Antti Suominen

TOIMINNALLINEN TURVALLISUUS PROSESSITEOLLISUU-DESSA

TOIMINNALLINEN TURVALLISUUS PROSESSITEOLLISUUDESSA

Antti Suominen
Opinnäytetyö
Syksy 2019
Sähkö- ja automaatiotekniikan
tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Sähkö- ja automaatiotekniikan tutkinto-ohjelma, Automaatiotekniikka.

Tekijä: Antti Suominen
Opinnäytetyön: Toiminnallinen turvallisuus prosessiteollisuudessa
Työn ohjaajat: Tero Hietanen (OAMK) ja Timo Järvinen (Elomatic Oy)
Työn valmistumislukukausi ja -vuosi: Syksy 2019
Sivumäärä: 44

Tässä opinnäytetyössä paneudutaan prosessiteollisuuden toiminnalliseen turvallisuuteen, riskien- ja turvallisuuden eheyden tason määrittelyyn, vikaantumislaskentaan sekä turvallisuuteen liittyvien laitteiden ja toimintojen todentamiseen laskennallisesti.

Työn tarkoituksena oli tarkastella mitä asioita tulee ottaa huomioon turvallisuuden huomioimisessa sähkö- ja automaatiosuunnittelussa ja tuottaa toimeksiantajalle materiaalia suunnittelijoiden tueksi ja herättää keskustelua turvallisuuteen liittyvistä toimintatavoista. Opinnäytetyön tietoperusta pohjautuu kansainvälisiin standardeihin ja säädöksiin, jotka määrittelevät toiminnallisen turvallisuuden kriteerit.

Työn toimeksiantaja on Elomatic Oy, joka on suomalainen yksityisomistuksessa oleva insinöörisuunnittelutoimisto. Elomatic pyrkii kehittämään suunnittelutoimintaansa turvallisuuslähtöisemmäksi. Sähkö- ja automaatiosuunnittelua voidaan tehostaa turvallisuuslähtöisemmäksi yhtenäisillä toimintamalleilla ja -tavoilla, sekä kouluttamalla suunnittelijoita. Opinnäytetyö tehtiin kehitysprojektina Elomaticin Espoon EI&A-osastolla.

Opinnäytetyön tuloksena syntyi materiaalia riskiarvioinneista, riskien kohdistamisesta, vikaantumislaskennasta sekä turvatoimintojen todentamisesta laskennallisesti. Työn pohjalta syntyi myös Riskigraafi-lomake, jolla voidaan määritellä tarkasteltavan kohteen vaadittava turvallisuuden eheyden taso. Työ tehtiin kehitysprojektina, joten muodostuneen materiaalin konkreettinen soveltaminen ja kehittäminen tapahtuu tulevaisuudessa

Asiasanat: toiminnallinen turvallisuus, turvallisuuden eheyden taso, vikaantumislaskenta, riskigraafi

ABSTRACT

Oulu University of Applied Sciences
Electrical and Automation Engineering, Automation Engineering

Author: Antti Suominen
Title of thesis: Functional Safety In Process Industry
Supervisors: Tero Hietanen (OAMK) and Timo Järvinen (Elomatic oy)
Term and year when the thesis was submitted: autumn 2019
Pages: 44

This thesis focuses on the functional safety in process industry, defining the risks and safety integrity level, fault calculation and verification of safety-related devices and functions by calculation.

The purpose of this thesis was to look at what issues to consider when considering safety in electrical and automation design, and develop material to the Elomatic Oy to support designers.

The thesis was commissioned by Elomatic Oy, a privately owned Finnish consulting and engineering firm. Elomatic strives to make its design activities more safety-oriented. Electrical and automation design can be made more safety-oriented through consistent operating models and practices, and by training designers. The thesis was done as a development project at Elomatic's EI&A department in Espoo.

The thesis resulted in material on risk assessments, risk targeting, fault calculations and verification of safety functions by calculation. The work also resulted a risk graph form, which can be used to determine the required safety integrity level. The thesis was done as a development project, so the concrete application and development of the material will take place in the future.

Keywords: functional safety, safety integrity level, fault calculation, risk graph

ALKULAUSE

Osoitan kiitokseni Elomatic Oy:lle toimeksiannosta tälle opinnäytetyölle. Haluan myös kiittää työn ohjaajaa Timo Järvistä ja Espoon EI&A-osaston henkilöstöä mittaamattomasta tietämyksestä ja kokemuksesta alalta.

30.11.2019

Suominen Antti

SISÄLLYS

SANASTO

EI&A	**E**lectrical, **I**nstrumentation and **A**utomation (suom. sähkö, instrumentointi ja automaatio)
HAZOP	**H**azard **A**nd **O**perability **S**tudy (suom. vaara- ja poikkeamatarkastestelu)
IEC-standardi	Kansainvälinen sähkötekniikkaa koskeva sähköalan standardi
MTTR	Mean Time To Repair (suom. keskimääräinen korjausaika)
PFD	**P**robability of **F**ailure on **D**emand (suom. keskimäärinen vikaantumistodennäköisyys)
PFD_{FE}	average **P**robability of **F**ailure of the **f**inal **e**lement on **D**emand (loppuelementin keskimääräinen vikaantumistodennäköisyys)
PFD_{L}	average **P**robability of **F**ailure of the **l**ogic **s**olver on **D**emand (logiikan keskimääräinen vikaantumistodennäköisyys)
PFD_{S}	average **P**robability of **F**ailure of the sensor on **D**emand (sensorin keskimääräinen vikaantumistodennäköisyys)
PI-kaavio	**P**utkisto- ja **I**nstrumentointikaavio
RRF	**R**isk **R**eduction **F**actor (suom. riskin vähentämiskerroin)
SIF	**S**afety **I**nstrumented **F**unction (suom. turvatoiminto)
SIL	**S**afety **I**ntegrity **L**evel (suom. turvallisuuden eheyden taso)
SIS	**S**afety **I**nstrumented **S**ystem (suom. turvajärjestelmä)

TLJ	**T**urvallisuuteen **L**iittyvä **J**ärjestelmä
λ_D	assumed constant failure rate for **D**angerous failures (suom. vaaralliset vikaantumiset)
λ_{DD}	assumed constant failure rate for **D**angerous failures **D**etected by automatic diagnostics (suom. havaitut vaaralliset vikaantumiset)
λ_{DU}	assumed constant failure rate for **D**angerous failures **U**ndetected by automatic diagnostics (suom. havaitsemattomat vaaralliset vikaantumiset)

1 JOHDANTO

Toiminnallinen turvallisuus vaikuttaa kaikilla prosessiteollisuuden osa-alueilla. Teollisissa prosesseissa käytetään mm. paljon painelaitteita ja vaarallisia kemikaaleja, jotka tarjoavat mittavia vaaroja niin henkilö-, ympäristö- kuin taloudelliseen turvallisuuteen, jos prosessi ei toimi sille tarkoitetulla tavalla tai laitteisto vikaantuu kriittisesti. Nämä tekijät velvoittavat käyttäjiänsä ja suunnittelijoita huomioimaan turvallisuuden jo ennen laitoksen rakentamista. Turvallisuuteen pitää nykypäivänä panostaa kasvavissa määrin, koska turvallisuuteen liittyvät säädökset ja vaatimukset ovat tiukentuneet viime vuosikymmeninä. Säädökset ja vaatimukset koskevat niin uusia kuin myös vanhoja laitoksia. Turvallisuuden edistäminen vanhoissa laitoksissa voi olla haastavaa, sillä laitoksien rakennusvaiheessa ei ole huomioitu nykyaikaisia säädöksiä ja vaatimuksia.

Tässä opinnäytetyössä tarkastellaan, mitä asioita tulee ottaa huomioon turvallisuuden huomioimisessa sähkö- ja automaatiosuunnittelussa niin riskien kohdistamisesta ja määrittämisestä kuin turvallisuuteen liittyvien järjestelmien laskennallisesta todentamisesta.

Työn toimeksiantaja on Elomatic Oy, joka on suomalainen yksityisomistuksessa oleva insinööri-suunnittelutoimisto. Elomatic työllistää noin 850 työntekijää ja toimii 80 maassa. Suomessa toimistoja sijaitsee Oulussa, Jyväskylässä, Tampereella ja Helsingissä. Yhtiön pääkonttori sijaitsee Turussa. (1.)

Elomaticin tuote- ja palvelutarjonta sisältää teollisuuden suunnittelu- ja asiantuntija-, projekti- sekä elinkaaripalvelut, teknologiaratkaisut ja tuotteet valikoiduilla erikoisalueilla. Elomatic tarjoaa myös kokonaistoimittajille, suunnittelutoimistoille ja teollisuudelle suunnattuja suunnittelu- ja tiedonhallintaohjelmistoja. Elomatic toimii mm. laivanrakennus- ja offshore -teollisuudessa; asiakkaisiin kuuluvat telakat ja varustamot sekä näiden laite- ja järjestelmätoimittajat, metalliteollisuudessa; koneita ja laitteita kehittävät ja valmistavat yritykset sekä prosessi- ja energiateollisuudessa ml. ravinto- ja lääketeollisuus; investoijat, prosessi- ja energiateollisuuden tuotantolaitokset sekä näiden teknologiatoimittajat. (1.)

