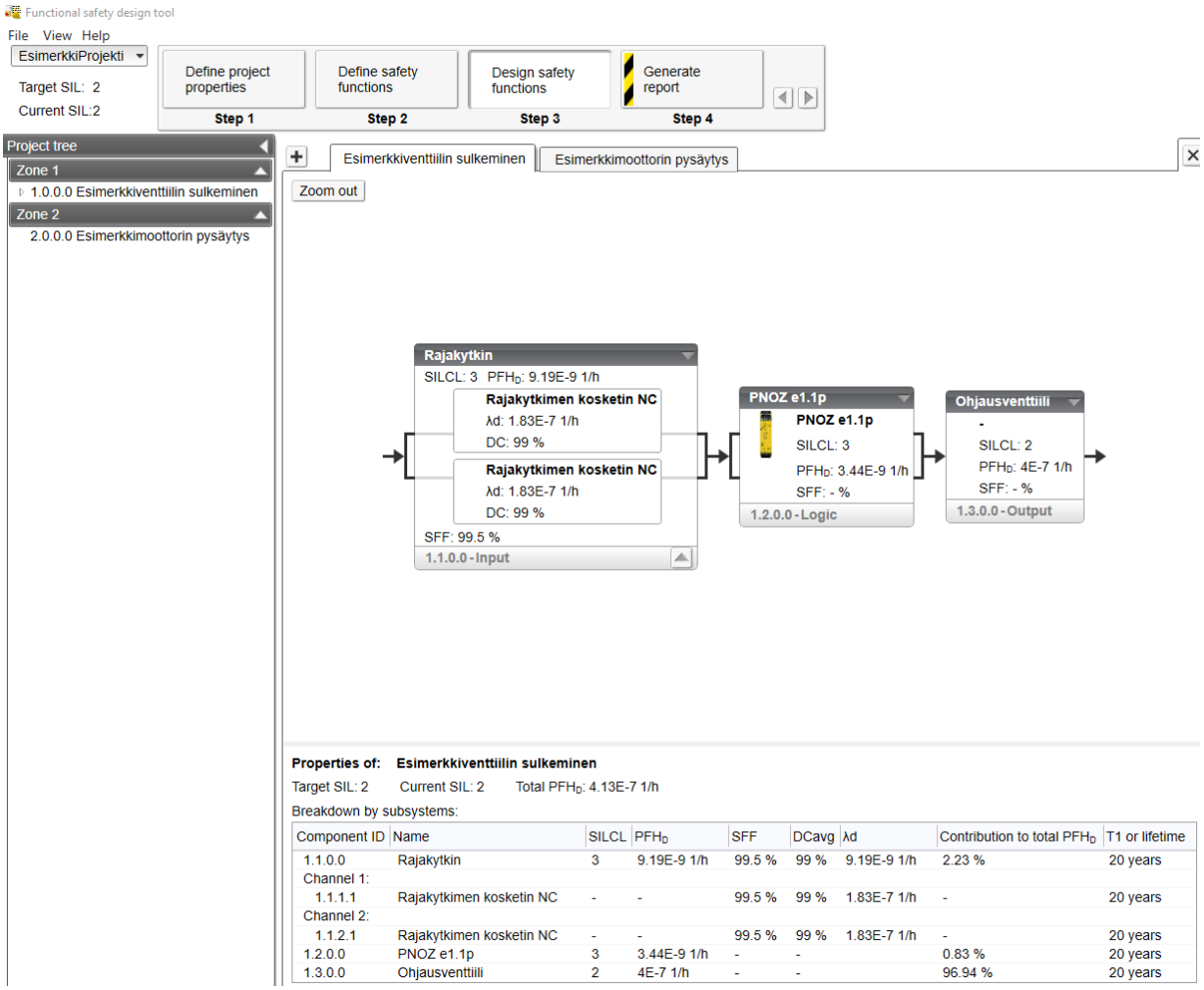
Kun projekti on saatu luotua, luodaan kuvion 9 mukaisesti turvatoiminnot. Tavoitteellinen PL tai SIL valitaan joko käsin tai arvioidaan riskigraafista tai matriisista. Valinnaisina tietoina turvatoiminnolle voidaan syöttää vaara, turvatoiminnon laukaiseva tekijä, vasteaika ja turvallinen tila. Mikäli

turva-alueet ovat valittu käyttöön luodessa projektia, kohdennetaan turvatoiminnot tässä vaiheessa omille turva-alueilleen.



Kuvio 9. ABB FSDT-01 turvatoimintojen määrittely

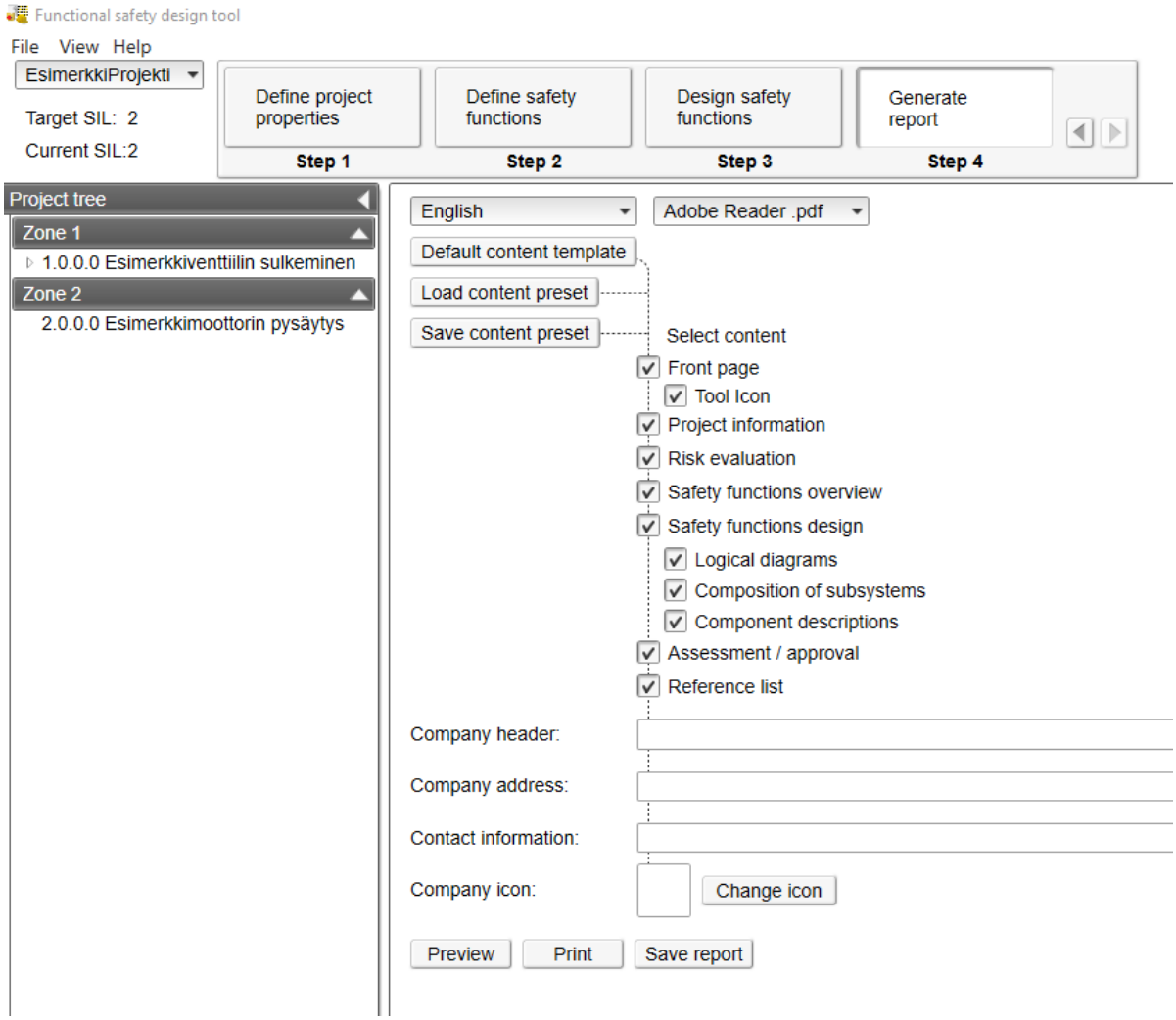
Kolmannessa vaiheessa aloitetaan turvatoimintojen suunnittelu. Aluksi voidaan valita yleisimmin käytössä olevia malleja, joihin on helppo lisätä alajärjestelmien tiedot. ABB:n ohjelmistossa turvatoimintojen alajärjestelmät ja elementit esitetään käyttöliittymässä graafisesti, mikä erottuu edukseen verrattuna SISTEMAan. On mahdollista luoda 2-kanavaisia alajärjestelmiä, joissa on useita sarjaan kytkettyjä elementtejä. Kuviossa 10 on näkymä turvatoimintojen suunnitteluun. Tässä esimerkissä on suojus, turvarele ja ohjausventtiili.



Kuvio 10. ABB FSDT-01 turvatoimintojen suunnittelu

Neljäntenä ja viimeisenä vaiheena on raportin generoiminen. Pakollisena valintana on raportin kieli ja tiedostoformaatti. Toistaiseksi raportin tiedostoformaatti on ainoastaan PDF. Raportin sisältää oletuksena kaiken luodun informaation, mutta sisällöstä voidaan rajata pois osa tiedoista en-

nen tulostusta kuvion 11 mukaisesti. Valmiiseen raporttiin tulee oma kenttä hyväksyntää ja allekirjoitusta varten.



Kuvio 11. ABB FSDT-01-raportin generointi

Kuin SISTEMAssa, myös ABB:n ohjelmistossa on mahdollista käyttää valmistajien tarjoamia komponenttikirjastoja. Kirjastot ovat aiemmin mainitun VDMA 66413-spesifikaation mukaisia. Itse luotuja alajärjestelmiä ja elementtejä voi tallentaa kirjastoihin myöhempää käyttöä varten.

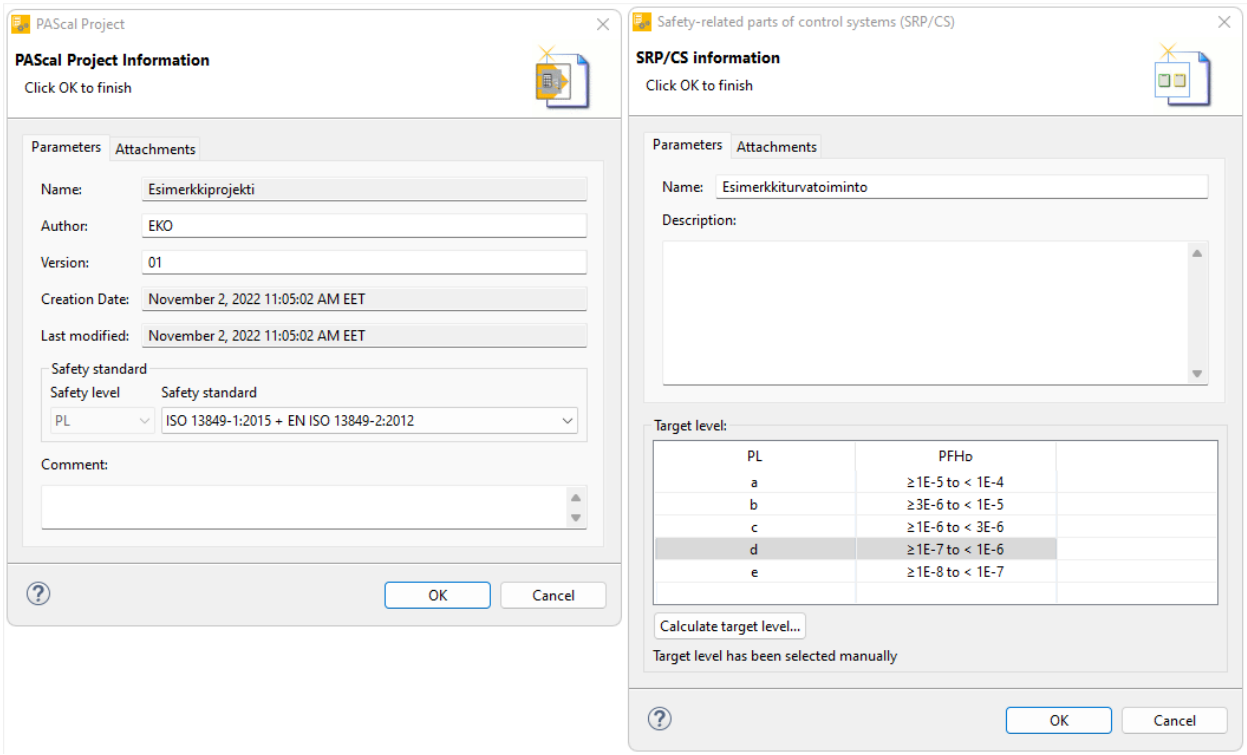
3.3 PILZ PAScal

PAScal Safety Calculator on turvakomponenttivalmistaja Pilz:n ohjelmisto standardin SFS-EN ISO 13849-1 tai SFS-EN-IEC 62061 mukaiseen turvatoimintojen PL/SIL arviointiin ja todentamiseen. Ohjelmistosta on ilmainen versio saatavilla rajoitetuin ominaisuuksin. Saadakseen kaikki ominaisuudet käyttöön on ostettava lisenssi. Myös tämä ohjelmisto tukee VDMA-spesifikaation mukaisia komponenttikirjastoja. (Calculate the performance level using the PAScal Safety Calculator n.d)

Käytännössä ilmaisen version ominaisuudet ovat niin rajalliset, että se pakottaa ostamaan lisenssin, mikäli ohjelmistoa on tarkoitus käyttää kaupallisiin tarkoituksiin. Demo- versiolla voi ainoastaan avata standardin SFS-EN-IEC 62061 mukaisen projektin. Projekteja ei voi olla auki, kuin yksi kerrallaan ja muokattavien turvatoimintojen määrä on rajoitettu kymmeneen. Vuonna 2023 yhden työaseman lisenssi, jolla saadaan kaikki ohjelmiston ominaisuuden käyttöön maksaa verkkokaupan mukaan 397.51 €. Toiselle työasemalle lisenssin hinta on 264.60 €. Rajoittamattomat käyttäjät/työasemat saadaan käyttöön ”Multi user”-lisenssillä, joka maksaa 2459.06 €.

