Tuomas Veikkola

Turva-automaatiotoiminnon eheystason todentaminen

Opinnäytetyö
Kevät 2019
SeAMK Tekniikka
Automaatiotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Insinööri (AMK), Automaatiotekniikka

Suuntautumisvaihtoehto: Sähköautomaatio

Tekijä: Tuomas Veikkola

Työn nimi: Turva-automaatiotoiminnon eheystason todentaminen

Ohjaaja: Heikki Rajala

Vuosi: 2019 Sivumäärä: 34

Tämän opinnäytetyön toimeksiantajana oli Pöyry Finland Oy, joka on kansainvälinen konsultti- ja suunnitteluyritys. Työn tarkoituksena oli selvittää, miten turva-automaatiojärjestelmä todennetaan sekä luoda aiheesta syvällinen tietopohja, jota voidaan tulevaisuudessa hyödyntää yrityksen turva-automaatioon liittyvissä projekteissa.

Prosessiteollisuudessa esiintyy vaaroja sekä riskejä, joiden aiheuttajina on prosessiin liittyvät laitteet tai kemikaalit. Turva-automaatio on tärkeä varautumismenetelmä prosessiteollisuuden toiminnallisen turvallisuuden varmentamisessa. Turva-automaatiojärjestelmällä pyritään estämään henkilö-, ympäristö- tai omaisuusvahinkoja. Vakavassa häiriö- tai vaaratilanteessa järjestelmän tehtävänä on pysäyttää prosessi tai laite ja ohjata se turvalliseen tilaan. Turva-automaatiojärjestelmän sopivuus määritetyille turva-automaatiotoimille on aina todennettava.

Opinnäytetyön tavoitteena oli perehtyä prosessiteollisuuden toiminnalliseen turvallisuuteen. Teoriaosuudessa käydään läpi standardien vaatimukset sekä turva-automaatiojärjestelmä. Tutkimusosiossa selvitetään esimerkin avulla, miten turva-automaatiotoiminnon turvallisuuden eheystaso todennetaan.

Työn aikana huomataan SFS-standardien antavan ainoastaan vaadittava turvallisuuden eheystaso sekä tason määritys. Työn edetessä huomattiin turva-automaatiotoimintojen monimutkaisuus, mikä vaikeuttaa turvallisuuden eheystason todentamista. Pohdinnassa pääteltiin, että turvallisuuden eheystason todentamiseen tarvitaan IEC-standardeja.

Avainsanat: turva-automaatio, turvallisuuden eheystaso, toiminnallinen turvallisuus, prosessiteollisuus

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Automation Engineering

Specialisation: Electric Automation

Author: Tuomas Veikkola

Title of thesis: Verification of a Safety Instrumented Function

Supervisor: Heikki Rajala

Year: 2019 Number of pages: 34

The objective of the thesis was to clarify how a safety instrumented function can be verified. The thesis was commissioned by Pöyry Finland Oy, which is an international consulting and engineering company. The thesis also studied basic information about safety automation which can be utilised in the company's future projects.

Process industry contains risks and dangers, which can be caused by process devices or chemicals. A safety instrumented system is designed to prevent an accident, if the system is detecting a serious fault or a dangerous situation. A safety instrumented system consists of defined safety instrumented functions, the suitability of which must be verified.

The objective of the thesis was to study functional safety in process industry. In the theory part of this thesis the demands and standards concerning safety automation systems were studied. In the practical part of the thesis, it was clarified, for example, how to verify the safety integrity level of a safety instrumented function.

As the result of the thesis it could be concluded that IEC-standards are needed when verifying the safety integrity level of safety instrumented functions. During this work it was noticed that SFS-standards give only requirements and do not pay attention to how verifying is made.

Keywords: safety automation, safety integrity level, functional safety, process industry

SISÄLTÖ

Opinnäytetyön tiivistelmä 2
Thesis abstract 3
SISÄLTÖ 4
Kuvio- ja taulukkoluettelo 6
Käytetyt termit ja lyhenteet 7
1 Johdanto 8
1.1 Työn tausta 8
1.2 Työn tavoite 8
1.3 Työn rakenne 8
1.4 Yritysesittely 9
2 Toiminnallinen turvallisuus 10
2.1 SFS-EN 61508 10
2.2 SFS-EN 61511 10
2.3 Rakenne 11
2.4 Vaatimukset 12
2.5 Tavoite 12
2.6 Vaara- ja riskianalyysi 13
2.7 Turvallisuuden eheystaso ja sen määritys 14
3 Turva-automaatiojärjestelmä 19
3.1 Rakenne 19
3.1.1 Turva-automaatiotoiminto 20
3.1.2 Turva-automaatiolaitteet 20
3.2 Suunnittelu 21
3.3 Laitteistorakenne 22
3.4 Laitearkkitehtuuri 23
3.5 Vikaantuminen 23
4 Turva-automaatiotoiminnon eheystason todentaminen 25
4.1 Exida 25
4.2 PFDavg-arvoon vaikuttavat tekijät 25
4.2.1 IEC 61508 26

4.3 Turva-automaatiotoiminnon todentamisen malli 28
4.3.1 Pintakytkin 29
4.3.2 Logiikka 29
4.3.3 Taajuusmuuttaja 30
4.3.4 Yhteenveto 30
5 Pohdinta 31
LÄHTEET 32

Kuvio- ja taulukkoluettelo

Kuvio 1. Riskin pienentämisen yleiset periaatteet 16

Kuvio 2. Riskigraafin yleinen kuvaus 17

Kuvio 3. Riskigraafi: ympäristonsuojelullinen menetys 18

Kuvio 4. 1oo2-äänestysrakenne 22

Kuvio 5. 2oo3-äänestysrakenne 23

Taulukko 1. Turva-automaatiojärjestelmän turvallisuuden elinkaaren yleiskatsaus 12

Taulukko 2. Turvallisuuden eheyden vaatimukset: keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä 14

Taulukko 3. Turvallisuuden eheyden vaatimukset: turva-automaatiotoiminnon vaarallisen vikaantumisen keskimääräinen taajuus 15

Taulukko 4. Prosessiteollisuuden riskigraafin parametrien kuvaukset 17

Taulukko 5. Pienin sallittu laitteiston vikasietoisuus turvallisuuden eheyden tason mukaisesti. 24

Taulukko 6. PFDavg-laskennan muuttujat 26

Käytetyt termit ja lyhenteet

S/E/OE	Sähköinen/elektroninen/ohjelmoitava elektroninen
PFD	Vaarallisen vikaantumisen todennäköisyys vaadittaessa
PFD_{avg}	Keskimääräinen vaarallisen vikaantumisen todennäköisyys vaadittaessa
PFH	Vaarallisen vikaantumisen keskimääräinen taajuus [h-1]
FIT	Vikaantumisten määrä joita voidaan odottaa 1x10^9 tunnissa (eng. Failures In Time)
TAJ (SIS)	Turva-automaatiojärjestelmä (eng. Safety Instrumented System)
SFS	Suomen Standardisoimisliito
IEC	International Electronechnical Commission, kansainvälinen sähköalan standardisoimisorganisaatio

1 Johdanto

1.1 Työn tausta

Tämä opinnäytetyö toteutettiin toimeksiantona Pöyry Finland Oy:lle. Yritys suunnittelee muun muassa laitoskokonaisuuksia prosessiteollisuuteen. Laitosten prosessit ovat yksilöllisiä eikä niitä voida vertailla keskenään. Prosessilaitoksissa voi syntyä riskejä ja vaaroja, joiden aiheuttajina on prosessiin liittyvät laitteet tai kemikaalit. Näistä voi johtua henkilövahinkoja tai päästöjä ympäristöön. Usein laitoksissa turvaudutaankin perusautomaation lisäksi erilliseen turva-automaatiojärjestelmään. Turva-automaatiojärjestelmä suunnitellaan erillisenä kokonaisuutena. Vakavassa häiriö- tai vaaratilanteessa turva-automaatiojärjestelmän tehtävänä on pysäyttää prosessi tai laite ja ohjata se turvalliseen tilaan. Turva-automaatiojärjestelmän sopivuus määritetyille turva-automaatiotoimille on todennettava.

1.2 Työn tavoite

Työn tavoitteena on perehtyä prosessiteollisuuden toiminnalliseen turvallisuuteen sekä selvittää miten määritettyjen turva-automaatiotoimintojen turvallisuuden eheystaso todennetaan. Lisäksi työssä käydään läpi turva-automaatiojärjestelmän vaatimukset ja rakenne. Tutkimuksessa ei oteta kantaa turva-automaatiojärjestelmän ohjelmointivaatimuksiin.

1.3 Työn rakenne

Työn ensimmäisessä osassa käydään läpi työn tausta, tavoite ja rakenne sekä esitellään työn toimeksiantaja.

Toisessa luvussa perehdytään toiminnalliseen turvallisuuteen. Osiossa käydään läpi toiminnallisen turvallisuuden vaatimukset, tavoitteet sekä tarvittavat määritte-

lyt. Lisäksi perehdytään toiminnallisen turvallisuuden standardiin sekä prosessiteollisuuden alakohtaiseen standardiin.

