jamk.fi

Eräkeittämöprosessin turva-automaatioratkaisut ja niiden vaatimusten täyttymisen osoittaminen

Mikko Rauvola

Opinnäytetyö
Huhtikuu 2019
Tekniikan ala
Insinööri (AMK), sähkö- ja automaatiotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Rauvola, Mikko	Opinnäytetyö, AMK	Elokuu 2019
	Sivumäärä 62	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Eräkeittämöprosessin turva-automaatioratkaisut ja niiden vaatimusten täyttymisen osoittaminen

Tutkinto-ohjelma

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

Työn ohjaaja(t)

Ari Kuisma, Veli-Matti Häkkinen

Toimeksiantaja(t)

Proense Oy

Tiivistelmä

Turva-automaation rooli prosessiteollisuudessa on erittäin tärkeä. Sen avulla pyritään pienentämään riskiä siedettävälle tasolle, mikäli siihen ei muilla keinoilla pystytä. Vaatimustenmukaisuustodistuksen saamiseksi on pystyttävä osoittamaan, että turva-automaation toiminta on riittävän todennäköistä vaadittaessa. Turva-automaatiojärjestelmään kohdistuvat vaatimukset on esitetty standardeissa SFS-EN 61508 ja SFS-EN 61511.

Opinnäytetyön tavoitteena oli selvittää, mitkä tekijät vaikuttavat turvallisuuden eheyden tason määräytymiseen turvatoiminnoilla. Samalla osoitettiin, että Valmetin projektissa Belgian Burgo Ardennesin eräkeittämöllä turva-automaatioratkaisut ovat riittäviä. Kaikki turvatoiminnot on kahdennettu, joten haluttiin myös selvittää, onko kahdennus välttämätön. Pienempi laitemäärä laskisi kustannuksia huomattavasti. Lisäksi käyttökatkokset vähenisivät, koska kun vikaantuminen havaitaan, prosessi ohjataan aina turvalliseen tilaan.

Vikaantumistodennäköisyyslaskennoissa hyödynnettiin laskentatyökalu Sistemaa. Sistema on luotu auttamaan koneiden ja ohjausjärjestelmien suunnittelussa. Laskentamenetelmät ovat samat kuin prosessiteollisuudessa, joten siksi sitä voitiin hyödyntää laskennoissa. Arkkitehtuurin rajoitusten arviointi on myös toteutettava jokaiselle turvatoiminnolle.

Työn tuloksena toimeksiantaja sai tiedon, ovatko projektissa tehdyt turva-automaatio ratkaisut standardien vaatimusten mukaisia. Työn pohjalta toimeksiantaja voi luoda laitevalintoja koskevan suunnitteluohjeen tuleviin projekteihinsa.

Avainsanat (asiasanat)

Turva-automaatio, turvallisuuden eheyden tasot, Sistema, arkkitehtuurin rajoitukset,

Muut tiedot (Salassa pidettävät liitteet)

.

jamk.fi

Description

Author(s)	Type of publication	Date
Rauvola, Mikko	Bachelor's thesis	August 2019
		Language of publication: Finnish
	Number of pages: 62	Permission for web publication: x

Title of publication

Proving compliance of safety automation solutions and safety functions of batch cooking project

Degree programme

Bachelor's Degree Programme in Electrical and Automation Engineering

Supervisor(s)

Kuisma, Ari & Häkkinen, Veli-Matti

Assigned by

Proense Oy

Abstract

Safety automation has a very important role in the process industry. It is used for reducing the risks to a tolerable level in case other ways do not lower the risks enough. To gain the Clarification of Conformity, the working of a safety related system needs to be proved probable enough. The requirements of safety related systems are presented in standards SFS-EN 61508 and SFS-EN 61511.

The goal was to find out which factors affect the safety integrity levels of safety functions. Additionally, it was proved that the solutions of the safety related systems on Valmets Burgo Ardennes batch cooking project were sufficient. All safety functions were redundant, and it needed to be found out if they were necessary. A lower number of equipment would decrease the costs and downtime, because every time the failure is detected, the process is forced into safe state.

Sistema software was used with the failure calculations. Sistema has been created to help with designing machines and control systems. Because the calculation principles are the same with process industry it was allowed to be used. Also, the evaluation of architectural constraints needed to be done for safety functions.

As a result, the customer will get the information that the solutions correspond the standards. With the knowledge of the factors affecting safety integrity levels, the customer could create instruction for choosing the instruments.

Keywords/tags (subjects)

Safety Integrity Levels, Sistema, Architectural constraints, Safety automation

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Termit

S/E/OE	Turvallisuuteen liittyvä järjestelmä
OL	Ohjattava laitteisto
PFD	Vaarallisen vikaantumisen todennäköisyys vaadittaessa
PFH	Vaarallisen vikaantumisen keskimääräinen taajuus
λ_d	Vaaralliset vikaantumiset
λ_s	Turvalliset vikaantumiset
λ_{dd}	Vaaralliset havaitut vikaantumiset
λ_{du}	Vaaralliset havaitsemattomat vikaantumiset
λ_{sd}	Turvalliset havaitut vikaantumiset
λ_{su}	Turvalliset havaitsemattomat vikaantumiset
Alajärjestelmä	Turvallisuuteen liittyvän järjestelmän ylätason arkkitehtuurirakenteen itsenäinen kokonaisuus, jossa alajärjestelmän vaarallinen vikaantuminen johtaa turvatoiminnon vaaralliseen vikaantumiseen
TET	Turvallisuuden eheyden taso (Engl. Safety Integrity Level, SIL)

1 Johdanto

Turva-automaatio on tärkeässä roolissa prosessiteollisuudessa. Sitä käytetään lähes jokaisella teollisuudenalalla onnettomuuksien ennaltaehkäisyyn. Turva-automaatiojärjestelmät parantavat prosessien turvallisuutta pienentämällä riskejä. Turva-automaatiojärjestelmät koostuvat laitevalmistajien laitteista, jotka on luokiteltu eri standardien mukaan. Prosessiteollisuuden toiminnalliseen turvallisuuteen liittyvä standardi on SFS-EN 61511, joka pohjautuu standardiin SFS-EN 61508, joka puolestaan on yleisesti pätevä kaikille teollisuuden aloille. Muita toiminnalliseen turvallisuuteen liittyviä standardeja ovat esimerkiksi SFS-EN-ISO 13849-1 ja SFS-EN 62061, jotka keskittyvät koneturvallisuuteen.

Prosessia joudutaan pohtimaan turvallisuuden näkökulmasta jo suunnitteluvaiheesta asti. Riskejä sisältävästä prosessista on tehtävä riskianalyysi, jonka pohjalta ruvetaan pohtimaan keinoja riskien pienentämiseksi. Laitevalinnoilla ja riittävän konfiguraation valinnalla voidaan vaikuttaa turvajärjestelmän varmempaan toimintaan sitä vaadittaessa. Prosessien turvallisuuteen on viime vuosina alettu kiinnittämään enemmän huomiota. Sen lisäksi, että turva-automaatiojärjestelmiin liittyvät säädökset ovat tiukentuneet, yritykset kiinnittävät enemmän huomiota turvallisuusasioihin oman imagonsa säilyttämiseksi. Myös maissa, joissa turvallisuusasiat eivät ole ennen olleet tärkeitä, on turvallisuuteen alettu kiinnittää yhä enemmän huomiota.

Opinnäytetyön toimeksiantaja on Proense Oy, ja opinnäytetyö tehtiin toimeksiantona Valmetille, joka on yksi maailman johtavista sellu- ja paperitehtaiden toimittajista. Valmetilla on myös vankka asema teknologian, automaation ja palveluiden toimittajana, sekä sellu-, paperi-, ja energiateollisuuden kehittäjänä. Valmet työllistää n. 13000 henkilöä, joista Suomessa työskentelee n. 5100. Toimeksianto liittyi Valmetin käynnissä olevaan eräkeittämöprojektiin Belgian Burgo Ardennesissa. (Valmet Suomessa, n.d.)

Opinnäytetyössä tuli tarkastella, mitkä asiat vaikuttavat turva-automaatiojärjestelmän turvallisuuden eheyden tason määräytymiseen standardin SFS-EN 61508 ja SFS-EN 61511 mukaan. Lisäksi tuli tehdä vikaantumistodennäköisyyslaskelmat kolmen eri

päätyypin turvapiireille hyödyntäen Sistema-laskentatyökalua. Tavoitteena oli selventää toimeksiantajalle, mitkä tekijät vaikuttavat turvallisuuden eheyden tason määräytymiseen, jotta tutkimuksen perusteella toimeksiantaja voi luoda suunnitteluohjeen turva-automaatiolaitteiden valintaan. Toisena tavoitteena oli optimoida laitemääriä ja työssä selvitettiinkin, onko mahdollista saavuttaa tavoiteltava turvallisuuden eheyden taso pienemmällä laitemäärällä. Pienempi laitemäärä vähentää prosessin käyttökatkoksia ja lisäksi kustannukset laskevat huomattavasti.

2 Turva-automaation rooli prosessiteollisuudessa

Prosessilaitosten ja prosessien riskien pienentäminen on mahdollista toteuttaa monin erilaisin keinoin. Hyvä laitos- ja prosessisuunnittelu mahdollistaa pienemmän riskin saavuttamisen. Turva-automaatiojärjestelmä on avainasemassa riskien pienentämisessä, mikäli prosessia tai konetta ei saada turvalliseksi muilla menetelmillä. Se on laitteen käyttöautomaatiosta erillinen järjestelmä, jonka tehtävänä on saattaa prosessi tai laite turvalliseen tilaan vikaantumisen tai häiriön tapahduttua, mikäli käyttöautomaatiojärjestelmä tai muu varautuminen pettävät. Turva-automaatiojärjestelmän pettämisellä saattaa olla vakavat seuraukset. Seurauksena voi olla esimerkiksi henkilö-, ympäristö- tai omaisuusvahinkoja. (Turva-automaatio prosessiteollisuudessa 2007, 3.)

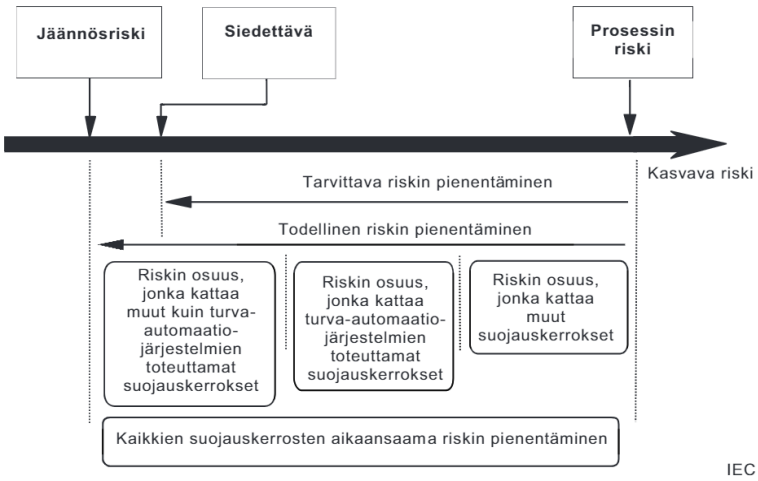
Turva-automaatiolla pyritään varmentamaan prosessin toiminnallinen turvallisuus. Turvatekniikan keskus määrittelee toiminnallisen turvallisuuden seuraavasti: *“Toiminnallisella turvallisuudella tarkoitetaan sitä osaa kokonaisturvallisuudesta, joka riippuu järjestelmien ja laitteiden oikeasta ja oikea-aikaisesta toiminnasta. Toiminnallinen turvallisuus voidaan todeta riittäväksi, kun järjestelmät on määritetty oikein, niiden toiminta on luotettavaa ja toiminta suunniteltua. Turva-automaatio järjestelmän on sovelluttava käyttötarkoitukseensa toiminnan ja rakenteensa puolesta ja lisäksi on varmistuttava siitä, että se on olosuhteisiin sopiva*.” (Mts. 4.)

Turva-automaatiojärjestelmille on asetettu useita vaatimuksia, jotka niiden tulee täyttää. Niiden tulee olla riippumattomia muista järjestelmistä. Suunnitteluvaiheessa

on otettava huomioon, että niiden toiminnan on oltava riittävän luotettavaa vaadittaessa. Turva-automaatiojärjestelmien on sovelluttava kohteisiin ja niiden turvallisuus ja luotettavuus on pystyttävä osoittamaan ja arvioimaan. Niissä tulisi käyttää ensisijaisesti laitteita, jotka ovat turvakäyttöön sertifioituja. Laitteiden valinnoissa on otettava huomioon huollettavuus ja koestettavuus. Laitteiden vikaantuessa niiden tulisi siirtyä turvalliseen tilaan. Turva-automaatiojärjestelmät eivät myöskään saa aiheuttaa tarpeettomia ja turvallisuutta vaarantavia alasajoja. Prosessin on myös oltava manuaalisesti pysäytettävissä. (Mts. 4.)

3 Riskit ja niiden vähentäminen

Riskillä tarkoitetaan negatiivisen lopputuloksen mahdollisuutta. Laitosten suunnitteluvaiheessa prosessille tehdään riskianalyysi, jossa riskit arvioidaan ja määritellään turvallisuuden eheyden taso, jonka mukaan varaudutaan riskille. Riskianalyysimenetelmiä on useita. Yksi prosessiteollisuudessa yleisimmin käytetyistä menetelmistä on HAZOP-analyysi. Riskinvähennys ja järjestelmien riittävyys riippuu prosessin luonteesta. Mitä vaarallisempi prosessi, sitä enemmän riskinvähennykseltä vaaditaan luotettavuutta. (Turva-automaatio prosessiteollisuudessa 2007, 5.)



Kuvio 1. Riskien vähennys (SFS-EN 61511-3, 2017, 14)

Kuviossa 1 on esitetty riskien vähennyksen perusperiaatteet. Riskien vähennys on mahdollista toteuttaa monin eri menetelmin. Turva-automaation avulla toteutetaan vain osa prosessin riskin vähennyksestä. Muita menetelmiä riskin vähentämiseen ovat esimerkiksi muut turvalaitteet ja järjestelmät, ohjeet ja suojavallit. Turva-automaatiolta edellytettävä riskinvähennyksen määrä on arvioitava ja määriteltävä tapauskohtaisesti. (Mts. 4.)

Kuviossa 1 esiintyvät riskit on määritelty standardissa SFS-EN 61511-3 (2017, 13) seuraavasti:

> *-Prosessin riski: Määrätyissä vaarallisissa tapahtumissa olemassa oleva riski prosessille, prosessin käyttö- ja perusautomaatiojärjestelmälle ja siihen liittyville inhimillisille tekijöille, kun tämän riskin arvioinnissa ei ole tarkasteltu mitään toteutettua turvallisuuteen liittyvää suojausominaisuutta.*
>
> *-Siedettävä riski (esim. prosessiturvallisuuden tavoitetaso): riski, joka on hyväksytty määrätyssä asiayhteydessä yhteiskunnassa vallitsevien sen hetkisten arvojen mukaan.*
>
> *-Jäännösriski: tämän standardin asiayhteydessä jäännösriski on vaarallisen tapahtuman esiintymisen riski suojauskerrosten lisäämisen jälkeen.*

4 Turvallisuuden eheyden tasot ja suoritustasot

Turvallisuutta voidaan mitata eri standardien mukaan. Standardissa SFS-EN ISO 13849-1 on esitetty suoritustasot (Performance Level), kun taas standardissa SFS-EN 61508 turvallisuutta mitataan turvallisuuden eheyden tasoilla (Safety Integrity Level). Suoritustasoja on olemassa viisi: a-, b-, c-, d- ja e-tasot. Prosessiteollisuudessa turvallisuuden eheyden tasoja on käytössä kolme: SIL-1, SIL-2 ja SIL-3. SIL-4 luokka on myös

olemassa, mutta se on käytössä ainoastaan suuren onnettomuuden vaaran omaavissa laitoksissa, esimerkiksi ydinvoimaloissa. Taulukosta 1 nähdään, että suoritustasojen ja turvallisuuden eheyden tasojen välillä on selkeä yhteys vaarallisen vikaantumisen todennäköisyyden suhteen. Suoritustasot b ja c vastaavat SIL-1 luokkaa. Suoritustaso d, vastaa luokkaa SIL-2 ja e puolestaan luokkaa SIL-3. (Robinson. n.d.)