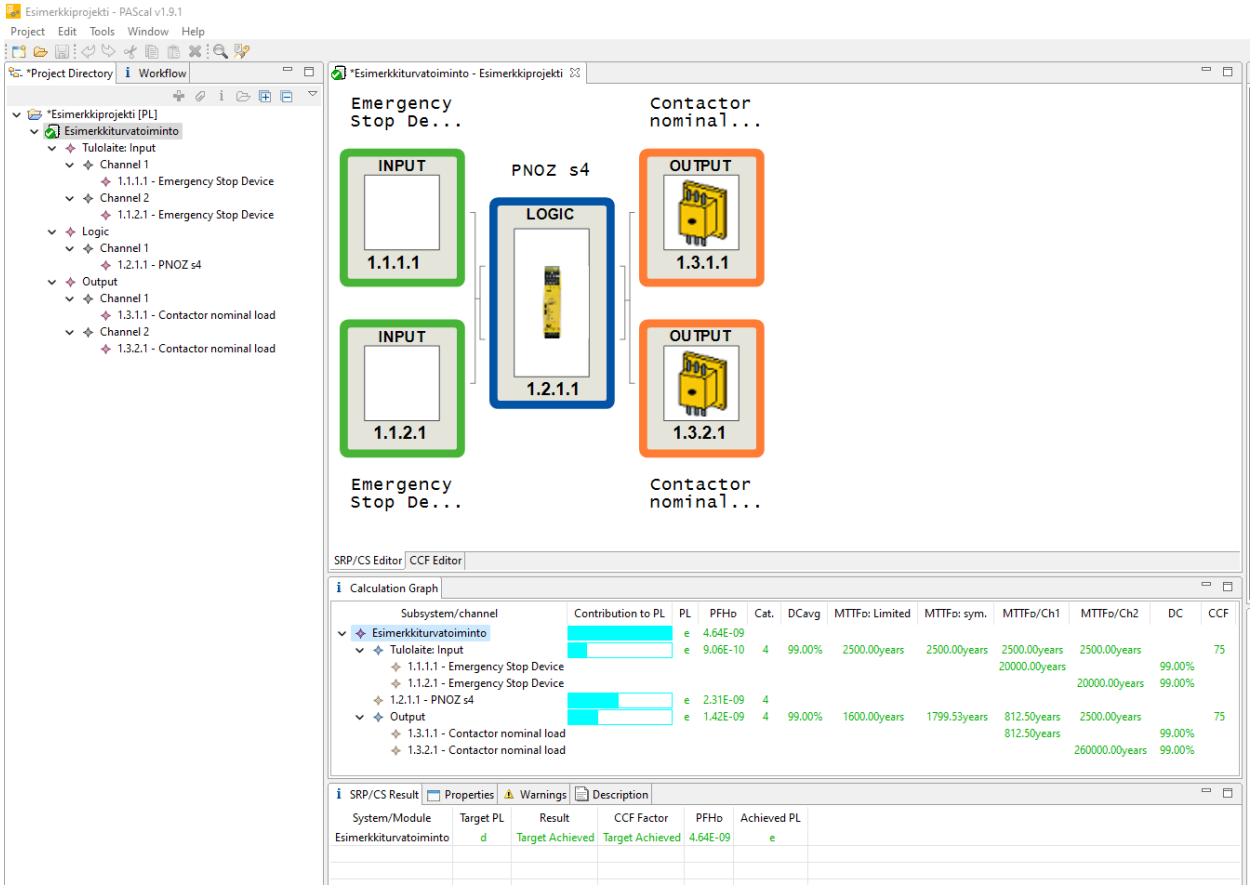
Ohjelmisto laskee annettujen tietojen perusteella turvatoiminnolle $\mathrm{PFH_D}$- arvon sekä saavutettavan suoritustason tai turvallisuuden eheyden tason. Ohjelmistolla on mahdollista luoda omia komponenttikirjastoja. Poikkeavuutena ABB:n ohjelmistoon PAScal:lla voi käyttää SISTEMAn kirjastoja (.slb), sillä ohjelmisto kääntää ne VDMA-spesifikaation mukaiseksi. SISTEMAn kirjastoista puuttuu osa tiedoista ja ne täytyy manuaalisesti määrittää käännettäessä. (PAScal Online help from V1.9.1 n.d.)

PAScal:ssa luodaan aluksi projekti ja valitaan, kumman standardin mukaisesti edetään. Verrattuna muihin ohjelmistoihin, PAScal:ssa on suppeasti kenttiä, joihin kirjoittaa yksityiskohtaista tietoa projektista tai turvatoiminnoista (ks. kuvio 12). Kuin muissakin ohjelmistoissa, niin PAScal:ssa on mahdollista lisätä projektiin, turvatoimintoihin, alajärjestelmiin tai elementteihin liitetiedostoja esimerkiksi komponenttien sertifikaateista tai datalehdistä.



Kuvio 12. Pilz PAScal-projektin ja turvatoiminnon luominen

Turvatoimintojen laskennan tulos näytetään kuviossa 13 alimmassa kentässä, jossa vihreällä värillä ilmoitetaan kaiken olevan kunnossa ja punainen väri indikoi virheitä tai puutteellisia syötteitä. Keskimmäisessä kentässä näytetään alajärjestelmien osien turvallisuuteen liittyvät arvot sekä sinisin palkein $\mathrm{PFH_D}$-arvon jakauma eri alajärjestelmille. Ylimmässä kentässä tapahtuu turvatoiminnon osien luominen loogiseen blokkikaavioon. Turvatoiminnon osat voidaan raahata komponenttikirjastosta, tai syöttää tiedot manuaalisesti. Vasemmassa kentässä on puukaavio projektista, joka on jokaisessa tässä opinnäytetyössä vertailtavissa laskentaohjelmistoissa samankaltainen.



Kuvio 13. Pilz PAScal turvatoiminnon suoritustason laskenta

3.4 Laskentaohjelmistojen yhteenveto

Liitteessä 2 on pisteytetty tarkasteltavien laskentaohjelmistojen ominaisuudet. Vertailtavista ohjelmistoista SISTEMA ja ABB FSDT-01 olivat maksuttomia. Pilz PAScal:n ilmainen versio on rajatuin ominaisuuksin lähinnä kokeilua varten tarkoitettu. Näin ollen PAScal:iin olisi ostettava lisenssi muuhun kuin demonstraatiokäyttöön. Tarkasteltavilla ohjelmistoilla ei voinut laskea harvojen vaateiden turvatoimintoja.

Vertailussa jokainen ominaisuus pisteytettiin asteikolla 1–5. Suurin saavutettavissa oleva pistemäärä oli tällä arviointitaulukolla 100 pistettä Liitteen 2 taulukossa on esitetty kunkin ominaisuuden pisteytys ja perustelut ohjelmistokohtaisesti. Vertailun perusteella eniten kokonaispisteitä sai SISTEMA 80. Pilz:n ohjelmisto kokonaispistemäärällä 78 ja ABB:n ohjelmisto 72 pisteellä eivät pärjänneet SISTEMAlle. Tämä vertailu ei suoraan osoita ohjelmistojen soveltuvuutta eri käyttötarpeisiin, mutta kuitenkin antaa yleisen käsityksen kunkin ohjelmiston ominaisuuksista. Vertailun pisteytystä ei ole painotettu osa-alueittain ja näin ollen käyttäjävaatimusten vaikutusta ei ole huomioitu.

3.4.1 Standardituki

Ensimmäisen pisteytettävän ominaisuuden kohdalla arvioitiin ohjelmistojen kykyä laskea eri standardien mukaisesti. Ohjelmistoista ABB:llä ja Pilz:llä oli tuki molempiin koneturvallisuuden standardeihin. SISTEMA tuki laskentaa vain mukaisesti SFS-EN ISO 13849-1:2015. SISTEMAan oli silti mahdollista syöttää sellaisten komponenttien tietoja, jotka ovat toisen standardin mukaisia. Toisin sanoen SISTEMA osaa muuttaa SIL-tason vastaamaan PL-tasoa. Mikäli ABB:n tai Pilz:n ohjelmistolla haluttaisiin lisätä SFS-EN ISO 13849-1 mukaiseen projektiin komponentti, jolle valmistaja on ilmoittanut pelkästään SIL-tason ja $\mathrm{PFH_D}$-arvon, täytyy se manuaalisesti kääntää vastaamaan PL-tasoa. Mikäli vaatimuksena on saada raportti, jossa on SIL-tasot, ei SISTEMA sovellu siihen käyttötarkoitukseen.

3.4.2 Käyttöliittymä

Toinen pisteytettävä ominaisuus koski ohjelmiston käyttöliittymää. Projektipuu oli hyvin saman kaltainen kaikissa tarkastelluissa ohjelmistoissa. Sinänsä projektipuu on toimiva ratkaisu tähän käyttötarkoitukseen ja mielestäni sitä ei voi paremmaksi kehittää. SISTEMA oli ainut, jossa ei ollut graafista esitystä turvatoiminnon osista. Sen sijaan ABB:n ja Pilz:n ohjelmistoissa turvatoiminnon osat esitettiin loogisena blokkikaaviona. Molempien ohjelmistojen blokkikaavioissa oli esitetty komponentin pikkukuva (thumbnail) sekä toiminto (input, logic tai output), mutta vain ABB:n blokkikaaviossa esitettiin turvallisuuteen liittyvät ominaisarvot. Vain Pilz:n blokkikaaviossa toiminnon tyyppi oli havainnollistettu värein, kuvion 13 mukaisesti.

Mielestäni tärkeä ominaisuus oli turvatoiminnon $\mathrm{PFH_D}$-arvon jakautumisen esittäminen joko prosentuaalisesti tai visuaalisesti, koska sillä pystyy helposti päättelemään, mikä komponentti on suurimmassa roolissa eli ”pullonkaula”. Näin ollen tiedetään heti, mikä komponentti kannattaisi vaihtaa luotettavampaan laskennan osoittaessa, ettei turvatoiminto saavuta sille vaadittua turvallisuustasoa. Ohjelmistoista parhaiten tätä ominaisuutta toteutti Pilz, jossa $\mathrm{PFH_D}$-arvon jakautuminen esitettiin sekä visuaalisesti että prosentuaalisesti. SISTEMAssa esitettiin kunkin komponentin $\mathrm{PFH_D}$-arvo, mutta jakautumista ei esitetty prosentuaalisesti eikä visuaalisesti. ABB:n ohjelmistossa $\mathrm{PFH_D}$-arvon jakautuminen esitettiin prosentuaalisesti.

SISTEMAn käyttöliittymän kieli vaikutti pisteytykseen positiivisesti, sillä se oli ainut ohjelmisto, joka oli käännetty suomen kielelle. Vaikka Pilz:n kielivalikoima oli laaja, ei sillä tässä käyttötarkoituksessa ollut merkitystä. Monikielisyys saattaisi olla relevantti ominaisuus, mikäli vaatimus tulisi asiakkaalta eli raportin käyttäjältä.

SISTEMA erottui edukseen monipuolisilla tietokentillään. Projektiin, turvatoimintoon, alajärjestelmään ja elementtiin oli mahdollista syöttää muun muassa positio, revisio ja lisätietoja. Erityisen tärkeä ominaisuus toimeksiantajan asiakasprojekteissa on turvatoimintojen komponenttien yksilöinti positionumerolla. SISTEMAlla positiotunnukselle oli oma kenttä. ABB:lla eikä PilZ:lla kyseistä kenttää ei ollut, vaan ”Component ID” oli juokseva merkkijono numeroita ja pisteitä. Ja näin ollen komponenttien positiotunnus saatiin lisättyä vain ”kuvaus”-kenttään.

3.4.3 Ohjeet ja tukipalvelut

Suurin hajonta pisteissä oli osiossa ”Ohjeet ja tukipalvelut”. SISTEMAn ohjelmisto oli käännetty hyvälle suomen kielelle. Vaikka englannin kielellä pärjää hyvin, on suomenkielinen ohjelmisto ehdottomasti hyvä ominaisuus. SISTEMAn ohjeet olivat selkeät ja eivät ainoastaan keskittynyt itse ohjelmiston käyttämiseen, vaan myös teoriaan laskennan taustalla. IFA:n toimesta on julkaistu yhteensä kuusi opastavaa ”keittokirjaa”, joiden avulla SISTEMAn käyttäjät voivat paremmin ymmärtää ohjelmiston toimintaa laskennan taustalla. IFA on julkaissut koneiden toiminnallista turvallisuutta koskevan raportin (Apfeld ja muut 2019), jossa on yhteensä 38 erilaista turvatoimintoa ja niihin liittyvät SISTEMA-projektit. Lisäksi SISTEMAn 4. ”keittokirja” sisältää muutaman esimerkkiprojektin (Hauke, Apfeld, Huelke, Bömer & Werner 2020).