2 TOIMINNALLINEN TURVALLISUUS

Tässä luvussa tarkastellaan toiminnallista turvallisuutta prosessiteollisuudessa. Toiminnallisella turvallisuudella tarkoitetaan sitä osaa turvallisuudesta, joka on riippuvainen järjestelmien ja laitteiden oikeasta ja oikea-aikaisesta toiminnasta. Toiminnallinen turvallisuus on riittävää silloin, kun prosessi sekä siihen liittyvät järjestelmät on määritetty oikein, silloin ne toimivat luotettavasti ja ennakoidusti, eivätkä aiheuta vaaraa tai vahinkoa.

2.1 IEC 61508

Standardi IEC 61508 on toiminnalliseen turvallisuuteen keskittyvä perusturvallisuusjulkaisu, johon monet toimialakohtaiset toiminnallisen turvallisuuden standardit perustuvat. Standardi toimii niin sanotusti kattostandardina ja sitä käytetään pohjana usealle alakohtaiselle standardille. Standardi kattaa turvallisuuden koko elinkaaren, alun riskiarvioinnista aina järjestelmän käytöstä poistoon. (2.)

2.2 IEC 61511

Standardi IEC 61511 määrittää prosessiteollisuuden turvallisuusteknisten järjestelmien minimivaatimukset. Se perustuu standardiin IEC 61508, mutta se on räätälöity prosessiteollisuudelle. (3.)

Standardi on jaettu kolmeen osaan:

- Osa 1: Yleistä, käsitteet, vaatimukset järjestelmille, ohjelmistoille ja laitteille
- Osa 2: Osan 1 käyttöohjeet
- Osa 3: Tarvittavan turvallisuuden eheyden tason määritysohjeet.

2.3 Riskianalyysit

Toiminnallinen turvallisuus perustuu riskianalyyseistä saatuun informaatioon ja informaation soveltamiseen. Riskianalyysin menetelmät voidaan jakaa vaarojen tunnistamismenetelmiin, onnettomuuksien mallintamismenetelmiin sekä seurausanalyyseihin.

Vaarojen tunnistamismenetelmät soveltuvat rajattujen kohteiden, toimintojen tai työvaiheiden yksityiskohtaiseen tarkasteluun. Niiden avulla tunnistetaan vaara- ja haittatekijöitä. Prosessiteollisuudessa poikkeamatarkastelu (HAZOP) on eniten käytetty vaarojen tunnistamismenetelmä. (4, s. 6.)

Onnettomuuksien mallintamismenetelmiä käytetään onnettomuuksien ja tapaturmien tutkimiseen. Menetelmät kuvaavat yksityiskohtaisesti tapahtumien kulkua ja antavat pohjan onnettomuuksien todennäköisyyden arvioinnille. Prosessiteollisuudessa käytetyimpiä onnettomuuksien mallintamismenetelmiä ovat tapahtumapuuanalyysi (TPA) ja vikapuuanalyysi (VPA) sekä näiden yhdistelmä syy-seuraus -kaavio (SSK). (4, s. 6 - 7.)

Seurausanalyyseillä arvioidaan mahdollisten onnettomuuksien, kuten vaarallisten aineiden päästöjen, tulipalojen, räjähdysten ja törmäyksien, välittömiä seurausvaikutuksia. Seurausanalyyseissä vaikutukset voivat kohdistua ihmisiin, ympäristöön tai omaisuuteen. (4, s. 7.)

2.4 Prosessien riskit ja riskien vähennys

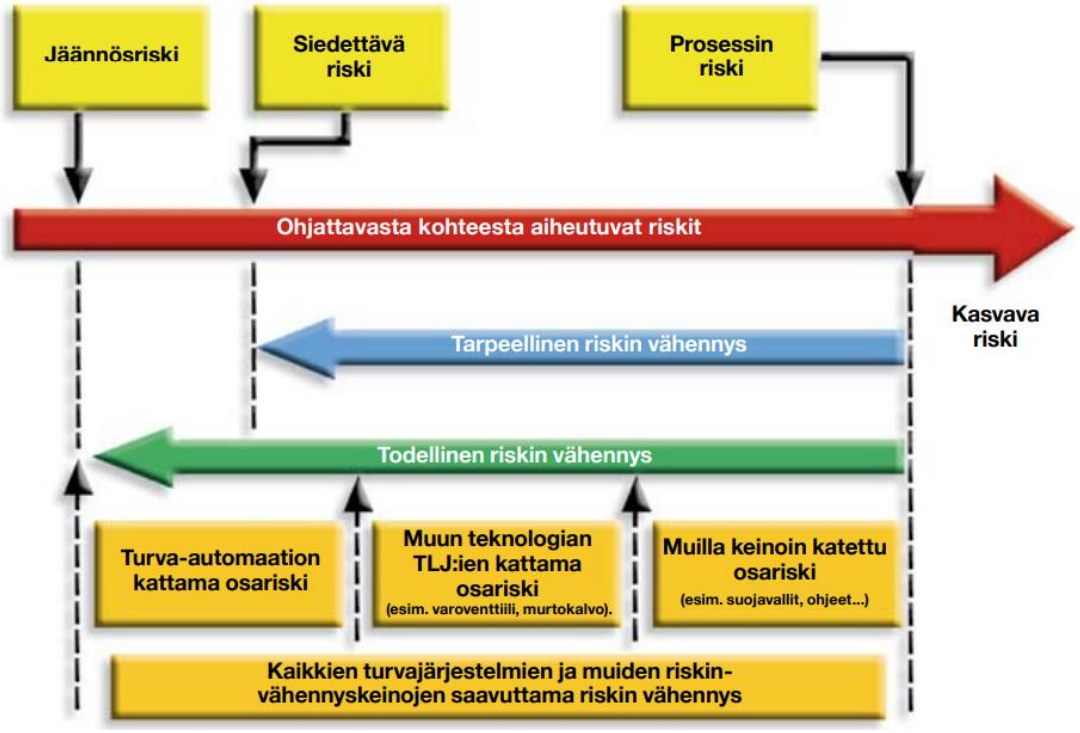
Prosessilaitosten ja prosessien riskejä voidaan vähentää monin eri tavoin, ensisijaisesti hyvällä prosessi- ja laitossuunnittelulla. Yhtenä riskinvähennyskeinona toimii turva-automaatiojärjestelmä, joka on prosessin tai laitteen normaalista käyttöautomaatiosta erillinen järjestelmä. Turva-automaatiolla pysäytetään tai ohjataan prosessi tai laite turvalliseen tilaan häiriö- tai vaarallisessa tilanteessa. Turva-automaatiojärjestelmä on aina riippumaton käyttöautomaatiojärjestelmästä. (5, s. 1.)

Prosessilaitosten ja vaarallisten laitteiden suunnittelun yleinen periaate on, että riskit arvioidaan ja varautuminen tehdään riskin edellyttämällä tasolla. Mitä vaarallisempi prosessi on, sitä enemmän luotettavuutta on vaadittava riskienvähennykseltä (esim. turva-automaatiolta tai turvatoiminnolta) ja järjestelmien kattavuuksien osoittamiselta. Toiminnallisen turvallisuuden lähtökohtana on kohteen riskien arviointi ja vaatimusten määrittely, joiden perusteella määritellään varautumiselle tarvittava turvallisuuden eheyden taso (SIL). (5, s. 5.)

Turva-automaatio on vain osa prosessin kokonaisriskien vähentämisestä. Riskejä voidaan vähentää myös mm.

- ulkoisten riskien vähentämismenetelmillä (käyttäjämanuaalit, koulutus, työluvat, kulunvalvonta, jne.)
- muiden teknologioiden riskien vähennysmenetelmillä (varoventtiilit, murtolevyt, jne.)
- muilla turvallisuuteen liittyvillä järjestelmillä (TLJ).

On tarkasteltava ja määritettävä aina tapauskohtaisesti kuinka paljon riskien vähennystä edellytetään. Kuvassa 1 esitetään yleiset periaatteet riskien vähennyksessä.

