Opinnäytetyö (AMK / YAMK)

Tieto- ja viestintätekniikka

2018

Emmi Elo

TURVALLISUUDEN EHEYDEN TASON TARKASTELU JA TOTEUTUS KAASUNVALVONTALAITTEILLE

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2018 | 34 + 4 liitettä

Emmi Elo

TURVALLISUUDEN EHEYDEN TASON TARKASTELU JA TOTEUTUS KAASUNVALVONTALAITTEILLE

Nykypäivänä tarkemmiksi muuttuneet turvallisuusvaatimukset luovat paineita teollisuuden yrityksille omien ohjelmien ja laitteistojen turvallisuuden eheystasojen suhteen. Tämä edellyttää, että laitteiden turvallisuutta ja luotettavuutta tulee seurata laitteiden koko eliniän ajan. Jotta asiakkaiden turvallisuusvaatimuksiin pystyttäisiin vastaamaan entistä paremmin, on yrityksen syytä kehittää laitteidensa turvallisuustasoa ja näin ollen mahdollistettava niiden käyttö mahdollisimman monille teollisuuden asiakkaille.

Tämän opinnäytetyön tarkoituksena oli tarkastella turvallisuuteen liittyvälle sähköiselle ohjausjärjestelmälle ja sen ohjaustoiminnoille luotua turvallisuuden eheyden vaatimusten mukaista laskentatapaa SIL (Safety Integrity Level). Työssä tarkasteltiin eri standardien SIL2-tason turvallisuusvaatimuksia ja niiden toteuttamista Detector Oy:n kaasunvalvontalaitteissa. Tarkastelussa käytiin läpi kaasunvalvontalaitteiden ohjelmiston ja järjestelmän yhteensopivuutta standardeihin IEC 61508 ja SFS-EN 50402, ja selvitettiin keinoja niiden täyttämiseksi.

Työ toteutettiin tutkimalla katalyyttisten kaasunilmaisimien mahdollisuutta turvallisuuden eheyden tasoon kaksi. Kaasunilmaisimien toimintaa ja dokumentaatiota verrattiin turvallisuusstandardien vaatimuksiin.

Kaasunvalvontajärjestelmästä tuotettiin vikapuumalli ja toteutettiin vika- ja vaikutusanalyysi. Kaasunilmaisimien ohjelmistolle suoritettiin testauksia, koodin kommentointia ja dokumentaatiota parannettiin. Työn tuloksena saatiin laskettua vikaantumisaikoja kaasunilmaisimien komponenteille ja tuotettiin tuotteiden turvallisuuskäsikirja. Työ toi yritykselle paljon uutta tietoa turvallisuuteen liittyvien laitteiden suunnittelusta ja toteutuksesta.

ASIASANAT:

kaasu, turvajärjestelmä, turvallisuusanalyysi

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communication technology

2018 | Total number of pages 34 + 4 attachments

Emmi Elo

REVIEW AND IMPLEMENTATION OF SAFETY REQUIREMENTS FOR GAS MONITORING EQUIPMENT

The security requirements that have changed present create pressures for industrial companies with respect to their products safety integrity levels. The devices safety and reliability should be monitored troughout their lifetime. In order to meet customer requirements in terms of safety, the company needs to develop the safety of its equipment and thus enable them to be used by many industrial customers.

The subject of the thesis was to study a safety-related electronic control system and the method of calculation for the safety requirements for its control functions. This thesis examines the safety requirements of the different standards for SIL2 level and their implementation in Detector Ltd gas control equipment. Gas control equipment software and system are compared to the IEC 61508 and SFS-EN 50402 and are investigated to determine whether and how they meet the standard requirements.

The investigation was carried out by examining the potential of the catalytic gas detectors on the safety integrity level two. The operation and documentation of the gas detectors were compared to the requirements of safety standards.

The gas control system fault tree analysis was produced and failure mode and effect analysis was performed. The gas detectors software was tested, the code was annotated and documentation was improved. As a result of the work, the failure times for gas detector components were calculated and a product safety manual was produced. The work brought a great amount new information for the company about the design and implementation of the safety related systems.

KEYWORDS:

gas, security system, safety analysis

SISÄLTÖ

LIITTEET

Liite 1. Kaasunvalvontajärjestelmän vikapuumalli.
Liite 2. FMEA-taulukko.
Liite 3. Vikaantumislaskennat kaasunilmaisimille.
Liite 4. Turvallisuuskäsikirja.

KÄYTETYT LYHENTEET

DC	Diagnostiikan kattavuus (engl. Diagnostic coverage)
DGTk2	Katalyyttisen kaasunilmaisimen tuotenimi
DGTkex	Katalyyttisen kaasunilmaisimen tuotenimi
LEL/LFL	Alempi syttymisraja
MTBF	Keskimääräinen vikaantumisaika (engl. Mean time between failures)
MTTF	Keskimääräinen vikaantumisaika (engl. Mean time to failure)
$MTTF_d$	Vaarallinen keskimääräinen vikaantumisaika (engl. Mean time to dangerous failure)
OL	Ohjattava laitteisto
PFD_{avg}	Keskimääräinen vaarallisen vikaantumisen todennäköisyys tunnissa (engl. Average probability of dangerous failure on demand)
PFH	Keskimääräinen vaarallisen vikaantumisen taajuus tunnissa (engl. Average probability of dangerous failure on demand)
S/E/OE	Sähköinen/elektroninen/ohjelmoitava elektroninen (engl. E/E/PE, Electrical/Electronic/Programmable Electronic)
TET (SIL)	Turvallisuuden eheyden taso (engl. Safety integrity level)
VTT	Valtion teknillinen tutkimuskeskus
VVA (FMEA)	Vika- ja vaikutusanalyysi (engl. Failure Mode and Effect Analysis)
λ	Vikaantumistaajuus (engl. Failure rate)

1 JOHDANTO

Toiminnallisen turvallisuuden tärkeys ja sen mukanaan tuomat vaatimukset ovat kasvaneet teollisuudessa viimeisen vuosikymmenen aikana. Teollisuudessa toimivien järjestelmien ei tulisi aiheuttaa missään tilanteessa vaaraa ihmiselle tai aiheuttaa vikatilanteessa häiriöitä toisille järjestelmille. Laitteiden turvallisuutta ja luotettavuutta tulisi seurata laitteiden suunnittelusta aina sen elinkaaren päättymiseen asti. Tämä luo yrityksille valtavasti paineita, jotta pystytään kehittämään omia ohjausjärjestelmiä ja niiden ohjaustoimintojen turvallisuutta vastaamaan teollisuuden vaatimuksia.

Tässä opinnäytetyössä perehdytään turvallisuuden eheyden vaatimusten mukaiseen laskentatapaan SIL (Safety Integrity Level) ja tarkastellaan standardia IEC 61508 ja sen vaatimuksien toteuttamista kaasunvalvontalaitteille. Työn toimeksiantajana toimii Detector Oy. Työssä tutustutaan kaasunilmaisimien toimintaan niiden ohjelmistojen sekä myös itse elektronisen laitteiston kautta. Tarkoituksena oli kehittää toimeksiantajan kaasunilmaisimia niin, että ne saavuttaisivat standardissa määritellyn turvallisuuden eheyden tason kaksi.

Samantapaisia töitä on ainakin Anni Grönin Turva-automaation kartoitus prosessilaitokseen [1], jossa laaditaan ohjeistus turva-automaation kartoitukseen ja suunnitteluun, jossa on myös käytetty lähteenä toiminnallisen turvallisuuden esittävää standardia IEC 61508. Työtä ei kuitenkaan tulla käyttämään paljoakaan lähteenä, sillä tässä työssä kyseistä standardia tarkastellaan kokonaisuutena turvallisuuden eheyden saavuttamiseksi jo olemassa oleville laitteille.

Projektin aihe on mielenkiintoinen, sillä se sisältää monipuolisen tutustumisen kaasunvalvontajärjestelmiin. Työssä tarkastellaan syvällisesti kaasunvalvontalaitteiden ohjelmallista sekä elektronista puolta, joita vertaillaan ja kehitetään turvallisuuden standardeihin sopivaksi. Työn keskeisenä asiana on myös yleinen laadunvalvontaan perehtyminen. Erityisesti työssä keskitytään tarkastelemaan jo olemassa olevia dokumentaatioita ja toimintaperiaatteita sekä mietitään, miten niitä voitaisiin parantaa myös halutun turvallisuuden eheyden tason saavuttamiseksi.

2 LÄHTÖKOHDAT

2.1 Kaasunvalvontajärjestelmät

Kaasunvalvontajärjestelmä on kokonaisuus, jonka oikealla valinnalla pystytään havaitsemaan räjähdysvaarallisen hiilivety/ilmaseoksen syntyminen ennen kuin pitoisuus ylittää syttymis- ja räjähdysrajan. Järjestelmä voi koostua keskuksesta, useammista kaasunilmaisimista ja joskus myös alakeskuksesta, joka voidaan tarpeen vaatiessa kytkeä myös asiakkaan järjestelmään. Yleensä järjestelmät ovat kiinteästi asennettavia, mutta saatavilla on myös kannettavia kaasunilmaisimia. [3]

Monet teollisuuden prosessit käyttävät tai tuottavat erilaisia kaasuja, joista osa on myrkyllisiä. Kaasunvalvonta tällaisissa kohteissa on tärkeää, jotta voidaan varmistaa kaasujen läsnä ollessa henkilökunnan, prosessien ja ympäristön suojaaminen. Kaasut voivat olla syttyviä, myrkyllisiä ja tukahduttavia. Ne voivat aiheuttaa räjähdyksiä, heikentää happipitoisuutta, vaurioittaa terveyttä tai aiheuttaa kuoleman. Syttyvissä kaasuissa nopea havainnointi on tärkeää, jolloin on vielä aikaa hallita vuotoa ja estää mahdollinen tulipalo- ja räjähdysvaara. Kaasut voivat aiheuttaa myös tukehtumisvaaran, jonkin kaasun aiheuttama hapen syrjäyttäminen ja happipitoisuuden laskeminen alle normaalin 20.9& arvon voi aiheuttaa jopa kuoleman. [4]