Käyttäessä mitä tahansa ohjelmistoa, vaatii se käyttäjältä tietämystä laskennan taustalla olevasta ajattelutavasta ja standardeista. Tällaisen tietämyksen kehittämiseksi SISTEMA tarjosi kattavat materiaalit. ABB: n ohjeissa oli vain välttämätön tieto ohjelmiston käyttämiseksi. Pilz:n ohjeissa oli jonkin verran avattu teoriaa laskennan taustoista.

3.4.4 Raportti

Jokaisesta tarkasteltavasta laskentaohjelmistosta saa generoitua raportin, joka sisältää muun muassa projektin, turvatoimintojen ja komponenttien tiedot. SISTEMAssa yksityiskohtaisuuden asteen voi valita generoidessa raporttia. Ja näin ollen riippuen tarpeesta raporttiin voidaan sisällyttää esimerkiksi komponenttien osanumerot, joita voidaan tarvittaessa hakea myöhemmin PDF-tiedostosta. ABB:n raportin yksityiskohtaisuuden asteen voi myös valita, mutta kuitenkin suppeammin kuin SISTEMAssa. ABB:n raportissa ei ole omaa kenttää komponentin positiolle tai osanumerolle. Pilz:n raportin sisältöä ei voi valita ilman lisenssiä.

SISTEMAn raporttiin ei saa sisällytettyä graafista esitystä turvatoiminnoista. Sen sijaan ABB:n ja Pilz:n raportissa voidaan sisällyttää kuvat turvatoimintojen loogisista blokkikaavioista. Tämä on ehdottomasti hyvä ominaisuus. SISTEMAn raportissa ei ole erillistä komponenttiluetteloa. ABB:n ja Pilz:n raporttien loppuun on sisällytetty komponenttiluettelo.

Jokaisen tarkasteltavan laskentaohjelmiston raportin tiedostoformaatti oli PDF. Ainostaan Pilz:n raportin pystyy generoimaan DOC-formaattiin, mutta ei ilman lisenssiä. Mielestäni olisi hyvä ominaisuus, jos koko projektin tiedot saisi generoitua taulukkolaskentaohjelmistojen tukemaan tiedostoformaattiin. Tällöin laskentaohjelmistolla luotua dataa saisi hyödynnettyä muussa teknisessä dokumentaatiossa. Voitaisiin esimerkiksi välittää positioiden perusteella komponenttien turvallisuuteen liittyvät ominaisarvot toisiin taulukkoihin.

Huono ominaisuus raporteissa on suuri sivumäärä, mikäli turvatoimintoja on useita ja raportti halutaan yksityiskohtaisena. Esimerkiksi SISTEMAlla tehdyssä 60 turvatoiminnon projektissa raportin laajuus on pienimmillään 206 sivua ja yksityiskohtainen raportti on laajuudeltaan 416 sivuinen. Toki luettelo kyseisen projektin turvatoiminnoista alajärjestelmineen on laajuudeltaan vain 35 sivuinen raportti, mutta tämä ei sisällä mielestäni kaikkia tarpeellisia tietoja.

Raporttien paisuessa satasivuisiksi oli laajojen projektien tarkastelu huomattavasti selkeämpää laskentaohjelmistojen käyttöliittymällä. Raporttiin verrattuna laskentaohjelmistojen käyttöliittymillä tieto oli muutamalla klikkauksella nähtävillä. Lisäksi laskentaohjelmistojen hakutoiminnot toimivat varsin hyvin.

3.4.5 Komponenttikirjastot

Jokaisella tarkasteltavalla laskentaohjelmistolla oli oma tiedostoformaatti komponenttikirjastoille. Kuitenkin kaikki ohjelmistot tukivat universaalia VDMA 66413 -formaattia. Erityisenä ominaisuutena Pilz:n ohjelmistossa oli kyky muuntaa SLB-kirjasto VDMA-kirjastoksi. ABB:n ja Pilz:n ohjelmistot tukivat SISTEMAn kirjastojen formaattia.

Operointi komponenttikirjastoissa oli yksi arvioitava ominaisuus. Kaikille ohjelmistoille yhteistä oli sama syntaksi komponenttien siirtämiseksi projektiin. Siirtäminen tapahtui yksinkertaisesti raahaamalla komponentti projektin haluttuun kohtaan.

SISTEMA ja Pilz PAScal erottuivat edukseen ABB FSDT-ohjelmistosta tietojen esittämisessä, kun komponenttien kaikki lisätiedot olivat helposti nähtävillä tehdessä valintaa. Sen sijaan ABB FSDT ei

näyttänyt kuin komponentin nimityksen ja näin ollen lisätiedot näkivät vasta lisättyään komponentin projektiin.

Jokaisella tarkasteltavalla laskentaohjelmistolla oli mahdollista hakea komponentteja kirjastosta hakusanoilla. SISTEMAn hakutoiminto oli kuitenkin paras ja nopein, koska eteneminen hakutuloksesta seuraavaan tapahtui yksinkertaisesti Enter-näppäintä painamalla. ABB FSDT-ohjelmistolla ei ollut varsinaista hakutoimintoa vaan kehno suodatustoiminto, jolla hakusana täytyi olla spesifi. Pilz PAScal-ohjelmiston haku toimi yhtä hyvin kuin SISTEMAn, mutta hakutuloksista seuraavaan eteneminen ei toiminut samalla tavalla kuin SISTEMAssa.

4 Suunnitteluohje

Toimeksiantajan sisäisen suunnitteluohjeen tarkoitus on koota yhteen sekä tässä opinnäytetyössä käsiteltyjä toiminnallisen turvallisuuden standardeja että käytännön opastusta suunnittelun eri vaiheista. Ohjeen tavoitteena on tukea toiminnallisen turvallisuuden parissa jonkin verran työskentelevien suunnittelijoiden työtä. Tällaisia suunnittelijoita voivat olla esimerkiksi sähkösuunnittelijat. Automaatio- ja instrumentointisuunnittelijalle toiminnallinen turvallisuus saattaa olla jokapäiväistä. Suunnitteluohjeen tavoitteena on toimia eräänlaisena muistilistana, jotta toiminnallinen turvallisuus tulisi arvoisensa huomion kohteeksi projektin eri vaiheissa.

4.1 Lähtötilanteen kartoittaminen

Ennen suunnitteluohjeen kirjoittamista, kartoitettiin toimeksiantajan henkilöstön nykytilanne. Tällä kartoituksella tavoitteena oli saada tietoon toiminnallisen turvallisuuden parissa ajoittain työskentelevien suunnittelijoiden nykytietämys ja kokemukset aiheesta. Suunnitteluohjetta alettiin laatia haastattelujen sekä omien kokemusten perusteella.

Käytännössä tein ensin alustavat kysymykset, joihin haastateltavat saivat vastata sähköpostilla. Kirjallisten vastausten läpikäymisen jälkeen esitin vielä tarkentavia kysymyksiä, joihin sain vastaukset suullisella haastattelulla. Haastateltavien määrä oli vähäinen, mutta laadukas.

4.1.1 Haastattelujen analysointi

4.1.2 Teollisuusautomatio, projektipäälikkö

Haastatteluissa selvisi, että teollisuusautomaation parissa työskentelevällä projektipäälliköllä oli vahvin kokemus turva-automaatiosta ja näin ollen myös toiminnallisesta turvallisuudesta. Turvallisuuden eheyden tasot olivat arkipäiväisiä asioita laitevalintoja tehdessä. Kuitenkaan turvatointojen todentamista hän ei ollut tehnyt paljoa. Vaatimukset turvallisuuden eheyden tasoihin ja muihin turvatoiminnon ominaisuuksiin oli kuitenkin tullut pääsääntöisesti asiakkailta, joten riskinarviointiprosessiin hän ei usein ollut ottanut osaa.

4.1.3 Sähkötekniikka, projektipäälikkö

Sähkösuunnittelun parissa 20 vuotta työskennellyt nykyinen projektipäällikkö kertoi suunnitelleen moottorilähtöjen pysäytyksiä turvarelein. Hän oli valinnut taajuusmuuttajalähtöjen (turva)kortteja, joiden vaatimuksena oli ollut SIL 2. Hätäseispiirejä hän oli suunnitellut muun muassa kouluihin ja teollisuuteen, jolloin toteutus oli usein kahdennettu. Tiedon lähteenä on ollut netti, laitevalmistajat ja kollegat. Turvatoimintojen todentamiseen tai eheystasojen laskemiseen hän ei kuitenkaan ole ottanut osaa milloinkaan.

4.2 Suunnitteluohjeen laatiminen

Suunnitteluohjeeseen sisällytettiin alustus, joka vastaa kysymykseen, miksi tätä tehdään? Lainsäädännöllinen velvoite ja viittaukset relevantteihin standardeihin sisällytettiin myös suunnitteluohjeeseen. Lisäksi sisällytettiin suunnittelun ja ohjelmistojen ”sudenkuoppia”, jotka huomioimalla säästyy turhalta työltä. Tämä opinnäytetyö ja suunnitteluohje luotiin tukemaan toinen toisiaan, jolloin suuri osa teoriasta löytyy opinnäytetyöstä ja detaljitiedot suunnitteluohjeesta.

5 Pohdinta

Opinnäytetyön tavoitteena oli selvittää toiminnallisen turvallisuuden arviointiin ja todentamiseen tarkoitetut laskentaohjelmistot sekä valita niistä soveltuvin A-insinöörien käyttöön. Toinen päätavoite oli luoda toimeksiantajan sisäiseen käyttöön suunnitteluohje, koskien turvatoimintojen todentamista ja muita huomioitavia seikkoja. Työn alussa esitettyihin tutkimuskysymyksiin saatiin vastaukset.

Kysymys 1. *Mitä täytyy tietää ollessaan tekemisissä toiminnalliseen turvallisuuteen liittyvien suunnittelutehtävien parissa ja mistä tämän tiedon löytää?*

Kysymys 2. *Mikä turvatoimintojen laskentaohjelmisto on soveltuvin toimeksiantajan käyttöön?*

Ensimmäiseen tutkimuskysymykseen vastaus löytyy opinnäytetyön tulokseksi tehdystä suunnitteluohjeesta ja osittain myös tästä opinnäytetyöstä. Lyhyesti sanottuna suunnittelijoiden täytyy sisäistää turvallisuuden perusperiaatteet ja ymmärtää miksi ja miten turvatoimintojen todennus suoritetaan. Lisäksi täytyy osata kysyä asiakkaalta suunnittelun lähtötietoina käytettäviä vaatimuksia.

Toisen tutkimuskysymyksen vastaukseen selvyys saatiin kokeilemalla ja vertailemalla kolmea eri laskentaohjelmistoja. Useamman viikon käytön jälkeen kullekin laskentaohjelmistolle annettiin liitteen 2 mukainen pisteytys ominaisuuksien mukaisesti ja päädyttiin valitsemaan toimeksiantajan sen hetkisten vaatimusten perusteella eniten pisteitä saanut ohjelmisto. Ohjelmistoksi valikoitui A-insinöörien käyttöön SISTEMA. Vaikka pisteytyksessä ei lopuksi ollut suurta eroa ohjelmistojen välillä, käytön tuoma kokemus osoitti valinnan olevan oikea. Ohjelmistoja vielä testattiin luomalla jokaisella ohjelmistolla sama turvatoiminto samoilla komponenteilla. Ohjelmistokohtaiset raportit tästä esimerkkiturvatoiminnosta on esitetty liitteissä 3–5. Tuloksena saatiin selvyys vuonna 2022 markkinoilla olevista toiminnallisen turvallisuuden arviointiin ja todennukseen tarkoitetuista laskentaohjelmistoista. Tulokseksi saatu konkreettinen dokumentti valinta perusteluineen on liitteen 2 arviointitaulukko.

Jatkotutkimusidea liittyy toiminnallisen turvallisuuden yhteen osa-alueeseen. Tästä opinnäytetyöstä rajattiin harvojen vaateiden turvatoiminnot pois eli periaatteessa prosessisektorilla yleiset turvatoiminnot. Opinnäytetyössä tutkituilla laskentaohjelmistoilla ei pysty todentamaan harvojen vaateiden turvatoimintoja. Luonnollinen jatkumo olisi tutkia harvojen vaateiden turvatoimintojen todentamiseen tarkoitettuja laskentaohjelmistoja ja koostaa saman sisältöinen vertailu kuin tässä opinnäytetyössä. Ja näin ollen laajentaa suunnitteluohje käsittelemään myös harvojen vaateiden turvatoimintoja ja todentamista.

Suunnitteluohjetta tullaan jatkuvasti parantamaan uusien kokemusten ohjaamalla tavalla palvelemaan yhä monipuolisemmin A-Insinöörien suunnittelijoiden tarpeita. Suunnitteluohjeen yhteyteen voisi tehdä lyhyitä ja ytimekkäitä audiovisuaalisia tutoriaaleja suunnittelun eri vaiheista ja SISTEMAn tehokkaasta käytöstä.

Lähteet

A 12.6.2008/400. Valtioneuvoston asetus koneiden turvallisuudesta. Viitattu 30.9.2022. https://www.finlex.fi, ajantasainen lainsäädäntö.

A 12.6.2008/403. Valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta. Viitattu 30.9.2022. https://www.finlex.fi, ajantasainen lainsäädäntö.