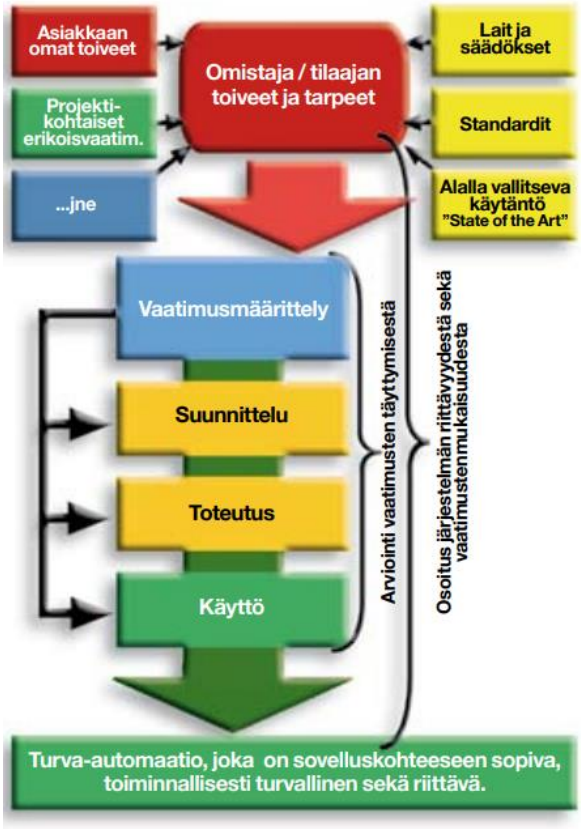


KUVA 1. Riskien vähennys: yleiset periaatteet (IEC 61508)

Kuvassa 1 prosessin riski tarkoittaa riskiä, joka voi aiheutua joko prosessista tai sen vuorovaikutuksesta ohjausjärjestelmänsä kanssa, mukaan lukien inhimilliset (esim. operaattorien) toimet. Siedettävä riski on määritelty riskinä, joka hyväksytään tietyssä yhteydessä yhteiskunnan arvojen mukaan. Se saattaa vaihdella eri maissa, toimialoilla ja yrityksissä. Jäännösriskin tulee olla aina pienempi kuin siedettävä riski. Tähän päästään erilaisilla riskinvähennyskeinoilla. (5, s. 5; 6.)

2.5 Elinkaarimalli

Laitteista tai järjestelmistä ei saa aiheutua vaaraa tai vahinkoa koko niiden suunnitellun elinkaaren aikana, ja siten toteuttamisessa keskeisimmät osa-alueet ovat toiminnallisen turvallisuuden järjestelmällinen hallinta sekä elinkaariajattelun noudattaminen. (5, s. 7.) Elinkaarimalli on esitetty kuvassa 2.



KUVA 2. Elinkaarimalli (IEC 61508)

Elinkaarimallissa projekti on jaettu vaiheisiin määrittelystä järjestelmän poistoon saakka. Vaiheille on määritelty puitteet, tavoitteet, vaatimukset sekä tulo- ja lähtötiedot. Toiminnallisen turvallisuuden varmistaminen tulee tehdä järjestelmän kaikille elinkaaren vaiheille lähtien vaatimusmäärittelystä, suunnittelusta, toteutuksesta ja käyttöönotosta edeten järjestelmän käyttöön, kunnossapitoon ja järjestelmän muutoksiin. (5, s. 7.)

2.5.1 Vaatimusmäärittely

Vaatimusmäärittelyn tärkein tehtävä on varmistaa, että toimintaan liittyvät ja toimialaa koskevat vaatimukset (säädökset ja standardit) sekä riskit on otettu riittävän hyvin huomioon. Myös asiakkaan tai tilaajan toiveet ja tarpeet pitää huomioida. Lähtökohtana vaatimusmäärittelyyn on laitteiden tai prosessin vaarojen tunnistus ja riskien arviointi sekä niiden perusteella tehty määrittely turvatoiminnoille, joilla riskiä voidaan vähentää hyväksyttävälle tasolle. Elinkaaren aikana esiintyvät

riskit tunnistetaan ja analysoidaan. Riskien arvioimisen ja eheyden tason valinnan tekee asiantunteva ryhmä. Turvallisuusratkaisuissa on kolme pääperiaatetta: vaarojen poistaminen ja pienentäminen, suojaustoimenpiteet vaarojen osalta, joita ei voida poistaa ja tiedottaminen vaaroista, jotka jäävät jäljelle. Arvioidaan määrittelyn riittävyys ja toteutuvatko edellytykset toteuttamiselle ja voidaanko suunnittelua jatkaa. (5, s. 8.)

2.5.2 Suunnittelu

Suunnitteluvaiheessa on otettava huomioon määrittelyvaiheen vaatimukset, vaadittu riskien vähennysvaatimus ja kaikki muut sellaiset tekijät, joiden ansiosta on mahdollista varmistaa laitoksen turvallisuus koko käyttöiän ajan. Toiminnallisen turvallisuuden saavuttamiseen liittyvät menettelytavat ja strategiat määritetään turvallisuussuunnitelmassa. Turva-automaation edellytyksenä on, että se pysäyttää prosessin tai saattaa sen turvalliseen tilaan vakavan häiriön sattuessa, eikä se saa aiheuttaa turvallisuuden kannalta tarpeettomia pysäytyksiä. Turva-automaation on oltava siten suunniteltu ja valmistettu, että se on luotettava, soveltuu suunniteltuihin käyttöolosuhteisiin ja laitteen huoltoa sekä koestusta koskevat vaatimukset on otettu huomioon. Turvalaitteiden on oltava muista toiminnoista riippumattomia, paitsi jos muut toiminnot eivät vaaranna turvalaitteiden toimintaa. Turvalaitteiden osalta tulee noudattaa laatujärjestelmien mukaisia toimintaperiaatteita, jotta sopiva ja luotettava suojaus saavutetaan. Näihin lukeutuu erityisesti turvallinen vikaantuminen, varmennus, erilaisuus ja itsediagnostiikka. Arvioidaan vastaako suunnittelu määritysvaiheessa asetettuja vaatimuksia ja todetaan edellytykset toteutusvaiheeseen jatkamiselle. (5, s. 8.)

2.5.3 Toteutus

Toteutusvaiheessa toteutetaan suunnitteluvaiheessa hyväksytyt suunnitelmat. Tavoitteena on toteuttaa turvallisuusvaatimusten määrittelyn mukaiset järjestelmät. Valmiiseen laitteeseen, laitekokonaisuuteen tai laitokseen liitetty turvajärjestelmä tai siihen liittyvät kenttälaitteet merkitään. Tarvittavat asiakirjat sekä käyttöohjeet laaditaan. Arvioidaan vastaako toteutus määrittely- ja suunnitteluvaiheessa asetettuja vaatimuksia ja todetaan edellytykset käyttöönottoon. (5, s. 9.)

2.5.4 Käyttö

Käyttövaiheessa huolehditaan, että järjestelmät toimivat edelleen suunnittelun mukaisesti. Muutoksia tehtäessä pitää huomioida turvallisuuden täydentyminen määrittelyiden mukaisesti. Käyttöönotettaessa ja määräajoin on varmistettava, että häiriötilanteissa laitoksen turvallisessa tilassa pitävät laitteet ja laitteistot toimivat. Jokaiselle turva-automaatioon kuuluvalle laitteelle määritetään määräaikaistarkastus- tai testausväli ja menettelyt, joilla järjestelmän luotettavuus kyetään ylläpitämään. Mikäli turva-automaatiota muutetaan, käydään läpi elinkaaren kaikki vaiheet, joihin muutos vaikuttaa. (5, s. 9.)

3 TURVALLISUUDEN EHEYDEN TASO

Mitä riskialttiimpi prosessi on, sitä luotettavampaa on oltava riskin vähennykseen käytetyn tekniikan. Turvallisuuden eheyden tasolla kuvataan todennäköisyyttä sille, että turvallisuuteen liittyvä järjestelmä toteuttaa hyväksytysti vaadittavat turvatoiminnat kaikissa määritellyissä olosuhteissa ja määriteltynä ajanjaksona. Lyhyesti ilmaistuna turvallisuuden eheyden taso määrittelee turvallisuuteen liittyvän järjestelmän luotettavuuden. Turvallisuuden eheyden tasoja kuvataan neljänä erillisenä tasona (1 - 4) ja kahtena erillisenä toimintatapana: jatkuvien ja tiheiden vaateiden toimintatapa ja harvojen vaateiden toimintatapa. nämä toimintatavat ovat käsitelty luvuissa 4.1 ja 4.2.

Turvallisuuden eheyden tasojen erot voidaan karkeasti ilmaista periaatteellisella tasolla seuraavasti:

- SIL1: Melko helppo saavuttaa noudattamalla laadukkaita toimintatapoja ja dokumentoimalla työvaiheet hyvin.

- SIL2: Ei merkittävästi eroa SIL1-tason vaatimuksista, mutta vaatii tarkempaa suunnittelua ja enemmän todentamista sekä testaamista.

- SIL3: Vaatii merkittävästi enemmän työtä kuin SIL2. Työvaiheissa on paljon todentamista ja lopputulos täytyy kelpuuttaa. Erikoismenetelmiä on käytettävä jonkin verran.

- SIL4: Vaatii erittäin paljon työtä ja resursseja. Yleensä SIL4-tason vaatimuksia yritetään välttää ja pyritään löytämään ratkaisu, joka johtaa SIL3-tason toteutukseen.

3.1 Jatkuvien ja tiheiden vaateiden toimintatapa

Jatkuvien ja tiheiden vaateiden toimintatapa on kyseessä, kun vaade turvatoiminnolle ilmaantuu useammin kuin kerran vuodessa tai jatkuvasti. Turvallisuuteen liittyvän järjestelmän vikaantumisen todennäköisyyttä kuvataan PFH-arvolla (Probability of dangerous Failure/hour), joka tarkoittaa vaarallisen vikaantumisen todennäköisyys tuntia kohden. (7, luku 1.) Taulukossa 1 esitetään turvallisuuden eheyden tasot ja niitä vastaavat todennäköisyydet sovellettaessa jatkuvien ja tiheiden vaateiden toimintatapaa.