Kolmannessa luvussa tutustutaan tarkemmin turva-automaatiojärjestelmään. Luvussa käydään läpi turva-automaatiojärjestelmän rakenne, suunnittelu, laitetyypit, laitearkkitehtuuri sekä vikaantuminen.

Neljännessä luvussa tutkitaan, mitä tietoja tarvitaan, jotta voidaan todentaa turva-automaatiotoiminnon eheystaso. Luvussa käsitellään tarvittavat todennäköisyyskaavat, joita tarvitaan todentamisessa.

Viimeisessä luvussa pohditaan työn merkitystä ja miten työssä onnistuttiin. Lisäksi pohditaan, miten turva-automaatiojärjestelmä tulisi suunnitella, sekä miten turva-automaatiotoiminnon turvallisuuden eheystaso tulisi todentaa.

1.4 Yritysesittely

Pöyry Oyj on kansainvälinen konsultointi- ja suunnitteluyritys, jolla on 115 toimipistettä 40 eri maassa. Pöyryllä työskentelee yhteensä 5500 eri alan asiantuntijaa. Pöyry Finland Oy on osa kansainvälistä Pöyry Oyj yritystä. (Pöyry 2018.)

Pöyry tarjoaa palvelujaan globaalisti energia-, teollisuus- ja infrahankkeisiin. Engineering News Record (ENR)-lehden vuonna 2016 julkaistun tutkimuksen mukaan Pöyry on maailmanlaajuisesti luotetuin metsäteollisuuden suunnitteluyritys sekä kuudenneksi luotetuin teollisuuden suunnittelussa. Pöyryn palveluihin kuuluu käytön tuki, liikkeenjohdon konsultointi, suunnittelupalvelut sekä projektien toteutus. Pöyry tunnetaan luotettavana ja vastuullisena yhtiönä, joka toimittaa järkeviä ratkaisuja asiakkailleen. Yrityksen mottona on ”Asiakas ensin”. (Pöyry 2018.)

Pöyryn teollisuusosaston asiantuntijapalvelut kattaa hankkeen kaikki vaiheet. Keskeisimmät toimialat ovat metsä-, bio-, kaivos-, metalli-, kemia-, ja elintarviketeollisuus. (Pöyry 2018.)

2 Toiminnallinen turvallisuus

Tässä luvussa tarkastellaan prosessiteollisuussektorin toiminnallista turvallisuutta, jonka tärkein osa on turva-automaatiojärjestelmä. Toiminnallisella turvallisuudella tarkoitetaan sitä osaa kokonaisturvallisuudesta, joka riippuu järjestelmien ja laitteiden oikeasta ja oikea-aikaisesta toiminnasta (Turva-automaatio prosessiteollisuudessa 2007, 5).

Toiminnallisen turvallisuuden tarkoitus on suojata prosessin aikana laitoksen työntekijät, laitteisto sekä ympäristö. Toiminnallinen turvallisuus pitää sisällään kaikki turvallisuuteen liittyvät ohjelmoitavat järjestelmät. Järjestelmät voivat sisältää S/E/OE-laitteita, hydraulisia tai pneumaattisia laitteita. Turvallisuus riippuu järjestelmien oikeasta toiminnasta.

2.1 SFS-EN 61508

SFS-EN 61508 on standardi, joka koskee toiminnalliseen turvallisuuteen liittyviä S/E/OE-järjestelmiä. Standardi on yleispohjainen ja sopii käytettäväksi turvallisuuteen liittyvissä järjestelmissä. Standardi toimii alakohtaisten standardien kattostandardina. (SFS-EN 61508-1 2011, 16.)

Standardi kattaa yleisen turvallisuuden koko elinkaaren, alun vaara-analyysista aina järjestelmän käytöstä poistoon. Standardissa esitetään tarpeelliset järjestelmänäkökohdat, joiden perusteella pystytään määrittelemään vaatimukset turvallisuuteen liittyville järjestelmille. (SFS-EN 61508-1 2011, 12.)

2.2 SFS-EN 61511

Prosessiteollisuuden toiminnallinen turvallisuus perustuu standardiin SFS-EN 61511, jossa käsitellään turva-automaatiojärjestelmän soveltamista kyseiselle sektorille. Standardi SFS-EN 61511 esittää vaatimuksia turva-automaatiojärjestelmän kokonaisuudelle. Usein standardissa viitataankin standardiin SFS-EN 61508, josta prosessisektorin standardi on määritetty. (SFS-EN 61511-1 2017, 8.)

Prosessiteollisuudessa käytetään vaarojen välttämiseksi turva-automaatiotoimintoja, jotka estävät näiden tapahtumisen (SFS-EN 61511-1 2017, 29). Standardi määrittää kuinka vaaralliset tapahtumat tunnistetaan, sekä miten arvioida tarvittava turvallisuuden eheystaso (SFS-EN 61511-1 2017, 44).

Turva-automaatiotoiminoille on annettu numeeriset turvallisuuden eheystasot, mitkä tulee saavuttaa. Standardin vaatimuksissa määritellään tavoitteet suunnittelulle, asennukselle, käytölle ja ylläpidolle. Vaatimukset on määritetty, että voidaan luottaa turva-automaatiojärjestelmän toimintaan. (SFS-EN 61511-1 2017, 46.)

Määrityksissä kerrotaan vaadittavat toimenpiteet ja tekniikat, miten turva-automaatiotoiminnolle tulee määritellä turvallisuuden eheystaso. Standardi ei määritä, miten turva-automaatiotoimintojen eheystaso todennetaan. (SFS-EN 61511-3 2017, 15-17.)

Standardissa on määritetty, miten turva-automaatiojärjestelmä kelpuutetaan. Kelpuutuksessa tarkastellaan turva-automaatiojärjestelmän oikeellisuutta, dokumentointia sekä tarvittavia toimintatestauksia. (SFS-EN 61511-1 2017, 82-85.)

2.3 Rakenne

Toiminnallinen turvallisuus on kokonaisuus, joka toteutetaan vaiheittain. Elinkaaren aikana huomioidaan kaikki turvallisuuteen liittyvät toiminnot. Toimintoihin kuuluu S/E/OE-laitteita, hydraulisia tai pneumaattisia laitteita sekä manuaalisia toimintoja. Taulukossa 1 on kuvattu turva-automaatiojärjestelmän turvallisuuden toteuttamisen vaiheet. Vaiheita käydään tarkemmin läpi tulevissa luvuissa.

Taulukko 1. Turva-automaatiojärjestelmän turvallisuuden elinkaaren yleiskatsaus (SFS-EN 61511-1, 2017, 44)

1	Prosessin vaaran ja riskin arviointi
2	Turvatoimintojen kohdentaminen
3	TET-määritys
4	TAJ:n suunnittelu
5	TAJ:n todennus
6	TAJ:n asennus
7	TAJ:n kelpuutus
8	TAJ:n ylläpito

2.4 Vaatimukset

Prosessiteollisuudessa käytetään laitteita ja kemikaaleja, joille on omat direktiivinsä, standardinsa ja lakinsa. Prosessiteollisuudessa esiintyviä vaatimuksia voi muun muassa olla painelaite, ATEX, kemikaali, koneturvallisuus sekä EMC. (SFS-EN 61511-1 2017, 9.)

Turva-automaatiojärjestelmästä on oltava kattavat ja oikeelliset dokumentaatiot, jotka ovat yksiselitteisesti ymmärrettävissä sekä jäljennettävissä. Dokumentointia tulee korjata ja päivittää, järjestelmän muuttuessa. Dokumentaation sisällön täytyy olla kaikkien osapuolien saatavilla. Tärkeimpinä dokumentteina ovat vaara- ja riskianalyysi, turvallisuuden eheystason määritys sekä turva-automaatiojärjestelmän turvatoimintojen eheystasojen todennukset. (SFS-EN 61508-1 2011, 24.)

2.5 Tavoite

Toiminallisen turvallisuuden tavoitteena on tunnistaa riskit, määritellä turvatoiminnot sekä suunnitella prosessista riittävän turvallinen. Tavoitteena on vähentää to-

dennäköisyyttä vaarallisille vikaantumisille sekä minimoida riski siedettävälle tasolle. (SFS-EN 61511-1 2017, 37.)

Turvallisuus pyritään ensisijaisesti saavuttamaan prosessin rakenteellisilla ratkaisuilla, riittävällä mitoituksella ja materiaalivalinnoilla sekä käyttämällä ensisijaisesti muita riskien vähennyskeinoja (esim. rakenteelliset ratkaisut) (Heikkinen 2015).

Turva-automaatiojärjestelmää käytetään riskin pienentämiseen, ellei riskiä pystytä vähentämään perusautomaatiolla siedettävälle tasolle (SFS-EN 61511-1 2017, 26). Turva-automaatiojärjestelmän tehtävä onkin valvoa prosessia sekä suorittaa turva-automaatiotoiminto vaateen sattuessa (SFS-EN 61511-3 2017, 12).