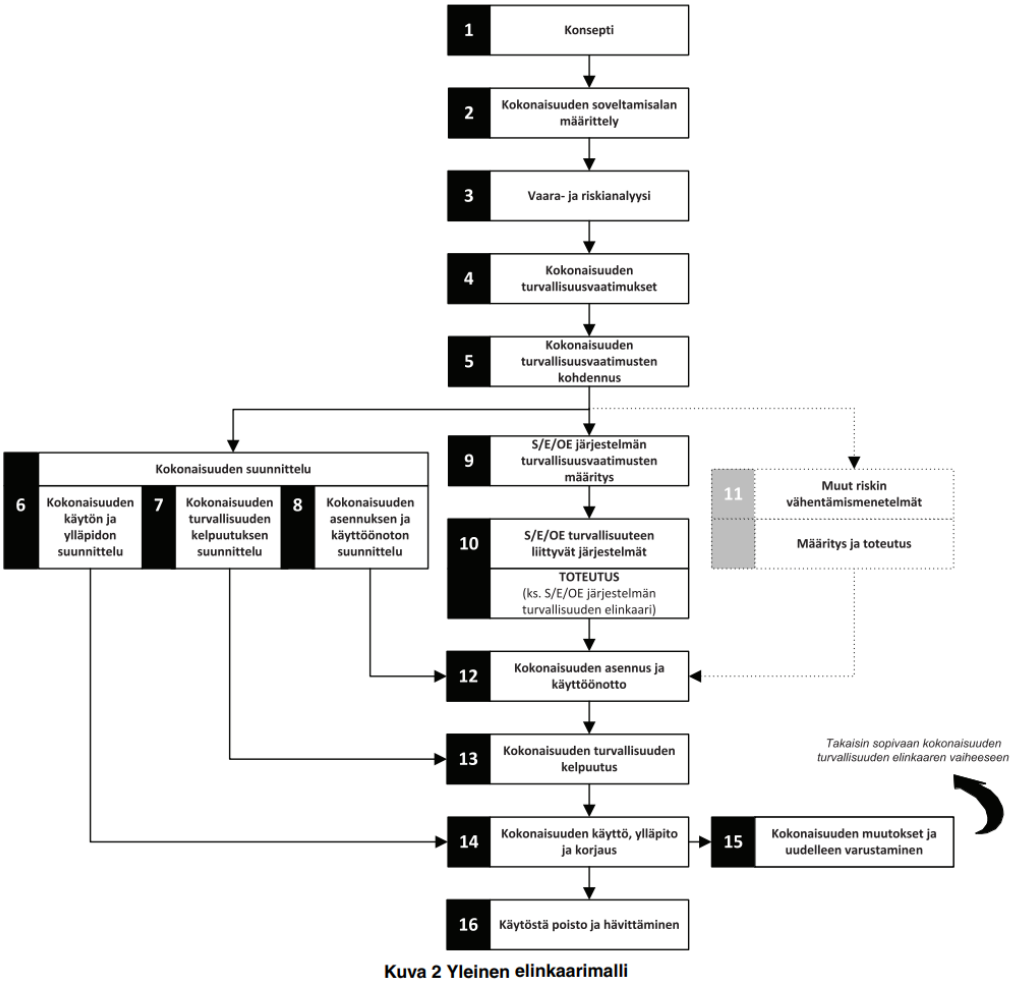
Taulukko 1. Suoritustasojen ja turvallisuuden eheyden tasojen vastaavuus (Robinson. n.d.)

EN ISO 13849-1 **Suoritustaso (PL)**	**Vaarallisen vikaantumisen todennäköisyys (1/h)**	**IEC 61508 Turvallisuuden eheystaso**
a	$\geq 10^{-5} \ldots < 10^{-4}$	Ei vastaavuutta
b	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	1
c	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$	1
d	$\geq 10^{-7} \ldots < 10^{-6}$	2
e	$\geq 10^{-8} \ldots < 10^{-7}$	3

5 Yleinen elinkaarimalli

Yleinen elinkaarimalli on esitetty standardissa SFS-EN 61508-3 (Ks. Kuvio 2). Elinkaarimallissa esitetään turva-automaatiojärjestelmän elinkaaren vaiheet aina analysoinnista toteutukseen ja testaukseen ja edelleen käyttö- ja huoltovaiheeseen asti. Jokaisessa elinkaaren vaiheessa on noudatettava olemassa olevia standardeja. Analysointivaiheessa määritellään turva-automaatiojärjestelmän vaatimukset. Riskianalyysi ja vaaditut turvallisuuden eheyden tasot määritellään analysointivaiheessa. Asennukset ja käyttöönottotarkastukset (FAT ja SAT) tehdään turva-automaatiojärjestelmille

suunnitelmien mukaan toteutusvaiheessa. Käyttö- ja huoltovaiheessa pidetään huolta siitä, että riskien vähennyksessä käytetyt järjestelmät toimivat suunnitellusti. Niiden pitää toimia luotettavasti koko elinkaarensa ajan. Tästä syystä laitteille on määritelty määräaikaistestausvälit. Laitteet on testattava vähintään vikaantumisto-dennäköisyyslaskennoissa käytetyn määräaikaistestausvälin mukaisesti. Näin voidaan varmistua siitä, että turvatoiminnot toimivat suunnitellusti sitä vaadittaessa. (SFS EN 61508-3:2010, 20.)



Kuvio 2. Yleinen elinkaarimalli (SFS EN 61508-3:2010, 20.)

6 Turvallisuuden eheyden tason määrittäminen riskigraafin avulla

Turvallisuuden eheyden taso määritetään turvatoiminnolle riskianalyysin avulla. Riskianalyysissä todetaan tarpeellinen riskin vähennys. Riskianalyysin perusteella määritellään turvatoiminnot ja niille turvallisuuden eheyden tasot. Vaadittu turvallisuuden eheyden taso voidaan määrittää esimerkiksi riskigraafin avulla ja se määritetään jokaiselle turvatoiminnolle erikseen. Määrittämällä riskiparametrit pystytään osoittamaan turvallisuuden eheyden taso, jonka turvatoiminnon on saavutettava. Kuviosta 3 nähdään, että riskiparametrejä on neljä: seuraukset, altistumisen taajuus ja kesto, mahdollisuus epäonnistua vaaran väistämisessä ja ei-toivotun tapahtuman todennäköisyys. Vaadittu turvallisuuden eheyden taso saadaan selville seuraamalla reittiä määritettyjen parametrien mukaan. Riskigraafin on oltava kalibroitu sopimaan riskin arviointiin. Kalibrointi tapahtuu antamalla parametreille numeeriset arvot, joiden mukaan riskiä arvioidaan. On pystyttävä perustelemaan, miten kyseinen reitti on muodostettu. (SFS-EN 61508-5:2010, 58-66.)

Standardissa SFS-EN 61508-5 (2010, 58-66) parametrit on määritelty seuraavasti:

Seuraukset (C)

- $C_{A=}$ *Lievä vamma*
- $C_{B=}$ *Vakava palautumaton vamma yhdelle tai useammalle henkilölle, yhden henkilön kuolema*
- $C_{C=}$ *Useamman henkilön kuolema*
- $C_{D=}$ *Hyvin monen henkilön kuolema*

Taajuus ja altistumisaika (F)

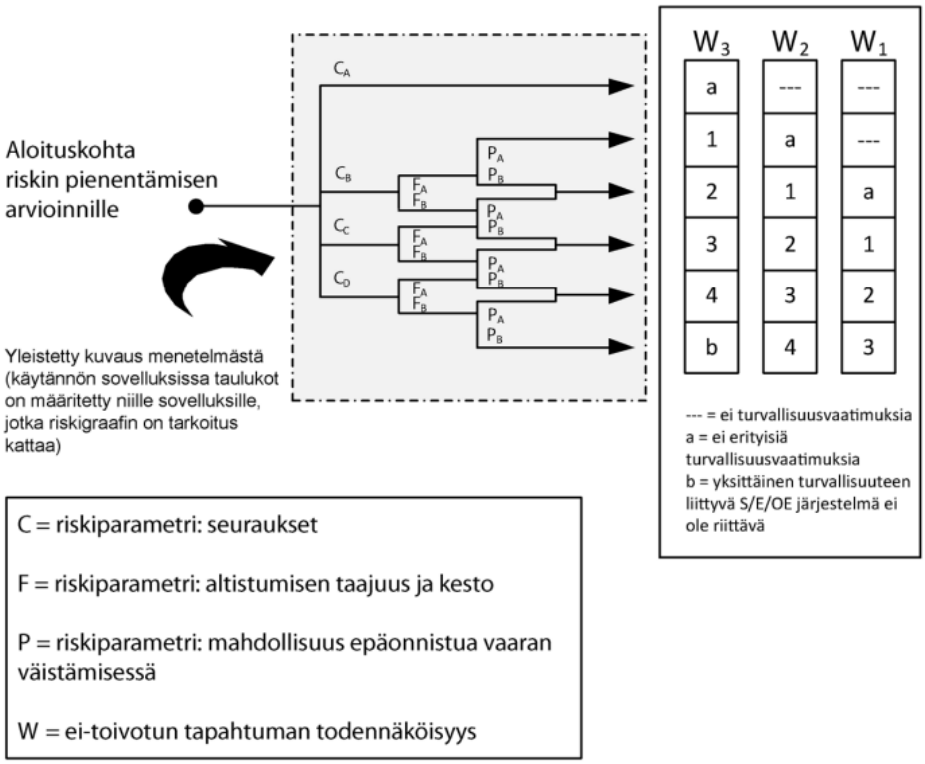
- $F_{A=}$ *Altistuminen vaaravyöhykkeellä harvoin tai melko usein*
- $F_{B=}$ *Altistuminen vaaravyöhykkeellä usein tai jatkuvasti*

Mahdollisuus välttää vaarallinen tapahtuma (P)

- *$P_{A=}$ Mahdollista määrätyissä olosuhteissa*
- *$P_{B=}$ Lähes mahdotonta*

Ei-toivotun tapahtuman todennäköisyys (W)

- *$W_{1=}$ Hyvin pieni todennäköisyys siihen, että ei-toivottuja tapahtumia sattuu ja vain muutama ei toivottu tapahtuma on todennäköinen*
- *$W_{2=}$ Pieni todennäköisyys siihen, että ei-toivottuja tapahtumia sattuu ja vain muutama ei-toivottu tapahtuma on todennäköinen*
- *$W_{3=}$ Suhteellisen suuri todennäköisyys siihen, että ei-toivottuja tapahtumia sattuu ja useat ei-toivotut tapahtumat ovat todennäköisiä*



Kuvio 3. Riskigraafi TET:n määrittämiseen (SFS-EN 61508-5:2010, 62.)

7 Vaatimukset turvallisuuden eheyden tasojen täyttymiseksi

7.1 Toimintatavan määräytyminen

Toimintatavalla tarkoitetaan tapaa, jolla turvatoiminta toimii. Toimintatapa on jaettu kolmeen eri tyyppiin. Standardissa SFS-EN 61508-4 (2010, 38) toimintatavat on jaoteltu ja määritelty seuraavasti kohdassa 3.5.16:

> *-Harvojen vaateiden tapa: missä turvatoiminta suoritetaan vain vaateesta OL:n siirtämiseksi määritettyyn turvalliseen tilaan, ja missä vaateiden taajuus ei ole suurempi kuin yksi vuodessa, tai*
>
> *-Tiheiden vaateiden tapa: missä turvatoiminta suoritetaan vain vaateesta OL:n siirtämiseksi määritettyyn turvalliseen tilaan, ja missä vaateiden taajuus on suurempi kuin yksi vuodessa, tai*
>
> *- Jatkuvan toiminnan tapa: missä turvatoiminta pitää OL:n turvallisessa tilassa osana normaalia toimintaa*

Toimintatavalla on vaikutus vikaantumistodennäköisyyslaskennassa käytettäviin kaavoihin. Harvojen vaateiden toimintatavalla laskettaessa vikaantumistodennäköisyys saadaan vuositasolla (PFD), kun taas tiheiden vaateiden toimintatavalla ja jatkuvan toiminnantavalla vaarallisen vikaantumisen keskimääräinen taajuus saadaan tuntia kohden (PFH). (SFS-EN 61508-4:2010, 46-50.)

7.2 Arkkitehtuurin rajoitukset

7.2.1 Arkkitehtuurin rajoitusten täyttyminen ja vikasietoisuus

Arkkitehtuurin rajoituksien täyttyminen on pystyttävä osoittamaan kaikilla turva-automaatiojärjestelmän laitteilla. Arkkitehtuurin rajoitusten täyttymisen osoittamiseen on olemassa kolme eri tapaa. Standardin SFS-EN 61508 mukaan käytössä olevat menetelmät ovat Reitti 1_H ja Reitti 2_H. Standardin SFS-EN 61511 mukaan arkkitehtuurin

valinta on sidoksissa turvallisuuden eheyden tasoon ja valittuun toimintatapaan. Standardin SFS-EN 61511 menetelmä on johdettu standardin SFS-EN 61508 reitti 2_H-menetelmästä. (Gruhn 2016, 1-6.)

Laitteiston vikasietoisuudella tarkoitetaan turvajärjestelmän kykenevyyttä toteuttaa turvatoiminto vaarallisen vikaantumisen esiintyessä. Taulukosta 3 nähdään, että vikasietoisuuden ollessa X, X+1 vaarallista vikaantumista johtaa turvatoiminnon menettämiseen. (Mts.)

Taulukko 2. Konfiguraatiot ja niiden vikasietoisuudet (Gruhn 2016, 2.)

Vikasietoisuus	**Konfiguraatiot**
0	**1oo1, 2oo2**
1	**1oo2,2oo3**
2	**1oo3,2oo4**

Standardissa SFS-EN 61511 on esitetty vikasietoisuuden perusvaatimukset kenttälaitteille eri turvallisuuden eheyden tasojen mukaan. Taulukosta 2 nähdään, että arkkitehtuurin vaatimukset saadaan täytettyä muuttamalla valittua konfiguraatiota standardin SFS-EN 61511 mukaan. SIL-2 tasolla on huomioitava myös toimintatapa (Mts.)

Taulukko 3. Kenttälaitteiden vikasietoisuustaulukko standardin SFS-EN 61511 mukaan (SFS-EN 61511-1:2017, 65.)