TAULUKKO 1. Turvallisuuden eheyden tasot (jatkuvien ja tiheiden vaateiden toimintatapa)

Turvallisuuden eheyden taso (SIL)	Jatkuva ja tiheä vaade PFH (vaarallisen vikaantumisen todennäköisyys tuntia kohden)	Riskin vähentämiskerroin (RFF = Risk Reduction Factor)
4	$\geq 10^{-9} \ldots < 10^{-8}$	100 000 000 – 1 000 000 000
3	$\geq 10^{-8} \ldots < 10^{-7}$	10 000 000 – 100 000 000
2	$\geq 10^{-7} \ldots < 10^{-6}$	1 000 000 – 10 000 000
1	$\geq 10^{-6} \ldots < 10^{-5}$	100 000 – 1 000 000

3.2 Harvojen vaateiden toimintatapa

Harvojen vaateiden toimintatapa on kyseessä, kun vaade turvatoiminnolle tulee harvemmin kuin kerran vuodessa. Turvallisuuteen liittyvän järjestelmän vikaantumisen todennäköisyyttä mitataan PFD-arvolla (Probability of Failure on Demand). (7, luku 1.) Taulukossa 2 esitetään turvallisuuden eheyden tasot ja niitä vastaavat todennäköisyydet sovellettaessa harvojen vaateiden toimintatapaa.

TAULUKKO 2. Turvallisuuden eheyden tasot (harvojen vaateiden toimintatapa)

Turvallisuuden eheyden taso (SIL)	Harva vaade PFD (vikaantumisen todennäköisyys turvatoimintoa vaadittaessa, yksikössä ”vuodessa”)	Riskin vähentämiskerroin (RFF = Risk Reduction Factor)
4	$\geq 10^{-5} \ldots < 10^{-4}$	10 000 – 100 000
3	$\geq 10^{-4} \ldots < 10^{-3}$	1000 – 10 000
2	$\geq 10^{-3} \ldots < 10^{-2}$	100 – 1000
1	$\geq 10^{-2} \ldots < 10^{-1}$	10 - 100

3.3 Riskin vähentämiskerroin

Taulukossa 1. ja 2. oikeanpuoleisin sarake ilmaisee vaaditun SIL-tason riskin vähentämiskertoimen. Tämä on PFD-arvon käänteisluku ja ilmaisee kuinka paljon riskiä on pienennettävä. On hyvä huomata, että riskin vähentämiskerroin toimii myös toiseen suuntaan. Sen avulla voidaan osoittaa esimerkiksi, että käyttöönotettu turvajärjestelmä madaltaa riskiä tietyn vaaran osalta 2 dekadia verrattuna suojaamattomaan järjestelmään.

3.4 Turvallisuuden eheyden määritys

Turvallisuuden eheyden taso voidaan määritellä usealla menetelmällä. Tässä opinnäytetyössä käsitellään kahta toisistaan erillistä menetelmää, jotka ovat seuraavat:

- Riskigraafi, menetelmä jolla voidaan suoraviivaisesti määritellä vaadittava eheyden taso tarkasteltavalle kohteelle. Riskigraafia voidaan käyttää henkilö-, ympäristö- ja taloudellisen turvallisuuden määrittämiseen. Tämä menetelmä kuvataan luvussa 4.

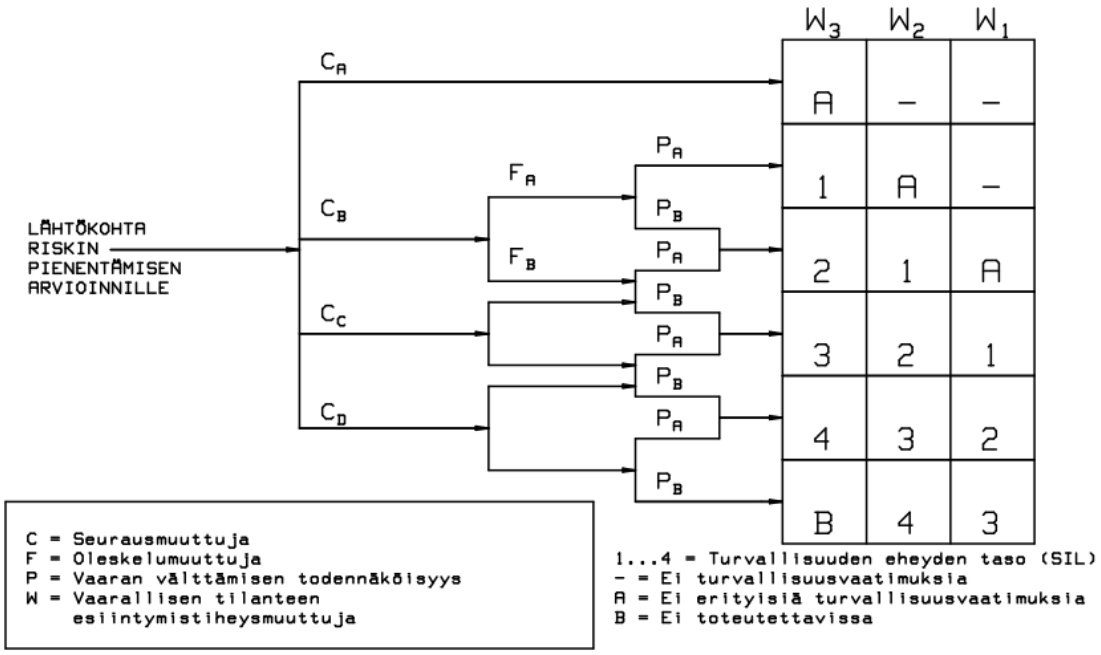
- Vikaantumislaskennallinen menetelmä standardin IEC 61508 mukaan. Menetelmässä suurin sallittu vikaantumistodennäköisyys (ts. eheyden

taso) määritellään laskennallisesti mm. suurimman siedettävän riskin, riskilähteiden lukumäärän, tekijöiden todennäköisyyksien ja vakavuuden mukaan. Tämä menetelmä kuvataan luvussa 6.

Molempien menetelmien lähtökohtana on kattava ja hyvin toteutettu riskien arviointi ja analyysi.

4 RISKIGRAAFI

Tässä luvussa käsitellään riskigraafia. Se on standardoitu menetelmä turvatoimintojen vaadittavan turvallisuuden eheyden tason määrittämiseen. Menetelmä on tapahtumapuun ja riskimatriisin yhdistelmä. (8.) Kuvassa 3 on esitetty yleinen riskigraafi-malli.



KUVA 3. Yleinen riskigraafi

Riskigraafissa huomioidaan neljä avainmuuttujaa, jotka ovat:

- C seurausmuuttuja
- F oleskelumuuttuja
- P vaaran välttämisen todennäköisyys
- W vaarallisen tilanteen esiintymistiheys.

Avainmuuttujien määrittely kuvataan luvuissa 4.1 – 4.4.

Riskigraafin kalibroinnissa annetaan avainmuuttujille arvot, jotka pitää arvioida aina yksityiskohtaisesti käsiteltävän tilanteen mukaan. Tässä työssä esitettävissä taulukoissa on esitetty malliratkaisuja muuttujien kalibroimiseksi. Nämä eivät ole valideja arvoja kaikissa tilanteissa, koska jokaisessa projektissa on omat lähtökohtansa vaarojen vakavuuksien ja niiden seurauksien suhteen.

Kalibroinnin jälkeen avainmuuttujat muodostavat ketjun, joka ohjaa riskigraafin tietylle turvallisuuden eheyden tasolle. Lopputulemana voi olla:

- — (= ei turvallisuusvaatimuksia)
- A (= ei erityisiä turvallisuusvaatimuksia)
- SIL 1
- SIL 2
- SIL 3
- SIL 4
- B (= ei toteutettavissa). (9.)

4.1 Seurausmuuttuja

4.1.1 Henkilöturvallisuus

Seurausmuuttuja voidaan määritellä vaarallisen tapahtuman seurauksen perusteella. Taulukossa 3 on esitetty yksi tapa määritellä muuttuja. Tämä on vain esimerkki ja seurausmuuttujaa pitää tarkastella aina kuitenkin tilannekohtaisesti.

TAULUKKO 3. Seurausmuuttuja henkilöturvallisuudessa

Seurausmuuttuja	**Selite**
C_A	Lievä vamma
C_B	Vakava pysyvä vamma yhdelle tai useammalle henkilölle, yksi kuolemantapaus
C_C	Monta kuolemantapausta
C_D	Erittäin monta kuolemantapausta

4.1.2 Ympäristöturvallisuus

Ympäristöturvallisuuden näkökannalta seurausmuuttuja voidaan määritellä taulukon 4 mukaisesti.