2.6 Vaara- ja riskianalyysi

Vaara- ja riskianalyysin tavoitteena on löytää prosessista tunnistamattomia vaaroja tai vaaranpaikkoja, jotka liittyvät prosessissa ohjattaviin laitteisiin. Prosessissa esiintyvien vaarojen tai vaarallisten tapahtumien todennäköiset lähteet on määritettävä. (SFS-EN 61508-1 2011, 50.)

Vaaralla tarkoitetaan tilannetta, jossa ihminen, laitteisto tai ympäristö joutuu vaaralliseen tilanteeseen (SFS-EN 61511 2017, 21). Riski on käsite joka sisältää vaarallisen vaateen esiintymisen sekä seurauksen. (SFS-EN 61511 2017, 28).

Analyysin määrittämisessä arvioidaan henkilö-, ympäristö ja materiaalivaarat. Määrittämisen yhteydessä on arvioitava, voidaanko riskejä eliminoida tai vähentää sekä aiheuttaako tulevan turvatoiminnon aktivointi mahdollisesti uuden vaaran. Analyysissa on huomioitava vaarallisten vikojen laukaisutyypit sekä vian laukeamisen syy. (SFS-EN 61511-3 2017, 52.)

Määrityksen tuloksena syntyy dokumentoitava vaara- ja riskianalyysi, joka on pohjana määritettäessä turvallisuuden eheystasoja (SFS-EN 61508-1 2011, 54).

2.7 Turvallisuuden eheystaso ja sen määritys

Turvallisuuden eheys on todennäköisyys siitä, miten varmasti turva-automaatiojärjestelmä toteuttaa turva-automaatiotoiminnon hyväksytysti, kaikissa olosuhteissa (SFS-EN 61508-4 2010, 34).

Turvallisuuden eheyden ajatellaan koostuvan seuraavista kahdesta elementistä: laitteiston sekä systemaattinen turvallisuuden eheys. Laitteiston eheys tarkoittaa laitevikaantumista, systemaattinen eheys kertoo turva-automaatiojärjestelmän systemaattisista virheistä. (SFS-EN 61511-3 2017, 12.)

Turvallisuuden eheystaso on vähimmäistaso, joka turva-automaatiojärjestelmän tulee saavuttaa toimiakseen siedettävällä turvallisuuden tasolla. Turvallisuuden eheystason vaatimukset ovat erilaiset harvoille ja tiheille vaateille.

Harvojen vaateiden kohdalla käytetään PFDavg-arvoa, joka on keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä. Standardissa SFS-EN 61511 määritetään harvojen vaateiden toimintatapa seuraavasti: turva-automaatiotoiminto suoritetaan vain vaateesta, prosessin siirtämiseksi määriteltyyn turvalliseen tilaan, ja vaateiden taajuus ei ole suurempi kuin yksi vuodessa. (SFS-EN 61511-1 2017, 23.) Harvojen vaateiden toimintavan turvallisuuden eheystasovaatimukset ilmenevät taulukosta 2.

Taulukko 2. Turvallisuuden eheyden vaatimukset: keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä (PFDavg) (SFS-EN 61511-3, 54)

VAATEIDEN TOIMINTATAPA		
Turvallisuuden eheyden taso TET	Keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä (PFDavg)	Vaadittu riskin pienennys
4	≥ 10−5 … < 10−4	> 10 000 … ≤ 100 000
3	≥ 10−4 … < 10−3	> 1000 … ≤ 10 000
2	≥ 10−3 … < 10−2	> 100 … ≤ 1000
1	≥ 10−2 … < 10−1	> 10 … ≤ 100

Tiheiden vaateiden kohdalla käytetään PFH-arvoa, joka on vaarallisen vikaantumisen keskimääräinen taajuus tuntia kohti. Standardissa SFS-EN 61511 määritetään tiheiden vaateiden toimintatapa seuraavasti: turva-automaatiotoiminto suoritetaan vain vaateesta, prosessin siirtämiseksi määriteltyyn turvalliseen tilaan, ja vaateiden taajuus on suurempi kuin yksi vuodessa. (SFS-EN 61511-3 2017, 24.) Jatku-

vien tai tiheiden vaateiden toimintatapojen turvallisuuden eheystasovaatimukset ilmenevät taulukosta 3.

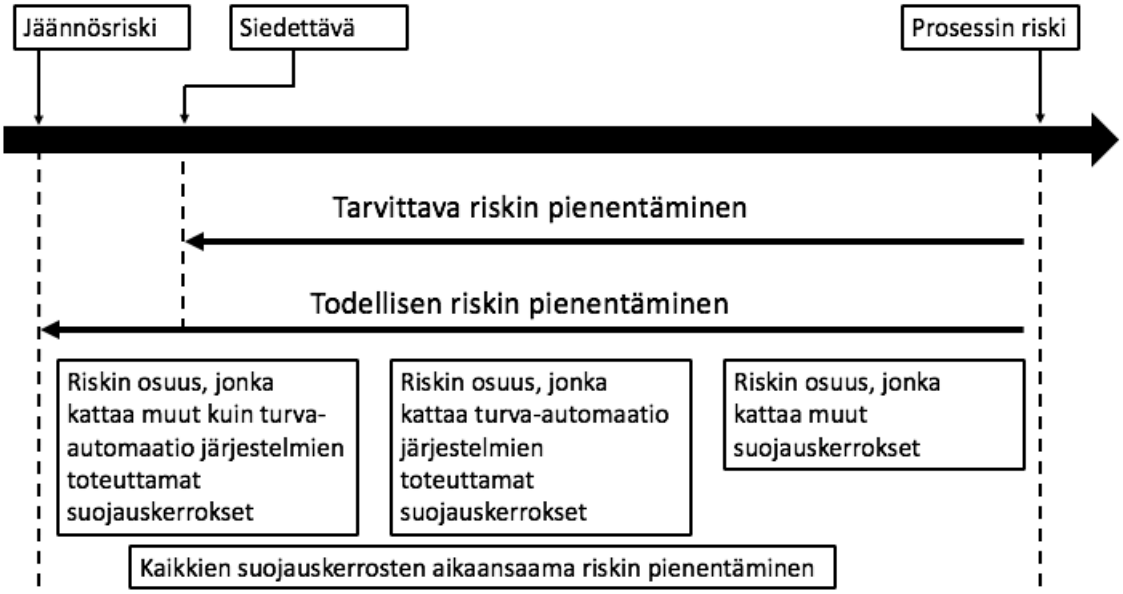
Taulukko 3. Turvallisuuden eheyden vaatimukset: turva-automaatiotoiminnon vaarallisen vikaantumisen keskimääräinen taajuus (SFS-EN 61511-3 2017, 55)

	JATKUVA TAI VAATEIDEN TOIMINTATAPA
Turvallisuuden eheyden taso TET	Vaarallisen vikaantumisen keskimääräinen taajuus (vikaa tuntia kohti)
4	≥ 10−9 ... < 10−8
3	≥ 10−8 ... < 10−7
2	≥ 10−7 ... < 10−6
1	≥ 10−6 ... < 10−5

Turvallisuuden eheystason määritys perustuu riskin tai riskien tarkasteluun, jonka perusteella vaaralliselle tapahtumalle määritetään turvallisuuden eheystaso. Määrityksessä on hyvä muistaa, että turvallisuuden eheystaso koskee ainoastaan tiettyä turva-automaatiotoimintoa eikä turva-automaatiojärjestelmää.

Riskien määrityksessä on havaittu prosessin riskin olevan sietämätön, jolloin havaittu riski tulee pienentää siedettävälle tasolle turva-automaatiojärjestelmän avulla. Siedettävä riski tulee määrittää tapauskohtaisesti. Siedettävän riskin arvioinnissa tulee huomioida vaaralliselle tapahtumalle altistuneiden henkilöiden havainnot sekä näkemykset. (SFS-EN 61511-3 2017, 12.)

Prosessin riskillä tarkoitetaan, miten vaarallinen tapahtumariski on perusautomaatiojärjestelmälle, kun tarkastelussa ei olla otettu huomioon turva-automaatiojärjestelmää. Siedettävä riski on tavoitetaso, joka määritellään tapauskohtaisesti. Jäännösriski on vaarallisten tapahtumien esiintyvyys turva-automaatiojärjestelmän lisäämisen jälkeen. (SFS-EN 61511-3 2017, 13.) Kuviossa 1 esitetään turva-automaatiojärjestelmällä toteutettava riskin pienentäminen.