Kaasunvalvontalaitteiden oikealla valinnalla ja vuotokohtien tuntemuksella pystytään varmistamaan mahdollisimman nopea hälytystieto mainittujen riskien läsnäollessa. Kun hälytystieto saadaan ajoissa on vielä mahdollista hallita vuotoa ja tehdä tarvittavia toimenpiteitä ihmisten, ympäristön ja tuotannon suojaamiseksi. [4]

2.2 Työssä tarkasteltavat kaasunilmaisimet

Teollisuudesta tulleiden kyselyiden takia turvallisuusluokituksen tarkasteluun päätettiin ensimmäisinä valita toimeksiantajan tuotevalikoimasta löytyvät katalyyttiset DGTkex-kaasunilmaisin (kuva 1) ja DGTk2-kaasunilmaisin (kuva 2). Valintaan vaikutti myös niiden mahdollisuus valvoa palavia kaasuja, jotka voivat aiheuttaa tulipalon ja räjähdysvaaran. Suuren turvallisuustaason riskin aiheuttavia kaasuja on tärkeä valvoa ja tähän tarkoitettujen laitteiden tulee olla mahdollisimman luotettavia ja turvallisia. Tästä

syystä on hyvä todeta laitteiden täyttävän turvallisuuden standardit. Katalyyttisten ilmaisimien pääkäyttökohteita ovat teollisuuden eri alat. Esimerkkeinä tällaisista ovat prosessi-, kemian- ja metalliteollisuuden laitokset, maakaasuasemat, valimot ja erilaiset liuotinvarastot. [5]

Kuva 1. Digitaalinen DGTkex-kaasunilmaisin. [5]

Katalyyttisen kaasunilmaisimen toiminta perustuu sähköisesti kuumennettuun katalyyttielementtiin, jonka pinnalla palava kaasu hapettuu. Hapettumisen seurauksena katalyyttielementin lämpötila muuttuu, josta seuraa elementin resistanssin muutos. Resistanssimuutos on suoraan verrannollinen kaasupitoisuuden muutokseen. Katalyytti-ilmaisin tarvitsee toimiakseen aina happea. Tästä syystä sillä voidaan ilmaista ainoastaan alemman räjähdyspisteen LEL/LFL-pitoisuuksia. Happea syrjäyttävät kaasut, esimerkiksi typpi, voivat saada ilmaisimen näyttämään liian pientä tai jopa nolla-arvoa. Käyttökohteessa, jossa esiintyy silikoni, rikki-, lyijy- tai fosforiyhdisteitä, tulee kiinnittää erityistä huomiota kaasunilmaisimien testaukseen, kalibrointiin ja suojaukseen mahdollisen katalyyttimyrkytyksen estämiseksi. [6]

Kuva 2. Digitaalinen DGTk2-kaasunilmaisin. [5]

3 TOIMINNALLINEN TURVALLISUUS

3.1 Yleisesti

Toiminnallinen turvallisuus on kehitetty laitteiden vika- tai vaaratilanteiden estämiseen ja hallitsemiseen. Tähän hyödynnetään tietokoneisiin perustuvaa teknologiaa. Toiminnallisen turvallisuuden standardointeja mietittäessä teollisuudessa toimivalle järjestelmälle tulisi laitteisto ottaa huomioon kokonaisuudessaan mukaan lukien sen toiminnallinen ympäristö. Sähköinen ohjausjärjestelmä ja sen ohjaustoiminnot eivät saisi aiheuttaa vaaraa sen käyttäjälle, muulle järjestelmälle tai ympäristölle. Vaara- ja vikatilanteita voi syntyä monista eri syistä, esimerkiksi laitteistovikaantumisten mekanismeista, ohjelmointivirheistä, inhimillisistä virheistä tai ympäristön vaikutuksista (lämpötila, sähkömagneettiset ilmiöt). [7]

Toiminnallista turvallisuutta on havaittavissa jokapäiväisessä elämässä kaikkialla. Työpaikkakulttuuriksikin kehittynyt turvallisuus on saanut yritykset haluamaan tuotteidensa olevan yhä luotettavampia. Henkilökunnan ja työympäristön turvallisuuteen ollaan valmiita panostamaan koko ajan enemmän. Järjestelmien luotettava toiminta vähentää syntyviä tapaturmariskejä ja mahdollisia ympäristövaikutuksia. Pidemmän ajanjakson kuluessa tämä tuo yrityksille myös taloudellista hyötyä. Esimerkkinä tällaisesta turvallisesta järjestelmästä ovat autojen lukkiutumattomat jarrut, joissa nopeuksien tunnistimet lähettävät tietoa auton valvontatietokoneelle renkaiden pyörimisnopeudesta. Näin ollen järjestelmä pystyy estämään ajoneuvon pyöriä lukkiutumasta voimakkaassa jarrutuksessa. Tämä parantaa ajoneuvon hallittavuutta kovastakin jarrutuksesta huolimatta. [7]

3.2 Historia

Toiminnallinen turvallisuus on saanut alkunsa 80-luvulla, jolloin on alettu kehittämään hajautettuja ohjausjärjestelmiä, jotka pystyivät huolehtimaan kokonaisen teollisuuslaitoksen kaikista ohjaus- ja säätötoiminnoista. Ohjausjärjestelmien ja prosessien kehittyessä haluttiin myös toiminnallisuutta sisältäviä turvatoimintoja. Varolaitteiden laukeaminen kuitenkin aiheutti koko laitoksen toiminnan pysähtymisen, jonka seurauksena haluttiin turvatoiminnot, jotka ohjaisivat järjestelmän tai laitoksen turvalliseen tilaan ennen varo-

laitteiden toimintaa. Ensimmäiset turvatoiminnot olivat toteutettu relekytkennöillä ja myöhemmin ryhdyttiin käyttämään elektroniikkaa sisältäviä laitteita, joissa ohjelmisto ohjasi toimintoja. [8]

IEC perusti vuonna 1985 työryhmän, jossa tutkittiin mahdollisuutta ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien yleiseen standardiin. Kymmenen vuotta myöhemmin syntyi ensimmäinen luonnos standardista IEC 1508, josta ei kuitenkaan milloinkaan julkaistu valmista versiota. Standardi IEC 61508 julkaistiin vuosina 1998 ja 2000, tämä toi riskiarvioon perustuvan turvallisuuden varmistamisen sekä erilaisia riskitasoja vastaavat turvallisuuden eheyden tasot (SIL, TET). Teollisuudessa ollaan turvallisuuden standardien myötä ajauduttu panostamaan instrumentoinneissa ratkaisuihin, joilla pystytään parantamaan luontaista turvallisuutta teollisuuden prosesseissa. [8]

3.3 Toiminnalliseen turvallisuuteen liittyvät standardit

IEC-61508 on toiminnalliseen turvallisuuteen keskittyvä standardi, johon monet toimialakohtaiset toiminnallisen turvallisuuden standardit perustuvat. Standardi sisältää vaatimuksia sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien laitteiden järjestelmille ja ohjelmistoille ja koskee erilaisia järjestelmiä sovelluksesta riippumatta. Turvallisuuden eheystasot on jaettu neljään osaan tuotteen vioittumistodennäköisyyden perusteella, taso 1 on alin mahdollinen ja taso 4 korkein. Standardissa esitetään taulukoiden avulla jokaiselle tasolle tarvittavat toimenpiteet, joiden tulisi täyttyä. [9]

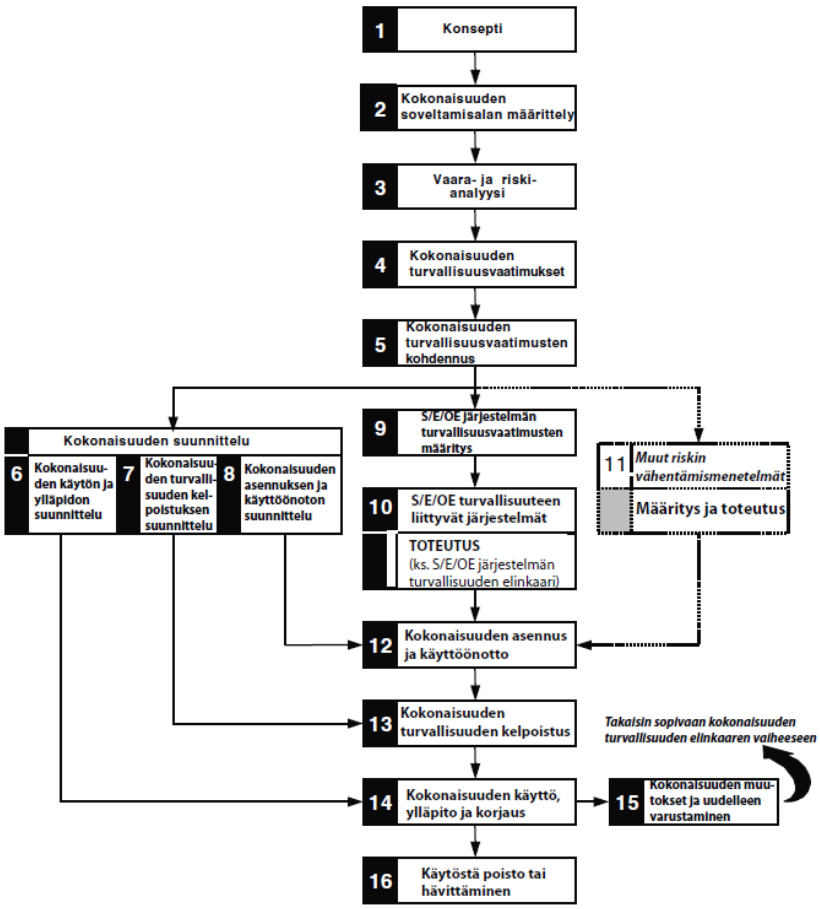
Kaasuntunnistusjärjestelmiin voidaan soveltaa standardia IEC-EN 50402, joka on palavien aineiden tai myrkyllisten kaasujen tai höyryjen tai hapen mittaamiseen tarkoitetuille sähkölaitteille luotu standardi. Tätä standardia voidaan soveltaa, jos kaasuntunnistusjärjestelmä sisältää esimerkiksi kaasun näytteenottoa, sensorin tai signaalinkäsittelyä ohjausyksikössä. [10]

Työssä tarkastellaan myös standardia ISO 13849-1, joka esiintyy standardissa IEC-EN 50402. Se on standardi koneturvallisuudessa esiintyville turvallisuuteen liittyville ohjausjärjestelmille. Työssä standardista on apua kaasunilmaisimien suoritustason, diagnostiikan kattavuuden ja vikaantumisaikojen tarkasteluissa. [11]

4 ELINKAARIMALLI

Tässä luvussa kerrotaan standardissa IEC 61508 esiintyvästä elinkaarimallista (kuva 3), joka määrittää turvallisuuden osat aina järjestelmän suunnittelusta käytöstä poistoon ja hävitykseen asti. Elinkaarimallia olisikin hyvä käyttää runkona turvallisuuden eheystason saavuttamiseksi [6].