TAULUKKO 4. Seurausmuuttuja ympäristöturvallisuudessa

Seurausmuuttuja	**Määrittely**	**Esimerkiksi**
C_A	Päästö, joka aiheuttaa pienen vahingon eikä ole kovin vakava. Ympäristön rasitus tai saastuminen tai lupaehdon ylitys. Vaikuttaa alueen ja laitoksen sisällä (paikallinen ympäristövahinko).	Kohtuullinen vuoto laipan tai venttiilin kautta. Pienen mittakaavan nestevuoto. Maaperän saastuminen pienessä mittakaavassa ilman, että vaikutetaan pohjaveteen.
C_B	Päästö prosessialueella merkittävin seurauksin. Rajoitettu tunnetun myrkyn päästö. Vaikuttaa lähiseudun ympäristöön.	Ei-toivotun aineen päästö kompressorin tiivistevuodon tai laipan tiivisteen vuodon kautta ja päästö kulkeutuu laitosrajojen yli.
C_C	Päästö prosessialueen ulkopuolelle merkittävin vahingoin. Voidaan puhdistaa nopeasti ilman merkittäviä pitkäaikaisia tai pysyviä seurauksia. Vakava ympäristövahinko. Lupaehtojen tai määräysten vakavia rikkomisia.	Höyry- tai aerosolipäästö, joka ilman nesteytymistä tai sen kanssa aiheuttaa väliaikaisen eläimistön ja kasvien vahingoittumisen. Yhtiö on velvollinen puhdistamaan saastuneen alueen alkuperäiseen tilaansa.
C_D	Päästö prosessialueen ulkopuolelle merkittävin vahingoin, joita ei voida puhdistaa nopeasti tai joilla on pysyviä seurauksia. Vakava häiriö ulottuen erittäin suurelle alueelle. Lupaehtojen ja määräysten jatkuvaa rikkomista.	Nestepäästö, joka voi vaikuttaa pohjaveteen, jokeen tai mereen. Höyry- tai aerosolipäästö, joka ilman nesteytymistä tai sen kanssa aiheuttaa pysyvän eläimistön ja kasvien vahingoittumisen. Kiintoainepäästö: pöly, katalyytti, noki, tuhka, …

4.1.3 Taloudellinen turvallisuus

Taloudellisia vahinkoja arvioidessa otetaan huomioon laitevauriot, korjaustyökustannukset sekä tuotantotappiot. Taulukossa 5 on esitetty seurausmuuttujan valinta kokonaisvahinkokustannuksien mukaan.

TAULUKKO 5. Seurausmuuttuja taloudellisessa turvallisuudessa

Seurausmuuttuja	**Kokonaisvahinko**	**Huomioita**
C_A	0,2 M€ - 2 M€	Kokonaisvahinko sisältää uudelleenrakennuskustannukset ja menetetyn tuotannon
C_B	>2 M€ - 20 M€	
C_C	>20 M€ - 100 M€	
C_D	>100 M€	

On hyvä ottaa huomioon kuitenkin taloudellisia vahinkoja arvioidessa, että rahallinen menetys on suhteellinen käsite. Toiselle yritykselle 2 M€:n menetys voi olla kriittinen ja johtaa toiminnan lopettamiseen, joten suhtautuminen taloudelliseen turvallisuuteen voi olla kriittisempää pienemmälläkin taloudellisella vahingolla. Tätä on hyvä käsitellä aina tapauskohtaisesti.

4.2 Oleskelumuuttuja

Oleskelumuuttuja kuvaa oleskelun taajuutta vaaralle alttiilla alueella eli osuutta ajasta, joka alueella oleskellaan. Taulukossa 6 esitetään oleskelumuuttujan määrittelyt.

TAULUKKO 6. Oleskelumuuttuja

Oleskelumuuttuja	**Määrittely**
F_A	Harvinainen oleskelu, <10% työvuoron pituudesta alueella
F_B	Toistuva tai jatkuva oleskelu, ≥10% työvuoron pituudesta alueella

Ympäristö- ja taloudelliselle riskille valitaan aina F_B, koska riskitekijä on jatkuvasti läsnä. On hyvä myös ottaa huomioon, että poikkeustilanteissa (esim. käynnistys, pysäytys, häiriö, jne.) miehitys on usein suurempi kuin normaalisti. (9.)

4.3 Vaaran välttämisen todennäköisyysmuuttuja

Vaaran välttämisen todennäköisyys kuvaa todennäköisyyttä välttää vaarallinen tapahtuma siinä tilanteessa, että turvatoiminto epäonnistuu. Huomioitavaa on, että P_A valitaan, jos kaikki kolme taulukossa 7 esitettyä ehtoa toteutuvat. Muussa tapauksessa valitaan P_B. Vaaran välttämisentodennäköisyysmuuttujan arvo määritetään tilanteessa, jossa tarkasteltava varautumistoiminto ei toimi. (8, s. 30; 9.)

TAULUKKO 7. Vaaran välttämisen todennäköisyysmuuttuja

Vaaran välttämisen todennäköisyys	**Selite/ehto**
P_A	- Suojauksen toimimattomuus voidaan havaita, ja - on aikaa ja keinot ohjata prosessi manuaalisesti turvalliseen tilaan, ja - on poistumistie ja turvalliseen poistumiseen on aikaa
P_B	Muissa tapauksissa

4.4 Vaarallisen tilanteen esiintymistiheysmuuttuja

Vaarallisen tilanteen esiintymistiheysmuuttujan W käsittely on samanlainen käsiteltäessä henkilö-, ympäristö- ja taloudellisen turvallisuuden riskigraafeja. Muuttuja W kuvaa vaarallisten tapahtumien esiintymistiheyttä tilanteessa, jossa suojajärjestelmää ei ole. (8, s. 31; 9.) Taulukossa 8 esitetään vaarallisen tilanteen esiintymistiheyden määritteet.

TAULUKKO 8. Vaarallisen tilanteen esiintymistiheysmuuttuja

Esiintymistiheysmuuttuja	**Esiintymistiheys/vuosi**
W_1	< 0.0333… (tapahtumaväli >33 vuotta)
W_2	0.0333… - 0.333… (tapahtumaväli 33 - >3 vuotta)
W_3	> 0.333… (tapahtumaväli >3 vuotta)

Esiintymistiheysmuuttujan määrittämisessä voidaan huomioida muiden riskialennusmenetelmien vaikutus, kuten esim. takaiskuventtiilit, murtolevyt, räjähdysluukut, jne.

5 VIKAANTUMISLASKENTA

Tässä luvussa käsitellään turvallisuuden eheystavoitteiden määrittämistä ja riskien kohdistamista laskennallisesti standardin IEC 61508 mukaan. Jokaiselle erilliselle vaaralle asetetaan suurin sallittu vikaantumistodennäköisyys, joka johtaa kunkin laitteen eheystavoitteeseen. Laskennan tulemana on vaadittu turvallisuuden eheyden taso (SIL).

5.1 Suurin siedettävä riski

Taulukossa 9 esitetään esimerkkejä suurimman siedettävän riskin arvoista ja rajoista. Jotta voidaan asettaa kohteelle turvallisuuden eheyden tavoite, on määriteltävä kohteen suurin siedettävä riski (7, luku 2).

TAULUKKO 9. Suurimman siedettävän riskin esimerkkiarvoja ja rajoja

	vuodessa
Kaikki onnettomuudet (per henkilö)	5×10^{-4}
Luonnon katastrofit (per henkilö)	2×10^{-6}
Onnettomuudet kotona	4×10^{-4}
Pahimmassa tapauksessa suurin hyväksyttävä riski (HSE R2P2 -asiakirjassa)	1×10^{-3}
”Erittäin pieni riski” kuten kuvataan HSE R2P2 -asiakirjassa	1×10^{-6}

Riskit käsitellään joko individuaalisesti tai yhteiskunnallisesti, ja lähestymistapa näissä on erilainen. Individuaalinen riski on yksittäisten hypoteettisten henkilöiden kuolemantapausten määrä tietyn vaaran seurauksena. Tämä eroaa yhteiskunnallisesta riskistä, jossa otetaan huomioon vaarat, joista aiheutuu useita kuolemantapauksia. Yhteiskunnallista riskiä lähestytään tiukemmilla ehdoilla yleisesti, sillä kymmenen ihmisen kuolemaan johtanut tapaturma nähdään huonompana kuin kymmenen erillistä yksittäiseen kuolemantapaukseen johtanutta tapaturmaa. (7, luku 2.)

Taulukossa 10 esitetään individuaalisen riskin sietokyvyn rajat ja se perustuu HSE:n ”Reducing risk, protecting people, 2001 (R2P2)”-käsikirjaan. Keskimmäinen sarake ilmaisee korkeimman sallitun riskin vuodessa ja oikeanpuoleinen sarake ilmaisee yleisesti käytetyn arvon toiminnallisessa turvallisuudessa. Taulukossa 10 alimmalla rivillä määritellään yleisesti hyväksyttävä riski. Tämä on riski, jonka alapuolella ei yleensä pyritä vähentämään riskejä. Se on noin kaksin- tai kolminkertaisesti pienempi kuin satunnaisriskien kokonaismäärä, johon jokainen altistuu jokapäiväisessä elämässä. (7, luku 2.)