Kuvio 1. Riskin pienentämisen yleiset periaatteet (SFS-EN 61511-3 2017, 14)

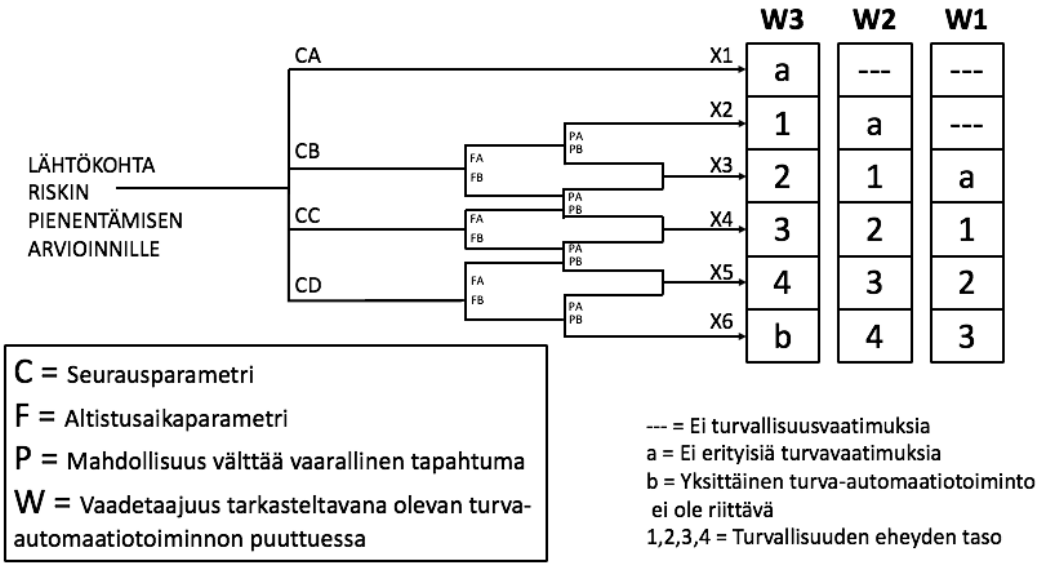
Turvallisuuden eheystaso määritetään käyttäen riskigraafia. Riskigraafin tuloksena saadaan turvallisuuden eheystaso turva-automaatiotoiminnolle. Määrityksen suorittaa työryhmä, johon kuuluu asiantuntijoita tilaajalta sekä toteuttajalta. Työryhmän jäsenillä tulee olla kattava kuvaus vaarallisesta tapahtumasta sekä riskin vähennyskeinoista. (SFS-EN 61511-3 2017, 35-37.)

Riskigraafissa määritellään vaarasta johtuvat seuraukset, oleskeluaika vaara-alueella, vaaran välttämisen todennäköisyys sekä vaarallisen tilanteen esiintymistiheys. Riskigraafi muodostuu neljästä parametrista, jotka on esitetty taulukossa 4. Ennen riskigraafin käyttöä parametrit kalibroidaan kyseiselle laitokselle tai prosessille. Riskigraafin kalibroinnissa asetetaan riskigraafin parametreille lukuarvot. (SFS-EN 61511-3 2017, 35.)

Taulukko 4. Prosessiteollisuuden riskigraafin parametrien kuvaukset (SFS-EN 61511-3 2017, 35)

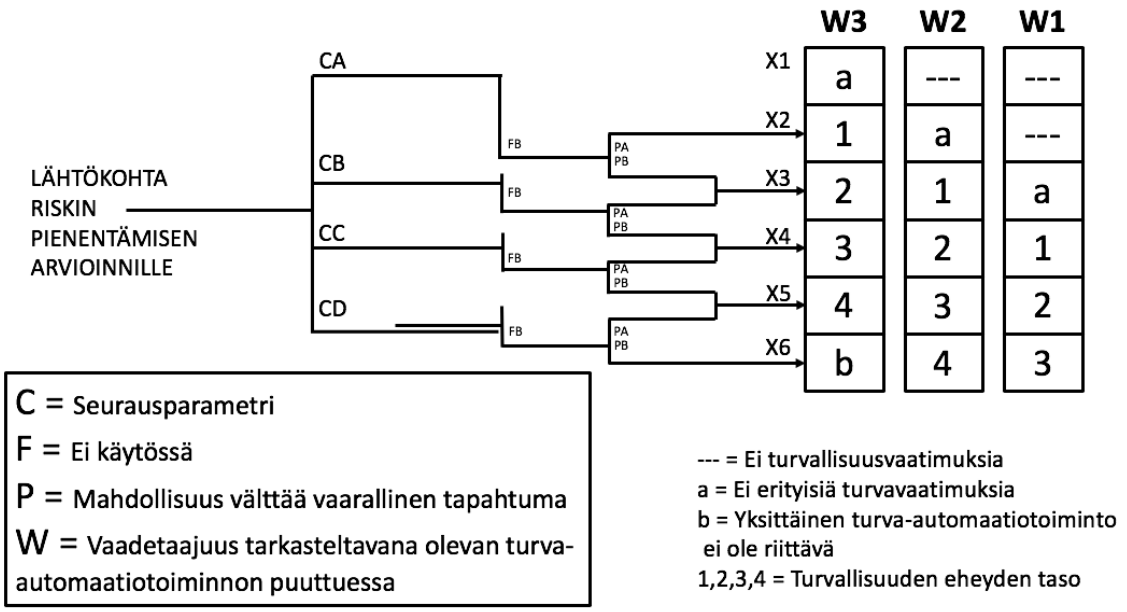
Parametri		Kuvaus
Seuraus	C	Kuolemantapausten ja/tai vakavien vammautumisten lukumäärä, joka todennäköisesti seuraa vaarallisen tapahtuman sattumisesta. Määritetään laskemalla ihmisten lukumäärä altistuneella alueella, kun alue on miehitetty, ottaen huomioon haavoittuvuus vaaralliselle tapahtumalle.
Miehitys	F	Todennäköisyys, että altistunut alue on miehitetty vaarallisen tapahtuman sattumisen ajankohtana. Määritetään laskemalla se aikavälin osa, jolloin alue on miehitetty vaarallisen tapahtuman sattumisen ajankohtana. Tässä voidaan ottaa huomioon mah dollisuus kasvaneesta todennäköisyydestä, että henkilöitä on altistuneella alueella tutkimassa poikkeavia tilanteita, joita voi olla vaaralliseen tapahtumaan johtavan kehityksen aikana (tarkastellaan myös muuttaako tämä parametrin C arvoa).
Todennäköisyys vaaran välttämiseen	P	Todennäköisyys, että altistuneet henkilöt kykenevät välttämään vaaratilanteen, joka esiintyy, jos turva-automaatiotoiminto epäonnistuu vaateen sattuessa. Tämä riippuu siitä, onko alueella riippumattomia menetelmiä varoittamassa altistuneita henkilöitä vaarasta ennen sen sattumista ja onko siellä pakenemisen mahdollisuutta.
Vaadetaajuus	W	Niiden tapausten lukumäärä vuotta kohden, joissa vaarallinen tapahtuma voisi sattua tarkasteltavana olevan turva-automaatiotoiminnon puuttuessa. Tämä voidaan määrittää tarkastelemalla kaikkia vikaantumisia, jotka voivat johtaa vaaralliseen tapahtumaan ja arvioimalla esiintymisen kokonaistaajuus. Muut suojauskerrokset tulisi ottaa mukaan tarkasteluun.

Riskigraafin toteutuksessa valitaan sopiva parametri ja yhdistetään valitut parametrit. Valitut parametrit muodostavat ketjun, joka ohjaa riskigraafin tietylle turvallisuuden eheystasolle (kuvio 2). Menetelmä toimii erilaisille turvallisuuden eheystasomäärityksille, koska riskigraafi on tarkoitettu havainnoimaan yleisiä periaatteita. (SFS-EN 61511-3 2017, 34.)



Kuvio 2. Riskigraafin yleinen kuvaus (SFS-EN 61511-3 2017, 38)

Riskigraafilla tapahtuvaa määritystä voidaan käyttää myös, jos vaarana on ympäristönsuojelullinen menetys tai yrityksen omaisuuden menetys. Mikäli riskigraafia käytetään näihin määrityksiin, riskigraafia tulee muokata näihin tarkoituksiin (kuvio 3). (SFS-EN 61511-3 2017, 34.) Ympäristövahinko on laitteiston vikaantumisesta tai inhimillisestä virheestä johtuva ympäristönsuojelullinen menetys. Omaisuuden menettäminen on kokonaistaloudellinen menetys, johon sisältyy uudelleenrakentamiskustannukset sekä tuotannon menetyksen. (SFS-EN 61511-3 2017, 40-41.)



Kuvio 3. Riskigraafi: ympäristonsuojelullinen menetys (SFS-EN 61511-3 2017, 41)

Turvallisuuden eheystason määrityksen aikana tehdyt valinnat tulee dokumentoida. Dokumenteista on oltava turva-automaation määrityslaajuus, josta ilmenee mitä riskiä turva-automaatiojärjestelmällä pyritään vähentämään. (SFS-EN 61511-3 2017, 37.) Tarvittavia dokumentteja on vaara- ja riskianalyysi, kokousasiakirjat, raportit, PI-kaaviot, määritysmenetelmä sekä turvallisuuden eheystason määritys. Dokumenteista esiintyvien valintojen tulee olla selkeästi ymmärrettävissä sekä perusteltavissa. (SFS-EN 61511-1 2017, 91-92.)