Turvallisuuden eheyden taso (SIL)	Pienin sallittu laitteiston vikasietoisuus
1 (Mikä tahansa toimintatapa)	**0**
2 (Harvojen vaateiden toimintatapa)	**0**
2 (Tiheiden vaateiden toimintatapa)	**1**
3 (Mikä tahansa toimintatapa)	**1**
4 (Mikä tahansa toimintatapa)	**2**

7.2.2 Reitin valinta

Reitin valintaan vaikuttavat monet eri tekijät, esimerkiksi sovellus ja soveltamisala. On otettava myös huomioon, että toiminnon vikaantuminen voi aiheuttaa uuden vaaran tai se voi olla uuden vaaran syntymissyynä. Redundanttista järjestelmää ei kaikissa tapauksissa ole mahdollista toteuttaa, joten se on myös yksi valintaan vaikuttava tekijä. Lisäksi käytettäessä Reitti 2_H:ta, korjaukselle on määritetty maksimiajat, jotka riippuvat siitä, miten määräaikaistestausvälit on latteille määritelty suunnitteluvaiheessa. Reitti 2_H:n käytön hyväksyntä ilmoitetaan yleensä laitteiden SIL-sertifikaateissa.

Kaikille laitteille ei ole mahdollista hyödyntää reitti 2_H:ta. Jotta sitä voidaan hyödyntää, on täytyttävä standardin SFS-EN 61508-2 (2010, 56) kohdan 7.4.4.3.3 ehdot.

> *Jos reitti 2_H valitaan satunnaisten laitteistovikaantumisten kvantifioimiseksi (katso 7.4.5), käytettyjen luotettavuustietojen on*
>
> *a) perustuttava käytöstä saatuun palautteeseen elementeille, joita on käytetty samanlaisessa sovelluksessa ja ympäristössä ja*

b) perustuttava tietoihin, jotka on kerätty kansainvälisten standardien (esim. IEC 60300-3-2 tai ISO 14224) mukaisesti ja

c) oltava arvioitu seuraavan mukaisesti:

i) käytöstä saadun palautteen määrä ja,

ii) nojautuminen asiantuntijalausuntoon ja tarvittaessa,

iii) erityisten testausten suorittaminen.

jokaisen laskennassa käytettävän luotettavuusparametrin (esim. vikatiheys) keskiarvon ja epävarmuustason (esim. 90 %:n luotettavuusväli tai todennäköisyysjakauma (ks. huomautus 2) arvioimiseksi.

7.2.3 Reitti 1_H

Reitti 1_H perustuu vikasietoisuuden ja turvallisien vikaantumisien osuuden (SFF) määrittämiseen. Laitteilla vikaantumiset voidaan jakaa neljään eri kategoriaan. Laitteiden vikaantumiset on jaettu turvallisiin ja vaarallisiin vikaantumisiin. Ne puolestaan on jaettu havaittuihin ja havaitsemattomiin vikaantumisiin. Kaikista vaarallisimpia niistä ovat vaaralliset ja havaitsemattomat vikaantumiset, koska ne aiheuttavat turvatoiminnon menettämisen ilman minkäänlaista varoitusta. Standardeissa vikaantumista kuvataan merkillä λ. (Paul Gruhn 2016, 1-6.)

Turvallisten vikaantumisten osuus voidaan määrittää laitteen tai alajärjestelmän vikaantumistietojen perusteella. Turvallisten vikaantumisten osa on siis turvallisten vikaantumisten ja vaarallisten havaittujen vikaantumisten summa, jaettuna kaikkien vikaantumisten yhteislukumäärällä. (Mts.)

$$SFF = \frac{\lambda_s + \lambda_{dd}}{\lambda_{total}}$$

Standardin SFS-EN 61508-2 (2010, 44-55) kohdissa 7.4.4.2.1, 7.4.4.2.3 ja 7.4.4.2.4 ohjeistetaan menettelytapa, jolla voidaan osoittaa korkein mahdollinen turvallisuuden eheyden taso turvatoiminnolle.

> *7.4.4.2.1 Korkeimman mahdollisen turvallisuuden eheyden tason, joka voidaan osoittaa määrätylle turvatoiminnalle, määrittämiseksi on noudatettava seuraavaa menettelytapaa:*
>
> *1) Määritellään alajärjestelmät, jotka muodostavat S/E/OE turvallisuuteen liittyvän järjestelmän*
>
> *2) Määritellään jokaiselle alajärjestelmälle ja kaikille alajärjestelmän elementeille erikseen turvallisten vikaantumisten osuus (eli yksittäisille elementeille kunkin elementin vikasietoisuuden ollessa 0). Redundanttisten elementtien konfiguraation tapauksessa turvallisten vikaantumisten osuus voidaan laskea ottamalla huomioon lisädiagnostiikat, jotka mahdollisesti ovat käytettävissä (esim. vertailemalla elementtejä)*
>
> *3) Käytetään jokaiselle elementille saavutettua turvallisten vikaantumisten osuutta ja laitteiston vikasietoisuutta 0 korkeimman mahdollisen osoitettavissa olevan turvallisuuden eheyden tason määrittämiseksi taulukon 2 sarakkeesta 2 (tyypin A elementeille) ja taulukon 3 sarakkeesta 2 (tyypin B elementeille).* (Kts. Liite 1 ja 2)
>
> *4) Korkeimman mahdollisen osoitettavissa olevan turvallisuuden eheyden tason määrittämiseksi käytetään kohtien 7.4.4.2.3 ja 7.4.4.2.4 mukaista menetelmää.*
>
> *5) Korkein mahdollinen turvallisuuden eheyden taso, joka voidaan osoittaa S/E/OE turvallisuuteen liittyvälle järjestelmälle, on määritettävä alhaisimman turvallisuuden eheyden tason saavuttaneen alajärjestelmän mukaan*

7.4.4.2.3 S/E/OE turvallisuuteen liittyvässä järjestelmässä, jossa useampi elementin turvatoiminta on toteutettu elementtien sarjayhdistelmänä (kuten kuvassa 5, liite 3), korkein osoitettavissa oleva turvallisuuden eheyden taso tarkasteltavalle turvatoiminnalle on määritettävä sen elementin mukaan, joka on saavutetulla turvallisten vikaantumisten osuudella ja laitteiston vikasietoisuudella 0 saavuttanut matalimman turvallisuuden eheyden tason.

7.4.4.2.4 S/E/OE turvallisuuteen liittyvässä järjestelmässä, jossa elementin turvatoiminta on toteutettu useiden kanavien kautta (rinnakkaisten elementtien yhdistelmä) ja jossa laitteiston vikasietoisuus on N, korkein osoitettavissa oleva turvallisuuden eheyden taso tarkasteltavalle turvatoiminnalle on määritettävä

a) ryhmittelemällä elementtien sarjayhdistelmä jokaiselle kanavalle ja määrittämällä sen jälkeen tarkasteltavan turvatoiminnan osalta kullekin kanavalle korkein osoitettavissa oleva turvallisuuden eheyden taso (katso 7.4.4.2.3) ja

b) valitsemalla kanava, jolla on tarkasteltavalle turvatoiminnalle saavutettu korkein turvallisuuden eheydentaso, ja sen jälkeen lisäämällä N turvallisuuden eheyden tasoa alajärjestelmän kokonaisyhdistelmän korkeimman turvallisuuden eheyden tason määrittämiseksi

Elementtien voidaan todeta olevan tyyppiä A, mikäli standardin SFS-EN 61508, kohdan 7.4.4.1.2 vaatimukset täyttyvät ja tyyppiä B, mikäli kohdan 7.4.4.1.3 vaatimukset täyttyvät. Tyypin A laitteita voidaan pitää “yksinkertaisina” laitteina, joiden vikaantumismuodot ovat tiedossa ja ennalta-arvattavissa. Tyypin B laittteet ovat “monimutkaisia” ja niiden vikaantumismuodot puolestaan ennalta-arvaamattomia ja tuntemattomia. Yleisesti ottaen mikroprosessorin sisältäviä laitteita voidaan pitää tyypin B laitteina, esimerkiksi ohjelmoitavat logiikat ja älykkäät lähettimet. (Gruhn 2016, 3-4.)

Standardissa SFS-EN 61508-2 (2010, 42-44) on määritelty A- ja B-tyypin laitteet seuraavasti:

> *7.4.4.1.2 Elementin voidaan katsoa olevan tyyppiä A, jos turvatoiminnan saavuttamiseksi tarvittaville komponenteille*
>
> *a) kaikkien osakomponenttien kaikki vikaantumismuodot ovat hyvin määriteltyjä ja*
>
> *b) elementin käyttäytyminen vikatilanteessa voidaan täydellisesti määrittää ja*
>
> *c) on olemassa riittävästi luotettavaa vikaantumistietoa havaituille ja havaitsemattomille vaarallisille vikaantumisille esitettyjen vikaantumistiheyksien täyttymisen osoittamiseksi (katso 7.4.9.3- 7.4.9.5)*
>
> *7.4.4.1.3 Elementin katsotaan olevan tyyppiä B jos turvatoiminnan saavuttamiseksi tarvittaville komponenteille*
>
> *a) yhdenkin osakomponentin vikaantumismuoto ei ole hyvin määritelty tai*
>
> *b) elementin käyttäytymistä vikatilanteessa ei voida täydellisesti määrittää tai*
>
> *c) ei ole olemassa riittävästi luotettavaa vikaantumistietoa havaituille tai havaitsemattomille vaarallisille vikaantumisille esitettyjen vikaantumistiheyksien tueksi (katso 7.4.9.3- 7.4.9.5)*

7.2.4 Reitti 2_H

Reitti 2_H perustuu loppukäyttäjiltä laitteista saatuihin luotettavuustietoihin, korotettuihin luotettavuustasoihin ja vikasietoisuuksiin, jotka on määritelty kullekin turvallisuuden eheyden tasolle. Reitti 2_H:n vikasietoisuustaulukko on vastaava standardin SFS EN-61511 vikasietoisuustaulukon kanssa (ks. Taulukko 2). Reitti 2_H:ta voidaan hyödyntää ainoastaan silloin, kun laite on hyväksytty Reitti 2_H laitteeksi. Ehdot on esitetty kappaleessa 7.3.1. (SFS-EN 61508.2:2010, 42)

Mikäli laite pitää sisällään ainoastaan tyypin A elementtejä, voidaan käyttää standardin SFS-EN 61508-2 (2010, 56) kohtaa 7.4.4.3.2, jonka mukaan vikasietoisuutta voidaan laskea, mikäli ehdot täyttyvät:

> *Vain tyypin A elementtien ollessa kyseessä: jos noudattamalla kohdan 7.4.4.3.1 laitteiston vikasietoisuuden vaatimuksia on määritetty tilanne, jossa laitteiston vikasietoisuuden on oltava suurempi kuin 0, mutta tämä aiheuttaisi lisää vikaantumisia ja johtaisi ohjattavan laitteen (OL) kokonaisturvallisuuden alenemiseen, niin tällöin voidaan toteuttaa vaihtoehtoisesti turvallisempi arkkitehtuuri, jossa on pienempi laitteiston vikasietoisuus. Tällaisessa tapauksessa tämä on perusteltava ja dokumentoitava.*

Taulukko 4. Reitti 2H:n kenttälaitteiden vikasietoisuustaulukko (Mts. 56.)

Turvallisuuden eheyden taso (SIL)	Pienin sallittu laitteiston vikasietoisuus
1 (Mikä tahansa toimintatapa)	**0**
2 (Harvojen vaateiden toimintatapa)	**0**
2 (Tiheiden vaateiden toimintatapa)	**1**
3 (Mikä tahansa toimintatapa)	**1**
4 (Mikä tahansa toimintatapa)	**2**

7.3 Vikaantumistodennäköisyyslaskenta turvatoiminnolle tiheiden vaateiden toimintatavalla

Vikaantumistodennäköisyyslaskenta suoritetaan jokaiselle alajärjestelmälle. Laskentakaava riippuu valitusta rakenteesta. Turvatoiminnon vaarallisen vikaantumisen keskimääräinen taajuus on kaikkien alajärjestelmien vaarallisien vikaantumisien keskimääräisten taajuuksien summa. Standardissa SFS-EN 61508-6 (2010, 43) kohdassa B.3.3.1 on esitetty kaava turvatoiminnon PFH:n laskennalle (Ks. kaava 1).

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \quad (1)$$

, missä
PFH_{sys} on turvallisuuteen liittyvän järjestelmän vaarallisen vikaantumisen keskimääräinen taajuus;
PFH_s on anturi alajärjestelmän vaarallisen vikaantumisen keskimääräinen taajuus;
PFH_L on logiikka alajärjestelmän vaarallisen vikaantumisen keskimääräinen taajuus;
PFH_{Fe} on päätelaite alajärjestelmän vaarallisen vikaantumisen keskimääräinen taajuus.

7.3.1 1oo1-arkkitehtuuri (yksi yhdestä)

1oo1-konfiguraatiolla tarkoitetaan rakennetta, jonka vikasietoisuus on nolla ja vaarallinen havaitsematon vikaantuminen johtaa suoraan turvatoiminnon menettämiseen. Standardin SFS-EN 61508-6 kohdassa B.3.3.2.1 on johdettu keskimääräinen vaarallisen vikaantumisen taajuus 1oo1-konfiguraatiolle. Mikäli turvajärjestelmä ohjaa laitteiston turvalliseen tilaan havaitessaan minkä tahansa vikaantumisen, voidaan johtaa kaava vaarallisen vikaantumisen keskimääräiselle taajuudelle 1oo1-konfiguraatiolla, joka on yhtä kuin vaaralliset vikaantumiset tuntia kohden (Ks. kaava 2). (SFS-EN 61508-6:2010, 43-44.)

$$PFH_{1oo1} = \lambda_{du} \qquad (2)$$

,missä
λ_{DU} *= vaaralliset havaitsemattomat vikaantumiset (1/h)*

7.3.2 2oo2-arkkitehtuuri (kaksi kahdesta)

2oo2-konfiguraatiolla tarkoitetaan arkkitehtuurin rakennetta, jonka vikasietoisuus on nolla. Vaarallinen vikaantuminen tapahtuu, kun yksi laite konfiguraatiosta vikaantuu vaarallisesti. Tästä syystä konfiguraatio on turvallisuuden näkökulmasta heikko valinta. Luotettavuusmielessä konfiguraatiovalinta on hyvä, koska prosessin ohjaaminen turvalliseen tilaan tapahtuu vasta molempien laitteiden vikaantuessa turvallisesti. Standardin SFS-EN 61508-6 kohdassa B.3.3.2.3 on johdettu keskimääräinen vaarallisen vikaantumisen taajuus 2oo2-konfiguraatiolle, joka on siis kaksi kertaa vaaralliset vikaantumiset tuntia kohden, mikäli oletetaan, että turvajärjestelmä ohjaa laitteiston turvalliseen tilaan, kun mikä tahansa vikaantuminen havaitaan (Ks. kaava 3). (SFS-EN 61508-6:2010, 43-44.)

$$PFH_{2002} = 2\lambda_{du} \qquad (3)$$

,missä
λ_{DU} *= vaaralliset havaitsemattomat vikaantumiset (1/h)*

7.3.3 1oo2-arkkitehtuuri (yksi kahdesta)