Työssä keskitytään tarkastelemaan S/E/OE elinkaarimallia turvallisuusvaatimusten määrittämisen, muutoksien ja uudelleenvarustamisen ja kelpoistuksen osalta, sillä turvallisuustarkasteluun valitut laitteet on jo suunniteltu ja jo tuotannossa olevia tuotteita. Kokonaisuuden suunnittelu sisältäen käyttöönotot ja asennukset on aina laitteen käytöstä poistoon asti jo olemassa. Näitä olemassa olevia käytäntöjä ja dokumentaatioita tullaan työssä vertailemaan ja tarpeen mukaan myös muokkaamaan turvallisuusstandardeihin sopiviksi.



Kuva 3. Kokonaisuuden turvallisuuden elinkaarimalli. [6]

4.1 Vaatimusmäärittely

Ensimmäisenä vaiheena elinkaarimallissa tulee varmistaa, että toimialaa koskevat standardit ja säädökset täyttyvät. Riskien tunnistaminen ja ja vaadittujen eheyden tasojen määrittäminen tapahtuu tässä vaiheessa. Vaatimusmäärittelyt ja riskien tunnistamisen suorittaa järjestelmän asiantunteva ryhmä. Riskien tunnistamisessa tulee määrittää ohjattavan laitteiston ja OL:n ohjausjärjestelmän vaarat, vaaratilanteet ja kaikki mahdolliset käytössä tapahtuvat vaaralliset tilanteet mukaan lukien ihmisen toiminta ja ulkoiset tapahtumat. Tunnistetuista riskeistä tulisi muodostaa vaara- ja riskianalyysi, määrittää vaarojen tapahtumaketjut ja seuraukset. [6]

Vaaditun turvallisuudentason todentamisen menetelmien tulee myös olla selvillä siten, että laitteiden ja laitteistojen arvioinnit, tarkastukset ja vaatimustenmukaisuudet on huomioitu [6]. Vaatimusten tarkastelusta kaasunilmaisimille kerrotaan lisää kappaleessa 5.

4.2 Vaara- ja riskianalyysi

Vaatimuksien tarkastelun jälkeen tulee määrittää ohjattavan laitteiston ja ohjattavan laitteiston ohjausjärjestelmän vaarat, vaaratilanteet ja kaikki mahdolliset käytössä tapahtuvat vaaralliset tapahtumat. OL:n kanssa vuorovaikutuksessa olevien laitteiden tai järjestelmien vaarat ja vaaralliset tilanteet mukaan lukien ihmisen toiminta ja ulkoiset tapahtumat on myös huomioitava vaara- ja riskianalyysissa. [6]

4.3 Toteutus ja käyttö

Laitteiden toteutuksessa ja käytössä on tärkeää noudattaa käytettyjä standardeja. Toteutuksen tulisikin vastata määrittelyvaiheen vaatimuksia. Turvaluokitukseen kuuluvasta laitteesta tulisi ilmetä silmämääräisesti turvaluokituksen todentavat merkinnät ja laitteen toimittajan tulisi antaa asiakkaalle dokumentaatiot laitteen toiminnasta ja käytöstä. [6]

Turvallisuusluokituksen säilymiseksi onkin erityisen tärkeää varmistaa laitteen turvallisuus myös tulevaisuudessa. Jos turvaluokituksen vikaantumislaskennoissa on käytetty kerran vuodessa tehtävää toiminnallista testiä, tulisi laite testata koko sen eliniän ajan

vähintään kerran vuodessa turvaluokituksen säilymiseksi. Myöhemmin laitteeseen tehtävien muutoksien vaikutukset kaikkiin elinkaaren vaiheisiin tulisi käydä läpi. Uusimiseen rinnastettavat muutokset tulisi hyväksyttää viranomaisella. [6]

4.4 Arviointi

Turvallisuusluokituksen arvioinnissa kaikki kokonaisuuden vaiheet arvioidaan ja tarkastetaan. Tarkastuslaitos suorittaa arvioinnin toteutettujen toimien ja annettujen lähtötietojen perusteella onko saavutettu riittävä toiminnallinen turvallisuus tavoitteisiin ja vaatimuksiin nähden. Luokituksen arvioinnista on tärkeää saada dokumentaatio siitä, että tarvittavat auditoinnit on tehty asiaankuuluvasti. Arvioinnit tekee aina tarkastuslaitos. [6]

5 VAATIMUSMÄÄRITTELY KAASUNILMAISIMILLE

Tässä luvussa kerrotaan tarkemmin vaatimusmäärittelystä kaasunilmaisimille. Ennen varsinaisen työn aloittamista VTT:n asiantuntija kävi konsultoimassa yritystä turvallisuusstandardeista ja niiden käytöstä. Konsultoinnin yhteydessä kartoitettiin myös muut mahdolliset työhön tarvittavat standardit ja niistä erityisesti työhön tarvittavat kohdat. Konsultoinnista saatiin myös käyntiraportti, jonka pohjalta työ oli helppo aloittaa.

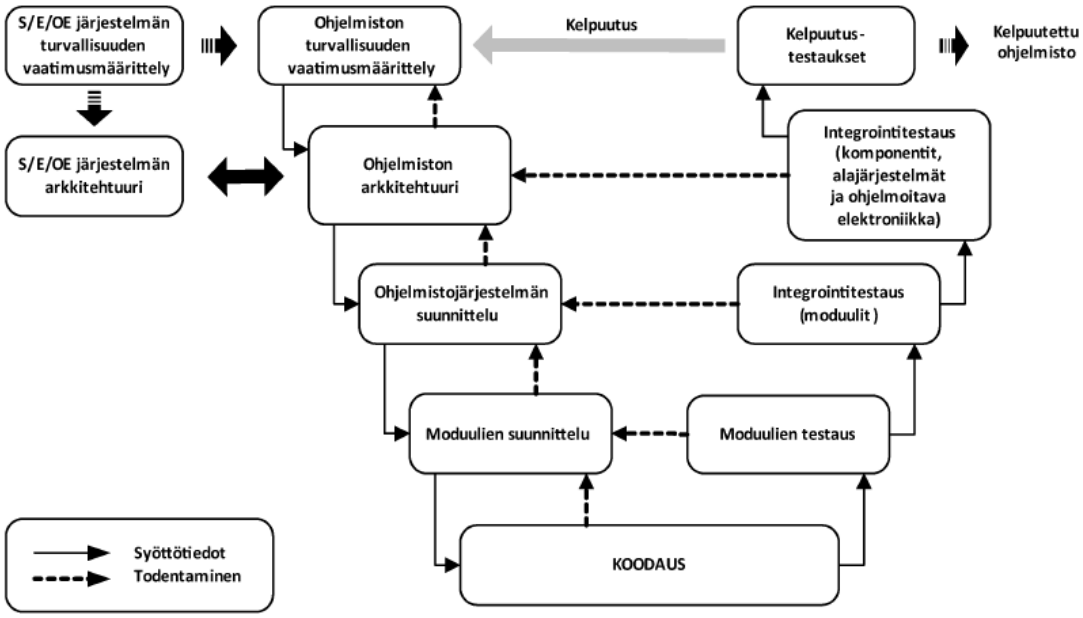
5.1 Ohjelmisto

Tutustuminen SIL2-luokituksen määrittelyihin aloitettiin ohjelmiston vaatimuksista. Ohjelmiston vaatimukset on esitetty turvallisuusstandardin osissa IEC 61508-3 ja 61508-7. Standardin osassa kolme on kerrottu jokaiselle vaaditulle suoritustasolle tarvittavat toimenpiteet ohjelmiston osalta. Standardin osassa seitsemän avataan vaatimuksia enemmän ja annetaan ohjeistuksia niiden suorittamiseen.

Standardien vaatimustaulukoissa on esitetty jokaiselle eheyden tasolle suositellut toimenpiteet ja tekniikat. Tekniikat on merkitty erittäin suositeltavista niihin, joita ei suositella kyseiselle turvallisuuden eheyden tasolle. Muitakin tekniikoita on mahdollista käyttää, kunhan varmistetaan vaatimuksien ja tavoitteiden täyttäminen. Suositellut ohjelmiston tekniikat auttavat yhdessä järjestelmän vaatimuksien kanssa havaitsemaan virheet mahdollisimman aikaisessa vaiheessa toimintaa. [12]

Ohjelmiston suunnittelussa ja toteutuksessa tulisi hyödyntää ohjelmistolle suunniteltua elinkaarimallia, niin sanottua V-mallia. V-malli on prosessimalli ohjelmiston suunnittelun ja toteutuksen helpottamiseksi. Elinkaarimallia voidaan mukauttaa sopivalla tavalla projektin erityistarpeisiin. Ohjelmiston koodin toteutus on mallin pohjalla. Tätä ennen on tehtävä turvallisuuden vaatimusten määrittely tavoitetulle turvallisuuden eheyden tasolle. Vaatimusten määrittelyn jälkeen vielä ennen varsinaisen koodin kirjoittamista on ohjelmistojärjestelmän ja moduulien suunnittelu. Ohjelmiston testauksia tulisi suorittaa jokaiselle järjestelmän osalle, johon ohjelmisto vaikuttaa. Nämä testaukset kulkevat rinnan ohjelmiston suunnittelujen kanssa ja varmistavat halutun turvallisuuden eheyden tason toteutumisen jokaiselle suunnitellulle osalle. Kelpuutustestauksissa varmistetaan ohjelmiston turvallisuusvaatimuksien täyttyminen tarkoitetulla turvallisuuden eheyden tasolla.