A-Insinöörien tarina. N.d. Artikkeli A-Insinöörien sivuilla. Viitattu 15.11.2022. https://www.ains.fi/yritys/tarina

Apfeld, R., Hauke, R. & Otto, S. 2015. The SISTEMA Cookbook 6. Definition of safety functions: what is important? Berlin: Deutsche Gesetzliche Unfallversicherung. Viitattu 31.10.2022. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook6_en.pdf

Ax-Suunnittelu on nyt A-Insinöörit. 2022. Uutinen A-Insinöörien sivuilla. Viitattu 15.11.2022. https://www.ains.fi/uutiset/ax-suunnittelu-on-nyt-a-insinoorit

Calculate the performance level using the PAScal Safety Calculator. N.d. Artikkeli Pilz:n sivustolla. Viitattu 2.11.2022. https://www.pilz.com/en-INT/products/software/services-software/pascal-safety-calculator

CEN ISO/TR 22100-1:2021:fi. Koneturvallisuus. suhteet standardiin ISO 12100. Osa 1: Miten B-tyypin ja C-tyypin standardit liittyvät standardiin ISO 12100. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 19.2.2021. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

Direktiivi 2006/42/EY. Euroopan parlamentin ja neuvoston direktiivi koneista. Euroopan unionin virallinen lehti 9.6.2006. Viitattu 4.10.2022. https://eur-lex.europa.eu/eli/dir/2006/42

EU ja standardisointi. N.d. Artikkeli Suomen standardoimisliiton sivuilla. Viitattu 3.10.2022. https://sfs.fi/standardeista/mika-on-standardi/eu-ja-standardisointi/

Guide to application of the Machinery Directive 2006/42/EC. 2019. Konedirektiivin soveltamisopas. uud. 2. p. https://ec.europa.eu/docsroom/documents/38022

Hauke, M., Apfeld, R., Huelke, M., Bömer, T. & Werner, W. 2020. The SISTEMA Cookbook 4. Berlin: Deutsche Gesetzliche Unfallversicherung. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook4_v2_en.pdf

Hauke, M., Schaefer, M., Apfeld, R., Werner, C., Bömer, T., Huelke, M., Steimers, A., Borowski, T., Büllesbach, K-H., Dorra, M., Foermer-Schaefer, H-G., Uppenkamp, J., Lohmaier, O., Heimann, K-D., Köhler, B., Zilligen, H., Otto, S., Rempel, P. & Reuß, G. 2019. IFA Report 2/2017e Functional safety of machine controls. Berlin: Deutsche Gesetzliche Unfallversicherung. Viitattu 8.11.2022. https://www.dguv.de/medien/ifa/en/pub/rep/pdf/reports-2019/report0217e/rep0217e.pdf

Hietikko, M., Malm, T., & Alanen, J. (2009). Koneiden ohjausjärjestelmien toiminnallinen turvallisuus: Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen. VTT Technical Research Centre of Finland. VTT Tiedotteita - Research Notes No. 2485 https://publications.vtt.fi/pdf/tiedotteet/2009/T2485.pdf

Huelke, M., Hauke, R. & Lungfiel, A. 2016. The SISTEMA Cookbook 5. Berlin: Deutsche Gesetzliche Unfallversicherung. Viitattu 31.10.2022. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook5_en_2_0.pdf

IEC/TR 61508-0:fi Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0: Toiminnallinen turvallisuus ja IEC 61508. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 21.11.2011. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

Introduction and Terminology for Functional Safety of Machines and Systems. 2020. Toiminnallisen turvallisuuden viitekäsikirja Siemensin sivuilla. Viitattu 24.11.2022. https://assets.new.siemens.com/siemens/assets/api/uuid:538c0aa8773783ef69be1d3077072688a1f1520f/introduction-terminology-for-functional-safety-of-machines-syste.pdf

Käyttöasetuksen soveltamissuosituksia. 2009. STM:n julkaisema soveltamisopas käyttöasetukselle. Tampere: Multiprint Oy. Viitattu 24.10.2022. https://www.tyosuojelupaallikko.fi/binary/file/-/fid/1367

L 23.8.2002/738. Työturvallisuuslaki. Viitattu 30.12.2022. https://www.finlex.fi, ajantasainen lainsäädäntö.

L 26.11.2004/1016. Laki eräiden teknisten laitteiden vaatimustenmukaisuudesta. Viitattu 30.12.2022. https://www.finlex.fi, ajantasainen lainsäädäntö.

Lentokonemekaanikko puristui lentokoneen rahtiruuman luukun väliin. 2005. TOT- raportti. http://totti.tvk.fi/tottipublic/totcasepublic.view?action=caseReport&unid=34

Malm, T. 2021. Introduction to IEC 62998 Standards. VTT Technical Research Centre of Finland. https://cris.vtt.fi/ws/portalfiles/portal/43576145/SafetySensors_1stdFIMA.pdf

Malm, T., Venho-Ahonen, O., Hietikko, M., Stålhane, T., de Bésche, C., & Hedberg, J. (2015). From risks to requirements: Comparing the assignment of functional safety requirements. VTT Technical Research Centre of Finland. VTT Technology No. 241 https://publications.vtt.fi/pdf/technology/2015/T241.pdf

Mitä standardi tarkoittaa? N.d. Artikkeli Suomen standardoimisliiton sivuilla. Viitattu 3.10.2022. https://sfs.fi/standardeista/mika-on-standardi/

Out of control. 2003. Kew: Health and Safety Executive. Viitattu 24.11.2022. https://www.hse.gov.uk/pubns/priced/hsg238.pdf

P 21.12.1994/1314. Valtioneuvoston päätös koneiden turvallisuudesta. Viitattu 14.11.2022. https://www.finlex.fi, ajantasainen lainsäädäntö.

PAScal Online help from V1.9.1. N.d. Pilz PAScal ohjelmiston käyttöohje, sovelluksen sisäinen. Viitattu 2.11.2022.

SFS-EN 61508-1:2011 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset. 2. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 24.1.2011. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN 61508-2:2011 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille. 2. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 24.1.2011. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN 61508-4:2010 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 4: Määritelmät ja lyhenteet. 2. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 22.11.2010. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN IEC 62061:2021. Turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. 2. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 6.8.2021. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN ISO 12100. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. 3. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 13.12.2010. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN ISO 13849-1:2015. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. 3. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 31.12.2015. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN ISO 13849-2:2012. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. 3. p. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 19.11.2012. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

SFS-EN ISO 14119. Koneturvallisuus. Suojusten kytkentä koneen toimintaan. Suunnittelu ja valinta. Helsinki: Suomen Standardisoimisliitto SFS. Julk. 9.12.2013. Viitattu 30.9.2022. https://janet.finna.fi, SFS Online.

Siirilä, T., Tytykoski, K. 2016. Koneturvallisuuden käsikirja. 2. p. Helsinki: Inspecta Oy.

Software-Assistent SISTEMA. N.d. Artikkeli Dguv:n sivustolla. Viitattu 28.10.2022. https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

Toiminnallinen turvallisuus. N.d. Artikkeli Seskon sivuilla. Viitattu 3.10.2022. https://sesko.fi/standardointi/toiminnallinen-turvallisuus/

Toimipaikkojen osoitteet. N.d. Artikkeli A-Insinöörien sivuilla. Viitattu 15.11.2022. https://www.ains.fi/yhteystiedot

Tsutsumi, K., van Gulijk, C. 2021. Safety in the future. IEC:n white paper. https://www.iec.ch/basecamp/safety-future

User's manual Functional safety design tool. 2019. Ohjelmiston käyttöohje ABB:n verkkosivuilla. Viitattu 1.11.2022. https://search.abb.com/library/Download.aspx?DocumentID=3AXD10000102417&LanguageCode=en&DocumentPartId=&Action=Launch

VDMA 66413. 2012. Universaali spesifikaatio toiminnallisen turvallisuuden arvojen dataformaatille. Viitattu 1.11.2022. https://www.vdma.org/c/document_library/get_file?uuid=88137cc0-57bc-46a8-a59e-5d43afd9a8f0&groupId=34570

Yozallinas, J. 2016. Functional Safety Evolution. Exidan blogi. Julkaistu 4.8.2016. Viitattu 24.1.2023. https://www.exida.com/blog/functional-safety-evolution

Liitteet

Liite 1. Suunnitteluohje (salassa pidettävä)

Liite 2. Ohjelmistojen arviointitaulukko

Ominaisuus		Pisteet 0-5	Sistema (Versio 2.0.8 Build 4)	Pisteet 0-5	ABB Functional safety desing tool (Version 1.2.0.2)	Pisteet 0-5	Pilz PAScal (Versio 1.9.1)
Standardituki		3	SFS-EN ISO 13849-1:2015 SFS-EN ISO 13849-2:2012	4	SFS-EN ISO 13849-1:2015 SFS-EN IEC 62061:2015	5	SFS-EN ISO 13849-1:2015 SFS-EN ISO 13849-2:2012 SFS-EN IEC 62061:2015
		5	Ohjelmistoon pystyy syöttämään standardin SFS-EN IEC 62061:2015 mukaisia ominaisarvoja. Ohjelmisto muuntaa ominaisarvot vastaamaan standardin SFS-EN ISO 13849-1:2015 mukaista yksikköjä.	2	Suunnitellessa turvatoimintoja standardin SFS-EN ISO 13849-1:2015 mukaan, ohjelmistoon ei pysty syöttämään standardin SFS-EN IEC 62061:2015 mukaisia ominaisarvoja. Näin ollen komponentille tulee manuaalisesti syöttää toisen standardin mukaiset tiedot.	2	Suunnitellessa turvatoimintoja standardin SFS-EN ISO 13849-1:2015 mukaan, ohjelmistoon pystyy luomaan komponentin standardin SFS-EN IEC 62061:2015 mukaisilla ominaisarvoilla. Ei kuitenkaan pysty nopeasti valitsemaan komponentin ominaisarvoja, kuten sistemassa pystyy.
	Yhteensä	**8**		**6**		**7**	
Käyttöliittymä		5	Looginen projektipuu hierarkisesti esitettynä	5	Looginen projektipuu hierarkisesti esitettynä	5	Looginen projektipuu hierarkisesti esitettynä
		2	Ei loogista blokkikaaviota, jossa turvatoiminnon komponentit esitetty	5	Looginen blokkikaavio, jossa turvatoiminnon komponentit esitetty visuaalisesti. Komponenttien turvallisuuteen liittyvät ominaisarvot on esitetty blokkikaaviossa	3	Looginen blokkikaavio, jossa turvatoiminnon komponentit esitetty visuaalisesti.
		4	Klikkaamalla projektipuusta turvatoiminnon osaa, ikkunassa esitetään kyseisen osan ominaisarvot.	4	Klikkaamalla projektipuusta tai blokkikaaviosta turvatoiminnon osaa, avautuu ikkuna kyseisen osan ominaisarvoista.	4	Oma ikkuna, jossa projektipuun lisäksi esitetään turvatoiminnon osien ominaisarvot.
		3	Esitetään turvatoiminnon kokonais PFHd, mutta ei prosenttiyksiköissä eikä visuaalisesti.	4	Esitetään turvatoiminnon kokonais PFHd:n jakautuminen eri osille prosenttiyksiköissä, mutta ei visuaalisesti.	5	Esitetään turvatoiminnon kokonais PFHd:n jakautuminen eri osille visuaalisesti sekä prosenttiyksiköissä.
		4	Kopiointi ja liittäminen onnistuu vaivattomasti projektipuussa	5	Kopiointi ja liittäminen onnistuu vaivattomasti projektipuussa sekä blokkikaaviossa	5	Kopiointi ja liittäminen onnistuu vaivattomasti projektipuussa sekä blokkikaaviossa
		5	Voidaan valita ohjelmiston kieleksi suomi, englanti, saksa tai japani.	3	Voidaan valita ohjelmiston kieleksi englanti tai saksa.	4	Voidaan valita ohjelmiston kieleksi englanti, saksa, ranska, italia, espanja tai japani. (Vaatii lisenssin)
	Yhteensä	**23**		**26**		**26**	
Ohjeet ja tukipalvelut		5	Ohjelmistossa on sisään rakennettuna erinomaiset suomenkieliset ohjeet, joissa avattu myös laskennan teoriaa.	3	Ohjelmistossa on sisään rakennettuna hyvät englanninkieliset ohjeet.	4	Ohjelmistossa on sisään rakennettuna hyvät englanninkieliset ohjeet, joissa avattu myös laskennan teoriaa.
		5	Ohjelmistoon on saatavilla esimerkkiprojekteja runsaasti.	2	Ohjelmistoon on saatavilla esimerkkiprojekteja vähäisesti.	2	Ohjelmistoon on saatavilla esimerkkiprojekteja vähäisesti.
	Yhteensä	**10**		**5**		**6**	
Kustannukset		5	Ohjelmistosta ei aiheudu kustannuksia ja kaikki ominaisuudet ovat käytössä.	5	Ohjelmistosta ei aiheudu kustannuksia ja kaikki ominaisuudet ovat käytössä.	2	Ilman lisenssiä ohjemistossa on rajoitetut ominaisuudet. Toistaiseksi voimassa oleva lisenssi verkkosivujen mukaan maksaa 397,51 €
	Yhteensä	**5**		**5**		**2**	
		4	Raportissa esitetään tieto teksimuodossa	5	Raportissa esitetään tieto teksimuodossa ja visuaalisesti	5	Raportissa esitetään tieto teksimuodossa ja visuaalisesti