3 Turva-automaatiojärjestelmä

Tässä luvussa käydään läpi turva-automaatiojärjestelmän rakenne sekä standardit SFS-EN 61508 sekä SFS-EN 61511, jotka antavat ohjeistuksia sekä esimerkkejä siitä, miten turva-automaatiojärjestelmä saavuttaa vaadittavan turvallisuuden eheystason prosessiteollisuudessa.

Turva-automaatiojärjestelmän tehtävänä on suorittaa määritetyt turva-automaatiotoiminnot automaattisesti, mikäli määritetyistä turva-parametreista poiketaan. Turva-automaatio on tärkeä varautumismenetelmä prosessiteollisuuden toiminnallisen turvallisuuden varmentamisessa. (Turva-automaatio prosessiteollisuudessa 2007, 4.)

3.1 Rakenne

Turva-automaatiojärjestelmä on kokonaisuus, joka koostuu turvalogiikasta ja kenttälaitteista. Järjestelmä sisältää turva-automaatiolaitteiden muodostamia turva-automaatiotoimintoja, joiden tehtävänä on ylläpitää toiminnallista turvallisuutta. Järjestelmän kenttälaitteita ovat tuntoelimet sekä toimilaitteet. (SFS-EN 61511-1 2017, 29.)

Tuntoelimien tehtävänä on kerätä tietoa, jotta logiikka voi päättää onko prosessi vaarallisessa tilassa. Tuntoelimiä voidaan kutsua myös antureiksi, jotka voivat mitata muun muassa lämpötilaa, painetta, virtausta, pinnankorkeutta tai tiheyttä. (Emerson Product Bulletin 2018.)

Logiikan tehtävä turva-automaatiojärjestelmässä on toimia tarkkailijana, joka analysoi tuntoelimen antamia signaaleita sekä tarpeen vaatiessa antaa toimilaitteelle käskyn ajaa prosessi turvalliseen tilaan. Laitteiston vikaantuessa logiikan tehtävänä on suorittaa turvatoiminto. (Emerson Product Bulletin 2018.)

Toimilaitteiden tehtävä on suorittaa logiikan määräämiä turva-automaatiotoimintoja. Tyypillisiä toimilaitteita, jotka tuovat prosessin turvalliseen

tilaan ovat muun muassa taajuusmuuttajat sekä sulkuventtiilit. (Emerson Product Bulletin. 2018.)

3.1.1 Turva-automaatiotoiminto

Turva-automaatiotoiminto on yksilöllinen turvatoiminto, joka toteutetaan turva-automaatiojärjestelmällä. Turva-automaatiotoiminto suunnitellaan alentamaan sietämätön riski siedettävälle tasolle. (SFS-EN 61511-1 2017, 29.)

Turva-automaatiotoiminto sisältää joukon laitteita, jotka yhdessä muodostavat turvapiirin. Turvapiiri sisältää tuntoelimen, joka havaitsee mahdollisen vaaratilanteen. Tuntoelin antaa signaalin turvalogiikkaan, joka käskee toimilaitetta tuomaan prosessin turvalliseen tilaan. Turva-automaatiotoiminnolla on kyky havaita, päättää sekä tuoda prosessi turvalliseen tilaan. Toiminto suunnitellaan turvallisuuden eheystason mukaiseksi. (Exida Glossary. [Viitattu 8.4.2019].)

3.1.2 Turva-automaatiolaitteet

Turva-automaatiojärjestelmän laitteet tulee valita turva-automaatiotoimintoon sopivaksi. Laitteen valinnassa on huomioitava riittävän pieni vaarallisten vikaantumisten todennäköisyys sekä arkkitehtuurinen rakenne. Laitteiden avulla saavutetaan riittävä riskin pienennys, tästä syystä laitevalinnoissa on huomioitava aiemmat käyttökokemukset. (SFS-EN 61511-2 2017, 50.)

Turva-automaatiolaitetta valittaessa on tärkeää varmistaa, onko valmistajan asettama laitteen turvallisuuden eheystaso tarpeeksi kyvykäs halutulle turva-automaatiotoiminnolle. Laitevalinnan yhteydessä on hyvä ymmärtää ettei pelkkä valmistajan lupaama turvallisuuden eheystaso takaa laitteen sopivuutta. (Schwartz & Hochleitner, [Viitattu 8.4.2019]).

Laitteen valinnassa on huomioitava turvallisen asennon merkitys prosessille. Esimerkiksi vaarallisen kemikaalin purkuletkun rikkoutumisessa toimilaitteen tulee sulkea venttiili. Turva-automaatiolaitteet erottuvat usein fyysisesti perusautomaatiolaitteista. (SFS-EN 61511-1 2017, 65-67.)

3.2 Suunnittelu

Turva-automaatiojärjestelmän (TAJ) suunnittelussa tulee huomioida vaadittava eheystaso sekä järjestelmän riippumattomuus muista automaatiojärjestelmistä. The Offshore and Onshore Reliability Data eli OREDA:n suorittaman tutkimuksen mukaan 65% automaatiojärjestelmien vioista on aiheutettu jo ennen järjestelmän varsinaista käyttöä. (Automaatioväylä verkkolehti 3/2015, 27.)

Perusautomaatiojärjestelmä voi hyödyntää turvalaitteiden mittaustuloksia tai ohjata lähtöjä, kuten solenoidiventtiileitä. Turvalaitteiden signaalien tulee kuitenkin kulkea perusautomaatioon TAJ:n kautta. TAJ:n ohjaaman turvatoiminnon tulee olla toimintakunnossa, vaikka perusautomaatiojärjestelmä vikaantuisi. (SFS-EN 61511-1 2017, 62.)

TAJ:n virransyötön on suositeltavaa olla akkuvarmennettu. (SFS-EN 61511-1, 2017, 63.) TAJ:n laitteiden virransyöttö tulisi suunnitella lepovirtaperiaatteella, jolloin kenttälaitteen katoaminen turva-automaatiojärjestelmästä aiheuttaa turvatoiminnon. Tällaisia tilanteita voivat olla esimerkiksi, laitteen energian syötön katkeaminen tai paineilman puuttuminen. Lepovirtamenetelmällä suojaudutaan ulkoisilta häiriöiltä, jotka voivat vaarantaa turvatoiminnon. Tällä menetelmällä varmistetaan turvalaitteiden toimintakunto vaateen sattuessa. (Automaatioväylä verkkolehti 3/2015, 28.)

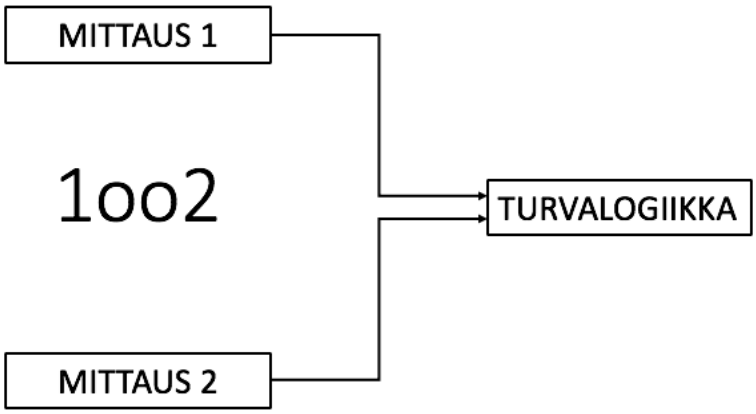
Turva-automaatiojärjestelmän suunnittelun päätavoite on toteuttaa turva-automaatiotoiminnot vastaamaan määritettyä turvallisuuden eheystasoa. Laitoksissa voidaan vaatia prosessin käyttövarmuutta. Tällöin tulee huomioida turva-automaatiojärjestelmän arkkitehtuurinen rakenne, etteivät laitteiden turvalliset vikaantumiset turhaan keskeyttäisi prosessia. (SFS-EN 61511-1, 2017, 62.)

Turva-automaatiosuunnittelussa on tärkeää valita sertifioituja laitteita, joista löytyy virallisia testidokumentteja. Laitteen valmistaja dokumentoi kaikki laitteen tiedot turvallisuuskäsikirjaan. (SFS-EN 61508-2 2010, 134.) Turva-automaatiotoiminnon eheystason todennuslaskelma on helpompaa suorittaa turvallisuuden eheystasoluokitelluilla turvalaitteilla.

3.3 Laitteistorakenne

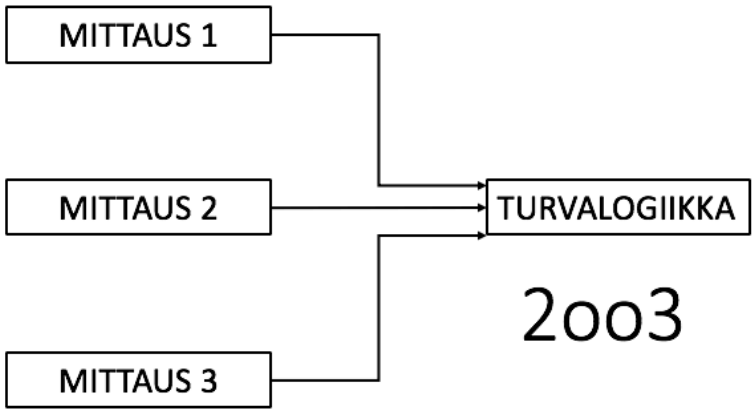
Turva-automaatiojärjestelmässä rakenteelliset suojat toteutetaan erilaisista laiterakenteista siten, että yksi mittalaite korvataan useammilla mittalaitteilla. Tätä kutsutaan redundanssiksi, jota käytetään tuomaan prosessille luotettavuutta tai käytettävyyttä. (SFS-EN 61508-5 2010, 22.)