Mahdollisten muutoksien yhteydessä tulee varmistua ohjelmiston systemaattisen kyvykkyyden pysymisestä ennallaan. Elinkaarimallin mukainen projekti saadaan päätökseen, kun ohjelmiston on käynyt todentamassa viranomainen. [12] Kuvassa 4 on esitettynä ohjelmiston elinkaarimalli.



Kuva 4. Ohjelmiston V-malli. [12]

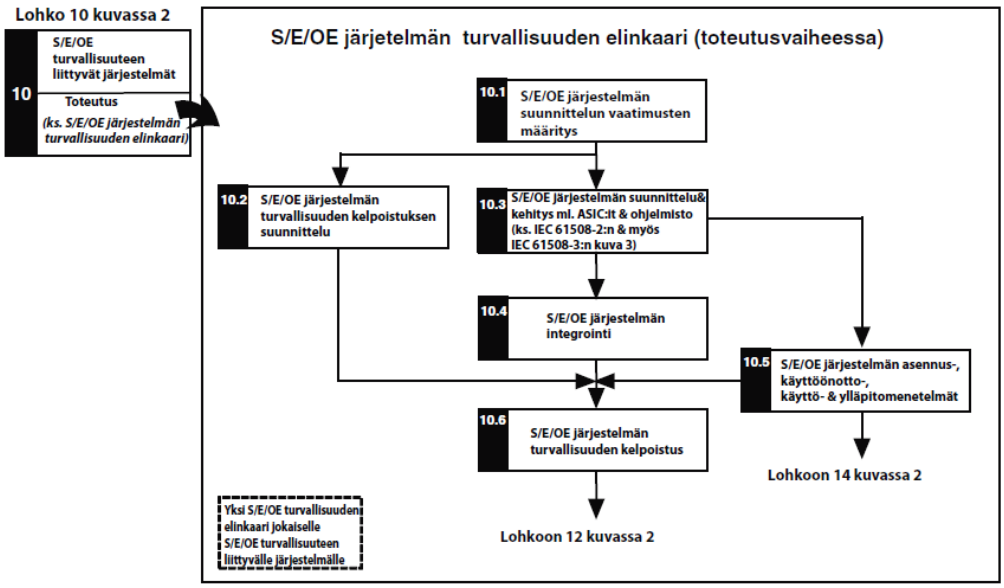
Vaatimusmäärittelyssä kaasunilmaisimien ohjelmistolle tulisi ottaa huomioon ohjelmistoprojektin kokonaisuus. On tärkeää määrittää halutut tavoitteet ja vaatimukset. Haluttujen tavoitteiden ja vaatimuksien suunnittelussa tulisi ottaa huomioon kaasunvalvonnan toimialaa koskevat säädökset ja standardit. Vaatimukset tulisi jaotella pääpiirteittäin toiminnallisiin ja ei-toiminnallisiin vaatimuksiin. Esimerkiksi ohjelmiston laatuun vaikuttavat vaatimukset ja resurssivaatimukset ovat ei-toiminnallisia vaatimuksia. Jo suunnitteluvaiheessa olisi hyvä miettiä ohjelmiston ympäristöä ja käyttäjiä. Ohjelmiston näkyvyys asiakkaalle ja sen sisältö tulisi miettiä yhdessä ja sopia yhdessä, mitä toimintoja mahdollisesti haluttaisiin ja mitä mahdollisesti voisi jättää vain laitevalmistajan nähtäväksi ja käytettäväksi. Suorituskykyyn, vasteaikoihin, ylläpidettävyyteen ja liittymien valintaan vaikuttavat yleensä vahvasti standardien vaatimukset ja niitä tulisi noudattaa ohjelmiston luotettavan toiminnan varmistamiseksi. [16]

Turvallisuuteen liittyvän ohjelmiston suunnittelussa tulisi ottaa huomioon myös vaadittavat turvatoiminnot, järjestelmän konfiguraatio ja arkkitehtuuri. Jo suunnitteluvaiheessa

pitäisi miettiä laitteen suorituskykyyn liittyviä asioita, vasteaikoja ja kapasiteettia. Ohjelmiston hallintalaitteiden ja käyttöliittymän suunnittelu ja niiden mahdollinen väärinkäyttö tulisi kohtuudella ennakoida, jotta voidaan varmistaa tuotteen luotettava toiminta myös virhetilanteissa. Turvallisuusvaatimusten määrittelyssä tulisi huomioida myös ohjelmiston itsevalvonta, jonka tulisi pystyä valvomaan laitteiston, tuntoelimien ja muiden toimilaitteiden oikeaa toimintaa. Testattavuus ohjattavan laitteen toiminnan aikana tulisi tehdä mahdolliseksi, jotta mahdolliset virheet ja vaaratilanteet olisi mahdollista ennakoida [12].

5.2 Järjestelmä

Järjestelmän vaatimukset on esitetty turvallisuusstandardin osissa IEC 61508-2 ja 61508-7. Standardin osassa kaksi (2) on kerrottu jokaiselle vaaditulle suoritustasolle tarvittavat toimenpiteet järjestelmän osalta ja osassa seitsemän (7) annetaan tietoja vaatimuksien suorittamiseen. Järjestelmää koskevassa turvallisuusstandardissa on myös kerrottu vaatimuksia vioille ja vikaantumisille, jotka ovat havaittavissa laitteiston vikaantumisten tekniikoilla ja menetelmillä. Näiden tekniikoiden avulla pystytään määrittelemään ja laskemaan diagnostiikan kattavuus turvallisuuteen liittyvälle laitteistolle. Kuvassa 5 on esitettynä S/E/OE-järjestelmän turvallisuuden elinkaarimalli toteutusvaiheessa. Työssä keskitytään tarkastelemaan järjestelmän kelpoistuksen suunnittelua, asennus-, käyttöönotto-, käyttö- ja ylläpitomenetelmiä sekä niiden dokumentaatioita.



Kuva 5. Järjestelmän elinkaarimalli. [17]

Vaatimusmäärittelyssä kaasunilmaisimien järjestelmälle tulisi ottaa huomioon menettelytavat, joilla voidaan varmistaa järjestelmän toiminnallinen turvallisuus sen asennuksen, käyttöönoton, käytön ja ylläpidon aikana. Menettelytavat tulisi olla dokumentoituna ja kaikkien niitä tarvitsevien saatavilla. Vaatimusmäärittelyssä tulee huomioida ominaisuudet, joilla laitteisto täyttää ympäristöolosuhteiden äärimmäiset vaatimukset (esimerkiksi lämpötila, kosteus, mekaaninen ja sähköinen ympäristö). Ympäristöön liittyvät vaatimukset tulisi ottaa huomioon valmistuksessa, kuljetuksessa, testaamisessa, asennuksessa, käyttöönotossa, käytössä ja ylläpidossa. Vaarallisen vikaantumisen ilmetessä laitteelle tehtävien toimenpiteiden miettiminen on tärkeää, ettei mittavia vahinkoja ilmenisi, vaan saataisiin ilmoitus vikatilanteesta ajoissa, ja vika voitaisiin korjata mahdollisimman nopeasti turvallisen toiminnan jatkamiseksi. [17]

Järjestelmän vaatimusmäärittelyssä on tärkeää varmistaa jo suunnitteluvaiheessa tuotteen luotettava toiminta tilanteesta riippumatta. On otettava huomioon vaatimukset alajärjestelmille ja niiden laitteisto- ja ohjelmistoelementtien integroinnille. Myös tarkkuus- ja stabiiliusvaatimukset mittauksille ja säädöille tulisi huomioida. Kaikkien laitteiston/ohjelmiston välisten vuorovaikutusten merkittävyys ja niiltä vaadittavat rajoitukset tulisi selvittää. Laitteistolle tulisi tehdä tasaisin väliajoin määräaikaistestaukset, joiden aikavälit tulisi päättää kunkin laitteiston tarpeisiin nähden. Määräaikaistestauksilla pystytään varmistamaan laitteen turvallinen toiminta. Turvatoiminnot, joilla varmistetaan turvallisuuteen liittyvien ohjausjärjestelmien toiminta eivät saisi olla riippuvaisia toisistaan. Laitteistolle tulee olla määritelty vikasietoisuus ja saavutettua vikasietoisuutta määritettäessä tiettyjä vikoja voidaan poissulkea edellyttäen, että niiden esiintymisen todennäköisyys on erittäin pieni suhteessa alajärjestelmän turvallisuuden eheyden vaatimuksiin. [17]

5.3 Dokumentaatio

Jotta S/E/OE-järjestelmän ja ohjelmiston turvallisuuden elinkaaret voidaan panna toimeen tehokkaasti, on dokumentaatio erittäin tärkeä. Dokumentaation ei tarvitse olla fyysinen dokumentti. Dokumentaation tulee kuitenkin olla informatiivista ja se voi koostua elementin toimittajan dokumentaatiosta. Dokumentaatio voi olla esimerkiksi tiedostoissa, filmillä tai tietovälineillä esitettäväksi kuvaruuduilla ja näytöillä. [6]

Dokumentaation tulisi olla tarkkaa ja suppeaa, helposti ymmärrettävissä niille henkilöille, joiden sitä pitää hyödyntää. Sen tulisi olla helposti saatavilla ja ylläpidettävissä tiedon

muokkaamiseksi muutoksien ilmetessä. Dokumentaation on sisällettävä riittävästi informaatiota jokaisesta valmiiksi saadusta kokonaisuudesta S/E/OE järjestelmän ja ohjelmiston turvallisuuden elinkaarien vaiheesta. Jotta dokumenttien hakeminen ja mahdollisten muutosten teko olisi helppoa, tulisi niiden olla otsikoituina ja niistä tulisi ilmetä versionumerot. Kaikki asiaankuuluvat dokumentit tulisi tarkistaa, muuttaa, arvostella ja hyväksyttää asianmukaisen dokumentoinnin valvontajärjestelyn alaisena. Dokumentteja tulisi päivittää säännöllisesti, jotta ne olisivat ajan tasalla ja kaikki uudetkin tiedot, ajatukset ja mahdolliset muutokset olisivat kaikkien saatavilla. [6]

6 TOTEUTUS

Vaatimusmäärittelyjen jälkeen työtä jatkettiin tutustumalla laitteiden toimintaan, jotta vaatimuksien toteuttaminen voitiin aloittaa. Tässä luvussa käydään läpi työn toteutuksen vaiheita ohjelmiston, järjestelmän ja kokonaisuuden osalta. Luvussa kerrotaan myös turvallisuuden eheyden tason saavuttamiseksi suoritetuista toimenpiteistä ja todentamisesta.