TAULUKKO 10. Yksilölliset riskitavoitteet kuolemantapauksiin johtuvissa vaaroissa (”Reducing risk, protecting people”, 2001 (R2P2)).

	HSE R2P2	Käytetään yleisesti toiminnallisessa turvallisuudessa
<u>Suurin Siedettävä Yksilöllinen Riski (vuodessa)</u>		
Työntekijä	1×10^{-3}	1×10^{-4}
Sivullinen	1×10^{-4}	1×10^{-5}
<u>Yleisesti Hyväksyttävä Riski (vuodessa)</u>		
Työntekijä ja sivullinen	1×10^{-6}	1×10^{-6}

On tärkeää huomata, että individuaaliset ja yhteiskunnalliset riskilaskelmat ovat pohjimmiltaan erilaisia, kun kyseessä on kuolemantapaukseen johtava vaara. Lähtökohdat suurimman siedettävän riskin osalta eivät näin ollen ole samanlaisia. Skenaariot, kuten laajat prosessialueet, merkitsevät yleensä riskiä samoille yksilöryhmille (olivat he paikan päällä tai muualla). Hajautetut riskit (esim. laajalla alueella olevat putkilinjat, junamatkat, tunnelit) joilla on nopeasti muuttuva identiteetti, ovat sellaisia skenaarioita, joiden osalta tahattoman riskin lähestymistapa on rajallinen. Yksi henkilö voi altistua kaksi minuuttia vuodessa (kulkea esimerkiksi putkilinjan läheisyydessä), kun taas milloin tahansa putkilinjan alla voi kulkea 100 yksittäistä ihmistä. Yhteiskunnallisen riskin lähestymistapa soveltuu tällaiseen tilanteeseen paremmin. (7, luku 2.)

Yleinen mielipide on, että monien kuolemantapausten pitäisi vaikuttaa myös suurimman sallitun yksilöllisen riskin valintaan. Taulukon 11 tavoitteet heijastelevat

pyrkimystä ottaa nämä ongelmat huomioon suhteellisen yksinkertaisella tavalla mukauttamalla Taulukon 10 yksilölliset riskitavoitteet. (7, luku 2.)

TAULUKKO 11. Useamman kuolemantapauksen riskitavoitteet

	1-2 kuolemantapausta	**3-5 kuolemantapausta**	**≥6 kuolemantapausta**
Suurin Siedettävä Yksilöllinen Riski (vuodessa)			
Työntekijä	1×10^{-4}	3×10^{-5}	1×10^{-5}
Sivullinen	1×10^{-5}	3×10^{-6}	1×10^{-6}
Yleisesti Hyväksyttävä Riski (vuodessa)			
Työntekijä ja sivullinen	1×10^{-6}	3×10^{-7}	1×10^{-7}

Paikka, johon kohdistuu riski, voi altistua useille mahdollisille riskilähteille. Herää kysymys, kuinka monta potentiaalista erillistä vaaraa yksittäiselle henkilölle tai ryhmälle jossakin paikassa ja ajassa kohdistuu. Jos altistutaan useille vaaroille kerralla, on pyrittävä sallimaan se määrittämällä jokaiselle vaaralle tiukempi riskitavoite. Esimerkiksi isommassa prosessikokonaisuudessa on otettava huomioon riskilähteiden suurempi lukumäärä. (7, luku 2.)

Tyypillisessä arviossa, joka koskee vain työntekijöitä paikan päällä, voidaan suurimpana siedettävän riskin kokoluokkana käyttää suositeltua $1x10^{-4}$ vuodessa (1-2 kuolemantapausta), mutta se voi koskea enimmillään kymmentä erillistä riskilähdettä kohdistuen yksittäiseen henkilöön. Jos riskilähteitä on yli kymmenen, käytetään suurimpana siedettävänä riskinä keskiarvoa $1x10^{-5}$ vuodessa ja yleisesti hyväksyttävänä riskinä $1x10^{-7}$ vuodessa. (7, luku 2.)

Huolimatta laajalti julkaistuista suurimman siedettävän riskin lukemista (Taulukko 10), pitäisi suurin siedettävä riski kohdistaa alemmalle tasolle lähemmäksi yleisesti hyväksyttävän riskin suuruusluokkaa. (7, luku 2.)

Taulukossa 12 esitetään riskitavoitteet loukkaantumiseen johtavissa vaaroissa. Eheyden arviointi ja tavoitteet asetetaan samalla tavalla kuin kuolemantapauksiin

johtavissa vaaroissa. Tavallisesti lukuarvot ovat suurempia kuin kuolemantapauksiin johtavissa vaaroissa. Absoluuttista sääntöä ei ole, mutta taulukko 12 on yleiskuva nykyisestä käytännöstä. (7, luku 2.)

TAULUKKO 12. Yksilölliset riskitavoitteet loukkaantumiselle

Suurin Siedettävä Riski	**(vuodessa)**
Työntekijä	1×10^{-3}
Sivullinen	1×10^{-4}
Yleisesti Hyväksyttävä Riski	
Työntekijä ja sivullinen	1×10^{-5}

5.2 Suurin sallittu vikaantumistodennäköisyys

Suurimman sallitun vikaantumistodennäköisyyden määrittämiseen sisällytetään ulkoisten suojaustasojen ja tekijöiden vaikutukset. Nämä tekivät voivat rajoittaa tapahtuman etenemistä tai leviämistä. (7, luku 2.) Taulukossa 13 on esimerkkejä erilaisista elementeistä, joita voidaan harkita käytettäväksi.

TAULUKKO 13. Suurimpaan siedettävään vikaantumiseen johtavat tekijät

Tekijä	**Todennäköisyys**	**Selite**
Riskiajan profiili	60%	Milloin riski voi tapahtua? Vaatiiko riskin toteutuminen tietyt realiteetit esim. virtaus, lämpötila, paine, jne. ovat riittäviä vain tiettyinä ajankohtina tai prosessi on käytössä vain tiettyinä ajankohtina.
Erillistä riskin hillitsemistä ei ole käytettävissä (esim. toisen asteen suojausta)	20%	Erilliset lieventävät tekijät ovat jätetty tulkinnasta pois ja eivät sisälly myöhempään mallintamiseen, jossa arvioidaan, täyttävätkö ne järjestelmän riskitavoitteet. Esimerkkejä ovat: - α alavirran lämpötila-, painemittaus, jne. johtaa manuaaliseen interventioon. - fyysinen suojaus (esim. alusastia) ei sisälly tulkintaan.
Tapahtuman kehittymisen todennäköisyys	70%	Esimerkkejä ovat: - säiliö/putkistolinja altistuu ylikuumenemiselle, ylipaineelle jne. - Paineen vapautuminen vaikuttaa ohi kulkevaan esim. ajoneuvoon.
Henkilö(t) altistuu riskille	25%	Työviikko on noin 25% viikon kokonaisajasta.
Syttymisen todennäköisyys	90%	Määritetään syttyykö / räjähtääkö vapautunut materiaali, ja millä todennäköisyydellä.
Kuolemaan johtavuus	25%	Todennäköisyys, että tapahtuma johtaa todella kuolemaan.

Suurin sallittu vikaantumistaajuus saadaan tässä esimerkkitapauksessa ottamalla yleisesti hyväksyttävä riski Taulukosta 11 ja jakamalla se Taulukon 12 tekijöiden todennäköisyyksien tuloilla. On hyvä huomata, että tässä esimerkissä lasketaan loukkaantumisen riskin tavoitteilla.

$$Suurin\ sallittu\ vikaantumistodennäköisyys = \frac{Yleisesti\ hyväksytty\ riski}{tekijöiden\ todennäköisyyksien\ tulo} = \frac{1x10^{-5}}{(0.6\ x\ 0.2\ x\ 0.7\ x\ 0.25\ x\ 0.9\ x\ 0.25)} = 2.1\ x\ 10^{-3}\ vuodessa$$

KAAVA 1

Verratessa lopputulemaa Taulukon 2 määrittelyihin päädytään esimerkissä SIL2-tason vaatimukseen (harva vaade).

5.3 Esimerkki vikaantumistodennäköisyyden laskemisesta

Kaasuvuodon (esim. kaasun vuotaminen säiliöstä) katsotaan olevan skenaario, joka johtaa yksittäiseen paikan päällä laitoksella tapahtuvaan kuolemaan ja kolmeen muualla kuin laitoksella tapahtuvaan kuolemaan. Sekä paikan päällä että ulkopuolella henkilön ja henkilöiden katsotaan altistuvan laitoksen aiheuttamalle riskille. Riskejä paikan päällä laitoksella ja laitoksen ulkopuolella oleville käsitellään erillisinä laskennallisesti, koska tekijät muuttuvat olennaisesti tarkastellessa riskejä eri näkökulmista. Tämä voidaan huomata vertaamalla esimerkkilaskennan tekijöitä keskenään taulukoista 14 ja 15.