1oo2-arkkitehtuurin rakenteella tarkoitetaan rakennetta, jonka vikasietoisuus on yksi ja kaksi kanavaa on kytketty rinnan. Turvatoiminto menetetään, kun molemmat konfiguraation laitteet ovat vikaantuneet vaarallisesti. Turvallisuuden näkökulmasta 1oo2-konfiguraatio on hyvä, mutta käytettävyysmielessä heikko, koska havaittaessa vikaantuminen prosessi ohjataan turvalliseen tilaan ja laitteiden lisääminen johtaa todennäköisempään vikaantumiseen. Standardin SFS-EN 61508-6 kohdassa B.3.3.2.2 on johdettu keskimääräinen vaarallisen vikaantumisen taajuus 1oo2-konfiguraatiolle. Oletuksena on, että turvajärjestelmä ohjaa laitteiston turvalliseen tilaan, kun molemmissa kanavissa on havaittu mikä tahansa vikaantuminen (Ks. kaava 4). (SFS-EN 61508-6:2010, 43-44.)

$$PFH_{1oo2} = 2\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \quad (4)$$

, missä

$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$

t_{CE} = kanavakohtainen alhaalla olo aika
β = osuus havaitsemattomista vikaantumisista, joille löytyy yhteinen tekijä (2%, 10% tai 20% olettaen, että $\beta=2*\beta_d$)
β_d = osuus diagnostiikalla havaittavista vikaantumisista, joille löytyy yhteinen tekijä (1%, 5% tai 10% olettaen, että $\beta=2*\beta_d$)
MRT = korjaukseen kuluva aika (h)
MTTR = palauttamiseen kuluva aika (h)
T1 = määräaikaiskoestuksen aikaväli (h)
λ_D = vaaralliset vikaantumiset (λ_{DD}+λ_{DU} 1/h)
λ_{DD} = vaaralliset havaitut vikaantumiset (1/h)
λ_{DU} = vaaralliset havaitsemattomat vikaantumiset (1/h)

7.3.4 2oo3-arkkitehtuuri (kaksi kolmesta)

2oo3-arkkitehtuurilla tarkoitetaan rakennetta, jonka vikasietoisuus on yksi. Siinä kolme kanavaa on kytketty rinnan ja käytetään enemmistöäänestysmenetelmää, jossa ulostulosignaalin tila määräytyy vähintään kahden signaalin tilan mukaan. 2oo3-konfiguraatio on hyvä valinta sekä turvallisuuden, että käytettävyyden kan-

nalta. Kyseinen konfiguraatio on huomattavasti kalliimpi toteuttaa kuin edellä mainitut. Standardin SFS-EN 61508-6 kohdassa B.3.3.2.5 on johdettu keskimääräinen vaarallisen vikaantumisen taajuus 2oo3-konfiguraatiolle. Oletuksena on, että turvajärjestelmä ohjaa laitteiston turvalliseen tilaan, mikäli missä tahansa kahdessa kanavassa havaitaan mikä tahansa vikaantuminen (Ks. kaava 5). (SFS-EN 61508-6:2010, 43-44.)

$$PFH_{2oo3} = 6\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \qquad (5)$$

, missä

$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$

t_{CE} = kanavakohtainen alhaalla olo aika
β = osuus havaitsemattomista vikaantumisista, joille löytyy yhteinen tekijä (2%, 10% tai 20% olettaen, että β=2β_d)*
β_d = osuus diagnostiikalla havaittavista vikaantumisista, joille löytyy yhteinen tekijä (1%, 5% tai 10% olettaen, että β=2β_d)*
MRT = korjaukseen kuluva aika (h)
MTTR = palauttamiseen kuluva aika (h)
T1 = määräaikaiskoestuksen aikaväli (h)
λ_D = vaaralliset vikaantumiset (λ_{DD}+λ_{DU} 1/h)
λ_{DD} = vaaralliset havaitut vikaantumiset (1/h)
λ_{DU} = vaaralliset havaitsemattomat vikaantumiset (1/h)

8 Laskentatyökalu Sistema

Vaarallisen vikaantumisen keskimääräisten taajuuksien laskennat voidaan tehdä käyttäen Sistema-laskentatyökalua. Sistema on Saksassa kehitetty tietokoneavusteinen suunnitteluohjelma, joka on luotu helpottamaan ohjausjärjestelmien suunnittelua. Se pohjautuu SFS-EN ISO 13849-1 standardiin. Standardi kattaa turvallisuuteen liittyvien turvajärjestelmien elinkaarivaiheet, tietolähteet ja suoritustasot ja niiden vaatimukset. Standardi on luotu koneiden ja ohjausjärjestelmien suunnittelijoille, asentajille ja käyttöönottajille ja ylläpidolle. Sistemaa ei ole suunniteltu suoraan käytettäväksi prosessiteollisuuteen, mutta laskentamenetelmät ovat samat. Lisäksi suoritustasot ja turvallisuuden eheyden tasot vastaavat toisiaan, joten ohjelmaa voidaan

käyttää turvatoimintojen turvallisuuden eheydentasojen osoittamiseen. (Sundcon. N.d.)

8.1 Projektin luominen

Projektin luonti tapahtuu ohjelman vasemmasta yläkulmasta kohdasta “file” ja ”new project”. Tällöin vasemmassa reunassa olevaan kenttään tulee näkyviin uusi projekti. Projektit näytetään kyseisessä puurakenteessa punaisilla kirjaimilla “PR”. Napsauttamalla projekti aktiiviseksi voidaan sille antaa lisätietoja aukeavaan ikkunaan, joita ovat projektin nimi, tila, numero ja tekijä. Projektin luonnin päivämäärä ja muutokset päivittyvät kenttiin automaattisesti. (Apfeld, Hauke, Schaefer, Rempel & Ostermann 2010, 16.)

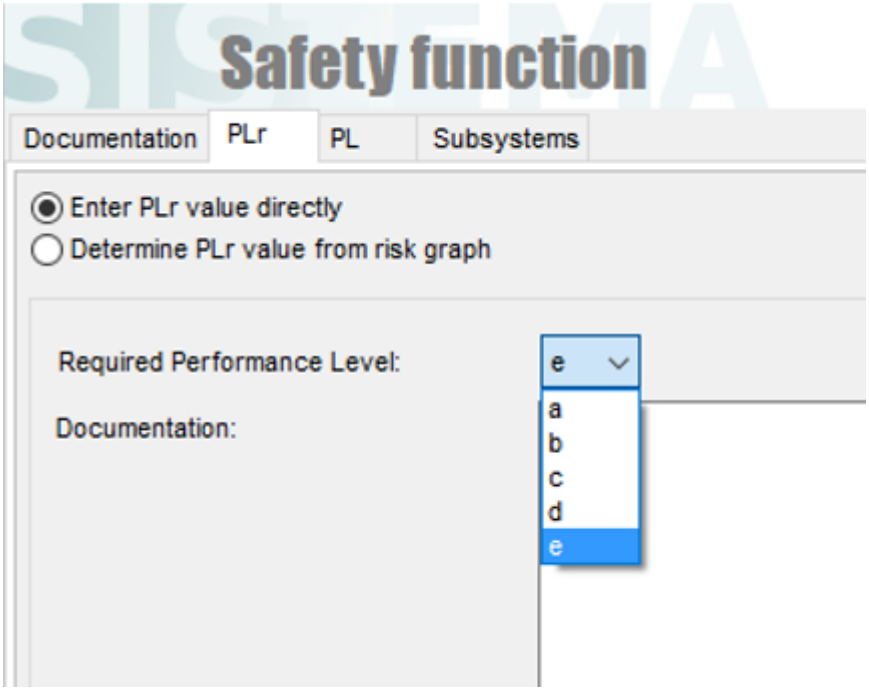
8.2 Turvatoiminnon luominen

Turvatoiminnon luominen tapahtuu napsauttamalla projekti aktiiviseksi. Tällöin projektipuun yläreunaan ilmestyy kenttä “Safety functions”. Napsauttamalla “safety functions” kenttä aktiiviseksi, aukeaa lista, jossa on näkyvillä kaikki luodut turvatoiminnot. Projektipuussa turvatoiminnot näytetään oranssilla tekstillä “SF”. Napsauttamalla turvatoiminto aktiiviseksi voidaan sille antaa lisätietoja, joita ovat esimerkiksi turvatoiminnon nimi, tyyppi, laukaiseva tekijä, toiminnan kuvaus ja turvallinen tila. (Apfeld, Hauke, Schaefer, Rempel & Ostermann 2010, 17.)

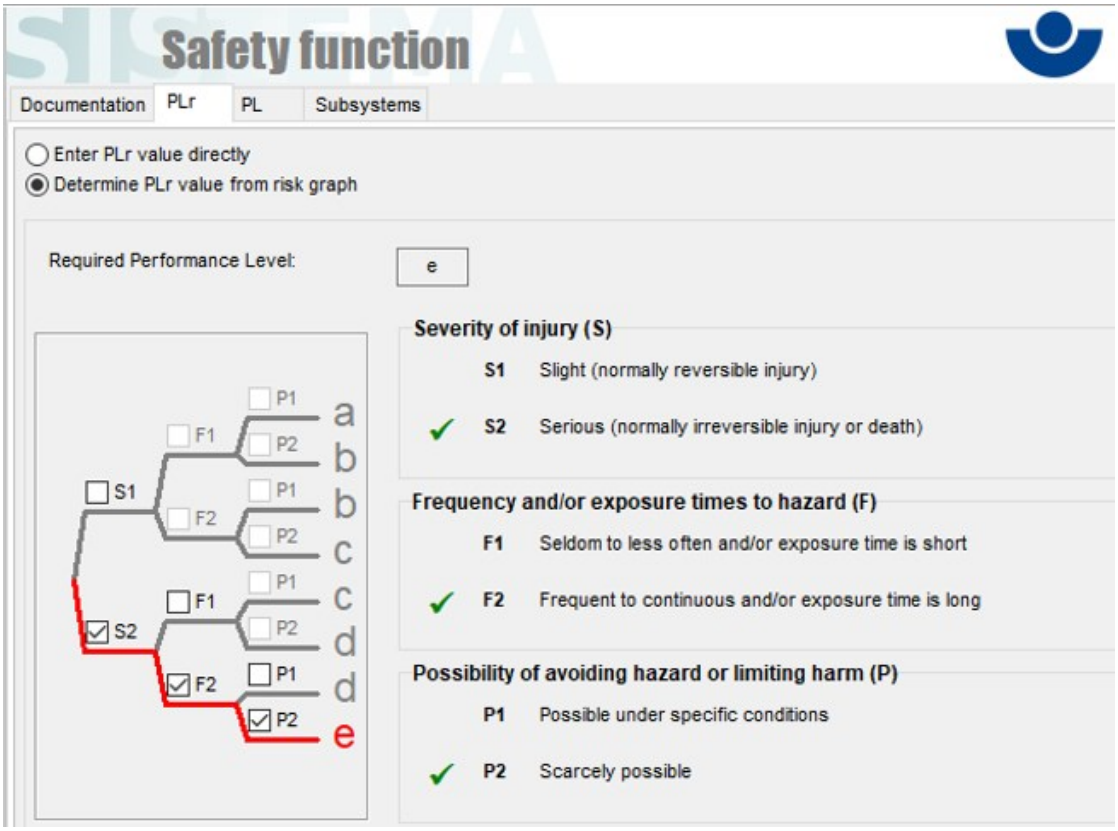
8.3 Vaaditun suoritustason määrittäminen turvatoiminnolle

Vaadittu suoritustaso (Required Performance level) määritetään turvatoiminnolle napsauttamalla haluttu turvatoiminto aktiiviseksi projektipuusta ja sen jälkeen siirtymällä PLr välilehdelle. Vaaditun suoritustason määrittämiseen on kaksi tapaa. Se voidaan määrittää joko riskigraafin avulla tai suoraan alasvetovalikosta, mikäli suoritustaso on jo valmiiksi tiedossa (Ks. taulukko 1). Standardin EN-ISO 13849-1 riskigraafin

parametrit ovat samankaltaiset kuviossa 2 esitetyn Standardin SFS EN-ISO 61508 riskigraafin kanssa. Riskigraafi ja alasvetovalikko on esitetty kuvioissa 4 ja 5. (Apfeld, Hauke, Schaefer, Rempel & Ostermann 2010, 17.)



Kuvio 4. Vaaditun suoritustason määrittäminen suoritustason ollessa selvillä



Kuvio 5. Vaaditun suoritustason määrittäminen riskigraafin avulla

8.4 Alajärjestelmän lisääminen ja vaarallisen vikaantumisen keskimääräisen taajuuden määrittäminen alajärjestelmälle

Alajärjestelmän luodaan napsauttamalla hiiren oikealla näppäimellä turvatoimintoa, jolle alajärjestelmä halutaan luoda ja sen jälkeen valitsemalla “new”. Alajärjestelmää merkataan projektipuussa vihrein kirjaimin “SB”. Napsauttamalla alajärjestelmä aktiiviseksi aukeaa ikkuna, johon voidaan syöttää lisätietoja alajärjestelmästä, joita ovat esimerkiksi alajärjestelmän nimi, laitevalmistaja, laiteryhmä ja laitteen tyyppi. Vaarallisen vikaantumisen keskimääräinen taajuus voidaan määritellä alajärjestelmälle neljällä eri tavalla. Tapa valitaan välilehdeltä ”PL”. Mikäli halutaan määrittää vaarallisen vikaantumisen keskimääräinen taajuus turvallisuuden eheyden tason perusteella, tehdään se valitsemalla ”Enter SIL/PFHD directly”. Tämän jälkeen syötetään laskettu tai valmistajan ilmoittama PFH-arvo sille tarkoitettuun kenttään. PFH-arvojen laskukaavat on esitetty luvuissa 6.2.1- 6.2.4. Ohjelman vasemmassa alakulmassa olevasta

kentästä voidaan seurata koko turvatoiminnon vaarallisen vikaantumisen todennäköisyyden kehittymistä. Mikäli todennäköisyys kasvaa liian suureksi (vaadittuun suoritustasoon ei ylletä), muuttuu turvatoiminnon vasemmassa reunassa oleva vihreä merkki punaiseksi ristiksi, jolloin tiedetään, että turvatoimintoon on tehtävä muutoksia. Mikäli merkki on keltainen, on turvatoiminnossa tai alajärjestelmässä virheitä tai kaikkia vaadittuja tietoja ole täytetty. Virheilmoitukset tulevat näkyviin ohjelman alareunassa olevaan kenttään. (Apfeld, Hauke, Schaefer, Rempel & Ostermann 2010, 17-22.)