Turva-automaatiojärjestelmässä käytetään redundanttisia äänestysrakenteita, kuten 1oo2 (1 out of 2). Tällainen äänestysrakenne sisältää kaksi erillistä laitetta (kuvio 4). Turva-automaatiojärjestelmä suorittaa turvatoiminnon toisen laitteen vioittuessa tai vaatiessa sitä. Myös molempien laitteiden vaatiessa suoritetaan turvatoiminto. (Heikkinen 2015.) Kyseinen äänestysrakenteen vikasietoisuus on 1. Toisen laitteen vaarallinen vikaantuminen ei vaikuta turvatoimintoon, koska turva-automaatiojärjestelmä pystyy toimimaan riittävällä todennäköisyydellä vaateen sattuessa. (SFS-EN 61511-2 2017, 46).



Kuvio 4. 1oo2-äänestysrakenne

Äänestysrakenne 2oo3 (2 out of 3) sisältää kolme laitetta (kuvio 5). Yhden laitteen vioittuminen ei laukaise turvatoimintoa. Kyseinen laiterakenne antaa prosessille turvallisuutta ja käytettävyyttä. (Heikkinen 2015.)



Kuvio 5. 2oo3-äänestysrakenne

3.4 Laitearkkitehtuuri

Turva-automaatiojärjestelmän laitteita on eri tyyppisiä. Turva-automaatiotoiminnon laitteet jaetaan alajärjestelmiin. Laitteet voidaan jakaa kahteen eri ryhmään, tyyppi A ja tyyppi B. Laitetyypit käyttävät eri taulukkoa laitteiston vikasietoisuuteen. (SFS-EN 61508-2 2010, 44.)

Tyypille A on määritelty kaikki vikaantumismuodot sekä laitteen käyttäytyminen pystytään ennakoimaan vikatilanteen sattuessa. Laitteen vikaantumisesta on riittävästi tietoa. (SFS-EN 61508-2 2010, 42.)

Tyypille B ei ole kaikki vikaantumismuodot tiedossa, eikä laitteen käyttäytymistä vikatilanteessa pystytä ennakoimaan (SFS-EN 61508-2 2010, 43).

3.5 Vikaantuminen

Turva-automaatiolaitteiden vikaantumiset voidaan jakaa kolmeen eri kategoriaan, joita on vaaralliset vikaantumiset, diagnostiikalla paljastuvat vaaralliset vikaantumiset sekä turvalliset vikaantumiset (Heikkinen 2015).

Vaarallisella vikaantumisella tarkoitetaan tilannetta, jossa laitteen vikaa ei huomata. Vaarallinen vikaantuminen estää laitetta reagoimasta vaadittaessa. Vikaantu-

miset voivat johtua järjestelmän vääränlaisesta määrittelystä, systemaattisesta tai satunnaisesta laitteiston vikaantumisesta, ohjelmistovirheestä tai järjestelmän toimintaympäristössä tapahtuneesta muutoksesta. (SFS-EN 61508-4, 2010, 44.)

Turvallisuuteen liittyvän järjestelmän vaarallinen vikaantuminen voi aiheuttaa onnettomuustilanteen, jos turva-automaatiojärjestelmä ei toimi oikein vaadetilanteessa (SFS-EN 61508-4 2010, 44). Laitteistonvikaantumisista johtuva matemaattinen vikaantumistodennäköisyystarkastelu perustuu käytännössä vaarallisiin vikaantumisiin (Heikkinen 2015).

Turvallisessa vikaantumisessa laite antaa virheellisen tiedon turva-automaatiojärjestelmälle, joka luulee prosessin olevan vaarallisessa tilassa ja suorittaa turva-automaatiotoiminnon. Tämä turvallisesta vikaantumisesta johtuva prosessin alasajo on virheellinen ja johtuu ainoastaan laitteen vikaantumisesta. (SFS-EN 61508-4 2010, 44.)

Turva-automaatiojärjestelmän turva-automaatiotoimintoon kuuluvat laitteet jaetaan alajärjestelmiin. Alajärjestelmiä ovat anturit, turvalogiikka ja toimilaitteet. (SFS-EN 61511-1 2017, 29-30.) Jokaiselle alajärjestelmälle määrätään laitteiston vikasietoisuus (SFS-EN 61511-1 2017, 64). Vikasietoisuusvaatimus riippuu turvatoiminnon toimintatavasta, joka ilmenee taulukosta 5.

Taulukko 5. Pienin sallittu laitteiston vikasietoisuus turvallisuuden eheyden tason mukaisesti. (SFS-EN 61511-1 2017, 65)

Turvallisuuden eheyden taso (TET)	Pienin sallittu laitteiston vikasietoisuus (HFT)
1 (mikä tahansa toimitapa)	0
2 (harvojen vaateiden toimitapa)	0
2 (tiheiden vaateiden tai jatkuva toimitapa)	1
3 (mikä tahansa toimitapa)	1
4 (mikä tahansa toimitapa)	2

4 Turva-automaatiotoiminnon eheystason todentaminen

Turva-automaatiojärjestelmä koostuu erikseen määritetyistä turva-automaatiotoiminnoista, joiden tulee saavuttaa määritetty turvallisuuden eheyden taso. Todentamisessa tarkistetaan laitteiden sopivuus suunnitellulle toiminnalle.

Turva-automaatiotoiminnon todentaminen tapahtuu matemaattisella tarkastelulla, jossa lasketaan toiminnon keskimääräistä vaarallisen vikaantumisen todennäköisyyttä vaateen sattuessa. Todentamisessa lasketaan turvatoiminnon kaikkien laitteiden PFDavg-arvot yhteen. Lasketun PFDavg-arvon tulee saavuttaa määritetyn turvallisuuden eheystason vaativa PFDavg-arvo. Laskennalla todennetaan saavuttaako laitteiden ja kytkentöjen muodostama turva-automaatiotoiminto tarvittavan turvallisuuden eheystason. (Heikkinen 2015.)

4.1 Exida

Exida on maailmanlaajuinen yritys, joka on erikoistunut toiminnallisen turvallisuuden edistämiseen, testaukseen sekä arviointiin (Exida. Who we are, [Viitattu 8.4.2019]). Yritys tarjoaa sertifiointipalvelua, jossa vahvistetaan laitteen sopivuus tietylle turvallisuuden eheystasolle. Exida ylläpitää kotisivuillaan laitelistaa laitteista, joille he ovat myöntäneet turvalaitesertifikaatin. Sertifikaatti pitää sisällään testiraportin, josta ilmenee miten arvot muodostuvat. (Exida. Certification, [Viitattu 8.4.2019])

Exida tarjoaa myös exSILentia-ohjelmistoaan, jonka avulla pystytään laskemaan saavuttaako turva-automaatiotoiminto määrityksessä vaadittavan turvallisuuden eheystason (Exida. exSilentia, [Viitattu 8.4.2019]).

4.2 PFDavg-arvoon vaikuttavat tekijät

PFDavg-arvo on keskimääräinen vaarallisen vikaantumisen todennäköisyys sitä vaadittaessa. Kyseinen arvo koostuu monista arvoista, jotka tulee tarvittaessa ottaa laskennassa huomioon. (Beurden & Goble 2018.)

Laskennan yhdeksän avainmuuttujaa ovat:

1. Vikaantumistavat sisältäen havaitut sekä havaitsemattomat vaaralliset vikaantumiset.
2. Laitteen elinikä.
3. Laitteen testausväli.
4. Laitteen testauksen tehokkuus.
5. Laitteen keskimääräinen korjausaika sekä diagnostiikan testausväli.
6. Laitteen testaukseen kuluva aika.
7. Laitteen testaus suorittamatta.
8. Laitoksen turvallisuusindeksi.
9. Redundanssi / Yhteisvikojen osuus. (Beurden & Goble 2018.)

PFDavg-arvon laskennassa tarvitaan näille avainmuuttujille realistiset ja turvalliset arvot. Arvojen määrityksessä tulisi käyttää aiempia kokemuksia sekä arvioitsijoiden tulisi olla päteviä ja koulutettuja. (Beurden & Goble 2018.) Taulukon 6 mukaan muuttujia ei kuitenkaan aina oteta laskennassa huomioon.

Taulukko 6. PFDavg-laskennan muuttujat (Beurden & Goble 2018.)