TAULUKKO 14. Kaasuvuoto esimerkin tekijät laitoksella

Tekijä	**Todenn.**	**Selite**
Ajan suhde, jolloin järjestelmä voi tarjota riskin	75%	40 viikkoa vuodessa
Syttymisen todennäköisyys	5%	Arvio
Vaarassa oleva henkilö	25%	Työviikko esim. 42h/168h
Kuolemantapauksen mahdollisuus	75%	Arvio

TAULUKKO 15. Kaasuvuoto esimerkin tekijät laitoksen ulkopuolella

Tekijä	**Todenn.**	**Selite**
Ajan suhde, jolloin järjestelmä voi tarjota riskin	75%	40 viikkoa vuodessa
Syttymisen todennäköisyys	5%	Arviointi
Vaarassa oleva henkilö(t)	33%	Liiketilat vieressä
Kolmen kuolemantapauksen mahdollisuus	10%	Toimistot ovat suojattu penkereillä

Suurin sallittu vikaantumistodennäköisyys lasketaan laitoksella olevalle seuraavasti:

Taulukossa 9 suurin siedettävä riski 1-2 kuolemantapaukseen johtavassa riskissä yksittäiselle henkilölle on $1x10^{-4}$ vuodessa. Soveltaessa tätä arvoa Taulukon 6 tekijöiden todennäköisyyksillä saadaan laskentakaavaksi:

$$Suurin\ sallittu\ vikaantumis\text{todennäköisyys}_{Laitoksella} = \frac{\text{Suurin siedettevä riski}}{\text{tekijöiden todennäköisyyksien tulo}}$$

$$= \frac{1x10^{-4}}{(0.75\ x\ 0.05\ x\ 0.25\ x\ 0.75)} = 1.4\ x\ 10^{-2}\ vuodessa$$

KAAVA 2

Suurin sallittu vikaantumistodennäköisyys lasketaan laitoksen ulkopuolella oleville seuraavasti:

Taulukossa 10 suurin siedettävä riski 3-5 kuolemantapaukseen johtavassa riskissä sivulliselle on $3x10^{-6}$ vuodessa. Laskentakaavaksi saadaan:

$$Suurin\ sallittu\ vikaantumis\text{todennäköisyys}_{Ulkopuolella} = \frac{\text{Suurin siedettävä riski}}{\text{tekijöiden todennäköisyyksien tulo}}$$

$$= \frac{3x10^{-6}}{(0.75\ x\ 0.05\ x\ 0.33\ x\ 0.1)} = 2.4\ x\ 10^{-3}\ vuodessa$$

KAAVA 3

Verratessa laskennan lopputuloksia ja tekijöitä keskenään voidaan huomata, että suurin sallittu vikaantumistodennäköisyys on pienempi laitoksen ulkopuolelle kohdistuviin vaaroihin, vaikka todennäköisyys tapahtumalle on 7,5-kertainen.

6 TURVATOIMINNON TARKASTELU

Tässä luvussa käsitellään turvatoiminnon tarkastelua laskennallisesti. Tarkastelun tarkoituksena on todeta, toteuttavatko valitut laitteet ja tehdyt kytkennät tarvittavan turvallisuuden eheyden tason (SIL) turvatoiminnolle. Laskennallisesti osoitetaan, että laitteen tai toiminnon keskimääräinen vikaantumistodennäköisyys (PFD_{avg}) on vaadittavan turvallisuuden eheyden tason (SIL) mukainen. Osoittamisessa käytetään luotettavuusmallia ja luotettavuuslaskentaa. Laskennassa ei välttämättä voida huomioida kaikkea ja joudutaan näin ollen tekemään oletuksia. Tässä opinnäytetyössä esitellään yksi laskentamalli, joka perustuu IEC 61508 standardiin ja on soveltuva 1oo1-laitearkitehtuurille.

6.1 Turvatoiminnon laskennallinen todentaminen

SIF, Safety Instrumented Function (suom. turvatoiminto), on laitekokonaisuus, joka on tarkoitettu vähentämään riskiä tietyn vaaran osalta. Sen tarkoituksena on:

1. ohjata prosessi automaattisesti turvalliseen tilaan, kun määriteltyjä ehtoja rikotaan

2. sallia prosessin siirtyminen turvallisella tavalla eteenpäin, kun määritetyt olosuhteet sallivat

3. ryhdyttävä toimiin vaaran seurausten lieventämiseksi.

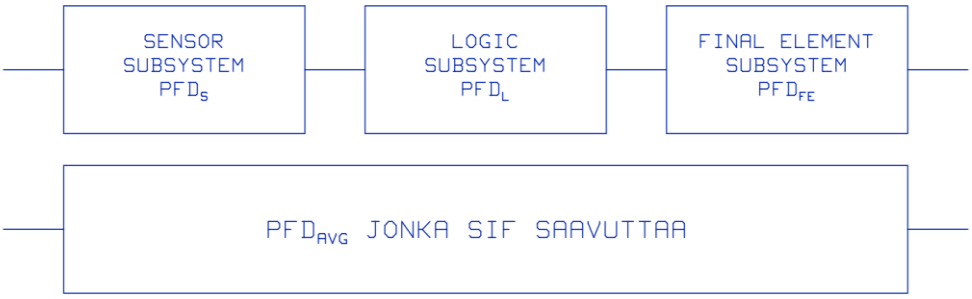
Turvatoiminto koostuu kolmesta osajärjestelmästä:

1. sensoreista (sensor)

2. logiikoista (logic solver)

3. loppuelementeistä (final element).

Kuvassa 3. on esitetty turvatoiminnon kokonaisjärjestelmän rakenne.



KUVA 3. Turvatoiminnon rakenne 1oo1-laitearkkitehtuurilla

Määrittäessä turvatoiminnon eheyden tasoa jokaiselle osajärjestelmälle (SUB-SYSTEM) lasketaan PFD_{avg}-arvo ja nämä lasketaan yhteen keskenään, jolloin saadaan turvatoiminnon (SIF) PFD_{avg}-arvo. Tämä määrittää turvatoiminnon täyttämän turvallisuuden eheyden tason (SIL). Kaavassa 4 on esitetty osajärjestelmän laskentakaava (arkkitehtuurilla 1oo1) ja Kaavassa 5 on esitetty turva-toiminnon laskentakaava (10).

$$PFD_{avg}(subsystem) = (\lambda_{DU} + \lambda_{DD})\, x\, \frac{\lambda_{DU}}{\lambda_D}\, X\, \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}\, x\, MTTR$$

KAAVA 4

missä,

λ_D = assumed constant failure rate for Dangerous failures (suom. vaaralliset vikaantumiset)

λ_{DD} = assumed constant failure rate for Dangerous failures Detected by automatic diagnostics (suom. havaitut vaaralliset vikaantumiset)

λ_{DU} = assumed constant failure rate for Dangerous failures Undetected by automatic diagnostics (suom. havaitsemattomat vaaralliset vikaantumiset)

MTTR = Mean Time To Repair (suom. keskimääräinen korjausaika)

$$PFD_{avg}(SIF) = PFD_S + PFD_L + PFD_{FE}$$ KAAVA 5

missä,

PFD_S = average Probability of Failure on Demand for Sensor (sensorin keskimääräinen vikaantumistodennäköisyys)

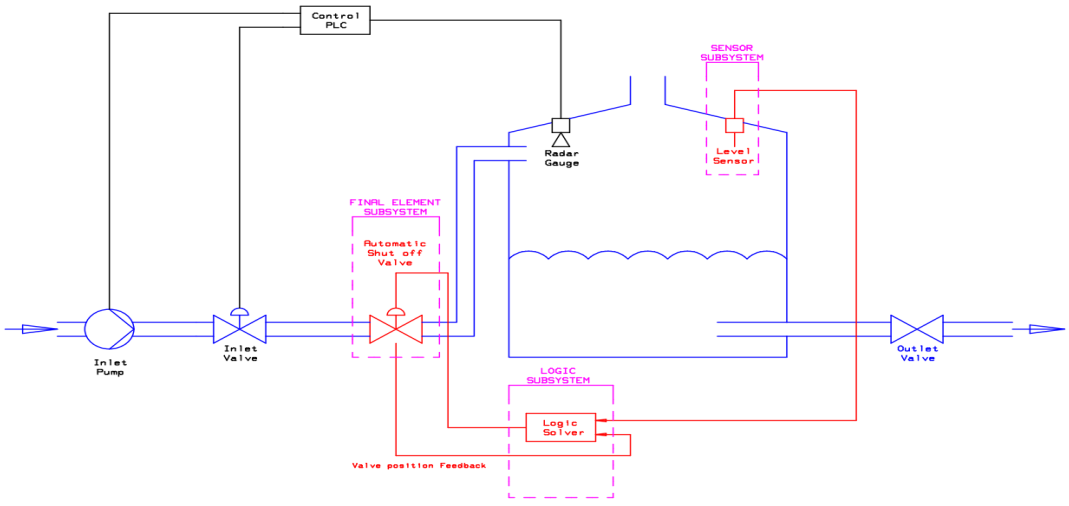
PFD_L = average Probability of Failure on Demand for Logic solver (logiikan keskimääräinen vikaantumistodennäköisyys)

PFD_{FE} = average Probability of Failure on Demand for Final Element (loppuelementin keskimääräinen vikaantumistodennäköisyys)

6.2 Esimerkki turvatoiminnon mallintamisesta ja todentamisesta

Tässä luvussa avataan esimerkki, miten voidaan yksinkertaisella turvatoiminnolla parantaa prosessiturvallisuutta ja todentaa se laskennallisesti.