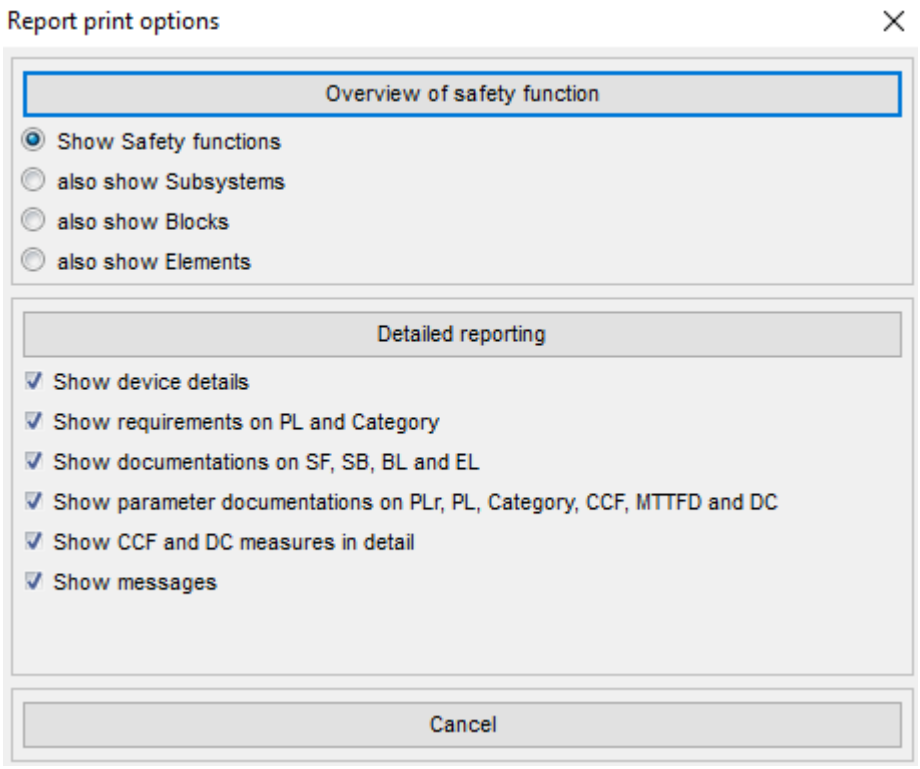
8.5 Laitevalmistajien kirjastojen hyödyntäminen

Laitevalmistajat tarjoavat komponenttikirjastoja omille laitteilleen. Kirjastojen hyödyntäminen helpottaa laskentojen suorittamista, sillä komponenteille on jo valmiiksi määritelty vikaantumisarvot. Kirjastojen hyödyntämiseksi on käyttäjän ladattava kirjaston sisältävä ZIP-tiedosto tietokoneelleen. Tiedostoa ei voi tallentaa verkkolevylle, vaan se on tallennettava kiinteään polkuun. Sistema tunnistaa kaksi tiedostotyyppiä: VDMA-kirjastot, joiden tiedostomuoto on “.xml” ja Sistemaa varten luodut tiedostot, jotka ovat tyypiltään “.slb”. Molempien kirjastotyyppien lisääminen tapahtuu ikkunan yläreunasta. Riippuen tiedostomuodosta valitaan joko ”VDMA-library” tai ”library”. Mikäli ollaan lisäämässä tavallista kirjastoa, napsautetaan ”Library” ja ”Add local library”. Tiedosto ladataan polusta, johon se on alun perin tallennettu. Mikäli ollaan lisäämässä VDMA-kirjastoa, napsautetaan VDMA-library ja add library ja sen jälkeen etsitään tiedosto polusta, johon se on tallennettu. Ladatut kirjastot löytyvät avatusta ikkunasta. Ennen käyttöä ne on vielä ladattava ohjelmaan erikseen. Kirjastoissa on listattu komponentteja, jotka voidaan lisätä haluttuihin turvatoimintoihin raahaamalla komponentti vasemmassa reunassa olevan turvatoiminnon päälle, johon komponentti halutaan lisätä. (Huelke, Lungfiel & Hauke 2016, 31-52.)

8.6 Raportin tulostus

Sisteman kautta on mahdollista tulostaa raportti, johon voidaan sisällyttää turvatoiminnoista haluttavia tietoja. Raportin tulostaminen tapahtuu napsauttamalla “Re-

port”, josta aukeaa kuviossa 6 esitetty ikkuna. Ikkunassa voidaan määritellä, mitä tietoja raporttiin halutaan sisällyttää. Raportteja voidaan tulostaa kahta eri tyyppiä. Mikäli halutaan tulostaa tiivis ja kapea raportti, valitaan “Overview of safety function”. Jos halutaan tulostaa laaja ja yksityiskohtainen raportti, valitaan puolestaan “Detailed reporting”. Ikkunassa voidaan myös määritellä, kuinka tarkka raportti halutaan riippuen siitä, mitä tarkastaja raportilta vaatii. Tärkeimpiä tietoja ovat turvatoiminnot, alajärjestelmät, laitetiedot, vaaditut suoritustasot. Tulostetussa versiossa näytetään joka tapauksessa turvatoiminto ja sen vaarallisen vikaantumisen taajuuden arvo riippumatta siitä, mitä raportin sisällöksi on valittu. (Lungfiel & Huelke 2016, 1.)



Kuvio 6. Raportin tulostaminen

9 Turvatoimintojen vaatimusten täyttymisen osoittaminen

Turvatoimintojen vaatimusten täyttymisen osoittaminen toteutettiin hyödyntämällä laskentatyökalu Sistemaa. Sistema on luotu koneteollisuuden turvatoimintojen vikaantumislaskentaan, mutta koska laskentamenetelmät ovat samat ja eräkeittämön turvatoiminnot on määritelty toimivan tiheiden vaateiden

toimintatavalla, voidaan Sistemaa hyödyntää vaatimusten täyttymisen osoittamiseen. Turvatoimnnot on toteutettu hyödyntäen reletekniikkaa. Kaikki eräkeittämön turvatoiminnot on suunniteltu fail-safe-periaatteella. Tällä tarkoitetaan sitä, että havaittaessa vikaantuminen prosessi ohjataan aina turvalliseen tilaan, jotta minimoidaan mahdolliset laite-, ympäristö- ja henkilövahingot. Raportissa esitellään keittimen kansiventtiilin, pumpun ja prosessiventtiilin turvatoiminnot. Riskianalyysivaiheessa kaikkien eräkeittämön turvatoimintojen vaadituksi turvallisuuden eheyden tasoksi on määritelty SIL-2.

9.1 Kansiventtiilin turvatoiminnot

9.1.1 Toiminnan kuvaus

Eräkeittämöllä on viisi keitintä. Jokaisella keittimellä on kansiventtiili, jonka kautta keitin täytetään hakkeella. Kansiventtiilien turvatoiminnot ovat keskenään identtisiä. Turvatoiminnot ovat osana prosessin normaalia toimintaa. Tästä syystä toimintatavaksi määräytyy tiheiden ja jatkuvien vaateiden toimintatapa. Turvatoimintoja kansiventtiilillä on kaksi: Kansiventtiili on lukittu kiinni ja sen avaaminen on estetty, kun keittimen paine on yli 0,5 baaria (PIZ-0x08 ja PICZ-0x26) ja kun evakkoventtiilin (HZ-0x02) on kiinni. Molemmat turvatoiminnot on kahdennettu. Keittimellä on kaksi painemittausta ja evakkoventtiilillä on olemassa kaksi rajakytkintä.

Painemittausten turvapiirit koostuvat lähettimestä, signaalin muuntimesta, turvareleestä ja magneettiventtiilistä. Painemittaus lähettää milliampeerisignaalin signaalimuuntimelle, joka muuttaa sen prosessiarvoksi. Signaalimuuntimen koskettimella ohjataan turvareleen kelaa, joka jännitteisenä vetää releen koskettimen kiinni. Signaalimuunnin on parametroitu toimimaan siten, että vikaantuessaan se antaa 23 mA:n signaalin ja vapauttaa releen koskettimen. Signaalimuunnin pystyy myös havaitsemaan mittalaitteen vikaantumisen tai johtimen katkeamisen. Myös tällöin se vapauttaa turvareleen koskettimen. Turvareleen koskettimella puolestaan katkotaan jännitettä magneettiventtiilin kelalta. Jännitteen katketessa kelalta magneettiventtiilin jousi palauttaa magneettiventtiilin asentoon, jolla katkaistaan ilma kansiventtiilin toimilaitteelta. Tällöin kansiventtiili ei voi vaihtaa asentoaan.

Evakkoventtiilin rajojen turvapiirit koostuvat rajakytkimestä, turvareleestä ja magneettiventtiilistä. Rajakytkimellä ohjataan turvareleen kelan jännitettä. Kelan ollessa jännitteisenä turvareleen kosketin on kiinni. Turvareleen koskettimella katkotaan jännitettä magneettiventtiilin kelalta. Jännitteen katketessa kelalta magneettiventtiilin jousi palauttaa magneettiventtiilin asentoon, jolla katkaistaan ilma kansiventtiilin toimilaitteelta. Tällöin kansiventtiili ei voi vaihtaa asentoaan.

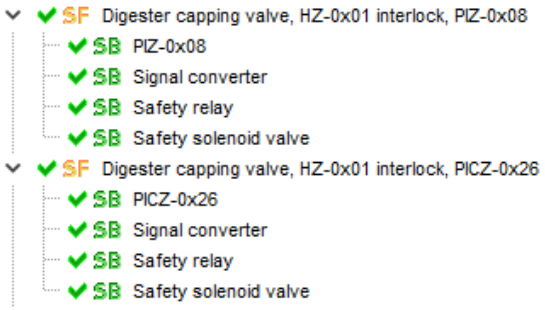
Alun perin turvatoiminto oli tarkoitus toteuttaa liitteessä 4 olevalla ”Jammerilla”, joka on mekaaninen laite, jolla kansiventtiili lukitaan kiinni- asentoon. Jammeria ei kuitenkaan ole hyväksytty turvalaitteeksi ja siltä puuttuvat sertifikaatit. Jammerit päätettiin kuitenkin jättää mukaan toimitukseen lisäämään turvallisuutta.

9.1.2 Vaarallisen vikaantumisen keskimääräisen taajuuden laskeminen kansiventtiilin turvatoiminnoille

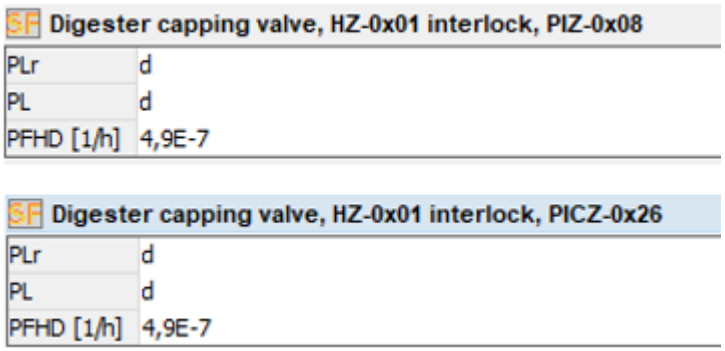
Kansiventtiilin turvatoimintoja käsiteltiin laskennoissa 1oo1-arkkitehtuurin mukaan. Luvussa 7.3.1 on esitetty laskukaava 2 laitteen vaarallisen vikaantumisen keskimääräiselle taajuuden laskemiselle. 1oo1-arkkitehtuurilla laitteen vaarallisen vikaantumisen keskimääräinen taajuus on λ_{du}. Koko turvapiirin vaarallisen vikaantumisen taajuus on kaikkien siinä olevien laitteiden keskimääräisten vaarallisien vikaantumisien summa.

Painelähettimen tyyppi on Emerson Rosemount 2051. Laitteen SIL-sertifikaatissa liitteessä 5 on korostettuna painelähettimen vikaantumisarvot. Signaalimuuntimen tyyppi on PRelectronics 9116B, jonka vikaantumisarvot on esitetty laitteen SIL-sertifikaatissa liitteessä 6. Analogiatulo on 4 - 20 mA:n virtasignaali ja lähtönä on rele. Turvareleen tyyppi on PILZ Pnoz s2. Liitteessä 7 on esitetty sivu PILZ:n turvareleiden SIL-sertifikaatti, jossa on korostettuna vaarallisen vikaantumisen keskimääräinen taajuus kyseisen tyypin turvareleelle. Turvatoiminnon toteuttaa Asco- magneettiventtiili, joka on tyypiltään SCG553A017L. Sen vikaantumistaajuudet ovat korostettuna SIL-sertifikaatissa, joka on liitteessä 8.

Turvatoiminnon vaarallisen vikaantumisen todennäköisyys saadaan luomalla Sistemaan turvatoiminto ”Safety functions”- välilehdeltä. Turvatoiminnolle luodaan alajärjestelmät, jotka esittävät turvapiirin laitteita. Alajärjestelmille annetaan PFH-arvot, jotka ovat 1oo1-arkkitehtuurilla havaitsemattomien vaarallisten vikaantumisien todennäköisyys tuntia kohden.



Kuvio 7. Painemittausten turvapiirien rakenne

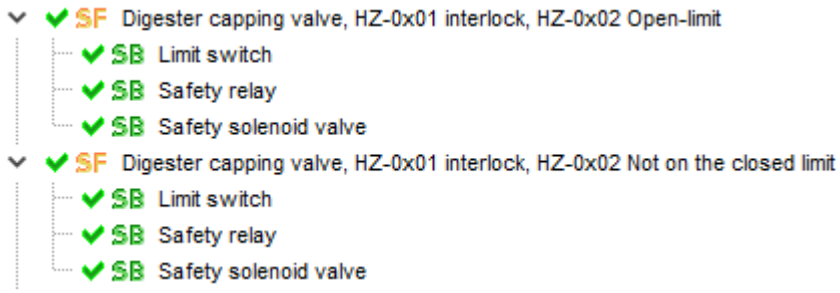


Kuvio 8. PIZ-0x08 ja PICZ-0x26 turvatoimintojen vaarallisen vikaantumisen keskimääräinen taajuus

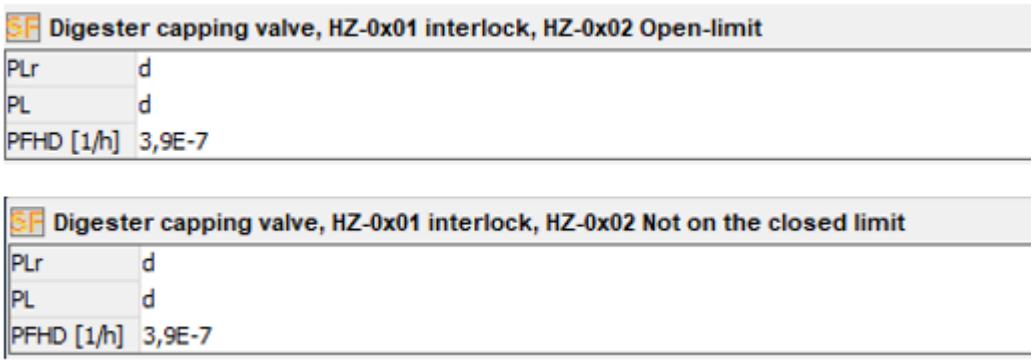
Kuvioista 7 ja 8 nähdään, että turvapiirien vaarallisen vikaantumisen todennäköisyys on $4{,}9*10^{-7}$ (1/h). Taulukosta 1 nähdään, että kyseinen arvo täyttää turvallisuuden eheyden tason 2 vaatimukset todennäköisyyksien osalta.

Turvatoiminnot, jotka liittyvät evakkoventtiilin auki olemiseen, koostuvat rajakytkimestä, turvareleestä ja magneettiventtiilistä. Rajakytkimet ovat Westlockin valmista-

mia, tyypiltään WE3545RBYN00043AAA-0R1 mikrokytkimiä. Westlockin rajakytkimien SIL-sertifikaatti on esitetty liitteessä 9. Turvarele on Pilzin Pnoz S2 ja magneettiventtiili Asco SCG553A017SL, joiden SIL-sertifikaatit ovat esitetty liitteissä 7 ja 8 Turvatoimintojen rakenne on esitetty Kuviossa 9.



Kuvio 9. Turvatoimintojen rakenne



Kuvio 10. Vaarallisen vikaantumisen keskimääräinen taajuus evakkoventtiilin rajaturvatoiminnolle

Kuvioista 9 ja 10 nähdään, että turvatoimintojen keskimääräinen vaarallisen vikaantumisen taajuus on $3{,}9*10^{-7}$. Taulukosta 1 nähdään, että turvatoiminnot täyttävät turvallisuuden eheyden tason 2 vaatimukset todennäköisyyden osalta.