6.1 Ohjelmisto

Tärkeänä osana vaatimusten ymmärtämistä käytännössä oli ymmärtää yleisiä ohjelmointikäytäntöjä ja tarkasteltavien laitteiden ohjelmistoja. Ohjelmistoja käytiin läpi kohta kohdalta jokaisen osan toiminnan ja tarkoituksen ymmärtämiseksi. Työn edetessä todettiin kuitenkin aikataulun olevan rajallinen ja ohjelmiston riittävän ymmärryksen vievän liikaa aikaa, joten ohjelmiston vaatimuksien täyttämiseksi tarvittiin apua yrityksen osaavalta ohjelmoijalta, joka toteutti tarvittavien ohjelmistomuutoksien tekemisen.

Nykyistä ohjelmistoa ei ollut lähdetty tekemään SIL näkökulmasta, joten elinkaaren suunnitteluvaiheen vaatimuksia ei oltu otettu huomioon. Tämänhetkiset ohjelmistotestit yltävät turvallisuuden eheyden tasolle SIL1, mutta SIL2-taso vaatisi syvällisempää testausta. Ohjelmointikieli, kääntäjät ja ohjelmistoarkkitehtuuri tarkastettiin ja todettiin niiden täyttävän standardin tärkeimmät vaatimukset. Koodin kommentointia päätettiin kuitenkin parantaa, jotta voitaisiin jatkossakin varmistaa sen helppo ymmärrettävyys henkilöstä riippumatta.

Ohjelmistojen, laitteiden ja yrityksen luotettavan ja turvallisen toiminnan perustan muodostavat hyvin dokumentoidut tiedot, joissa esimerkiksi versionumeroiden avulla on mahdollisuus jäljittää tietoja eteen- ja taaksepäin. Mahdollisten ongelmien ilmetessä on tärkeää, että niin koodista kuin muusta ohjelmiston informaatiosta on mahdollista jäljittää havaittu ongelmakohta ja saada tietoon, missä vaiheessa virhe on mahdollisesti syntynyt. [6]

6.1.1 Ohjelmistotestaus

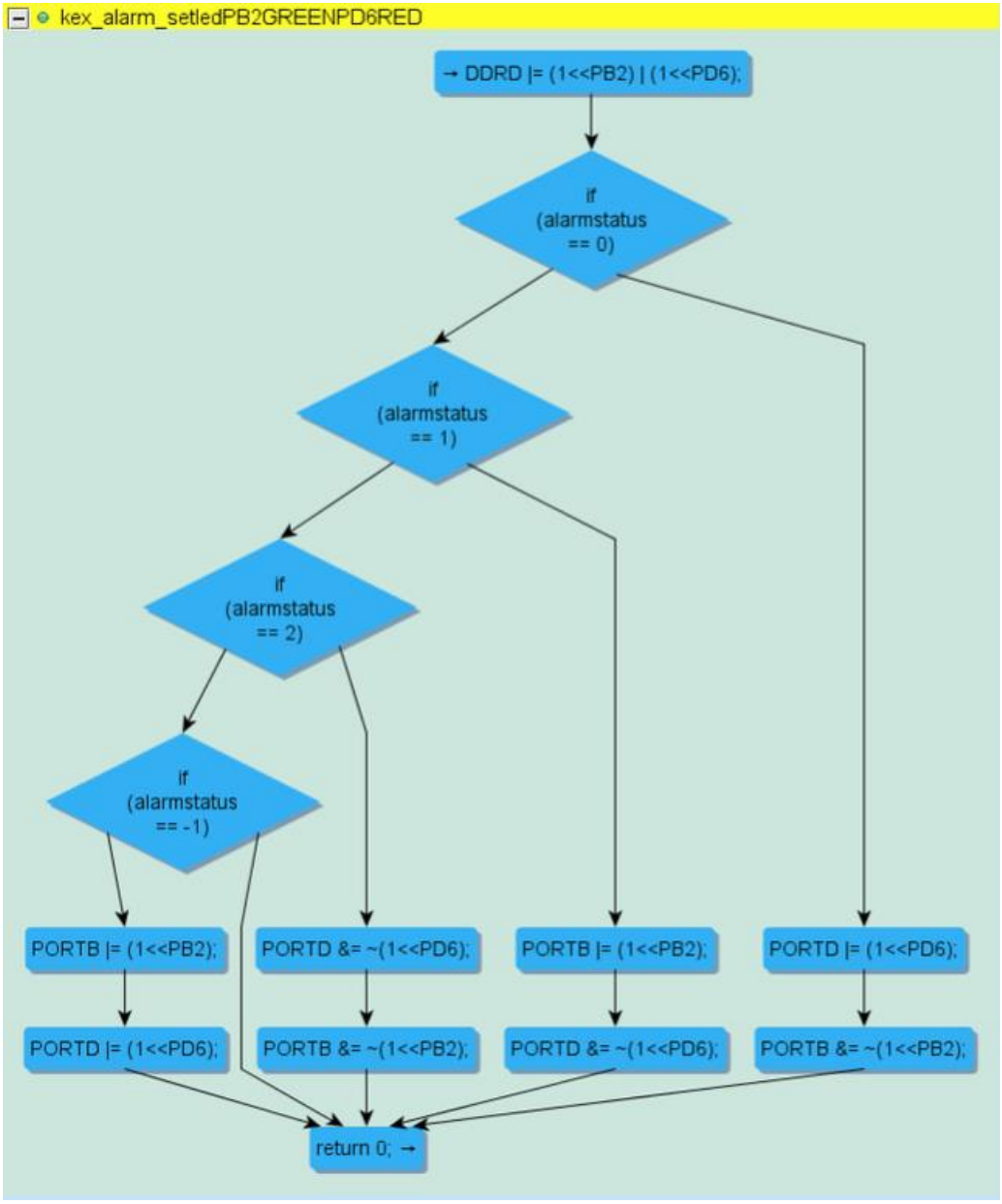
Vaatimuksista ohjelmiston osalta tärkeimmiksi nousivat erilaiset ohjelmistotestit, joilla varmistetaan ja todennetaan turvallisuuteen liittyvän ohjelmiston oikea toiminta erilaisissa tilanteissa. Tulee varmistua siitä, että kaikki ohjelmistomoduulit, elementit ja alajärjestelmät vaikuttavat oikealla tavalla toisiinsa. Myös ohjelmiston ja laitteiston keskinäinen yhteensopivuus tulee tarkistaa. Ohjelmistossa tulisi olla toimintoja, jotka tarkistavat ohjelmiston omia virheitä ja vikaantumisia. Vikaantumisesta riippuen laitteen tulisi joko pysyä turvallisessa tilassa tai saavuttaa turvallinen tila. Erilaiset ohjelmiston turvallisuuteen liittyvien toimintojen tulisi olla riippumattomia toisistaan. [12]

Ohjelmiston konfiguraation hallinnassa tarkoituksena on varmistaa tuoteryhmien johdonmukaisuus muutoksia tehdessä. Tämä vaihe koskee ohjelmiston lisäksi myös järjestelmää. On tärkeätä dokumentoida uusien ja vanhojen tuoteversioiden välinen yhteys [12]. Toimeksiantajan ohjelmiston konfiguraation seuranta ja tallennus hoidetaan versiohallinnalla, johon muokatut koodit tallennetaan ja dokumentoidaan. Versiohallintaohjelmistoon on annettu oikeudet tietyille henkilöille, vain nämä henkilöt voivat tarkastella ja muokata koodia. Toimeksiantajan versionhallinta ohjelmistolle ja raudalle tehdään koodissa, jossa on juokseva numero versionseurantaan, jota päivitetään muutoksia tehtäessä. [14]

Koodiin tehtävien muutoksien suunnitteluvaiheessa tulee ottaa huomioon muutoksien vaikutus muutettavaan ohjelmisto- ja muihin moduuleihin ja koodin osiin, joihin ne ovat yhteydessä [15]. Kun voidaan todeta muutoksen olevan riittävän suuri vaikuttamaan yksittäisen moduulin tai koko ohjelmiston toimintaan, tehdään tarvittavat ohjelmistotestit. Testaus tehdään joko yksittäiselle moduulille tai koko ohjelmiston kattavasti. Jos vaikutusanalyysissa muutoksen todetaan olevan merkittävä, on tarpeen uudelleen todentaa muutoksia koskevat ohjelmistomoduulit. [14]

Staattisen testin tarkoituksena on löytää virheitä ohjelman koodista ilman minkäänlaista ohjelman suoritusta. Esimerkkinä voidaan pitää kääntäjää, joka kääntämisen yhteydessä ilmoittaa koodista havaituista virheistä. Staattisen analyysiin kuuluvat ohjaus- ja tietovuoanalyysi. Tietovuoanalyysissa kerätään ohjelmistosta informaatiota eri pisteissä lasketuista mahdollisista arvoista. Ohjausvuoanalyysin tarkoituksena on määrittää ne ohjelman osat, joihin muuttujalle määritetty arvo saattaa vaikuttaa. [15] Analyysit suoritettiin

toimeksiantajan ohjelmistolle siihen tarkoitetulla ohjelmistolla eikä kyseisistä testeistä ilmennyt koodissa vikoja, jotka olisivat vaatineet jatkotoimenpiteitä [14]. Kuvassa 6 on esitettynä katalyyttisen kaasunilmaisimen DGTkex osa tietovuoanalyysista.