Esimerkkinä on kuvitteellinen prosessi, jossa ajetaan määrittelemätöntä nestettä säiliöön. Prosessia ohjaa käyttöautomaatio (control PLC), joka säätää sisääntulevan virtauksen määrää pumpun (inlet pump), venttiilin (inlet valve) ja pinnankorkeusmittauksen (radar gauge) avulla. Säädöllä pyritään pitämään pinnankorkeus säiliössä n. 70 % tasolla. Esimerkin PI-kaavio on esitetty kuvassa 4.



KUVA 4. Laskentaesimerkin PI-kaavio

Oletetaan, että vaarana on käyttöautomaatio osajärjestelmän vioittuminen ja näin säiliön täyttyminen ja siitä seuraava vuoto. Prosessissa käsiteltävän nesteen vuotaminen lähiympäristöön tarjoaa mahdollisuuden vaaraan ja riskigraafista saadun määrittelyn mukaan vaadittava SIL-taso turvatoiminnolle on SIL2.

Ehdotetaan turvatoiminnon lisäämistä prosessiin, joka koostuu tasomittauksesta (level sensor), logiikasta (logic solver) ja hätäsulkuventtiilistä ja sen toimilaitteesta (automatic shut off valve). Pinnankorkeuden saavuttaessa 90 % säiliöstä tasomittaus indikoi tiedon logiikkaan, joka ohjaa hätäsulkuventtiilin kiinni. Venttiilin toimilaite myös antaa tiedon venttiilin asennosta logiikalle. Turvatoiminto on kuvattu Kuvassa 4 punaisella.

Taulukossa 15 esitetään esimerkissä käytettävien osajärjestelmien kuvitteelliset vikaantumisarvot, jotka laitetoimittaja on ilmoittanut.

TAULUKKO 15. Esimerkissä käytetyt vikaantumisen arvot

PARAMETRI	**LEVEL SENSOR**	**LOGIC SOLVER**	**VALVE**
Dangerous detected failure rate, λ_{DD}	1.2×10^{-7}	1.4×10^{-7}	5.3×10^{-7}
Dangerous undetected failure rate, λ_{DU}	2.3×10^{-8}	7.6×10^{-8}	2.4×10^{-7}

Kaavoissa 6, 7 ja 8 lasketaan kaikkien kolmen osajärjestelmän PFD_{avg}-arvot kaavan 4 mukaisesti. Laskennassa oletetaan MTTR:n olevan 8 tuntia ja T_1:n olevan 8760 tuntia (= 1 vuosi).

$$PFD_{avg}(sensor) = (2.3\ x\ 10^{-8} + 1.2\ x\ 10^{-7})\ x\ \left(\frac{2.3\ x\ 10^{-8}}{1.43\ x\ 10^{-7}}\ X\ \left(\frac{8760}{2} + 8\right) + \frac{1.2\ x\ 10^{-7}}{1.43\ x\ 10^{-7}}\ x\ 8\right) = 1.01\ x\ 10^{-5} \quad \text{KAAVA 6}$$

$$PFD_{avg}(logic) = (7.6\ x\ 10^{-8} + 1.4\ x\ 10^{-7})\ x\ \left(\frac{7.6\ x\ 10^{-8}}{2.16\ x\ 10^{-7}}\ X\ \left(\frac{8760}{2} + 8\right) + \frac{1.4\ x\ 10^{-7}}{2.16\ x\ 10^{-7}}\ x\ 8\right) = 3.35\ x\ 10^{-4} \quad \text{KAAVA 7}$$

$$PFD_{avg}(valve) = (2.4\ x\ 10^{-7} + 5.3\ x\ 10^{-7})\ x\ \left(\frac{2.4\ x\ 10^{-7}}{7.7\ x\ 10^{-7}}\ X\ \left(\frac{8760}{2} + 8\right) + \frac{5.3\ x\ 10^{-7}}{7.7\ x\ 10^{-7}}\ x\ 8\right) = 1.05\ x\ 10^{-3}$$

KAAVA 8

Osajärjestelemien arvot lasketaan Kaavassa 9 yhteen Kaavan 5 mukaisesti seuraavasti:

$$PFD_{avg}(SIF) = \ 1.01\ x\ 10^{-5} + \ 3.35\ x\ 10^{-4} + \ 1.05\ x\ 10^{-3} = 1.40\ x\ 10^{-3}$$

KAAVA 9

Verratessa lopputulosta Taulukkoon 2 voidaan todeta laskelman osoittavan, että kyseinen turvatoiminta kattaa SIL2-tason vaatimukset ja alentaa riskiä vaaran osalta kaksi dekadia verrattuna suojaamattomaan prosessiin.

7 YHTEENVETO

Toiminnallinen turvallisuus prosessiteollisuudessa on hyvin laaja ja moninainen aihepiiri. Turvallisuuskysymykset ja toimintatavat poikkeavat toisistaan prosessialan mukaan, ja riskit sekä vaarat määräytyvät näin ollen eri asioista.

Työn kohdistaminen tuotti haasteita, koska pitää ymmärtää lähtötason ideologiaa niin prosessiteollisuuden toimintatavoista, riskiarvioinneista ja -analyyseistä sekä alalla vallitsevista standardeista ja säädöksistä.

Opinnäytetyön tuloksena syntyi materiaalia riskiarvioinneista, turvallisuuden eheyden tason määrittämisestä, vikaantumislaskennasta, laskennallisesta todentamisesta sekä riskigraafi-lomakepohja. Opinnäytetyön ohella ei ollut projektia käynnissä, jossa olisi voinut hyödyntää kyseisiä tietoja ja soveltaa tuotettua materiaalia käytännössä, joten materiaalin hyödyntäminen ja soveltaminen jää tulevaisuuteen.

Elomaticilla on ennestään materiaalia liittyen riskiarviointeihin ja -analyyseihin sekä toiminnalliseen turvallisuuteen, mutta tämä materiaali on tietyillä työryhmillä käytettävissä, tietyillä paikkakunnilla, ja näin ollen tieto ei ole helposti saatavilla jokaiselle työryhmälle tai yksittäiselle suunnittelijalle. Kehitysideana näkisin materiaalin tuottamisen ja tiedon jakamisen jokaisen saataville, tämä vaatii kuitenkin aikaa ja käytännön toteutuksia projekteissa, jotta materiaalista saadaan tuotettua mahdollisimman yleissoveltuvaa. Tämä edesauttaisi yhteisiä toimintatapoja.

Yhteiset toimintatavat parantavat niin henkilöstön työn laatua, perehdyttämistä, yhteisöllisyyttä, asiantuntevuutta ja yritysimagoa. Tämä vaatii kuitenkin isompia ponnistuksia ja paneutumista useilta henkilöltä tai jopa kokonaiselta työryhmältä. Näkisin tämän kuitenkin tärkeänä ja kunnianhimoisena tavoitteena, koska tulevaisuudessa prosessiteollisuus kehittyy huimalla vauhdilla teknologian edetessä ja turvallisuuskysymykset näyttelevät suurta osaa tästä kokonaisuudesta.

LÄHTEET

1. Elomatic Oy. Meidän tarinamme. Saatavissa: https://www.elomatic.com/fi. Hakupäivä 01.09.2019.

2. IEC 61508. Wikipedia. Saatavissa: https://en.wikipedia.org/wiki/IEC_61508. Hakupäivä 01.09.2019.

3. IEC 61511. Wikipedia. Saatavissa: https://en.wikipedia.org/wiki/IEC_61511. Hakupäivä 01.09.2019.

4. Ohje riskienhallinnan menetelmistä. Liikennevirasto 2011. Saatavissa: https://julkaisut.vayla.fi/pdf3/rtjj_ohje_riskienhallinnan.pdf. Hakupäivä 12.10.2019.

5. Turva-automaatio prosessiteollisuudessa. 2007. Turvatekniikan keskus. Saatavissa: https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0. Hakupäivä 15.09.2019.

6. Turva-automaatio. Metropolia Wiki. Saatavissa: https://wiki.metropolia.fi/display/alykas/Turva-automaatio. Hakupäivä 15.09.2019

7. Smith, David J. — Simpson, Kenneth L. 2016. The Safety Critical Systems Handbook, 4th Edition.

8. Vaara ja riskin arviointi & turvallisuuden eheyden tasojen (SIL) määritys (riskigraafi ja LOPA). Suomen automaatioseuran turvallisuusjaosto teema-

sarja. Saatavissa: https://www.automaatioseura.fi/site/assets/files/1431/asaf_teema_1_2011_riskin_arviointi_ja_sil_mitys.pdf. Hakupäivä 01.10.2019.

9. Heikkinen, Mauri 2005. Jaakko Pöyry Oy. Koulutusmateriaali. Riskien arviointi ja hallinta, Turvallisuuteen Liittyvät Järjestelmät.

10. Institute of Measurement & Control (2014). Koulutusmateriaali: Practical SIS design and SIL verification.