Ominaisuus		Pisteet 0-5	Sistema (Versio 2.0.8 Build 4)	Pisteet 0-5	ABB Functional safety desing tool (Version 1.2.0.2)	Pisteet 0-5	Pilz PAScal (Versio 1.9.1)
Raportti		5	Turvatoimintojen komponentteihin on mahdollista syöttää omiin kenttiinsä nimi, positio, valmistaja, osanumero ja laiteryhmä. Nämä tiedot saa halutessaan sisällytettyä raporttiin.	3	Komponenteille ei ole omia kenttiä positiolle, valmistajalle, osanumerolle ja laiteryhmälle. Vain nimi ja vapaamuotoinen kuvaus.	4	Turvatoimintojen komponentteihin on mahdollista syöttää omiin kenttiinsä nimi, valmistaja, osanumero ja laiteryhmä. Nämä tiedot saa halutessaan sisällytettyä raporttiin. (Vaatii lisenssin)
		5	Voidaan valita raportin kieleksi suomi, englanti, saksa tai japani.	3	Voidaan valita raportin kieleksi englanti tai saksa	4	Voidaan valita raportin kieleksi englanti, saksa, ranska, italia, espanja tai japani. (Vaatii lisenssin)
		5	Generoidessa raporttia voidaan valita, mitä tietoja raporttiin sisällytetään	5	Generoidessa raporttia voidaan valita, mitä tietoja raporttiin sisällytetään	5	Generoidessa raporttia voidaan valita, mitä tietoja raporttiin sisällytetään
		2	Raportin voidaan generoida pdf-formaattiin.	2	Raportin voidaan generoida pdf-formaattiin.	4	Raportin voidaan generoida pdf- ja doc-formaattiin. (Vaatii lisenssin)
	Yhteensä	**21**		**18**		**22**	
Mukautuvuus		1	Ohjelmistolla voidaan laskea vain jatkuvan- ja tiheiden vaateiden toimintatavan turvatoimintoja.	1	Ohjelmistolla voidaan laskea vain jatkuvan- ja tiheiden vaateiden toimintatavan turvatoimintoja.	1	Ohjelmistolla voidaan laskea vain jatkuvan- ja tiheiden vaateiden toimintatavan turvatoimintoja.
	Yhteensä	**1**		**1**		**1**	
Komponenttikirjastot		3	Tukee VDMA 66413 kirjastoja sekä sisteman omia "SLB"-kirjastoja	4	Tukee VDMA 66413 kirjastoja, sisteman "SLB"-kirjastoja sekä ABB:n omia "ABBlibary"-kirjastoja. Ohjelmistossa itse luotuja komponenttikirjastoja voidaan viedä (Export), mutta on yhteensopiva vain ABB:n ohjelmiston kanssa.	5	Tukee VDMA 66413 kirjastoja, sisteman "SLB"-kirjastoja sekä Pilz:n omia "PCL" - kirjastoja. Mahdollista muuntaa sisteman kirjasto VDMA-formaattiin.
		5	Komponenttien hakeminen on helppoa kirjastosta. Mahdollisuus suodattaa hakusanoilla Komponenttien kaikki tiedot ovat näkyvissä valintaa tehdessä yhden valikon takana.	2	Komponenttikirjastossa ei ole varsinaista hakuominaisuutta, vain suodatus. Valintaa tehdessä ei ole näkyvillä muuta tietoa kuin komponentin nimitys.	4	Komponenttien hakeminen on helppoa kirjastosta. Mahdollisuus suodattaa hakusanoilla Komponenttien kaikki tiedot ovat näkyvissä valintaa tehdessä kahden valikon takana.
	Yhteensä	**8**		**6**		**9**	
Vaadittavan PL tai SIL määritys (Riskiarvio)		4	Vaadittava PL syötetään suoraa tai arvioidaan sisäänrakennetusta riskigraafista	5	Vaadittava PL tai SIL syötetään suoraa tai arvioidaan sisäänrakennetusta riskigraafista (SFS-EN ISO 13849-1:2015) tai riskimatriisista (SFS-EN IEC 62061:2015)	5	Vaadittava PL tai SIL syötetään suoraa tai arvioidaan sisäänrakennetusta riskigraafista (SFS-EN ISO 13849-1:2015) tai riskimatriisista (SFS-EN IEC 62061:2015)
	Yhteensä	**4**		**5**		**5**	
Kokonaispisteet		80		72		78	
Maksimipisteet		100		100		100	

Liite 3. Moottorin hätäpysäytys SISTEMA-raportti

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

PR Projektin nimi: Moottorin hätäpysäytys

Projektitiedoston nimi:	C:\Users\eero.kohtala\OneDrive - A-Insinöörit Oy\Tiedostot\SISTEMA\Projects\Esimerkkiprojekti2.ssm
Valmistumisen päivämäärä:	16.03.2023 09.35.28
Projektin tila:	
Projektin numero:	12345Y
Projektin versio:	
Tekijät:	EEKOH
Projektista vastaavat:	
Tarkastajat:	
Vaarallinen kohta/kone:	Sekoitin
Dokumentaatio:	
Dokumentti:	
Ohjelmiston versio:	2.0.8 build 4
Standardin versio:	ISO 13849-1:2015, ISO 13849-2:2012
Tarkistussumma:	e6efedc84a2805a98e62c37fe848017a
Asetukset:	☑ Käytä DC:n väliarvoja PFHD:n laskentaan (tarkempi). ☐ MTTFD-arvon pienentäminen luokkaa 4 varten arvosta 2500 arvoon 100 vuotta.
Tila:	vihreä
Huomautus:	Tähän projektiin (tai siihen kuuluviin peruselementteihin) ei ole merkitty yhtään varoitusta.

Tulostusasetukset

- ☑ Näytä laitteen yksityiskohdat
- ☑ Näytä muuttujien SF, SB, BL ja EL dokumentaatio
- ☑ Näytä muuttujiin CCF ja DC liittyvien toimenpiteiden yksityiskohdat
- ☑ Näytä suoritustason PL ja luokan vaatimukset
- ☑ Näytä muuttujien PLr, PL, luokka, CCF, MTTFD ja DC dokumentaatiot
- ☑ Näytä viestit

Tähän kuuluvat turvatoiminnot

SF Nimi: Moottorin hätäpysäytys [SF1]

Vaadittu: PLr c	Saavutettu: PL c	PFHD [1/h]: 1E-7	Tila: vihreä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

Identifier of the Safety function:	SF1
Turvatoiminnon tyyppi:	Hätäpysäytystoiminto
Laukaiseva tapahtuma:	Hätäpysäytyspainikkeeseen vaikutetaan
Reaktio ja käyttäytyminen tehonsyötön vikaantuessa:	Moottorin tehon syöttö loppuu
Turvallinen tila:	Moottori ja vaarallinen liike pysähtynyt
Toimintatapa:	Tiheiden vaateiden
Vaadetaajuus:	1/a
Käyttöaika:	
Ensisijaisuus:	
Dokumentaatio:	
Dokumentti:	

Vaadittava suoritustaso Turvatoiminto

PLr (suora syöte):	c
Dokumentaatio:	KS erillinen riskiarviodokumentti 12345
Dokumentti:	
Lähde (esim. standardi):	
Tiedosto:	

Suoritustaso Turvatoiminto

Saavutettu PL: c **PFHD [1/h]: 1E-7**

Tila / Viestit Turvatoiminto

Tila:	vihreä

Alajärjestelmät (1 / 8)

SB Nimi: Hätäseispainike

Viitetunnus: HSZ1000 **Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	SE_VDMA_INPUT_2020_02_24
Laitetunnus:	E-stop, 2 contacts | Input devices
Laiteryhmä:	Input devices
Osanumero: E-stop, 2 contacts	**Muutos: 02. Feb**
Toiminto:	☑ Tulot ☐ Logiikka ☐ Lähdöt ☐ tuntematon
Käyttötapaus:	Input | - | - | - | -
Käyttötavan kuvaus:	

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

Dokumentaatio Alajärjestelmä

Dokumentaatio:	The emergency stopping function is a protective measure which complements the safety functions for the safeguarding of hazardous zones in accordance with EN ISO 12100. The safety values are calculated for 63 operations per year. B10 = 300 000, % of dangerous failures = 20%, B10d = 1 500 000, The MTTFd value will be calculated depending on the number of operations per year. With a 2-channel signal processing applicable up to PL=e.
Dokumentti:	.\pdf\Emergency_stop.pdf

Suoritustaso Alajärjestelmä

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)

PL: e	**Software suitable up to PL: n.a.**
Saavutettu PL: e	**PFHD [1/h]: 2,5E-8**
Dokumentaatio:	
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	4
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Alajärjestelmät (2 / 8)

SB Nimi: Turvalogiikka

Viitetunnus: SCZ1000	**Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	Honeywell
Laitetunnus:	
Laiteryhmä:	
Osanumero:	**Muutos:**
Toiminto:	☐ Tulot ☐ Lähdöt ☑ Logiikka ☐ tuntematon
Käyttötapaus:	

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF **Turvatoiminto: Moottorin hätäpysäytys**

Käyttötavan kuvaus:

Dokumentaatio Alajärjestelmä

Dokumentaatio:	Etukäteen suunniteltu alajärjestelmä.
Dokumentti:	

Suoritustaso Alajärjestelmä

PL määritys:	Syötä SIL/PFHD suoraan (valmistaja vastaa SIL-vaatimusten täyttymisestä standardin IEC 62061 mukaisesti)

Safety Integrity Level (SIL): 3	**PL: e**
Software suitable up to PL: n.a.	
Saavutettu PL: e	**PFHD [1/h]: 3,2E-8**
Dokumentaatio:	
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Tila / Viestit Alajärjestelmä

Tila:	vihreä
Viesti [Viestin tila]:	- Valmistajan ilmoittama SIL-taso tälle alajärjestelmälle oli muunnettu vastaavaksi PL-tasoksi standardin taulukon 3 mukaisesti (katso myös ISO/TR 23849). [vihreä]

Alajärjestelmät (3 / 8)

SB Nimi: Välireleistys

Viitetunnus: SICZ1000.K	**Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	Omron
Laitetunnus:	G7S-3A3B-E+P7S-14F-END
Laiteryhmä:	
Osanumero:	**Muutos:**
Toiminto:	☐ Tulot ☐ Logiikka ☑ Lähdöt ☐ tuntematon
Käyttötapaus:	
Käyttötavan kuvaus:	

Dokumentaatio Alajärjestelmä

Dokumentaatio:	
Dokumentti:	

Suoritustaso Alajärjestelmä

PL määritys:	Määritä PL/PFHD Luokan, MTTFD- ja DCavg-arvojen avulla

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

Software suitable up to PL:	n.a.
PL-vaatimukset:	täytetty
PL on määritettävä arvioimalla seuraavat kohdat:	- Turvatoiminnon käyttäytyminen vikatilassa (katso kohta 6) [täytetty] - turvallisuuteen liittyvän ohjelmiston kohdan 4.6 mukaisesti tai mitään ohjelmistoa ei ole mukana. [täytetty] - systemaattiset vikaantumiset (katso liite G) [täytetty] - Kyvykkyys suorittaa turvatoiminto odotettavissa olevissa ympäristöolosuhteissa [täytetty]
Saavutettu PL: e	**PFHD [1/h]: 4,3E-8**
Dokumentaatio:	

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	3
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	- Asiaan kuuluvien standardien mukaisesti kestää odotettavissa olevat vaikutukset. . [täytetty] - Turvallisuuden perusperiaatteita on käytetty. [täytetty] - Hyvin koeteltuja turvallisuuperiaatteita on käytetty. [täytetty] - Yhden vian vikasietoisuus ja riittävä vikojen paljastuminen. [täytetty] - MTTFD on vähintään Matala tai Keskitaso tai Korkea. [täytetty] - DCavg on vähintään Matala tai Keskitaso. [täytetty] - CCF-arviossa saavutetut pisteet ovat vähintään 65. [täytetty]
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

MTTFD ja toiminta-aika Alajärjestelmä

MTTFD [v]:	100 (Korkea)
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Diagnostiikan kattavuus Alajärjestelmä

DCavg [%]:	90 (Keskitaso)

Yhteisvikaantuminen Alajärjestelmä

CCF-pisteet:	75 (täytetty)
CCF-toimenpiteet:	- Erottelu (15 Pisteet) Signaalipolkujen välinen fyysinen erottelu, esimerkiksi: - langoituksen ja putkiston erottelu - oikosulussa olevien ja avoimien piirien tunnistaminen dynaamisella testauksella - jokaisen kanavan signaalipolun suojauksen erottelu - painettujen piirilkorttien riittävät väli- ja ryömintäetäisyydet- - Suunnittelu, soveltaminen ja käyttökokemukset (15 Pisteet) Suojaus jännitteen, paineen, sähkövirran, lämpötilan jne. ylitykselle. - Suunnittelu, soveltaminen ja käyttökokemukset (5 Pisteet)

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

CCF-toimenpiteet:	Käytetyt komponentit ovat hyvin koeteltuja. - Pätevyys ja koulutus (5 Pisteet) Suunnittelijat on koulutettu ymmärtämään yhteisvikaantumisten syyt ja seuraukset. - Ympäristöolosuhteet (25 Pisteet) Sähköisten ja elektronisten järjestelmien suojaaminen sekoamiselta ja sähkömagneettisilta häiriöiltä - EMC: suojaaminen soveltuvien standardien (esim. IEC 61326-3-1) mukaisesti - Hydraulijärjestelmät: hydarulinesteen suodatus, likaisen väliaineen syötön estäminen, paineilman kuivaus, esim. väliaineen puhtausvaatimusten täyttäminen komponenttivalmistajan vaatimusten mukaisesti. HUOM: Hydraulisten ja sähköisten järjestelmien yhdistelmien osalta on otettava huomioon molempien vaatimukset. - Ympäristöolosuhteet (10 Pisteet) Muita vaikutuksia - Asiaan kuuluvien ympäristövaikutusten vaatimusten ottaminen huomioon, kuten lämpötila, iskut, tärinä, koskteus (esim. siten kuin asianomaisissa standardeissa on määritetty).
Dokumentaatio:	
Dokumentti:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Kanavat/testikanavat (1 / 2)