9.1.3 Arkkitehtuurin rajoitusten täyttyminen kansiventtiilin turvatoiminnoilla

Arkkitehtuurin rajoituksien arvioiminen turvatoiminnoilla tehdään hyödyntäen luvun 7.3 menetelmiä. Helpointa arviointi on Standardin SFS-EN 61511- taulukon mukaan (Ks. Taulukko 3). Sekä paine- että rajaturvatoiminnot on kahdennettu ja suunniteltu

toimimaan siten, että vikasietoisuus on 1. Tiheiden ja jatkuvien vaateiden toimintapaa käytettäessä vikasietoisuuden on oltava 1. Arkkitehtuurin rajoitusten voidaan todeta olevan Standardin SFS-EN 61508 vaatimusten mukaisia.

9.2 Valkolipeäpumpun turvatoiminnot

9.2.1 Toiminnan kuvaus

Valkolipeäpumpulla on kaksi eri turvatoimintoa. Pumpun käynti estetään valkolipeäpaineastian paineen ylittäessä 8,5 baaria (PIZ-4301 ja PICZ-4302) tai poistolinjan paineen ylittäessä 14,5 baaria (PIZ-5101 ja PIZ-5102). Molemmat turvatoiminnot on kahdennettu ja kaikki neljä turvapiiriä ovat keskenään identtisiä. Valkolipeäpumpun turvatoimintoja käsiteltiin laskennoissa 1oo1-arkkitehtuurin mukaan. Kappaleessa 7.3.1 on esitetty laskukaava laitteen vaarallisen vikaantumisen keskimääräiselle taajuuden laskemiselle. 1oo1-arkkitehtuurilla laitteen vaarallisen vikaantumisen keskimääräinen taajuus on λ_{du}. Koko turvapiirin vaarallisen vikaantumisen taajuus on kaikkien siinä olevien laitteiden keskimääräisten vaarallisien vikaantumisien summa.

Turvapiirit koostuvat painelähettimestä, signaalinmuuntimesta, turvareleestä, kontaktorista ja kontaktorin kuittauspiirin kontaktorista. Painelähettimen tyyppi on Emerson Rosemount 2051, Signaalin muuntimen tyyppi on PR electronics 9116B ja turvareleen tyyppi on PILZ Pnoz s2. Edellä mainittujen laitteiden toimintaperiaatteet on esitetty luvussa 9.1.1. Erona on, että turvareleellä ohjataan tässä tapauksessa pumpun kontaktorin kelaa, joka puolestaan vaihtaa kontaktorin koskettimien asentoa. Pumpun kontaktori on Siemensin 3RT1065-6SF36-3PA0 ja kuittauspiirin kontaktori on myös Siemensin, mutta tyypiltään 3SK1121-AB40. Kuittauspiirin kontaktori jouduttiin lisäämään, koska Siemensin 3RT10xx-sarjan kontaktorit eivät täytä SIL-2 tason vaatimuksia ilman diagnostiikkaa. Kuittauspiirin kontaktori käyttää pumppua ohjaavan kontaktorin auki vaateen jälkeen. Näin saadaan poissuljettua kontaktorin ”kiinni hitsaantuminen”, joka on vaarallisen havaitsemattoman vikaantumisen muoto. Mikäli kontaktori ei vaihda asentoaan, saadaan siitä hälytys.

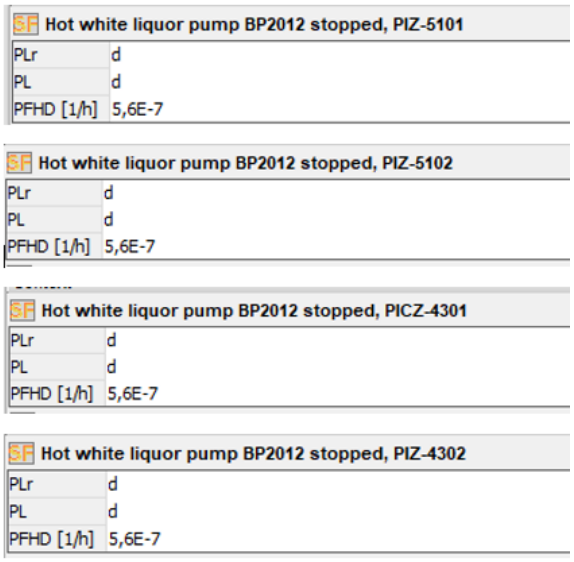
9.2.2 Vaarallisen vikaantumisen keskimääräisen taajuuden laskeminen valkolipeäpumpun turvatoiminnoille

Kaikki neljä paineen mukaan lukitsevaa turvapiiriä ovat keskenään identtisiä. Vaarallisen vikaantumisen keskimääräisen taajuus on laskettu 1oo1 konfiguraation laskukaavalla jokaiselle turvapiirille. Tällöin laitteen vaarallisen vikaantumisen keskimääräinen taajuus on λ_{du} (vaarallinen havaitsematon vikaantuminen) ja koko turvapiirin vaarallisen vikaantumisen taajuus on laitteiden vaarallisten ja havaitsemattomien vikaantumisien summa.

Sistemaan luodaan neljä turvatoimintoa ”safety functions-välilehdeltä”. Neljälle turvatoiminnolle luodaan alajärjestelmät, jotka kuvaavat piirien laitteita. Jokaisella turvapiirillä on 5 laitetta: painelähetin, signaalimuunnin, turvarele, kontaktori ja kuittauspiirin kontaktori. Painelähettimen vaarallisen vikaantumisen keskimääräinen taajuus tuntia kohden on $4{,}1*10^{-8}$, signaalimuuntimen $6{,}2*10^{-8}$, turvareleen $2{,}5*10^{-9}$. Siemensin VDMA-kirjastosta löytyy kontaktorit suoraan, joten ne voidaan lisätä turvatoimintoihin suoraan raahaamalla VDMA-kirjastosta. Turvatoimintojen rakenne on esitetty kuviossa 11.

Kuvio 11. Valkolipeäpumpun turvatoimintojen rakenne

Kuviossa 12 on esitetty turvatoimintojen vikaantumistaajuudet. Kaikilla turvatoiminnoilla se on $5,6*10^{-7}$. Taulukosta 1 nähdään, että turvatoiminnot täyttävät SIL-2 tason vaatimukset vikaantumistodennäköisyyksien osalta.



Kuvio 12. Valkolipeäpumpun turvatoimintojen keskimääräiset vaarallisien vikaantumisien taajuudet

9.2.3 Arkkitehtuurin rajoitusten täyttyminen valkolipeäpumpun turvatoiminnoilla

Arkkitehtuurin rajoitusten täyttyminen valkolipeäpumpun turvatoiminnoilla on helpointa osoittaa standardin SFS-EN 61511 taulukon mukaan (Ks. Taulukko 3). Molemmat turvatoiminnot on kahdennettu ja suunniteltu toimimaan siten, että vikasietoisuus on 1. Tiheiden ja jatkuvien vaateiden toimintapaa käytettäessä vikasietoisuuden on oltava 1. Arkkitehtuurin rajoitusten voidaan todeta olevan Standardin SFS-EN 61508 vaatimusten mukaisia.

9.3 Venttiilin FZ-5510 turvatoiminto

Venttiili FZ-5510 on sijoitettu prosessissa lämmönvaihtimien jälkeen. Lämmöntalteenotto tapahtuu lämmönvaihtimella, jossa ensiöpuolella olevaa kuumaa mustalipeää jäähdytetään siirtämällä lämpöä toisiopuolella olevaan veteen pystylämmönvaihtimella. Lämpöä käytetään hyväksi prosessin muissa vaiheissa. Venttiili FZ-5510 lukitaan kiinni, mikäli lipeän lämpötila vaihtimien jälkeen on yli 102°C. Turvatoiminto on kahdennettu. Turvapiirit koostuvat lämpötilalähettimestä (Emerson 644HANAQ4QTXA), Signaalimuuntimesta (PRelectronics 9116B), turvareleestä (PILZ pnoz S2), magneettiventtiilistä (Parker 799975-341N03-24VDC), venttiilin paineilmalla toimivasta toimilaitteesta (NAF 791292-3240) ja venttiilistä (NAF 791292-3240).

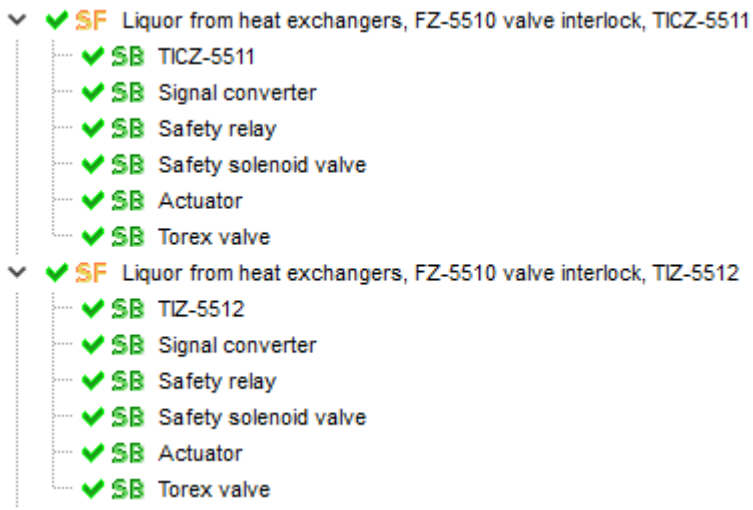
Turvapiirin toimintaperiaate on vastaava kansiventtiilin paineen mukaan tehtävän lukituksen kanssa. Lämpötilamittaus lähettää milliampeerisignaalin signaalimuuntimelle, joka muuttaa sen prosessiarvoksi. Signaalimuuntimen koskettimella katkotaan turvareleen kelan jännitettä. Jännitteisenä kela vetää releen koskettimen kiinni. Signaalimuunnin on parametroitu toimimaan siten, että vikaantuessaan se antaa 23 mA signaalin ja vapauttaa releen koskettimen. Signaalimuunnin pystyy myös havaitsemaan mittalaitteen vikaantumisen tai johtimen katkeamisen. Myös tällöin se vapauttaa turvareleen koskettimen. Turvareleen koskettimella puolestaan katkotaan jännitettä magneettiventtiilin kelalta. Jännitteen katketessa kelalta, magneettiventtiilin jousi palauttaa magneettiventtiilin asentoon, jolla katkaistaan ilma venttiilin FZ-5510 toimilaitteelta. Toimilaite on jousipalautteinen, joten paineilman katkaiseminen sulkee venttiilin.

9.3.1 Vaarallisen vikaantumisen keskimääräisen taajuuden laskeminen venttiilin FZ-5510 turvatoiminnolle

Venttiilin FZ-5510 turvatoimintoja käsitellään laskennoissa 1oo1-arkkitehtuurin mukaan. Kappaleessa 7.3.1 on esitetty laskukaava laitteen vaarallisen vikaantumisen keskimääräiselle taajuuden laskemiselle. 1oo1-arkkitehtuurilla laitteen vaarallisen vi-

kaantumisen keskimääräinen taajuus on λ_{du}. Koko turvapiirin vaarallisen vikaantumisen taajuus on kaikkien siinä olevien laitteiden keskimääräisten vaarallisien vikaantumisien summa.

Sistemaan luodaan kaksi turvatoimintoa ”safety functions”- välilehdeltä. Turvatoiminnolle luodaan alajärjestelmät, jotka kuvaavat piirien laitteita. Turvapiirit ovat keskenään identtisiä. Molemmilla turvapiireillä on 6 laitetta: Lämpötilalähetin, signaalimuunnin, turvarele, magneettiventtiili, venttiilin toimilaite ja venttiili. Lämpötilalähettimen vaarallisen vikaantumisen keskimääräinen taajuus tuntia kohden on $3{,}0*10^{-8}$ (Ks. Liite 11), signaalimuuntimen $6{,}2*10^{-8}$ (Ks. Liite 6), turvareleen $2{,}5*10^{-9}$ (Ks. Liite 7), magneettiventtiilin $1{,}7*10^{-8}$ (Ks. Liite 14), toimilaitteen $1{,}8*10^{-7}$ (Ks. Liite 12) ja venttiilin $3*10^{-7}$ (Ks. Liite 13). Turvatoimintojen rakenne on esitetty kuviossa 13.



Kuvio 13. Venttiilin FZ-5510 turvatoimintojen rakenne

Kuviosta 14 nähdään, että turvatoimintojen keskimääräinen vaarallisen vikaantumisen taajuus on $5{,}9*10^{-7}$. Taulukosta 1 nähdään, että turvatoiminnot täyttävät turvallisuuden eheyden tason 2 vaatimukset todennäköisyyden osalta.

SF Liquor from heat exchangers, FZ-5510 valve interlock, TICZ-5511	
PLr	d
PL	d
PFHD [1/h]	5,9E-7

SF Liquor from heat exchangers, FZ-5510 valve interlock, TIZ-5512	
PLr	d
PL	d
PFHD [1/h]	5,9E-7

Kuvio 14. Venttiilin FZ-5510 turvatoimintojen keskimääräiset vaarallisien vikaantumisien taajuudet

9.3.2 Arkkitehtuurin rajoituksien täyttyminen venttiilin FZ-5510 turvatoiminnolla

Arkkitehtuurin rajoitusten täyttyminen venttiilin FZ-5510 turvatoiminnoilla on helpointa osoittaa standardin SFS-EN 61511- taulukon mukaan (Ks. Taulukko 3). Turvatoiminto on kahdennettu ja suunniteltu toimimaan siten, että vikasietoisuus on 1. Tiheiden ja jatkuvien vaateiden toimintapaa käytettäessä vikasietoisuuden on oltava 1 turvallisuuden eheyden tasolla 2. Arkkitehtuurin rajoitusten voidaan todeta olevan Standardin SFS-EN 61508 vaatimusten mukaisia.

10 Pohdinta ja yhteenveto

Työn tavoitteina oli selvittää, täyttyvätkö standardien SFS-EN 61508 ja SFS-EN 61511 vaatimukset eräkeittämön turvatoiminnoilla. Toimeksiantaja halusi myös selvittää, onko mahdollista vähentää turvapiirejä. Kaikki turvatoiminnot on kahdennettu, joten haluttiin selvittää, mitkä ovat ehdot vaatimusten täyttymiseksi ja voidaanko kahdennus jättää tekemättä. Riskianalyysin perusteella kaikille turvatoiminnoille oli määritelty turvallisuuden eheyden tasoksi 2.

Vaatimustenmukaisuustodistuksen saamiseksi on osoitettava, että turvapiirit täyttävät vaatimukset sekä vikaantumistodennäköisyyksien että arkkitehtuurin rajoituksien

osalta. Vikaantumistodennäköisyyksien laskennassa hyödynnettiin Sistema-laskentatyökalua. Vikaantumistodennäköisyyksien osalta voidaan todeta, että 1oo1 konfiguraatiovalinta on riittävä nykyisillä laitevalinnoilla turvallisuuden eheyden tasoon 2 nähden. Ongelmaksi kuitenkin muodostuvat arkkitehtuurin rajoitukset. Nykyisillä laitevalinnoilla ei saada täytettyä arkkitehtuurin rajoituksien vaatimuksia 1oo1-konfiguraatiovalinnalla. Kaikkien laitteiden turvallisien vikaantumisien osuus ei täytä turvallisuuden eheyden tason 2 vaatimuksia. Näin ollen arviointi pitäisi tehdä hyväksikäyttäen Reitti 2_H-menetelmää. Standardissa SFS-EN 61508 on kuitenkin määritelty, että tiheiden- ja jatkuvienvaateiden toimintatavalla vikasietoisuuden on oltava vähintään 1. Tämä ei täyty ilman kahdennusta, joten siksi siitä ei voida luopua.