Kuva 6. Tietovuoanalyysi DGTkex-kaasunilmaisimelle.

Toinen vaativampi ohjelmistotesti on dynaaminen analyysi, jossa testausta tulisi suorittaa ohjelmiston ajon aikana. Dynaamisen analyysin testeihin sisältyy ohjelmiston rakenteiden testikattavuuden laskennat, ekvivalenssiluokat ja luokkia edustavien syötteiden testaus mukaan lukien raja-arvoanalyysit ja testitapausten suoritus raja-arvoanalyysin

perusteella. Näissä testeissä tarkoituksena on luoda ohjelmistoon testipohja, joka varmistaa ohjelmiston toiminnan monilta eri osa-alueilta. Ajon aikana testataan esimerkiksi ohjelmiston haarautumisia, tietovirtaa, perusreittiä, lähtöpistekattavuutta ja syöttöalueiden rajoja. Kyseiset testit osoittautuivat hankalammiksi niiden laajuutensa takia eikä niitä saatu työhön vaaditussa ajassa valmiiksi. Halutun turvallisuuden eheyden tason saavuttamiseksi dynaamisen analyysin testit ovat erittäin tärkeät ohjelmiston luotettavan toiminnan tarkistamiseksi myös sen ajon aikana. [15]

6.1.2 Ohjelmistoelementin turvallisuuskäsikirja

Turvallisuuskäsikirjalla voidaan varmistaa, että elementtiä käytettäessä mukana seuraa riittävän tarkka ja täydellinen kuvaus. Käsikirjan avulla voidaan arvioida kyseisen turvatoiminnon eheys, joka riippuu kokonaan tai osittain käytetystä elementistä. Näin annetaan kaikki tarvittavat tiedot ohjelmiston integroinnista vastaavalle henkilölle. Elementin toimittajan tulisi määritellä käsikirjan laajuus ja ajankohta. Nämä riippuvat siitä kuka käsikirjaa tulee soveltamaan, integraattorin tyypistä, elementin tarkoituksesta ja siitä, kuka käsikirjan toimittaa ja ylläpitää. [12]

Ohjelmistoelementin turvallisuuskäsikirjan tulisi sisältää elementin yksilöinnin, ohjelmiston konfiguraation ja ajonaikaisen ympäristön tiedot. Samoin tulisi mainita erityisten sovellustyökalujen pätevyysvaatimukset, elementille asetettavan luottamuksen aste sisältäen yksityiskohdat elementin sertifikaateista ja asennusohjeet siitä, miten valmis elementti tulisi asentaa yhdistettyyn järjestelmään. Turvallisuuskäsikirjassa tulisi kertoa syyt elementin julkaisemiseen, havaitut epäjohdonmukaisuudet ja tieto siitä, onko elementti sopiva aikaisempien julkaisujen tai järjestelmien kanssa. Olisi päätettävä menetelmät, miten muutospyynnöt käsitellään ja toteutetaan. Käsikirja voi koostua elementin toimittajan dokumentaatiosta, kunhan se on riittävä täyttämään standardin vaatimukset ja väittämät turvallisuuskäsikirjassa voidaan perustella riittävällä näytöllä. [12]

Työssä ei koettu tarpeelliseksi lähteä tekemään ohjelmistoelementin turvallisuuskäsikirjaa. Kaasunilmaisimien piirikortteihin asennetaan ohjelmisto heti niiden saapuessa tuotantoon, ja vain toimeksiantajan valtuuttamat henkilöt voivat asentaa ohjelmiston järjestelmään. Ohjelmiston asennuksesta on tuotettu jo aikaisemmin asennusohje, jossa mainitaan tarvittavat työvälineet ja ohjelmistot asennuksen onnistumiseksi. Asennusohjeessa on mainittu myös mahdolliset virhekoodit, joista huomataan ohjelmiston asennuksen ajonaikainen epäonnistuminen.

6.2 Järjestelmä

Kuten ohjelmistonkin vaatimusten tarkastelussa ja toteutuksessa, myös kaasunvalvontajärjestelmän toiminnan tunteminen oli tärkeää ennen järjestelmää koskevien vaatimusten ymmärtämisessä ja toteuttamisessa. Toimeksiantajan kaasunilmaisimet ovat toiminnallisesti hyvin yksinkertaisia ja yhden ilmaisimen toiminnan ymmärtämisen jälkeen ymmärtää myös muiden ilmaisimien käyttäytymismalleja. Katalyyttisten kaasunilmaisimien yksinkertainen rakenne on varmasti yksi syy laitteiden luotettavaan ja pitkäikäiseen toimintaan.

Toimeksiantajan kaasunvalvontajärjestelmän aikaisemmista toteutuksista ja testauksista löytyi helpommin tarvittavaa dokumentaatiota myös vaatimusten täyttämiseksi, mikä helpotti työn etenemistä. Jotta turvallisuuteen liittyvä järjestelmä olisi mahdollisimman luotettava, tulee sen kaikkien osien olla hyvin testattuja, käyttö- ja ylläpitoystävällisiä ja dokumentoituja. Tuotteen toiminnallisen turvallisuuden testaus tasaisin väliajoin on tärkeää, jotta voidaan todeta laitteen toimivan oikein. [17]

Standardissa esitettyjä vaatimuksia järjestelmälle vertailtiin jo olemassa oleviin käytäntöihin ja dokumentaatioihin. Työssä todettiin, että kaasunilmaisimien valmistuksessa käytetyt menetelmät ja testaukset vastaavat vaadittuja menetelmiä. Kun piirilevyt saapuvat tuotantoon ne ohjelmoidaan, jolloin pystytään jo erottelemaan ehjät levyt rikkinäisistä. Anturielementti kiinnitetään piirikorttiin, jonka jälkeen ne siirretään vanhenemaan. Vanhenemisen tarkoituksena on erotella heikot yksilöt, jotka olisivat ilman vanhennusta vioittuneet asiakkaalla. Ennen kuin tuote lähetetään asiakkaalle, suoritetaan kalibrointi valvottavalle kaasulle ja mitta-alue määritellään tapauskohtaisesti. Mitta-alueeseen vaikuttaa asiakkaan olosuhteet, valvottava kaasu ja sen pitoisuus. Virtaviesti, hälytysrajat ja mekaaninen toiminta tarkistetaan. Jokaiselle kaasunilmaisimelle annetaan oma sarjanumero, joka merkitään myös mukana annettavaan tarkastuspöytäkirjaan ja yrityksen laiterekisteriin. Sarjanumeron ja laiterekisterin avulla tuotteita pystytään seuraamaan tulevaisuudessakin.

Toimeksiantajan kaasunilmaisimille tehdään määräaikaistestaukset kerran vuodessa. Tällöin koulutettu huoltohenkilö käy toteamassa laitteiden oikean ja turvallisen toiminnan. Toiminnallisen turvallisuuden eheyden tason ylläpitämiseksi tuotteet tulisi testata vähintään neljä kertaa vuodessa sertifioiduilla testikaasuilla. Asiakas voi koulutuksen saatu-

aan suorittaa toiminnalliset testit myös itse. Määräaikaistestauksissa ilmaisimet kalibroidaan, virtalähdöt tarkistetaan ja varmistetaan jatkohälytyksien toiminta. Elinikänsä ylittäneet tuotteet pyritään aina uusimaan, sillä elinkaaren loppupäässä ei voida vakuuttaa laitteen toimivan luotettavasti. Mikäli asiakas ei halua uusia anturia, informoidaan asiakasta riskeistä. Huolloista tuotetaan aina pöytäkirjat, joissa kerrotaan asiakkaan nimi, laitteet niiden sarjanumeroineen, suoritetut toimenpiteet ja mahdolliset puutteet kirjataan tiedon säilyttämiseksi myös jatkossa.

6.2.1 Vika- ja vaikutusanalyysi

Työssä toteutettiin vika- ja vaikutusanalyysi eli FMEA-taulukko (Failure Mode and Effect Analysis). Vika- ja vaikutusanalyysissa on tarkoitus tunnistaa sellaisia vikamahdollisuuksia, joiden seurauksilla on merkittävä vaikutus tarkasteltavan tuotteen suorituskykyyn. Analyysi on hyvä perustyöväline tuotteiden laadun tarkkailemiseen. Menetelmällä voidaan paljastaa tuotteen osien ja komponenttien vikaantumismahdollisuuksia, vikaantumisten seurauksia ja parhaita mahdollisuuksia toimintavarmuuden kehittämiseen [18]. Analyysissa kartoitetaan kaikki mahdolliset tapahtuvat virheet ja häiriöt, joille arvioidaan niiden seurausten vaikutus, todennäköisyys ja havaittavuus. Jokaiselle vikamuodolle lasketaan riskiluku, joka saadaan vaikutukselle, esiintymistodennäköisyydelle ja havaitsemiselle arvioitujen numeroarvojen tulosta. Mitä korkeampi riskiluku sitä merkittävämpi vikamuoto on. [19]

Vika- ja vaikutusanalyysiin haluttiin ottaa huomioon kaasunvalvontajärjestelmä kokonaisuudessaan. Ensin luotiin kaasunvalvontajärjestelmän hierarkkinen vikapuumalli. Siinä huomioon otettiin keskus, kaasunilmaisin, merkinantojärjestelmä, GSM-modeemi ja väyläliitännät. Näille määritettiin yhdessä yrityksen huoltohenkilökunnan kanssa yleisimmin tapahtuvat vikaantumiset, joista muodostettiin FMEA-taulukko. Taulukkoon merkittiin jokaisen järjestelmän osa, toiminto ja potentiaalinen vika. Määritettiin ja arvioitiin jokaisen potentiaalisen vian aiheuttajat, vaikutukset ja havaittavuus sekä niiden merkittävyys kohteen turvalliselle toiminnalle. Havaittavuus arvioitiin miettien huoltohenkilön, asiakkaan ja järjestelmän vian havaitsemismahdollisuutta. Näistä laskimme keskiarvon lopulliseen analyysiin. Toimeksiantajan kaasunvalvontajärjestelmän vikaantumiset ovat yleensä harmittomia eivätkä aiheuta vaaraa ihmisille tai ympäristölle. Vikaantumisten helppo havaittavuus ja harva vikaväli jättivät riskiluvut mataliksi. Merkinantojärjestelmän riskiluvut

nousivat korkeiksi verrattuna muihin, mutta niiden toiminnan luotettavuuden edistämiseksi ei voida toimia muuten kuin vaatia vilkkujen ja sireenien toimittajalta laadukkaita tuotteita jatkossakin.