CH Nimi: Kanava 1

MTTFD [v]: 100

Lohkot (1 / 1)

BL Nimi: rele

Viitetunnus: SICZ1000.K10 **Inventointinumero:**

Laitetiedot Lohko

Laitevalmistaja:	Omron	
Laitetunnus:	G7S-3A3B-E+P7S-14F-END	
Laiteryhmä:		
Osanumero:	**Muutos:**	
Toiminto:	☐ Tulot ☑ Lähdöt	☐ Logiikka ☐ tuntematon
Teknologia:	tuntematon	
Luokka (Cat.):	-	
Käyttötapaus:		
Käyttötavan kuvaus:		

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF **Turvatoiminto: Moottorin hätäpysäytys**

Dokumentaatio Lohko

Dokumentaatio:

Dokumentti:

MTTFD ja toiminta-aika Lohko

MTTFD [v]: 9000000 (Korkea)

Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**
B10D [jaksoa]: 900000	**Nop [toimintajaksoa/vuosi]: 1**

Dokumentaatio:

Diagnostiikan kattavuus Lohko

DC [%]: 90 (Keskitaso)

Toimenpide:	Epäsuora valvonta (esim. painekytkimen tekemä valvonta, toimilaitteiden aseman sähköinen valvonta) (Lähtöön liitettävä laite) (90 % - 99 % sovelluksesta riippuen)
Dokumentaatio:	Valvotaan moottorin liikettä kahdennetulla nopeusmittauksella. Valvotaan taajuusmuuttajan tilatietoja väylän kautta (DCS)

Tila / Viestit Lohko

Tila:	vihreä

Kanavat/testikanavat (2 / 2)

CH Nimi: Kanava 2

MTTFD [v]: 100

Lohkot (1 / 1)

BL Nimi: rele

Viitetunnus: SICZ1000.K11	**Inventointinumero:**

Laitetiedot Lohko

Laitevalmistaja:	Omron	
Laitetunnus:	G7S-3A3B-E+P7S-14F-END	
Laiteryhmä:		
Osanumero:	**Muutos:**	
Toiminto:	☐ Tulot ☑ Lähdöt	☐ Logiikka ☐ tuntematon
Teknologia:	sähkömekaaninen	
Luokka (Cat.):	-	
Käyttötapaus:		
Käyttötavan kuvaus:		

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

Dokumentaatio Lohko

Dokumentaatio:

Dokumentti:

MTTFD ja toiminta-aika Lohko

MTTFD [v]: 9000000 (Korkea)

Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**
B10D [jaksoa]: 900000	**Nop [toimintajaksoa/vuosi]: 1**

Dokumentaatio:

Diagnostiikan kattavuus Lohko

DC [%]: 90 (Keskitaso)

Toimenpide:	Epäsuora valvonta (esim. painekytkimen tekemä valvonta, toimilaitteiden aseman sähköinen valvonta) (Lähtöön liitettävä laite) (90 % - 99 % sovelluksesta riippuen)
Dokumentaatio:	Valvotaan moottorin liikettä kahdennetulla nopeusmittauksella. Valvotaan taajuusmuuttajan tilatietoja väylän kautta (DCS)

Tila / Viestit Lohko

Tila:	vihreä

Alajärjestelmät (4 / 8)

SB Nimi: Taajuusmuuttaja FSO-12-kortti (DI)

Viitetunnus: SICZ1000 **Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	ABB Drives
Laitetunnus:	FSO, DI, 2-ch. pulsed
Laiteryhmä:	FSO-12/-21 subsystems
Osanumero: 1	**Muutos:**
Toiminto:	☑ Tulot ☐ Logiikka ☐ Lähdöt ☐ tuntematon
Käyttötapaus:	FSO, DI, 2-ch. pulsed | - | - | - | -
Käyttötavan kuvaus:	FSO 2-channel pulsed digital input. These results applies to FSO-12 and -21 products.

Dokumentaatio Alajärjestelmä

Dokumentaatio:	FSO 2-channel pulsed digital input. These values apply to FSO-12 and -21 products. Safety functions module for ACS880 drives.
Dokumentti:	

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF **Turvatoiminto: Moottorin hätäpysäytys**

Suoritustaso Alajärjestelmä

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)
PL: e	**Software suitable up to PL: n.a.**
Saavutettu PL: e	**PFHD [1/h]: 1,8E-12**
Dokumentaatio:	
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	2
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Alajärjestelmät (5 / 8)

SB Nimi: Taajuusmuuttaja FSO-12-kortti (Logic)

Viitetunnus: SICZ1000 **Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	ABB Drives
Laitetunnus:	FSO Logic 2
Laiteryhmä:	FSO-12/-21 subsystems
Osanumero: 1	**Muutos:**
Toiminto:	☐ Tulot ☑ Logiikka ☐ Lähdöt ☐ tuntematon
Käyttötapaus:	FSO Logic 2 | - | - | - | -
Käyttötavan kuvaus:	FSO Logic 2. These results applies to FSO-12 and -21 products.

Dokumentaatio Alajärjestelmä

Dokumentaatio:	Use "Logic 1" subsystem if the safety function contains a 1-channel digital input or output with non-pulsed signals. Otherwise use "Logic 2" subsystem. These values apply to FSO-12 and -21 products.
Dokumentti:	

Suoritustaso Alajärjestelmä

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)
PL: e	**Software suitable up to PL: n.a.**
Saavutettu PL: e	**PFHD [1/h]: 4,4E-11**
Dokumentaatio:	
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	3
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Alajärjestelmät (6 / 8)

SB Nimi: Taajuusmuuttaja FSO-12-kortti (STO output)

Viitetunnus: SICZ1000	**Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	ABB Drives
Laitetunnus:	FSO, STO output
Laiteryhmä:	FSO-12/-21 subsystems
Osanumero: 1	**Muutos:**
Toiminto:	☐ Tulot ☐ Logiikka ☑ Lähdöt ☐ tuntematon
Käyttötapaus:	FSO, STO output | - | - | - | -
Käyttötavan kuvaus:	FSO Safe Torque Off - output. These results applies to FSO-12 and -21 products.

Dokumentaatio Alajärjestelmä

Dokumentaatio:	FSO Safe Torque Off - output. These values apply to FSO-12 and -21 products. Safety functions module for ACS880 drives.
Dokumentti:	

Suoritustaso Alajärjestelmä

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

PL: e	**Software suitable up to PL: n.a.**
Saavutettu PL: e	**PFHD [1/h]: 1,8E-11**
Dokumentaatio:	
Toimita-aika [v]: 20	**Lyhin toiminta-aika [v]: 20**

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	3
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Alajärjestelmät (7 / 8)

SB Nimi: Taajuusmuuttaja FPTC-02-kortti

Viitetunnus: SICZ1000	**Inventointinumero:**

Laitetiedot Alajärjestelmä

Laitevalmistaja:	ABB Drives	
Laitetunnus:	FPTC-01/-02	
Laiteryhmä:	FPTC	
Osanumero: FPTC-01/-02	**Muutos:**	
Toiminto:	☐ Tulot ☐ Lähdöt	☑ Logiikka ☐ tuntematon
Käyttötapaus:	2 channels | - | - | - | -	
Käyttötavan kuvaus:		

Dokumentaatio Alajärjestelmä

Dokumentaatio:	Thermistor protection module FPTC-01/-02 is used with ACS880 product family
Dokumentti:	

Suoritustaso Alajärjestelmä

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)
PL: c	**Software suitable up to PL: n.a.**
Saavutettu PL: c	**PFHD [1/h]: 1,6E-9**

SF Turvatoiminto: Moottorin hätäpysäytys

Dokumentaatio:	
Toimita-aika [v]: 20	Lyhin toiminta-aika [v]: 20

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	1
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

Alajärjestelmät (8 / 8)

SB Nimi: Taajuusmuuttaja STO

Viitetunnus: SICZ1000	Inventointinumero:

Laitetiedot Alajärjestelmä

Laitevalmistaja:	ABB Drives
Laitetunnus:	ACS880 R4-R5 400V-500V
Laiteryhmä:	ACS880 (STO)
Osanumero: 1	Muutos:
Toiminto:	☐ Tulot ☐ Logiikka ☑ Lähdöt ☐ tuntematon
Käyttötapaus:	ACS880 R4-R5, STO - Dual Channel | - | - | - | -
Käyttötavan kuvaus:	Safe Torque Off function.

Dokumentaatio Alajärjestelmä

Dokumentaatio:	Applies to ACS880 Frame sizes R4-R5 400-500V and R5 690V (worst case)
Dokumentti:	

Suoritustaso Alajärjestelmä

PL määritys:	Syötä PL/PFHD suoraan (valmistaja vastaa luokan ja PL vaatimusten täyttymisestä)
PL: e	Software suitable up to PL: n.a.
Saavutettu PL: e	PFHD [1/h]: 3,2E-9
Dokumentaatio:	
Toimita-aika [v]: 20	Lyhin toiminta-aika [v]: 20

SISTEMA - Ohjelmistotyökalu konesovellusten turvallisuuden eheyden

Projektin nimi: Moottorin hätäpysäytys

Tiedoston päiväys: 17.03.2023 14.14.51 Raportin päiväys: 17.3.2023 Tarkistussumma: e6efedc84a2805a98e62c37fe848017a

SF Turvatoiminto: Moottorin hätäpysäytys

Luokka (Cat.) Alajärjestelmä

Luokka (Cat.):	3
Luokan vaatimukset:	täytetty
Luokan vaatimukset:	Koska valmistaja määrittää nimetyn rakenteen (luokan), hänen on varmistettava vaatimusten täyttyminen.
Dokumentaatio:	
Lähde (esim. standardi) Luokka (Cat.):	
Tiedosto:	

Tila / Viestit Alajärjestelmä

Tila:	vihreä

VASTUUVAPAUSLAUSEKE

Ohjelmiston tuotannossa on huolehdittu, että se on tehty nykytekniikan tason mukaisesti. Ohjelmisto on tarkoitettu käyttöönotettavaksi korvauksetta. Ohjelmiston käyttö tapahtuu käyttäjän omalla riskillä. Lainsäädännön antamissa rajoissa ei hyväksytä mitään lakiin perustuvaa vastuuta ohjelmistosta.

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

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

YHTEYS

Saksan sosiaalisen tapaturmavakuutuksen työterveyden ja työturvallisuuden laitos (IFA)
(Institute for Occupational Health and Safety of German Social Accident Insurance (IFA))
Osasto 5 (Tapaturmien ehkäisy/tuoteturvallisuus)
Osoite: Alte Heerstr. 111, 53754 Sankt Augustin
Sähköposti: sistema@dguv.de
Verkkosivu: www.dguv.de/ifa (Webcode e561582)

Nimi suuraakkosin:	**Päivämäärä, allekirjoitus:**
Tekijät	Tekijät
Tarkastajat	Tarkastajat

Liite 4. Moottorin hätäpysäytys Pilz PAScal-raportti

Project name: Moottorin hätäpysäytys
Project standard: ISO 13849-1

1 Project information

1.1 Tool mode

Safety zones:	Not applied
Tool language:	English

1.2 Project data

Project name:	Moottorin hätäpysäytys
Project ID:	12345Y
Project description:	
Project version:	000.000.001
Authors:	EEKOH
Approvers:	
Created date:	3/17/2023
Modified date:	3/22/2023
Project standard:	ISO 13849-1

2 Safety functions overview

2.1 Safety functions and data

2.1.1 Moottorin hätäpysäytys

Description	Moottorin liike pysäytetään taajuusmuuttajan STO-toiminnolla, kun hätäseis painikkeeseen vaikutetaan.
Hazard to mitigate	Sekoittimen vaarallinen liike
Triggering event	Hätäseis-painikkeeseen vaikutetaan
Response time	
Safe state	
Target performance level	c
Risk parameters	
1) Severity of injury (S) 2) Frequency and/or exposure to hazard (F) 3) Possibility of avoiding hazard or limiting harm (P)	n/a n/a n/a
Achieved performance level	c
Achieved PFH_D	1.06E-7 1/h