Muuttuja	Kuvaus	Tietolähde	Käytetään
1	Vaaralliset vikaantumiset, havaitut ja havaitsemattomat	Laitteen valmistaja	Aina
2	Laitteen elinikä	Käyttäjä	Aina
3	Laitteen testausväli	Käyttäjä	Aina
4	Laitteen testauksen tehokkuus	Käyttäjä	Aina
5	Laitteen keskimääräinen korjausaika	Käyttäjä	Aina
5	Diagnostiikan testausväli	Laitteen valmistaja	Ei olennainen,jos testausväli on pienempi kuin tunti.
6	Laitteen testaukseen kuluva aika	Käyttäjä	Jos testaus suoritetaan prosessin käydessä.
7	Laitteen testaus suorittamatta	Käyttäjä	Jos laitetta ei ole testattu 100% asennuksen jälkeen.
8	Laitoksen turvallisuusindeksi	Käyttäjä	Aina
9	Redundanssi / Yhteisvikojen osuus	Järjestelmän suunnittelija	HFT ≥1

4.2.1 IEC 61508

IEC 61508 on maailmanlaajuinen standardi. SFS-EN 61508 -standardi perustuu IEC-standardiin, mutta on supistettu versio IEC-standardista. Turva-

automaatiotoiminnon eheystason todennukseen tarvittavat laskentakaavat on käsitelty IEC 61508 -standardissa. Standardi määrittelee laskentakaavat PFDavg-arvolle. SFS-EN 61508 -standardi ohjaa ainoastaan laskemaan laitteiston PFDavg-arvot yhteen, mutta ei ota kantaa, mistä kyseinen arvo muodostuu. Prosessiteollisuudessa käytetään 95 prosenttisesti harvojen vaateiden toimintatapaa. (Sundquist 2010, 16.)

Standardissa IEC 61508-6 on esitetty laskentakaava keskimääräisen vaarallisen vikaantumisen todennäköisyydelle:

$$PFDavg = PFDs + PFDl + PFDfe \quad (1)$$

jossa, $PFDavg$ on turva-automaatiotoiminnon keskimääräinen vikaantumisen todennäköisyys vaateen ilmetessä. $PFDs$ on tuntoelimen keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä. $PFDl$ on logiikan keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä. $PFDfe$ on toimilaitteen keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä. (IEC 61508-6 2010, 28.) Turva-automaatiotoiminnon laitteiden PFDavg-arvojen summa muodostaa turva-automaatiotoiminnon turvallisuuden eheystason.

IEC 61508 -standardin osassa 6 esitetään laskentakaava siitä, miten PFDavg-arvo muodostuu yksinkertaisessa 1oo1-laiterakenteessa. Laskemiseen tarvitaan laitteen valmistajan turvallisuuskäsikirja, josta ilmenee laitteen arvot. Turvallisuuskäsikirja voi sisältää kolmannen osapuolen sertifikaatin sekä testausraportin.

Ensimmäiseksi lasketaan vaarallisten vikaantumisten osuus:

$$\lambda d = \lambda du + \lambda dd \quad (2)$$

jossa, λd on vaaralliset vikaantumiset. λdu on havaitsemattomat vaaralliset vikaantumiset. λdd on havaitut vaaralliset vikaantumiset. (IEC 61508-6 2010, 31.)

1oo1-laiterakenteen voidaan olettaa koostuvan kahdesta eri kanavasta. Nämä ovat laitteen havaitut ja havaitsemattomat vaaralliset vikaantumiset. Molemmille kanaville on mahdollista laskea keskimääräinen aika, jolloin laite ei ole toimintakunnossa:

$$tce = \frac{\lambda \mathrm{du}}{\lambda \mathrm{d}} \left(\frac{T1}{2} + MRT \right) + \frac{\lambda \mathrm{dd}}{\lambda \mathrm{d}} MTTR \quad (3)$$

jossa, tce on laiterakenteen toimimattomuusaika tunteina. $T1$ on laitteen testausväli tunteina. MRT on laitteen korjauksen keskiarvo tunteina. $MTTR$ on keskiarvo laitteen korjaukseen kuluva aika tunteina. Standardissa ohjeistetaankin, että $MTTR = MRT = 8h$. (IEC 61508-6 2010, 27.)

Edellä olevien arvojen perusteella laitteelle voidaan laskea PFDavg-arvo, jossa tarvittavia tietoja ovat laitteen havaitut ja havaitsemattomat vaaralliset vikaantumiset sekä laitteen toimimattomuusaika:

$$\mathrm{PFDavg} = (\lambda du + \lambda dd)\, tce \quad (4)$$

(IEC 61508-6 2010, 31.)

4.3 Turva-automaatiotoiminnon todentamisen malli

Todentaminen aloitetaan tutustumalla lähtötietoihin. Materiaaliin kuuluu turvallisuuden eheystason määritys, PI-kaaviot, sanalliset toimintaselostukset, piirikaaviot sekä laitelista. Seuraavaksi tarkistetaan laitteiden sopivuus suunniteltuun toimintaan. Tarkat tiedot löytyvät laitteen turvallisuuskäsikirjasta.

Esimerkki: Turva-automaatiotoiminnolle valittiin harvojen vaateiden toimintatapa, koska vaateita on harvemmin kuin yksi vuodessa. Turvallisuuden eheystason määrityksessä päädyttiin, että turva-automaatiotoiminnon tulee saavuttaa turvallisuuden eheystaso 1.

Turva-automaatiotoiminnon on tarkoitus pysäyttää pumppu, jos tankissa oleva vaarallisen nesteen pinnankorkeus saavuttaa tankissa sijaitsevan pintakytkimen. Pumppua pyöritetään taajuusmuuttajalla, jossa on STO-toiminto. STO-toiminto katkaisee taajuusmuuttajan energian syötön ja pumpun moottori pysähtyy vapaasti

pyörien. Laitteille on määritetty 8 tunnin korjausaika. Laskenta on yksinkertaistettu, joten siinä ei huomioida yhteisvikojen osuutta.

4.3.1 Pintakytkin

Krohne Optiswitch 5200C-turvallisuuskäsikirja (2013, 8) sisältää vikaantumistaulukon, jossa on eriteltynä suojauksen tyyppi. Tässä esimerkissä pintakytkintä käytetään estämään tankin ylitäyttö. Laitteen rakenne on 1oo1.

Valmistaja vakuuttaa laitteen sopivan turvallisuuden eheystaso 2-luokkaan asti. Laiteen vikasietoisuus on 0 ja sen laitetyyppi on A. Laitteen vaaralliset vikaantumiset on ilmoitettu FIT-asteikolla. Laskentaan FIT-arvot on muunnettu kaavan sopivaksi. tce-arvon laskemiseen käytetään kaavaa 3.

$$tce = \frac{2{,}5 * 10^{-7}}{3{,}3 * 10^{-7}} * \left(\frac{8760}{2} + 8\right) + \frac{1{,}41 * 10^{-6}}{3{,}3 * 10^{-7}} 8$$

tce-arvon tulokseksi saadaan 3360 tuntia. Pintakytkimen PFDavg-arvo saadaan, kun sijoitetaan laitteelle laskettu tce-arvo kaavaan 4.

$$\text{PFDavg} = (2{,}5 * 10^{-7} + 1{,}41 * 10^{-6}) * 3360 = 1{,}1 * 10^{-3}$$

4.3.2 Logiikka

ABB:n 800xA Safety -tuotteilla on Tüv Süd Functional Safety -serfitikaatti. Sertifikaatissa vakuutetaan logiikkaosan sopivan turvallisuuden eheystaso 2-luokkaan asti sekä tulo- ja lähtökorttimoduulien sopivan turvallisuuden eheystaso 3-luokkaan asti. (System 800xA Safety. 2016.)

Logiikka-osa jakaantuu kolmeen eri laitteeseen:

- Tulokortti (DI), ABB DI880
- Logiikka (CPU), ABB PM865 Single
- Lähtökortti (DO), ABB DO880 NE.

ABB antaa valmiit PFDavg-arvot, jotka on laskettu 20 vuoden testausvälillä. Laitteiden arvot summataan yhteen, josta muodostuu logiikan PFDavg-arvo.

$$\text{PFDavg} = 6{,}16 * 10^{-6} + 1{,}99 * 10^{-5} + 3{,}06 * 10^{-5} \; = \; 5{,}67 * 10^{-5}$$

4.3.3 Taajuusmuuttaja

Toimilaitteena on taajuusmuuttaja, joka ohjaa sähkömoottoria. Taajuusmuuttaja on ABB ACS880-01.

Taajuusmuuttaja sisältää Safe Torque Off –toiminnon (STO), joka on hyväksytty turva-automaatiotoiminto. STO toimii 1oo2-periaatteella. STO-toiminnon molemmat kanavat kaapeloidaan suoraan turvalogiikan lähtökorttiin, joka ohjaa taajuusmuuttajaa. Vaateen sattuessa turvalogiikka katkaisee ohjauksen STO-kanavista, jolloin taajuusmuuttaja katkaisee energian syötön sähkömoottorille. Jos STO laukeaa sähkömoottorin pyöriessä, se pysähtyy vapaasti pyörien. (ABB Industrial Drives 2017, 242.) PFD-arvo kyseiselle taajuusmuuttajalle on 2.42E-5. ABB antaa laitteen testausväliksi 2 vuotta. (ABB Industrial Drives 2017, 247.)