Kaasunvalvontajärjestelmän vikapuumalli on lisätty liitteeseen 1 ja keskuksen osio FMEA-taulukosta on esitetty liitteessä 2.

6.2.2 Vikaantumislaskennat

Vikaantumismuodot tulisi jaotella turvallisiin ja vaarallisiin vikaantumisiin. Vaarallinen vikaantuminen on turvatoiminnan toteuttamiseen osallistuvan elementin vikaantuminen, joka estää turvatoiminnan toimimista tai aiheuttaa turvatoiminnan epäonnistumisen. Turvallinen vikaantuminen on turvatoiminnan toteuttamiseen osallistuvan elementin vikaantuminen, joka johtaa virheellisen toiminnan tapahtuessa OL:n turvalliseen tilaan. Jokaiselle turvatoimintaan liittyvälle komponentille tulisi arvioida vaarallisten vikaantumisten osuus ja laskea vaarallisten vikojen kokonaistiheys. Elementille tulisi laskea diagnostiikan kattavuus ja turvallisten vikaantumisten osuus [17]. Diagnostiikan kattavuutta ja turvallisten vikaantumisten osuutta ei kuitenkaan lähdetty laskemaan, sillä kaasunilmaisimien rakenteessa ei esiinny diagnostiikkaa. Ilmaisimien rakenteesta ja luokituksesta kerrotaan lisää luvussa 6.2.3 Suoritustaso ja luokitus.

Vika- ja vaikutusanalyysin jälkeen laskettiin katalyyttisten ilmaisimien vikaantumisia. Laskentaan otimme mukaan tuotteiden tulon, logiikan ja lähdön komponentit. DGTkex- ja DGTk2 -rakenteissa ei ole paljoakaan eroa ja laskentoihin mukaan otetut komponentit ovatkin molemmissa samat. Komponenteille etsittiin valmistajien sivuilta vikaantumistaajuudet, jotka kullakin valmistajalla oli ilmoitettu FIT-arvoilla (Failures In Time). Vikaantumistaajuuksista saatiin laskettua jokaiselle komponentille keskimääräinen vikaantumisaika MTTF seuraavalla kaavalla:

$$MTTF = \frac{1}{\lambda} \quad [20]$$

Jokaisesta MTTF-arvosta oletetaan, että vain 50 % vikaantumisista on vaarallisia (MTTFd). Tämä on kaksi kertaa keskimääräinen vikaantumisaika (MTTF). Kaasunilmaisimen keskimääräinen vikaantumisaika saadaan summaamalla jokaisen komponentin keskimääräiset vikaantumisajat. [11]

Katalyyttisten kaasunilmaisimien kentällä tapahtuvista vikaantumisista ei löytynyt paljoakaan tietoa yrityksen reklamaatioista, jonka takia päädyttiin vikaantumislaskuissa käyttämään kokemuksen perusteella saatuja tietoja. Ilmaisimille laskettiin keskimääräinen vikaväli (MTBF) kaavalla:

$$MTBF = \frac{\Sigma(start\ of\ downtime - start\ of\ uptime)}{number\ of\ failures} \quad [21]$$

Työhön otettiin katalyyttisten kaasunilmaisimien annetun eliniän perusteella (5 vuotta) lähteneet ilmaisimet laiterekisteristä, joten tällä hetkellä ilmaisimia kentällä pitäisi olla noin 1000, joista vaarallisesti vikaantuu vuosittain vain noin kymmenesosa. Toiminnallisten testausten aikaväli (Tp) ilmaisimilla on vähintään neljä kertaa vuodessa, jolloin testausväli on 2190 tuntia. Annettujen tietojen perusteella pystyttiin laskemaan kaasunilmaisimien vikaantumistaajuus (λ) ja keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä (PFDavg). PFDavg saatiin kaavalla:

$$PFDavg = 0.5 \times \lambda \times Tp \quad [22]$$

Vikaantumislaskennoista saatujen arvojen todettiin vastaavan halutun turvallisuuden eheyden tason vaatimuksia. Vikaantumisista saadut arvot esitetään myös jatkossa ilmaisimien mukana annettavassa turvallisuuden käsikirjassa. Liitteessä 3 on esitetty vikaantumislaskennat ja niiden tulokset.

6.2.3 Suoritustaso ja luokitus

Turvallisuuteen liittyvien ohjausjärjestelmien on kuuluttava johonkin standardissa IEC 13849-1 esitettyyn luokkaan. Luokkia on yhteensä viisi, jotka jaotellaan vikakestoisuuden ja suorituskyvyn avulla. Myös tarkasteltavan järjestelmän rakenne vaikuttaa saavutettavaan luokkaan. Luokka B on yksinkertaisin ja se voi paljastaa muutamia vikoja, muttei kaikkia. Luokka 4 on turvallisin ja viat paljastuvat ajoissa turvatoiminnon menettämisen estämiseksi. Työssä todettiin kaasunilmaisimien vastaavan luokan 1 esitettyjä vaatimuksia. Järjestelmä on suunniteltu ja toteutettu käyttäen hyvin koeteltuja komponentteja ja noudattaen hyvin koeteltuja turvallisuusperiaatteita. Luokassa 1 ei järjestelmän rakenteessa ole turvatoiminnon suorittavaa testauslaitteistoa, eikä siinä ole lainkaan diagnostiikan kattavuutta. Tällaisten yksikanavaisten järjestelmien rakenteiden yhteisvikaantumisen tarkastelulla ei näin ollen ole merkitystä. [11]

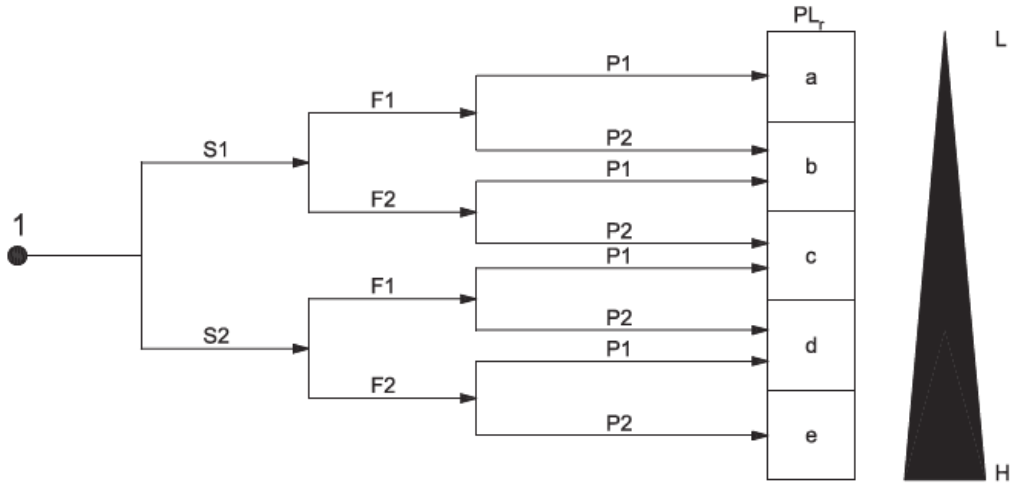
Kaasunilmaisimen rakenne on hyvin yksinkertainen, ja se sisältää tuloyksikön, logiikan ja lähtöyksikön. Ilmaisimen tuloyksikkönä toimii anturi, logiikkana mikroprosessori ja lähtöyksikkönä signaali, josta saadaan selville mitattavan kaasun pitoisuus. Tarkasteltavissa ilmaisimissa ei ole turvatoimintoja tarkistavaa testilaitteistoa, jonka vuoksi ei voitu saavuttaa standardissa esitettyä luokkaa 2. Luokan 1 suoritustaso ja rakenne eivät myöskään riitä halutun turvallisuuden eheyden tason kaksi (2) saavuttamiseen. Komponenteille aikaisemmin työn aikana lasketut vaaralliset keskimääräiset vikaantumisajat ja vaarallisen vikaantumisen todennäköisyys tunnissa olisivat riittäneet haluttuun luokkaan 2. Kuvassa 7 on esitettynä luokan 1 mukainen nimetty rakenne.