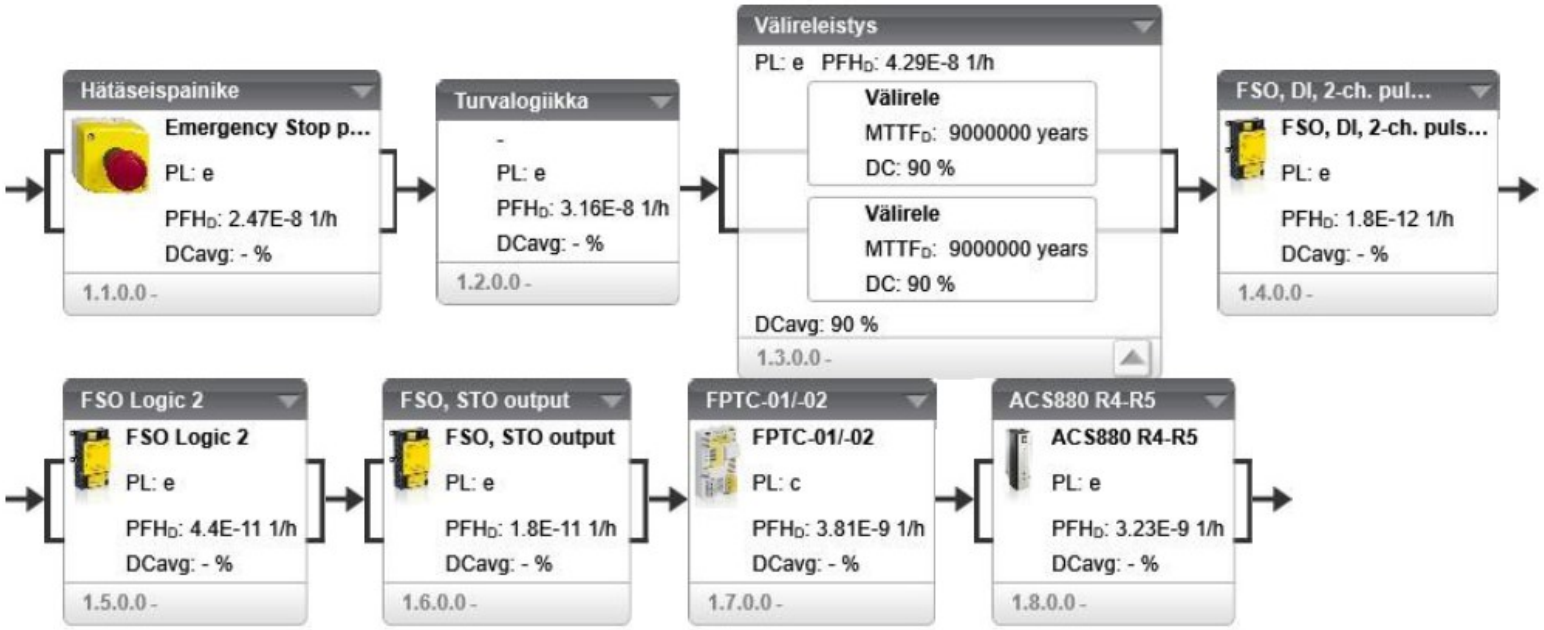
2.2 List of safety functions and performance

Safety functions name	Target PL	Achieved PL	PFH_D	Target achieved	Lowest lifetime for subsystems	Lowest lifetime for elements
1.0.0.0 Moottorin hätäpysäytys	c	c	1.06E-7 1/h	Yes	20	20

3 Safety function design

3.1 Moottorin hätäpysäytys

3.1.1 Moottorin hätäpysäytys: Logical diagram



3.1.2 Moottorin hätäpysäytys Composition of subsystems

Target PL				c					
Achieved PL				c					
ID	Subsystem name	PL	PFHD	Cat	MTTFD	DCavg	Contr. to PFHD	Lifetime	CCF
1.1.0.0	Hätäseispainike	e	2.47E-8 1/h	4	-	-	23.24 %	20 years	-

12345Y Moottorin hätäpysäytys

1.2.0.0	Turvalogiikka	e	3.16E-8 1/h	-	-	-	29.73 %	20 years	-
1.3.0.0	Välireleistys	e	4.29E-8 1/h	3	100 years	90 %	40.36 %	20 years	80
1.4.0.0	FSO, DI, 2-ch. pulsed	e	1.8E-12 1/h	2	-	-	0 %	20 years	-
1.5.0.0	FSO Logic 2	e	4.4E-11 1/h	3	-	-	0.04 %	20 years	-
1.6.0.0	FSO, STO output	e	1.8E-11 1/h	3	-	-	0.02 %	20 years	-
1.7.0.0	FPTC-01/-02	c	3.81E-9 1/h	1	-	-	3.58 %	20 years	-
1.8.0.0	ACS880 R4-R5	e	3.23E-9 1/h	3	-	-	3.04 %	20 years	-

Hätäseispainike

Description of subsystem/component	
Description	HSZ1000
Library data	SE_VDMA_INPUT_2020_02_24 V2.0 /SE_VDMA_INPUT_2020_02_24 /Input /Input devices
Device name	Emergency Stop push button
Use case	H1: Input H2: - H3: - H4: - H5: -
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	2.47E-8 1/h
Category	Category 4
Category requirement	Basic safety principles applied Well tried safety principles applied Design is single fault tolerant Accumulation of faults does not lead to loss of safety function
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	No

Turvalogiikka

Description of subsystem/component

12345Y Moottorin hätäpysäytys

Description	SCZ1000 Honeywell etukäteen suunniteltu aljärjestelmä. Valmistaja vasta PL- ja PFHd-arvoista
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	3.16E-8 1/h
Category	-
Category requirement	
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	Yes

Välireleistys

Description of subsystem/component	
Description	SICZ1000 Kaksi välirelettä
Overall subsystem performance/data	
Type	Subsystem designed with elements
PL	e
PFH_D	4.29E-8 1/h
Category	Category 3
Category requirement	Basic safety principles applied Well tried safety principles applied Design is single fault tolerant Well tried components applied (optional)
CCF points	80
CCF table	1, 3.1, 3.2, 4, 5, 6.1, 6.2 Refer to the ISO CCF check list in the appendix of the report for the description of selected CCF IDs
$MTTF_D$	100 years
DCavg	90 %

12345Y Moottorin hätäpysäytys

Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	Yes

Subsystem internal composition										
	ID	Element name	$MTTF_D$	MTTF	B_{10D}	B10	nop	DC	Lifetime	T_{10D}
Channel 1	1.3.1.1	Välirele	9000000 years	9000000 years	900000 cycles	900000 cycles	1 o/year	90 %	20 years	900000 years
Channel 2	1.3.2.1	Välirele	9000000 years	9000000 years	900000 cycles	900000 cycles	1 o/year	90 %	20 years	900000 years

Välirele

Description of element/component	
Description	SICZ1000.K10 Omron G7S-3A3B-E+P7S-14F-END
Overall element performance/data	
Type	Wearing
$MTTF_D$	9000000 years
MTTF	9000000 years
B_{10D}	900000 cycles
B10	900000 cycles
RDF	100 %
Lifetime	20 years
DC	90 %
DC measure description	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators) Valvotaan moottorin liikettä kahdennetulla nopeusmittauksella. Valvotaan taajuusmuuttajan tilatietoja väylän kautta (DCS)
Operating days per year	-
Operating hours per day	-
Time between operations	-
nop	1 o/year
T_{10D}	900000 years

Välirele

12345Y Moottorin hätäpysäytys

Description of element/component	
Description	SICZ1000.K11 Omron G7S-3A3B-E+P7S-14F-END
Overall element performance/data	
Type	Wearing
$MTTF_D$	9000000 years
MTTF	9000000 years
B_{10D}	900000 cycles
B10	900000 cycles
RDF	100 %
Lifetime	20 years
DC	90 %
DC measure description	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators) Valvotaan moottorin liikettä kahdennetulla nopeusmittauksella. Valvotaan taajuusmuuttajan tilatietoja väylän kautta (DCS)
Operating days per year	-
Operating hours per day	-
Time between operations	-
nop	1 o/year
T_{10D}	900000 years

FSO, DI, 2-ch. pulsed

Description of subsystem/component	
Description	SICZ1000
Library data	ABB Drives V1.0 /ABB Drives /Input /FSO-12/-21 subsystems
Device name	FSO, DI, 2-ch. pulsed
Use case	H1: FSO, DI, 2-ch. pulsed
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	1.8E-12 1/h
Category	Category 2
Category requirement	Basic safety principles applied Well tried safety principles applied

	Diagnostic checks performed at suitable intervals Fault reaction after detection is appropriate. - For PLr = d the output (OTE) initiates a safe state. - For PLr = a, b, or c, whenever practicable the output (OTE) initiates a safe state. If not practicable, OTE provides a warning.
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	No

FSO Logic 2

Description of subsystem/component	
Description	SICZ1000
Library data	ABB Drives V1.0 /ABB Drives /Logic /FSO-12/-21 subsystems
Device name	FSO Logic 2
Use case	H1: FSO Logic 2
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	4.4E-11 1/h
Category	Category 3
Category requirement	Basic safety principles applied Well tried safety principles applied Design is single fault tolerant
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years

12345Y Moottorin hätäpysäytys

Subsystem settings	
Symmetrization formula applied	No

FSO, STO output

Description of subsystem/component	
Description	SICZ1000
Library data	ABB Drives V1.0 /ABB Drives /Output /FSO-12/-21 subsystems
Device name	FSO, STO output
Use case	H1: FSO, STO output
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	1.8E-11 1/h
Category	Category 3
Category requirement	Basic safety principles applied Well tried safety principles applied Design is single fault tolerant
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	No

FPTC-01/-02

Description of subsystem/component	
Description	SICZ1000
Library data	ABB Drives V1.0 /ABB Drives /Logic /FPTC
Device name	FPTC-01/-02
Use case	H1: 1 channel
Overall subsystem performance/data	

12345Y Moottorin hätäpysäytys

Type	PL/PFH_D
PL	c
PFH_D	3.81E-9 1/h
Category	Category 1
Category requirement	Basic safety principles applied Well tried safety principles applied Well tried components applied
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-
Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	No

ACS880 R4-R5

Description of subsystem/component	
Description	SICZ1000
Library data	ABB Drives V1.0 /ABB Drives /Output /ACS880 (STO)
Device name	ACS880 R4-R5
Use case	H1: ACS880 R4-R5, STO - Dual Channel
Overall subsystem performance/data	
Type	PL/PFH_D
PL	e
PFH_D	3.23E-9 1/h
Category	Category 3
Category requirement	Basic safety principles applied Well tried safety principles applied Design is single fault tolerant
CCF points	-
CCF table	-
$MTTF_D$	-
DCavg	-

12345Y Moottorin hätäpysäytys

Lifetime	20 years
Subsystem settings	
Symmetrization formula applied	No

4 Summary of warnings and project information

NO	Criticality	Message
1	Info	All devices/components must be applied, operated, and installed according to its technical specification. It must be ensured that characteristic data for devices used in safety functions corresponds to the physical usage of the device. Ensure that all requirements from relevant standards, such as CCF and category requirements checklists, are fulfilled.
2	Info	1.4.0.0 FSO, DI, 2-ch. pulsed : $MTTF_D$, test channel > 1/2 $MTTF_D$, functional channel not confirmed for category 2.
3	Info	1.4.0.0 FSO, DI, 2-ch. pulsed : Demand rate, not confirmed by user

5 Summary of applied components

Subsystem name	Element name	Library	Manufacturer	Device category	Device group	Device name	Use case name	Identifier	Part number
1.0.0.0 Moottorin hätäpysäytys									
Hätäseispainike		SE_VDMA_INPUT_2020_02_24 V2.0	SE_VDMA_INPUT_2020_02_24	Input	Input devices	Emergency Stop push button	H1: Input H2: - H3: - H4: - H5: -	E-stop, 2 contacts | Input devices	E-stop, 2 contacts
Turvalogiikka									
Välireleistys									
Channel 1	Välirele								
Channel 2	Välirele								
FSO, DI, 2-ch. pulsed		ABB Drives V1.0	ABB Drives	Input	FSO-12/-21 subsystems	FSO, DI, 2-ch. pulsed	H1: FSO, DI, 2-ch. pulsed	FSO, DI, 2-ch. pulsed	1
FSO Logic 2		ABB Drives V1.0	ABB Drives	Logic	FSO-12/-21 subsystems	FSO Logic 2	H1: FSO Logic 2	FSO Logic 2	1
FSO, STO output		ABB Drives V1.0	ABB Drives	Output	FSO-12/-21 subsystems	FSO, STO output	H1: FSO, STO output	FSO, STO output	1
FPTC-01/-02		ABB Drives V1.0	ABB Drives	Logic	FPTC	FPTC-01/-02	H1: 1 channel	FPTC-01/-02	FPTC-01/-02
ACS880 R4-R5		ABB Drives V1.0	ABB Drives	Output	ACS880 (STO)	ACS880 R4-R5	H1: ACS880 R4-R5, STO - Dual Channel	ACS880 R4-R5 400V-500V	1

6 Assessment/approval

Project and calculations are assessed and verified against standards: ISO 13849-1

[ ]Approved [ ]Not approved

(Name of the Approver) Signature of approver

7 Terms and conditions

Tool name: Functional safety design tool
Tool version: 1.2.0.2

Libraries used:

Library	Version
SE_VDMA_INPUT_2020_02_24	002.000.001
ABB Drives	001.000.111

THANK YOU FOR PURCHASING AND USING THIS ABB PRODUCT. IT IS IMPORTANT THAT YOU CAREFULLY READ THIS LICENCE. BY INSTALLING, COPYING, OR OTHERWISE USING THE PRODUCT YOU AGREE TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS LICENCE AGREEMENT. IF YOU DO NOT ACCEPT OR AGREE TO THESE TERMS YOU SHALL NOT USE THE PRODUCT.

SOFTWARE LICENCE AGREEMENT

ABB Oy grants you a non-exclusive, non-transferable licence to use this copy of the program and the acccompanying documentation according to the following terms:

LICENCE:

You may:

- install and use the program only on a single computer; and
- make one (1) copy of the program solely for backup purposes, provided that you reproduce all proprietary notices on the copy; and
- use the installed program from another computer, provided that the program is used only on one computer at a time.

You may not:

- install and use the program on more than one computer or workstation at a time; new download with registration is needed if more copies are needed
- modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or copy (except for the backup copy) the program or the accompanying documentation;
- rent, transfer or grant any rights in the program or accompanying documentation in any form to any person without the prior written consent of ABB Oy; or
- remove any proprietary notices, labels, or marks on the program and accompanying documentation. This licence is not on sale. Title and copyrights to the program, accompanying documentation and any copy made by you remain with ABB Oy. Unauthorized copying of the program or the accompanying documentation, or failure to comply with the above restrictions, will result in automatic termination of this licence and will make available to ABB Oy other legal remedies.