Laskennoissa hyödynnettäväksi ohjelmaksi valikoitui Sistema, joka osoittautui erittäin hyväksi valinnaksi. Muina vaihtoehtoina olivat Excel sekä laitevalmistajien omat ohjelmat. Sistemaa ei varsinaisesti ole tarkoitettu prosessiteollisuuden vikaantumistodennäköisyyksien laskentoihin, mutta laskentojen tekeminen onnistui yllättävän hyvin. Sistema sisältää paljon eri toimintoja ja laskutapoja, mutta ne on tarkoitettu hyödynnettäväksi koneiden ja ohjausjärjestelmien suunnittelussa. Prosessiteollisuuden laskennoissa niistä ei ollut hyötyä.

Joihinkin turvapiireihin jouduttiin tekemään muokkauksia, kun todettiin, että turvallisuuden eheyden tason 2 vaatimukset eivät täyty. Tärkeimpänä muutoksena kansiventtiilin turvatoimintoon lisättiin magneettiventtiili. Vaatimuksien täyttyminen olisi hyvä osoittaa jo suunnitteluvaiheessa, koska muutoksien tekeminen jälkikäteen vaikuttaa muuhun suunnitteluun ja korjattavaa on enemmän (esim. koteloiden ja turvakaappien layoutit).

Aiheena toiminnallinen turvallisuus on erittäin laaja. Selvitystyöhön ja standardeihin tutustumiseen kului erittäin paljon aikaa. Toiminnalliseen turvallisuuteen liittyvää kirjallisuutta ja artikkeleita on olemassa erittäin paljon. Lisäksi Exidan verkkosivulla on selitetty standardien sisältöä kattavasti ja helpommin ymmärrettävässä muodossa.

Lähteet

Apfeld, R. Hauke,M. Schaefer,M. Rempel, P. Ostermann, B. 2010. The Sistema Cookbook 1- From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA. Institut Für Arbeitsschutz. Viitattu 26.8.2019. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook1_end.pdf

Gruhn,P. 2016. Understanding SIS Field Devive Fault Tolerance Requirements. aeSolutions. Viitattu 26.8.2019. http://www.aesolns.com/wp-content/uploads/2016/04/aesolutions_understanding_sis_field_device_fault_tolerance_requirements.pdf

Huelke, M. Lungfiel,A. Hauke,M. 2016. The Sistema cookbook 5- Sistema libraries. Institut Für Arbeitsschutz. Viitattu 26.8.2019. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/kochbuch/sistema_cookbook5_en.pdf

Lungfiel, A. & Huelke,M. 2016. Sistema- Getting started. Institut Für Arbeitsschutz. Viitattu 26.8.2019. https://www.dguv.de/medien/ifa/en/pra/softwa/sistema/getting_started.pdf

Ohjelmistotyökalu Sistema koneiden turvatoimintojen suunnitteluun. N.d. Sundcon. Viitattu 26.8.2019. https://www.sundcon.fi/turvallisuus/sistema-ohjelmistotyoekalu.html

Robinson, S. N.d. SIL or PL? What is the difference? TÜV SÜD. Viitattu 26.8.2019. https://www.tuv-sud.co.uk/uploads/images/1397220180236544250395/sil-or-pl.pdf

SFS-EN 61508-2:2010. Sähköisten/ Elektronisten/ Ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille.. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 24.1.2011. Viitattu 26.8.2019.

SFS-EN 61508-4:2010. Sähköisten/ Elektronisten/ Ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 4: Määritelmät ja lyhenteet. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 22.11.2010. Viitattu 26.8.2019.

SFS-EN 61508-5:2010. Sähköisten/ Elektronisten/ Ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 24.1.2011. Viitattu 26.8.2019.

SFS-EN 61508-6:2010. Functional safety of Electrical/Electronic/Programmable electronic safety-related systems- Part 6: Guidelines on the application of IEC61508-2 and IEC61508-3 (IEC 61508-6:2010). Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 24.1.2011. Viitattu 26.8.2019.

SFS-EN 61511-1:2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 1 Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 5.5.2017. Viitattu 26.8.2019.

SFS-EN 61511-3:2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 3 Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiseenv. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 5.5.2017. Viitattu 26.8.2019.

Turva-automaatio prosessiteollisuudessa. 2007. Helsinki: Turvatekniikan keskus. Viitattu 26.8.2019.
https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0

Valmetin toiminnot Suomessa. N.d. Valmetin koti-sivut. Viitattu 26.8.2019.
https://www.valmet.com/fi/

Liitteet

Liite 1. Korkein sallittu turvallisuuden eheystaso tyypin A turvallisuuteen liittyvän elementin tai alajärjestelmän toteuttamalle turvatoiminnalle (SFS-EN 61508-2, 46, Taulukko 2)

Elementin turvallisten vikaantumisten osuus	Laitteiston vikasietoisuus		
	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

HUOM. 1 Tätä taulukkoa yhdessä kohtien 7.4.4.2.1 ja 7.4.4.2.2 kanssa käytetään korkeimman mahdollisen alajärjestelmälle osoitettavan turvallisuuden eheyden tason (SIL) määrittämiseen, kun alajärjestelmän vikasietoisuus ja käytettyjen elementtien turvallisten vikaantumisten osuus tunnetaan:

i) yleiseen soveltamiseen mihin tahansa alajärjestelmään, katso 7.4.4.2.1.

ii) soveltamiseen alajärjestelmiin, jotka koostuvat kohdan 7.4.4.2.2 erityiset vaatimukset täyttävistä elementeistä. Jos osoitetaan suoraan tästä taulukosta, että alajärjestelmä täyttää määritellyn turvallisuuden eheystason, on tarpeellista täyttää kaikki kohdan 7.4.4.2.2 vaatimukset.

HUOM. 2 Tätä taulukkoa yhdessä kohtien 7.4.4.2.1 ja 7.4.4.2.2 kanssa voidaan käyttää myös:

i) laitteiston vikasietoisuuden vaatimusten määrittämiseen alajärjestelmälle, kun vaadittu turvatoiminnon turvallisuuden eheystaso ja käytettävien elementtien turvallisten vikaantumisten osuudet tunnetaan.

ii) turvallisten vikaantumisten osuuksien vaatimusten määrittämiseen elementeille, kun vaadittu turvatoiminnon turvallisuuden eheystaso ja alajärjestelmän laitteiston vikasietoisuus tunnetaan.

HUOM. 3 Kohtien 7.4.4.2.3 ja 7.4.4.2.4 vaatimukset perustuvat tässä taulukossa ja taulukossa 3 määriteltyihin tietoihin.

HUOM. 4 Katso liitteestä C tarkemmat tiedot siitä, kuinka turvallisten vikaantumisten osuus lasketaan.

Liite 2. Korkein sallittu turvallisuuden eheystaso tyypin B turvallisuuteen liittyvän elementin tai alajärjestelmän toteuttamalle turvatoiminnalle (SFS-EN 61508-2, 48, Taulukko 3)

Elementin turvallisten vikaantumisten osuus	**Laitteiston vikasietoisuus**		
	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

HUOM. 1 Tätä taulukkoa yhdessä kohtien 7.4.4.2.1 ja 7.4.4.2.2 kanssa käytetään korkeimman mahdollisen alajärjestelmälle osoitettavan turvallisuuden eheyden tason (SIL) määrittämiseen kun alajärjestelmän vikasietoisuus ja käytettyjen elementtien turvallisten vikaantumisten osuus tunnetaan:

i) yleiseen soveltamiseen mihin tahansa alajärjestelmään, katso 7.4.4.2.1

ii) soveltamiseen alajärjestelmiin, jotka koostuvat kohdan 7.4.4.2.2 erityiset vaatimukset täyttävistä elementeistä. Jos osoitetaan, suoraan tästä taulukosta, että alajärjestelmä täyttää määritellyn turvallisuuden eheystason, on tarpeellista täyttää kaikki kohdan 7.4.4.2.2 vaatimukset.

HUOM. 2 Tätä taulukkoa yhdessä kohtien 7.4.4.2.1 ja 7.4.4.2.2 kanssa voidaan myös käyttää

i) laitteiston vikasietoisuuden vaatimusten määrittämiseen alajärjestelmälle, kun vaadittu turvatoiminnon turvallisuuden eheystaso ja käytettävien elementtien turvallisten vikaantumisten osuuksien arvot tunnetaan

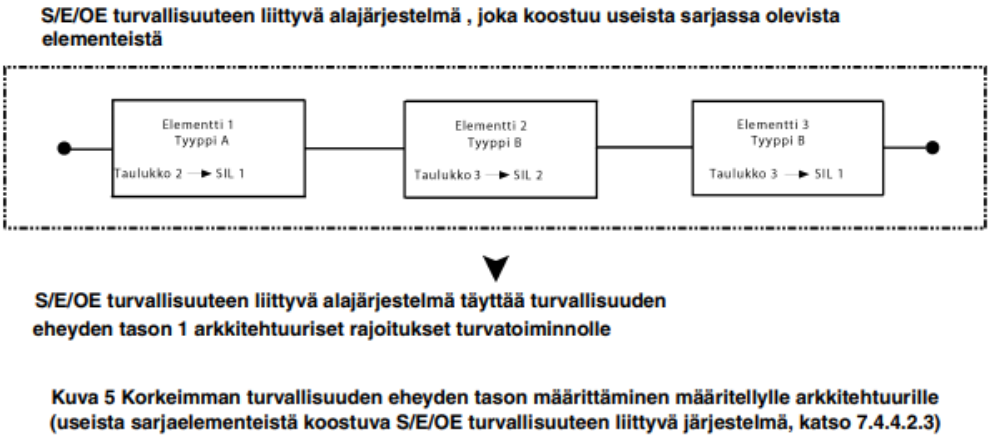
ii) turvallisten vikaantumisten osuuksien arvojen vaatimusten määrittämiseen elementeille, kun vaadittu turvatoiminnon turvallisuuden eheystaso ja alajärjestelmän laitteiston vikasietoisuus tunnetaan.

HUOM. 3 Kohtien 7.4.4.2.3 ja 7.4.4.2.4 vaatimukset perustuvat tässä taulukossa ja taulukossa 2 määriteltyihin tietoihin.

HUOM. 4 Katso liitteestä C tarkemmat tiedot siitä, miten turvallisten vikaantumisten osuus lasketaan.

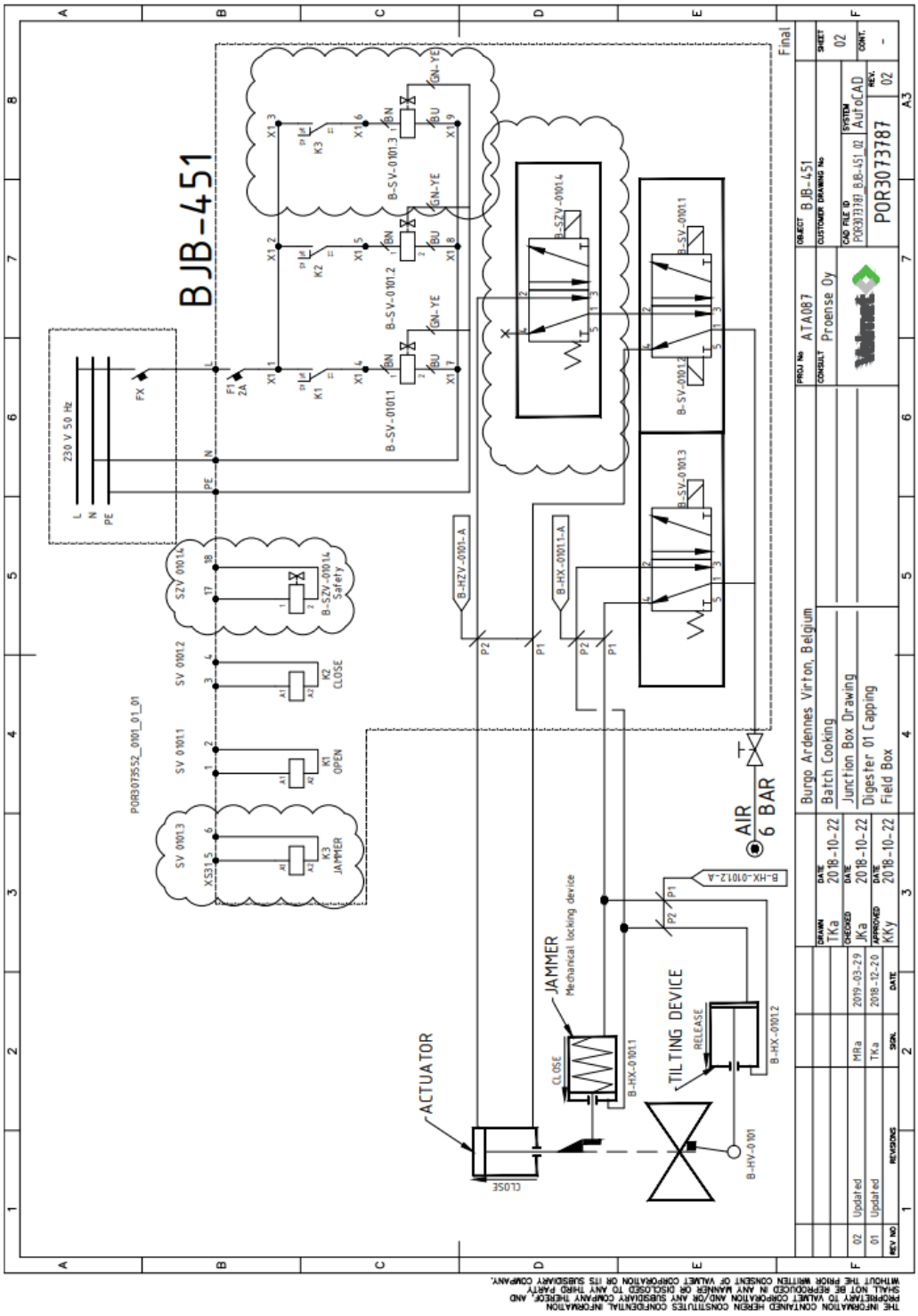
HUOM. 5 Käytettäessä kohtaa 7.4.4.2.1 tyypin B elementtien yhdistelmälle, jossa laitteiston vikasietoisuus on 1 ja jossa molempien elementtien turvallisten vikaantumisten osuus on vähemmän kuin 60 %, korkein sallittavissa oleva turvallisuuden eheyden taso yhdistelmän suorittamalle turvatoiminnolle on turvallisuuden eheyden taso 1.