Selite

i_m Liitäntävälineet
I Tuloyksikkö (esim. anturi)
L Logiikka
O Lähtöyksikkö (esim. pääkontaktori)

Kuva 7. Luokan 1 mukainen nimetty rakenne. [11]

Suoritustasolla ilmaistaan turvallisuuteen liittyvien ohjausjärjestelmän osien kykyä toteuttaa turvatoiminto. Suoritustaso jokaiselle turvallisuuteen liittyvälle ohjausjärjestelmälle on määritettävä arvioimalla muun muassa jokaiselle turvatoimintoon osallistuvalle komponentille vaarallinen keskimääräinen vikaantumisaika ($MTTF_D$), diagnostiikan kattavuus, yhteisvikaantuminen, rakenne, käyttäytyminen vikatilanteessa, turvallisuuteen liittyvä ohjelmisto, systemaattinen vikaantuminen ja kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa. Kaasunilmaisimien suoritustaso saatiin määriteltyä standardissa esitetyn riskigraafin avulla, josta ilmeni suoritustason mahdollisuus olla tasolla PLd. Luokka 1 eli korkein saavutettavissa oleva suoritustaso on kuitenkin vain PLc eli määritettyä matalampi. Kuvassa 8 esitettynä riskigraafi vaadittavan suoritustason PLr määrittämiseksi turvatoiminnolle. [11]



Selite

1	Aloituskohta turvatoiminnon osuudenarvioimiseksi riskin pienentämisessä
L	Osuus riskin pienentämisessä pieni
H	Osuus riskin pienentämisessä suuri
PL_r	Vaadittava suoritustaso
Riskimuuttujat:	
S	Vamman vakavuus
S1	Lievä (tavallisesti palautuva vamma)
S2	Vakava (tavallisesti palautumaton vamma tai kuolema)
F	Vaaralle altistumisen taajuus ja/tai kesto
F1	Harvoin...toisinaan ja/tai lyhyt altistumisaika
F2	Toistuvasti...jatkuvasti ja/tai pitkä altistumisaika
P	Mahdollisuus välttää vaaraa tai rajoittaa vahinkoa
P1	Mahdollista tietyissä olosuhteissa
P2	Tuskin mahdollista

Kuva 8. Kuvaaja vaaditun suoritustason PLr määrittämiseksi. [11]

6.2.4 Tuotteiden turvallisuuskäsikirja

Tuotteiden turvallisuuskäsikirjan tarkoituksena on koota kaikki tiedot, jotka liittyvät vaatimusten mukaiseen tuotteeseen. Siinä dokumentoidaan tiedot, jotta päästäisiin standardin vaatimusten mukaiseen tuotteeseen. Turvallisuuskäsikirja tulisi antaa jokaisen vaatimustenmukaisen tuotteen mukana, jonka väitetään olevan IEC 61508 -sarjan vaatimusten mukainen. [17]

Vaatimusten mukaisen tuotteen toiminnot tulisi määritellä turvallisuuskäsikirjassa, sekä toimintojen tulo- ja lähtörajapinnat tulisi olla selkeästi kuvattuina. Käsikirjassa pitäisi esittää rajoitukset tuotteen käytölle. Määräaikaistestien ja ylläpidon vaatimukset olisi myös määriteltävä. Tuotteen vikaantumismuodot ja vikatiheydet olisi esitettävä turvallisuuskäsikirjassa. Laitteen luokittelu tyypiksi A tai tyypiksi B olisi selvitettävä ja ilmoitettava. [17]

Liitteessä 4 on esitettynä toimeksiantajan katalyyttiselle DGTkex-kaasunilmaisimelle tehty tuotteen turvallisuuskäsikirjan pohja. Käsikirjassa kerrotaan yleisesti katalyyttisen DGTkex-kaasunilmaisimen toiminnasta, asennukseen ja ylläpitoon liittyvistä tärkeistä toiminnoista ja vaatimuksista laitteen oikean ja turvallisen toiminnan varmistamiseksi. Tuotteen todettiin olevan tyyppiä B, sillä kaikkien osakomponenttien vikaantumismuodot ei ole hyvin määritettyjä. Ei ole olemassa riittävästi luotettavaa vikaantumistietoa havaituille ja havaitsemattomille vaarallisille vikaantumisille esitettyjen vikaantumistiheyksien tueksi [17], vaan tiedot perustuvat yrityksen vuosien aikana saatuihin kenttä- ja käyttökokemuksiin. Turvallisuuskäsikirjan loppuun tehtiin taulukot kaasunilmaisimen teknisistä tiedoista, sekä vikaantumistaajuudet. Myös laitteen jo olemassa olevat sertifikaatit mainitaan käsikirjan lopussa.

Turvallisuuskäsikirjaa on tarkoitus käyttää yhdessä kaasunilmaisimen asennusohjekirjan kanssa, jossa kerrotaan lisää ilmaisimen asennuksesta ja käyttöönotosta sekä esimerkkejä kaapeloinneista. Käsikirjasta tehtiin yksinkertainen, jotta sen päivittäminen ja ylläpito käyvät kätevästi tulevaisuudessakin. Myös asiakkaan kannalta on mukavampaa, jos dokumentti on lyhyt ja selkolukuinen.

7 YHTEENVETO

Työssä kartoitettiin katalyyttisten kaasunilmaisimien mahdollisuutta turvallisuuden standardeissa esitettyihin vaatimuksiin eheyden tason kaksi saavuttamiseksi. Työ oli odotettua haastavampi ja opinnäytetyöhön varattu aika venyi muutamalla kuukaudella. Muutamien muutoksien avulla laitteiden olisi mahdollista saavuttaa SIL2-taso. Työstä saatiin paljon uutta tietoa projektin jatkamiselle.

Opinnäytetyön tuloksena saatiin testattua ohjelmistoja ja kehitettyä niiden dokumentaatiota. Saatiin myös tietoa ohjelmistotestien tärkeydestä luotettavuuden toteamisessa. Kaasunvalvontajärjestelmälle tuotettiin vikapuumalli ja tehtiin vika- ja vaikutusanalyysi. Näiden avulla voidaan seurata potentiaalisten vikaantumisten vaikutuksia ja seurata tarvittavien muutoksien toteuttamista riskien pienentämiseksi. Kaasunilmaisimien komponenteille laskettiin vikaantumisaikoja, mutta tuotteiden vikaantumisia tulisi testata paremmin vikaantumisaikojen luotettavuuden todentamiseksi. Vikaantumisten testaus tukisi kokemuksista saatuja tietoja laitteiden turvallisuuden toteamisessa.

Työssä todettiin turvallisuuden standardien tarkastelun olevan järkevämpää uusille tuotteille, jolloin voidaan vaikuttaa jo laitteiden suunnitteluvaiheessa epäkohtiin, joita tässä tarkastelussa huomattiin. Työstä saatuja tuloksia voidaan hyödyntää suoraan uusien tuotteiden suunnittelussa ja toteutuksessa.

LÄHTEET

[1] Anni Grön, Opinnäytetyö, Turva-automaation kartoitus prosessilaitokseen, 2017

[2] Detector, Yleisesite [www-sivu] Saatavilla: http://www.detector.fi/media/tiedostot/esitteet/20-715-101-detector_yleisesite-rev.-1.6.pdf (Luettu: 12.3.2018)

[3] Detector, Yleistietoa kaasuista [www-sivu] Saatavilla: http://www.detector.fi/yleistietoa-kaasuista.html (Luettu: 5.3.2018)

[4] Greenham, L., The CoGDEM guide to gas detection, Iso-Britannia: ILM Publications, 2012

[5] Detector, kaasunilmaisimet [www-sivu]. Saatavilla: http://www.detector.fi/tuotteet-ratkaisut-ja-referenssit/kaikki-tuotteet/kaasuilmaisimet.html (Luettu: 5.3.2018)

[7] SFS-EN 61508-1:fi. 2011. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset

[7] Wikipedia, lukkiutumattomat jarrut [www-sivu]. Saatavilla: https://fi.wikipedia.org/wiki/Lukkiutumattomat_jarrut (Luettu: 1.3.2018)

[8] Wiki, Vikaantumislaskenta [www-sivu]. Saatavilla: https://wiki.metropolia.fi/display/alykas/Vikaantumislaskenta (Luettu: 1.3.2018)

[9] IEC/TR 61508-0:fi. 2011. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0: Toiminnallinen turvallisuus ja IEC 61508)

[10] SFS-EN 50402:2005. Electrical apparatus for the detection and meadurement of combustible or toxic gases or vapours or of oxygen – Reguirements on the functional safety of fixed gas detection systems

[11] SFS EN ISO 13849-1:2015. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet

[12] SFS-EN 61508-3:fi. 2011. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 3: Ohjelmistovaatimukset

[13] Detector Oy, Kaasunvalvontajärjestelmän ylläpito, [PDF] Yrityksen sisäinen koulutusmateriaali (Luettu 14.3.2018)

[14] Detector Oy, Ohjelmistotestaus [dotx] Yrityksen sisäinen materiaali (Luettu 15.3.2018)

[15] SFS-EN 61508-7:2011. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overviw of techniques and measures

[16] Wikipedia, ohjelmiston vaatimusmäärittely [www-sivu]. Saatavilla: https://fi.wikipedia.org/wiki/Ohjelmiston_vaatimusm%C3%A4%C3%A4rittely (Luettu 16.3.2018)

[17] SFS-EN 61508-2:2011. Säköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille

[18] Wikipedia, Failure mode and effect analysis [www-sivu]. Saatavilla https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis (Luettu: 5.1.2018)

[19] Ramentor Oy, ELMAS 4 – Vika-, vaikutus- ja kriittisyysanalyysi [PDF]. Saatavilla http://ramentor-com-bin.aldone.fi/@Bin/ab9fab745eba3a33f9091fe2133fe96b/1521462355/application/pdf/1583477/ELMAS%204%20-%20FMEA.pdf (Luettu: 5.1.2018)

[20] Turun Ammattikorkeakoulun opetusmateriaali, Luotettavuus [PDF]. Saatavilla http://griet.pp.fi/elsu/elsu17/luotettavuus%202018.pdf (Luettu: 24.1.2018)

[21] Wikipedia, Mean time between failures [www-sivu]. Saatavilla https://en.wikipedia.org/wiki/Mean_time_between_failures

[22] Dräger, Functional Safety and Gas Detection Systems [PDF]. Saatavilla https://www.draeger.com/Products/Content/functional_safety_sil_br_9046256_en.pdf