LIMITED WARRANTY AND DISCLAIMER

12345Y Moottorin hätäpysäytys

ABB Oy warrants that, for a period of ninety (90) days from the date of delivery to you as evidenced by a copy of your receipt, the distribution media on which the program is furnished under normal use will be free from defects in materials and workmanship and the program under normal use will perform without significant errors that make it unusable. ABB Oy's entire liability and your exclusive remedy under this warranty will be, at ABB Oy's option, to attempt to correct or help you around errors with efforts which ABB Oy believes suitable to the problem, to replace the program or distribution media with functionally equivalent software or distribution media, as applicable, or to refund the purchase price and terminate this Agreement.

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTIES, ABB OY MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

ABB Oy does not warrant that the operation of the program will be uninterrupted or error free.ABB Oy does not make any assurances with regard to the accuracy of the selections or any other output deriving from the use of software. Knowledge and correct application of the relevant standards and directives, in particular ISO 13849-1 and IEC 62061 are a requirement for using this tool.

LIMITATION OF LIABILITY

IN NO EVENT SHALL ABB OY BE LIABLE TO YOU OR TO ANY THIRD PARTY FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA, LOST PROFITS OR OPERATIONS, COST OF CAPITAL OR OTHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES ARISING FROM THE USE OF THE PROGRAM OR ACCOMPANYING DOCUMENTATION, HOWEVER CAUSED AND UNDER ANY LEGAL THEORY. THIS LIMITATION WILL APPLY EVEN IF ABB OY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT THE LICENCE FEE REFLECTS THIS ALLOCATION OF RISK.

GENERAL

This Agreement will be governed by the laws of Finland. This Agreement is the entire agreement between us and supersedes any other communications or advertising with respect to the program and accompanying documentation. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect.

Any disputes or differences which may arise out of or in connection with this program or its use, shall be settled in the Helsinki City Court in accordance with Finnish Law.

8 Appendix

8.1 ISO CCF check list

1) Separation/Segregation		
	15	Physical separation between signal paths: separation in wiring/piping. sufficient clearances and creepage distance on printed-circuit boards. detection of short circuits and open circuits in cables by dynamic test. separate shielding for the signal path of each channel.
2) Diversity		
	20	Different technologies/design or physical principles are used, for example: first channel electronic or programmable electronic and second channel electromechanical hardwired, different initiation of safety function for each channel (e.g. position, pressure, temperature) and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures.
3) Design/application/experience		
3.1)	15	Protection against over-voltage, over-pressure, over-current, over-temperature etc.
3.2)	5	Components used are well-tried.
4) Assessment/analysis		
	5	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.
5) Competence/training		
	5	Training of designers to understand the causes and consequences of common cause failures.
6) Environmental		
6.1)	25	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered.
6.2)	10	Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).

Liite 5. Moottorin hätäpysäytys ABB FSDT-01-raportti

PILZ

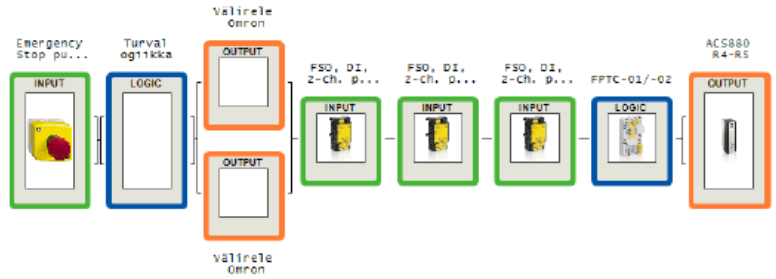
Project name	Moottorin hätäpysäytys
Safety standard	ISO 13849-1:2015 + EN ISO 13849-2:2012
Author	EEKOH
Company name	
Company address	
Version	
Creation Date	April 5, 2023 12:44:22 PM EEST
Last saved date	April 5, 2023 12:44:22 PM EEST
Pilz PAScal	Version v1.9.1 Build 24

Using Version 4.0 of the calculation algorithm in accordance with EN ISO 13849-1
Using Version 3.1 of the calculation algorithm in accordance with EN/IEC 62061

SRP/CS overview

System/Module	Target PL	Result	CCF Factor	PFH_D	Achieved PL
Moottorin hätäpysäytys	c	Target Achieved	Target Achieved	1.04E-07	c

details: Moottorin hätäpysäytys



Name	Moottorin hätäpysäytys
Comment	SF1 Laukaiseva tekijä: Hätäpysäytyspainikkeeseen vaikutetaan Reaktio ja käyttäytyminen tehonsyötön katketessa: moottorin tehonsyöttö loppuu Turvallinen tila: Moottori ja vaarallinen liike pysähtynyt Toimintatapa: Tiheiden vaateiden Turvatoiminnon vaateiden taajuus: 1/a
Target PL	c
Result	Target Achieved
CCF Factor	Target Achieved
PFH_D	1.04E-07
Achieved PL	c

CCF result

Separation/segregation	**Point(s):15/15**
1	Yes (15)
Diversity	**Point(s):0/20**
2	No (0)
Design/application/experience	**Point(s):20/20**
3.1	Yes (15)
3.2	Yes (5)
Assessment/analysis	**Point(s):0/5**
4	No (0)
Competence/training	**Point(s):5/5**
5	Yes (5)

Environmental	Point(s):35/35
6.1	Yes (25)
6.2	Yes (10)

PILZ

Subsystem details: Moottorin hätäpysäytys

Subsystem	Author	Type	Number of physical elements/channels	Cat.	Diagnostic coverage [%]
Subsystem 1		Input	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 2		Logic	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 3		Output	Two	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 4		Input	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 5		Input	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 6		Input	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 7		Logic	One	Category calculated by PAScal	Created from DC for the elements contained
Subsystem 8		Output	One	Category calculated by PAScal	Created from DC for the elements contained

Device	Subsystem	Operational hours per day	Operational days per year	Time between two operations	Calculated Number of Operations [per hour]	Mission time [year(s)]	Fault detection on wiring	Diagnostic coverage [%]	Demand mode <= 1/100 test rate (Category 2)	$MTTF_D$ [year(s)]
1.1.1.1 - Emergency Stop push button[1] [***]	Subsystem 1	-	-	-	-	20.00	None	-	No	-
1.2.1.1 - Turvalogiikka [2] [***]	Subsystem 2	-	-	-	-	20.00	None	-	No	-
1.3.1.1 - Välirele Omron[3] [**] [***]	Subsystem 3	24	365	1.00 year(s)	0.00011	20.00	None	90.00	No	9000000.00

Device	Subsystem	Operational hours per day	Operational days per year	Time between two operations	Calculated Number of Operations [per hour]	Mission time [year(s)]	Fault detection on wiring	Diagnostic coverage [%]	Demand mode <= 1/100 test rate (Category 2)	$MTTF_D$ [year(s)]
1.3.2.1 - Välirele Omron[3] [**] [***]	Subsystem 3	24	365	1.00 year(s)	0.00011	20.00	None	90.00	No	9000000.00
1.4.1.1 - FSO, DI, 2-ch. pulsed[4] [***]	Subsystem 4	-	-	-	-	20.00	None	-	No	-
1.5.1.1 - FSO, DI, 2-ch. pulsed[4] [***]	Subsystem 5	-	-	-	-	20.00	None	-	No	-
1.6.1.1 - FSO, DI, 2-ch. pulsed[4] [***]	Subsystem 6	-	-	-	-	20.00	None	-	No	-
1.7.1.1 - FPTC-01/-02 [5] [***]	Subsystem 7	-	-	-	-	20.00	None	-	No	-
1.8.1.1 - ACS880 R4-R5[6] [***]	Subsystem 8	-	-	-	-	20.00	None	-	No	-

[**]The user has changed the value specified by PAScal for diagnostic coverage. PAScal uses this parameter to calculate the safety-related characteristic data. If the diagnostic coverage is incorrect, PAScal may calculate the safety level of SRP/CS to be higher than it actually is.
[***]Replace the components after the specified number of years. Please include this in your user manual.
[Number] : See component data for details

PL/PFH_D Calculation Data

Subsystem/channel	PL	PFH_D	Cat.	DCavg	$MTTF_D$: Limited	$MTTF_D$: sym.	$MTTF_D$ values for Channel 1	$MTTF_D$ values for Channel 2	DC	CCF
Moottorin hätäpysäytys	c	1.04E-07								
1.1.1.1 - Emergency Stop push button	e	2.47E-08	4							
1.2.1.1 - Turvalogiikka	e	3.20E-08	4							

Subsystem/channel	PL	PFH_D	Cat.	DCavg	$MTTF_D$: Limited	$MTTF_D$: sym.	$MTTF_D$ values for Channel 1	$MTTF_D$ values for Channel 2	DC	CCF
Output	e	4.29E-08	3	90.00%	100.00 years	100.00 years	100.00 years	100.00 years		75
1.3.1.1 - Välirele Omron							9000000.00 years		90.00%	
1.3.2.1 - Välirele Omron								9000000.00 years	90.00%	
1.4.1.1 - FSO, DI, 2-ch. pulsed	e	1.80E-12	2							
1.5.1.1 - FSO, DI, 2-ch. pulsed	e	1.80E-12	2							
1.6.1.1 - FSO, DI, 2-ch. pulsed	e	1.80E-12	2							
1.7.1.1 - FPTC-01/-02	c	1.60E-09	1							
1.8.1.1 - ACS880 R4-R5	e	3.23E-09	3							

Component data

Number	Component type	Name	PL	PFHD [per hour]	B10D	MTTFD [year(s)]
1	Input	Emergency Stop push button	e	2.47E-8	-	-
	Selected device	E-stop, 2 contacts | Input devices				
	Selected limitations	Input | - | - | - | -				
2	Logic	Turvalogiikka	e	3.2E-8	-	-
	Selected device	1234 V1.1.1				
	Selected limitations	Logic unit				
3	Output	Välirele Omron	-	-	900,000	-
	Selected device	G7S-3A3B-E+P7S-14F-END				
	Selected limitations	#ConstraintsNotAvailable				
4	Input	FSO, DI, 2-ch. pulsed	e	1.8E-12	-	-
	Selected device	FSO, DI, 2-ch. pulsed				
	Selected limitations	FSO, DI, 2-ch. pulsed				
5	Logic	FPTC-01/-02	c	1.6E-9	-	-
	Selected device	FPTC-01/-02				
	Selected limitations	2 channels				
6	Output	ACS880 R4-R5	e	3.23E-9	-	-
	Selected device	ACS880 R4-R5 400V-500V				
	Selected limitations	ACS880 R4-R5, STO - Dual Channel				

CCF questions (EN ISO 13849-1)

ID	Group	Question
1	Separation / segregation	Physical separation between signal paths e.g. separation in wiring/piping, e.g. sufficient clearances and creepage distances on printed-circuit boards
2	Diversity	Different technologies/design or physical principles are used e.g. first channel programmable electronic and second channel hardwired e.g. kind of initiation e.g. pressure and temperature Measuring of distance and pressure e.g. digital and analogue Components of different manufacturers.
3.1	Design / application / experience	Protection against over-voltage, over-pressure, over-current, etc.
3.2		Components used are well-tried.
4	Assessment / analysis	Are the results of a failure mode and effect analysis taken into account to avoid common-cause failures in design?
5	Competence / training	Have designers/maintainers been trained to understand the causes and consequences of common-cause failures?
6.1	Environmental	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.
6.2		Other influences: Are the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) considered?

Questions about risk analysis (EN ISO 13849-1)

Risk parameter	Examination	Evaluation
Severity	Severity of Injury	Slight (normally reversible injury) Serious (normally irreversible injury including death)
Frequency/ Exposure	Frequency and/or exposure to a hazard	Seldom to less often and/or the exposure time is short Frequent to continuous and/or the exposure time is long
Possibility of Avoidance	Possibility of avoiding the hazard or limiting the harm	Possible under specific conditions Scarcely Possible

PILZ

Explanation of category (EN ISO 13849-1)

The results of the calculation will only be valid if the following requirements are also met.

Category	Summary of requirements	System behaviour
B	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance wit relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.
1	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.
2	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.
3	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that - a single fault in any of these parts does not lead to the loss of the safety function, and - whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.
4	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that - a single fault in any of these parts does not lead to a loss of the safety function, and -the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.

END USER DISCLAIMER FOR PASCAL

The PAScal calculation tool can help you to define the Performance Level in accordance with EN ISO 13849-1 and the SIL in accordance with EN/IEC 62061. Additional requirements of the standards (e.g. requirements for safety-related software and systematic safety integrity) must be considered separately. Knowledge and correct application of the relevant standards and directives, in particular EN ISO 13849-1, EN/IEC 62061 and IEC 61508 are therefore a requirement for using this tool. Warranty and liability claims will be rendered invalid if damages can be attributed to a failure to follow the guidelines in the operating manual, if the libraries used are not current, or if the user of this software is not suitably qualified.

All calculations are made in accordance with the current status of the standards and to the best of our knowledge and belief. While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular it should be noted that the calculation results do not have the legal quality of assurances or assured properties. The plausibility of these results should therefore be validated.

The following libraries are used to calculate the safety functions:

Manufacturer	Library	Version
SE_VDMA_INPUT_2020_02_24	Schneider Electric SE_VDMA	2.0.1
ABB Drives	ABB Drives VDMA library format v1_8	001.000.111
Oma	omakirjasto	1.1.1

Use only libraries of trusted sources. Make sure to verify the origin of the used libraries. Confirm the device data against documentation and certificates provided by device manufacturers.

Please note: Latest versions of the libraries in PAScal format are available on:www.pilz.com/PAScal_Lib

Libraries in other formats are typically available directly on the device manufacturers' web sites.

PAScal is a tool produced by Pilz

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Germany
Tel.: +49 711 3409-0
Fax: +49 711 3409-133
www.pilz.com