Liite 3. S/E/OE turvallisuuteen liittyvä järjestelmä, joka koostuu useista sarjassa olevista elementeistä (SFS-EN 61508, 50, Kuva 5)



Kuva 5 Korkeimman turvallisuuden eheyden tason määrittäminen määritellylle arkkitehtuurille (useista sarjaelementeistä koostuva S/E/OE turvallisuuteen liittyvä järjestelmä, katso 7.4.4.2.3)

Liite 4. Kansiventtiilin piirikaavio



Liite 5. Emerson Rosemount 2051 painelähettimen SIL-sertifikaatti s.2

Emerson's Rosemount® 2051 Pressure Transmitter with 4-20mA HART

Certificate / Certificat / Zertifikat / 合格証

ROS 1107062 C002

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element
SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H
For models where SFF ≥ 90%

SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints for each element.

IEC 61508 Failure Rates in FIT[1]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Rosemount® 2051 Coplanar Differential & Coplanar Gage	0	84	258	32	91%
Rosemount® 2051 Coplanar Absolute, In-line Gage & Absolute	0	94	279	41	90%

Route 2_H Table[2]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Rosemount® 2051 Coplanar Differential & Coplanar Gage	0	84	258	32
Rosemount® 2051 Coplanar Absolute, In-line Gage & Absolute	0	94	279	41
Rosemount® 2051 Flowmeter Series based on 1195, 405, or 485 Primaries				
Flowmeter Series[3]	0	92	258	41
Rosemount® 2051 Level Transmitter: (w/o additional Seal)				
Coplanar Differential & Coplanar Gage	0	84	258	67
Coplanar Absolute, In-line Gage & Absolute	0	94	279	75
Rosemount® 2051 with Remote Seals[4]				

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of this certification:
Assessment Report: ROS 11/07-062 R005 V3R2
Safety Manual: 00809-0100-4107

[1]FIT = 1 failure / 10^9 hours

[2]SFF not required for devices certified using Route 2_H data. For information detailing the Route 2_H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components".

[3]Refer to ROS 13/04-008 R001 V1R0 "Primary Element FMEDA for Flowmeters" report for models that are excluded.

[4]Refer to the Remote Seal (ROS 1105075 R001 V2R1) FMEDA report for the additional failure rates to use when using with attached Remote Seals, or use exSILentia.

exida®

80 N Main St
Sellersville, PA 18960

T-002, V3R8

Liite 6. PR electronics 9116B signaalinmuuntimen SIL-sertifikaatti s.2

Certificate / Certificat / Zertifikat / 合格証

PREI 070902 P0002 C005

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Device

PFD_{AVG} and Architecture Constraints must be verified for each application

9116 Universal Converter

Systematic Capability:

The Product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

9116 Universal Converter Configurations	λ_{Safe}	λ_{DD}	λ_{DU}
Resistance / RTD temperature / TC temperature Inputs, Current Output	278	352	43
Resistance / RTD temperature / TC temperature Inputs, Relay Output	359	230	62
Current Input, Current Output	444	554	42
Current Input, Relay Output	636	320	62
Voltage Input, Current Output	395	479	56
Voltage Input, Relay Output	480	353	76

All failure rates are given in FIT (failures / 10^9 hours)

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: 0709-02C R014 V1R1

Safety Manual: 9116 Safety Manual V1R0

exida

64 N Main St
Sellersville, PA 18960

T-062, V1R7

Page 2 of 2

1 Grundgeräte / Basic modules

Typ Type	Sach-Nr.[1] Oder No.	Version	Internal Test-Report	Sicherheitsrelevante Strompfade Safety related circuits Safety Output	PFH$_D$	SIL CL[3]	Cat	PL[3]	Bemerkung Remark[2]
PNOZ s1 24VDC	750101 751101	1.0	717509892 V1.0	13-14 23-24	$2{,}00 \cdot 10^{-07}$	2	3	c	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s2 24VDC	750102 751102	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}50 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s3 24VDC	750103 751103	1.0	717509892 V1.0	13-14 23-24	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s4 24VDC	750104 751104	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s4 24VDC coated	751184	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s4 48-240VACDC	750134 751134	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}31 \cdot 10^{-09}$	3	4	e	–
PNOZ s4.1 24VDC	750124 751124	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
PNOZ s4.1 48-240VACDC	750154 751154	1.0	717509892 V1.0	13-14 23-24 33-34	$2{,}31 \cdot 10^{-09}$	3	4	e	–
PNOZ s5 24VDC	750105 751105	1.2	717509892 V1.0	13-14 23-24	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level
				37-38 47-48	$2{,}34 \cdot 10^{-09}$	3	4	e	Verzögerte Kontakte, Einsatz bis 5000m über NN delayed contacts, For use up to 5000m over sea level
PNOZ s5 24VDC coated	751185	1.2	717509892 V1.0	13-14 23-24	$2{,}31 \cdot 10^{-09}$	3	4	e	Einsatz bis 5000m über NN For use up to 5000m over sea level

TÜV SÜD RAIL GmbH
Barthstraße 16
D-80339 München
Tel.: +49 (89) 5791-3198, Fax: -2933
E-Mail: Jens.Luther@tuev-sued.de

Liite 8. ASCO 551&553-sarjojen SIL-sertifikaatti s.2

Series 551 and 553 Pilot Operated Spool Valves

Certificate / Certificat / Zertifikat / 合格証

ASC 1301001 C005

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability :

These products have met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with these products must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

Applications

Series 551 & 553 Spool Valves	3/2, NC, De-energize To Trip (DTT) and 5/2 (DTT)

IEC 61508 Failure Rates in FIT[1]

Failure Category	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
3/2 Single, NC, DTT, <2W Coil	0	209	0	329
3/2 Single, NAMUR, NC, DTT, <2W Coil	0	304	0	378
3/2 Single, NF Operator, NC, DTT, 9-16 W Coil	0	572	0	316
3/2 Single, NAMUR, NF Operator, NC, DTT, 9-16 W Coil	0	666	0	365
3/2 Redundant, NC, DTT, <2W Coil	0	187	0	369
5/2 Single, DTT, <2W Coil	0	234	0	378
5/2 Single NAMUR, DTT, <2W Coil	0	256	0	432
5/2 Single, NF Operator, DTT, 9-16 W Coil	0	597	0	365
5/2 Single, NAMUR, NF Operator, DTT, 9-16 W Coil	0	618	0	419
5/2 Redundant, DTT, <2W Coil	0	197	0	418
Adder for Coils[2] 9-16 Watts	0	299	0	0
Adder for Class H Coils 16–30 Watts	0	729	0	0

[1] FIT = 1 failure / 10^9 hours

[2] Failure Rate Adders for other Coil Options available from ASCO

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: ASC 13/01-001 R003 V1 R4 (or later)

Safety Manual: V9629R8 (or later)

80 N Main St
Sellersville, PA 18960

T-061, V3R1

Liite 9. Westlockin rajakytkimien SIL-sertifikaatti s.2

AccuTrak Position Monitor Series: 2200, 2300, 2600, 3000, 3200, 3300, 3400, 3500, 8300, 8400 and 8500

80 N Main St
Sellersville, PA 18960

T-061, V3R1

Certificate / Certificat / Zertifikat / 合格証

WES 1505053 C002

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

These Products have met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with these products must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This Device meets *exida* criteria for Route 2_H.

Versions:

Series	Switch Quantity and Type (Option Code)
AccuTrak 2200	1 to 6 SPDT Microswitches (5) 1 to 4 DPDT Microswitches (6) 1 to 6 P&F Inductive Sensor (7) 1 to 6 Magnum Switches (9)
AccuTrak 2300	
AccuTrak 2600	
AccuTrak 3000	
AccuTrak 3200	
AccuTrak 3300	
AccuTrak 3400	
AccuTrak 3500	
AccuTrak 8300	
AccuTrak 8400	
AccuTrak 8500	

IEC 61508 Failure Rates[1] in FIT[2]

AccuTrak Series Switch Circuit Qty (Option Code)	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
1 Switch Circuit (5, 6, 7 or 9)	0	11	0	94
2 Switch Circuits (5, 6, 7 or 9)	0	23	0	119
3 Switch Circuits (5, 6, 7 or 9)	0	34	0	149
4 Switch Circuits (5, 6, 7 or 9)	0	45	0	174
6 Switch Circuits (5, 6, 7 or 9)	0	68	0	229
8 Switch Circuits (6)	0	80	0	239
1 Switch Circuit (5, 6, 7 or 9) w/PVST[3]	11	0	86	8
2 Switch Circuits (5, 6, 7 or 9) w/PVST	23	0	110	9
3 Switch Circuits (5, 6, 7 or 9) w/PVST	34	0	139	10
4 Switch Circuits (5, 6, 7 or 9) w/PVST	45	0	163	11
6 Switch Circuits (5, 6, 7 or 9) w/PVST	68	0	216	13
8 Switch Circuits (6) w/PVST	80	0	225	14

[1] Failure Rates listed are only applicable if the switch contacts current is limited to 60% of the switches rated capacity and the end user has added external transient protection if being used with non-resistive loads.
[2] FIT = 1 failure / 10^9 hours
[3] PVST = Partial Valve Stroke Test of a final element Device

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: WES 15/05-053 R002 V2 R1 (or later)

Safety Manual: TECHUK-78

Liite 10. Siemensin kontaktorin 3RT10xx datalehti s. 8- 9

Safety related data	
Safety device type acc. to IEC 61508-2	Type B
B10 value	
• with high demand rate acc. to SN 31920	1 000 000
Safety Integrity Level (SIL) acc. to IEC 61508	2
SIL Claim Limit (subsystem) acc. to EN 62061	2
Performance level (PL) acc. to EN ISO 13849-1	c
Category acc. to EN ISO 13849-1	2
Stop category acc. to DIN EN 60204-1	0
Proportion of dangerous failures	
• with low demand rate acc. to SN 31920	40 %
• with high demand rate acc. to SN 31920	73 %
Product function	
• Mirror contact acc. to IEC 60947-4-1	Yes
• positively driven operation acc. to IEC 60947-5-1	No
PFHD with high demand rate acc. to EN 62061	0.00000045 1/h

PFDavg with low demand rate acc. to IEC 61508	0.007
MTBF	75 y
Hardware fault tolerance acc. to IEC 61508	0
T1 value for proof test interval or service life acc. to IEC 61508	20 y
Protection against electrical shock	finger-safe when touched vertically from front acc. to IEC 60529

Liite 11. Lämpötilalähettimen Emerson 644HANAQ4QTXA SIL-sertikaatti

Rosemount 644
4-20mA HART
Temperature
Transmitter

80 N Main St
Sellersville, PA 18960

T-002, V5R2

Certificate / Certificat / Zertifikat / 合格証

ROS 1204020 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 1 @ HFT = 0; SIL 2 @ HFT = 1; Route 1_H

SIL 2 @ HFT = 0; SIL 3 @ HFT = 1, Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT[2,3]

Application/Device/Configuration	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}	#	SFF
644 Single T/C mode	0	0	362	39	136	90.3%
644 Dual T/C mode	0	0	371	39	140	90.5%
644 Single RTD mode	0	0	317	30	133	91.4%
644 Dual RTD mode (3-wire RTD)	0	0	330	31	135	91.4%

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: ROS 12/04-020 R002 V2 R4

Safety Manual: 00809-0200-4728 Section 7

1. BR6 must be ordered with option code QT for this certificate to be valid below -40C.

2. FIT = 1 failure / 10^9 hours

3. 644 can be configured with single or dual RTD or Thermocouple sensors. The failure rates of the device vary with sensor configuration as well as other device configuration paramenters. See FMEDA for details on how to calculate the failure rates based on the configuration.

4. It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

Liite 12. NAF 791292-3240 toimilaitteen SIL-sertifikaatti

Turnex Series
Pneumatic Actuators

Certificate / Certificat / Zertifikat / 合格証

NAF 070721 C003

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT[1]

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Single Acting, Spring Return	0	199	0	473
Single Acting, Spring Return with PVST[2]	199	0	291	182

[1] FIT = 1 failure / 10^9 hours
[2] PVST = Partial Valve Stroke Test

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: NAF 07/07-21 R005 V3 R1

Safety Manual: NFENDS7459

64 N Main St
Sellersville, PA 18960

Liite 13. NAF 791292-3240 venttiilin SIL-sertifikaatti

Torex Series
Butterfly Valves

Certificate / Certificat / Zertifikat / 合格証

NAF 070721 C004

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT[1]

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Full Stroke, Clean Service	0	0	0	540
Tight Shut-Off, Clean Service	0	0	0	1303
Open on Trip, Clean Service	0	128	0	406
Full Stroke with PVST[2], Clean Service	0	0	240	300
Tight Shut-Off with PVST, Clean Service	0	0	279	1024
Open on Trip with PVST, Clean Service	128	0	240	166
Full Stroke, Severe Service	0	0	0	931
Tight Shut-Off, Severe Service	0	0	0	2338
Open on Trip, Severe Service	0	249	0	676
Full Stroke with PVST, Severe Service	0	0	384	547
Tight Shut-Off with PVST, Severe Service	0	0	423	1915
Open on Trip with PVST, Severe Service	249	0	384	292

[1] FIT = 1 failure / 10^9 hours
[2] PVST = Partial Valve Stroke Test

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: NAF 07/07-21 R005 V3 R1

Safety Manual: NFENDS4142

64 N Main St
Sellersville, PA 18960

Liite 14. Parkerin magneettiventtiilin 799975-341N03-24VDC SIL-sertifikaatti

Parker Lucifer SA
16 Ch. Fbg de Cruseilles
CH-1227 Carouge - Geneva
Tel. +41 22 3077 111
Fax +41 22 3077 110

Parker Lucifer SA certified

SIL - DECLARATION OF CONFORMITY
DECLARATION DE CONFORMITE - SIL
SIL - KONFORMITÄTSERKLÄRUNG

E Below mentioned parameters serve to the end user/plant projectors to define the Safety Integrity Level (SIL) according to IEC 61508 standard for the complete safety loop of an installation with mentioned Parker Lucifer solenoid valves/electrical parts.

F Les paramètres mentionnés ci-dessous servent aux utilisateurs/Ingénieurs de projet pour le calcul du degré de sécurité "Safety Integrity Level" (SIL) selon la norme IEC 61508 pour la boucle de sécurité complète d'une installation incluant les électrovannes / parties électriques Parker Lucifer mentionnées.

D Die untenstehenden genannten Parameter dienen dem Betreiber/Anlagenplaner zur Ermittelung der Sicherheits-Integritätsstufen "Safety Integrity Level" (SIL) nach IEC 61508 für die gesamte Sicherheitsschlaufe einer Anlage mit den erwähnten Parker Lucifer Elektromagnetventilen -Steuerteilen.

Valve 341N03 - Coil 496131 - -

SFF	Safe Failure Fraction [%]	**75%**
λ_S	Lambda – Safe detected/undetected [defects per hour]	**3.3E-08**
λ_{DD}	Lambda Dangerous Detected [defects per hour]	**1.7E-08**
λ_{DU}	Lambda Dangerous Undetected [defects per hour]	**1.7E-08**
λ_T	Lambda Total [defects per hour]	**6.7E-08**
PFD	Probability of Failure on Demand (based on 8760 hours -1year & MTTR 24h)	**7.4 E-05**
MTBF	Mean Time Between Failure (hours)	**15.0 E06**
Systematic Integrity: SIL 4 Capable The Product is classified as a **Type A** Device, having a **H**ardware **F**ault **T**olerance **(HFT) of 0**.		

Application restrictions:
The unit must be properly designed into a Safety Instrumented Function per the requirements in the installation, Operation and Maintenance Manual for the respective valve type

Genève le
Geneva, 31 March 2010
Genf den,

Gérard Chassot
Quality Assurance Manager