4.3.4 Yhteenveto

Yhteenvedossa lasketaan kaavan 1 avulla turva-automaatiotoiminnon laitteiden PFDavg-arvot yhteen. Arvon täytyy saavuttaa määritetty turvallisuuden eheystaso.

$$\text{PFDavg} = 1{,}1 * 10^{-3} + 5{,}67 * 10^{-5} + 2{,}42 * 10^{-5} \; = \; 1{,}18 * 10^{-3}$$

Vikaantumistodennäköisyystarkastelu sallisi käyttää kyseistä laitteiden muodostamaa turva-automaatiotoimintoa turvallisuuden eheystasolla 2. Tarkastelun tuloksena huomataan turva-automaatiotoiminnon saavuttavan määritetyn turvallisuuden eheystason.

5 Pohdinta

Tämän opinnäytetyön tavoitteena oli perehtyä prosessiteollisuuden toiminnallisen turvallisuuden vaatimuksiin sekä turva-automaatiojärjestelmän rakenteeseen. Työn tutkiva osuus koostuu turva-automaatiotoiminnon turvallisuuden eheystason todentamisesta, jota on havainnollistettu esimerkkilaskennalla. Työ suoritettiin Pöyry Finland Oy:n toimeksiantona. Yrityksen luovuttama turva-automaatiojärjestelmän koulutusmateriaali toimi opinnäytetyön lähtöaineistona.

Tutkimuksessa saavutettiin opinnäytetyölle asetetut tavoitteet. Työssä todennettiin esimerkkiä hyödyntäen määritetyn turva-automaatiotoiminnon turvallisuuden eheystaso sekä kiteytettiin turva-automaatiojärjestelmän vaatimukset ja rakenne standardien avulla. Opinnäytetyön aiheesta on saatavilla runsaasti yleissivistävää materiaalia, mutta yksityiskohtaisia turvallisuuden eheystason laskukaavoja ei ole yleisesti saatavilla. Tämä tuotti osittain haasteita todentamisen laskennassa.

Prosessiteollisuuden toiminnallinen turvallisuus on käsitelty standardissa SFS-EN 61511, joka perustuu standardiin SFS-EN 61508. Standardeissa asetetaan ainoastaan vaadittava turvallisuuden eheystaso, eivätkä standardit näin ollen ota yksityiskohtaisesti kantaa siihen, miten vaadittavaan eheystasoon päästään. Tästä voidaankin päätellä, ettei SFS-standardien antamat ohjeistukset yksinään riitä, vaan näiden lisäksi tulisi käyttää IEC-standardeja. Turvallisuuden eheystasojen todentamislaskennat ovat riippuvaisia työryhmän määrittämistä lähtöarvoista, jonka vuoksi vaatimuksia ei tulisi asettaa liian koviksi.

Työn edetessä huomattiin, että turva-automaatiotoimintojen monimutkaistuessa on entistä vaikeampi huomioida kaikki laskentaan vaikuttavat muuttujat. Käyttämällä todentamiseen kehitettyjä ohjelmistoja voitaisiin pienentää inhimillisen virheen todennäköisyyttä, jolloin kaikki muuttujat tulisivat huomioiduksi. Ohjelmisto laskee automaattisesti turvallisuuden eheystason syötettyjen lähtötietojen perusteella. Lähtötietojen syöttäjällä on kuitenkin oltava tarvittava pätevyys sekä käsitys turva-automaatiojärjestelmän toiminnasta.

LÄHTEET

ABB Automation Technologies AB. 2005. Sertifikaatti. [Verkkosivu]. ABB Oy. [Viitattu 8.4.2019]. Saatavissa: https://library.e.abb.com/public/52a5e9588a341435c1257217007933f7/3BNP015134_B_en_800xA_Safety__TUV_certificate.pdf?x-sign=YKb20rNJV3cQqbb3jF+haZW8VzaPk43X/QmMtfILHVOP6GM5OfHZlXg290ww2ys6

ABB Industrial Drives. 2017. Laiteopas ACS880-01-taajuusmuuttajat. [Verkkosivu]. ABB Oy. [Viitattu 8.4.2019]. Saatavissa: https://library.e.abb.com/public/86ac21c012164a8cb0f7f6ada2c4ea85/FI_ACS880_01_HW_M_A5_screen.pdf?x-sign=XdlYsvTEMSWm7c++EguBseitsScZ7kSf40ralYFiA4sX7QYY/VQ06ODI44cM9Ped

Automaatioväylä verkkolehti 3/2015. 2015. Kenttälaitteiden toiminnallinen turvallisuus. [Verkkosivu]. Automaatioväylä. [Viitattu 8.4.2019]. Saatavissa: http://www.automaatiovayla.fi/wordpress/wp-content/uploads/2016/05/Automaatiovayla_3_2015.pdf

Beurden & Goble. 2018. The Key Variables Needed for PFDavg Calculation. [Verkkosivu]. Exida. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/articles/White%20Paper%20Key%20Variables%20Needed%20for%20PFDavg%20Calculation%20Feb%202018%20Rev2.1.pdf

Emerson Product Bulletin. 2018. Safety Instrumented Systems. [Verkkosivu]. Emerson. [Viitattu 8.4.2019]. Saatavissa: https://www.emerson.com/documents/automation/product-bulletin-safety-instrumented-systems-fisher-en-4189360.pdf

Exida Glossary. Ei päiväystä. SIF – Safety Instrumented Function. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/Resources/Term/SIF-Safety-Instrumented-Function

Exida. Ei päiväystä. exSilentia. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/exSILentia

Exida. Ei päiväystä. Funtional Safety Certification. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/Certification/Functional-Safety

Exida. Ei päiväystä. Who we are. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/Company/About

Functional Safety. 2016. Electric actuators for safety-related system up to SIL 3. [Verkkosivu]. AUMA. [Viitattu 8.4.2019]. Saatavissa: https://www.auma.com/index.php?eID=ix_product_ajax&action=download&fileUID=1662

Heikkinen M. 2015. Turva-automaation eheystason todentaminen. [Viitattu 8.4.2019]. Saatavissa: Vain yrityksen sisäisessä käytössä.

IEC 61508-6. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Geneva: International Electrotechnical Commission.

Krohne. 2013. Safety Manual Optiswitch series 5000. [Verkkosivu]. [Viitattu 8.4.2019]. Saatavissa: https://cdn.krohne.com/dlc/AD_OPTISWITCH5xx0_2wire_SIL_en_150311.pdf

Schwartz & Hochleitner. Ei päiväystä. 3 Important Factors in Evaluating your SIL Certified Device. [Verkkosivu] Exida. [Viitattu 8.4.2019]. Saatavissa: https://www.exida.com/articles/3-Important-Factors-in-Evaluating-your-SIL-Certified-Device.pdf

Pöyry. 2018. Pöyry yleisesittely. [Verkkosivu]. [Viitattu 8.4.2019]. Vain yrityksen sisäisessä käytössä.

SFS-EN 61508-1. 2011. Sähköisten/Elektronisten/Ohjelmoitavien elektronisesti turvallisuuteen liittyvien järjestelmien toiminallinen turvallisuus. Osa 1: Yleiset vaatimukset. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61508-2 2011. Sähköisten/Elektronisten/Ohjelmoitavien elektronisesti turvallisuuteen liittyvien järjestelmien toiminallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61508-4. 2010. Sähköisten/Elektronisten/Ohjelmoitavien elektronisesti turvallisuuteen liittyvien järjestelmien toiminallinen turvallisuus. Osa 4: Määritelmät ja lyhenteet. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61508-5. 2011. Sähköisten/Elektronisten/Ohjelmoitavien elektronisesti turvallisuuteen liittyvien järjestelmien toiminallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61511-1.2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille Osa 1: Rakenne, määritelmät, järjestelmä, laitteiston ja sovellusohjelmoinnin vaatimukset. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61511-2. 2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille Osa 2: Ohjeita standardin IEC 61511-1:2016 soveltamiseen. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 61511-3. 2017. Sähköisten/Elektronisten/Ohjelmoitavien elektronisesti turvallisuuteen liittyvien järjestelmien toiminallinen turvallisuus. Osa 3: Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiseen. Helsinki: Suomen Standardisoimisliitto.

Sundquist M. 2010. Toiminnallinen turvallisuus. [Verkkosivu]. Sundcon Oy. [Viitattu 8.4.2019]. Saatavissa: https://www.automaatioseura.fi/site/assets/files/1431/iec61508_m_sundquist1.pdf

System 800xA Safety. 2016. AC 800M High Integrity Reliability and Availability. ABB. [Viitattu 8.4.2019]. Vain yrityksen sisäisessä käytössä.

Turva-automaatio prosessiteollisuudessa. 2007. [Verkkosivu] Turvatekniikan keskus. Saatavissa: https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081?version=1.0