Tampereen yliopisto

Kalle Syrjä

TURVALLISUUDEN EHEYSTASON VAIKUTUS TURVA-AUTOMAATIOSOVELLUKSEN ARKKITEHTUURIIN

Kandidaatintyö
Tekniikan ja luonnontieteiden tiedekunta
toukokuu 2021

TIIVISTELMÄ

Kalle Syrjä: Turvallisuuden eheystason vaikutus turva-automaatiosovelluksen arkkitehtuuriin
Tampereen yliopisto
Automaatiotekniikan tutkinto-ohjelma
Kandidaatintyö
Toukokuu 2021

Valmistavassa teollisuudessa suoritettavat prosessit mahdollistavat uusien tuotteiden saapumisen markkinoille. Osa näistä prosesseista on niin vaativia, että ilman huolellisesti toteutettuja turvatoimia niiden merkittävän tapaturman riski ylittää siedettävän tason. Turva-automaatio on eräs yleisesti sovellettu keino tämänlaisten riskien pienentämisessä. Turva-automaatiojärjestelmän jokainen osuus toteutetaan riskinarvioinnissa määritellyn turvallisuuden eheystason vaatimuksia noudattaen. Kaikkia riskejä ei ole mahdollista poistaa, mutta oikeanlaisella turvatoiminnalla ne voidaan minimoida hyväksyttäviksi. Oikein toteutetulla turva-automaatiolla yhdessä muun turvallisuuteen liittyvän toiminnan kanssa vaativienkin prosessien riskit voidaan pienentää niin pieniksi, että käyttöä voidaan pitää turvallisena.

Tämä kandidaatintyö on kirjallisuuskatsaus, jonka tavoitteena on tarjota tiivistetty esitys turvallisuuden eheystasoista sekä niiden vaikutuksesta turva-automaatiosovelluksen arkkitehtuuriin. Työn sisältö on toteutettu hyödyntäen useita aiheisiin liittyviä kirjoja, artikkeleita, standardeja sekä tutkimuksia. Kandidaatintyössä on pyritty tarkastelemaan useiden eri henkilöiden sekä tutkimusryhmien teoksia, jotta esitetty tieto olisi yleisesti hyväksyttyä sekä tutkittua.

Työn varsinainen käsittelyosa alkaa toisesta luvusta, jossa käydään läpi turva-automaation yleiset piirteet sekä toimintaympäristö. Tämän tarkoituksena on toimia pohjustuksena työn varsinaisille tutkimuskysymyksille. Turvallisuuden eheystasoja käsittelevä luku sisältää turvallisuuden eheystasojen yleisen esittelyn sekä yleisesti käytettyjä analysointimenetelmiä turvallisuusuhkien tunnistamiseen ja turvallisuuden eheyden määrittämiseen. Tämän lisäksi työ sisältää vielä luvun, jossa käsitellään mitä vaikutusta turvallisuuden eheystasolla on turva-automaatiosovelluksen arkkitehtuuriin. Tässä osuudessa esitellään muun muassa mihin asioihin eheystasolla on vaikutusta ja miten eheystason asettamiin vaatimuksiin voidaan arkkitehtuurissa vastata.

Työn tuloksena saatiin tiivis katsaus, josta eheystasoista tai turva-automaatiosta kiinnostunut lukija voi saada hyviä ideoita ja näkemyksiä tiedon tarkempaa etsimistä varten. Kirjoitetun sisältönsä lisäksi tämä kandidaatintyö tarjoaa lukijalleen myös johdatuksen useisiin aihepiirin kattavampiin teoksiin.

Avainsanat: Turva-automaatio, Turvallisuuden eheystaso, Turva-automaatiojärjestelmä

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

C	engl. *Consequence or severity of the hazardous event*, vaarallisen tapahtuman seuraukset tai vakavuus
F	engl. *Frequency of, and exposure time in, or the occupancy of the hazardous zone*, vaarallisen alueen käyttöaste ja altistumisen taajuus
FRGM	engl. *Funnel risk grap method*, suppiloriskikaaviomenetelmä
FTA	engl. *Fault tree analysis*, vikapuuanalyysi
HAZOP	*Hazard and Operability Study*, poikkeamatarkastelu
HFT	engl. *Hardware fault tolerance*, vikasietoisuus
IEC	engl. *International Electrotechnical Commission*, kansainvälinen sähköalan standardointiorganisaatio
LOPA	engl. *Layers of Protection Analysis*
M	Resurssien tai osajärjestelmien lukumäärä
MFM	engl. *Multilevel flow model*, monitasoinen virtausmalli
$MTTF_d$	engl. *Mean Time to Failure*, keskimääräinen aika vaaralliseen vikaantumiseen
MooN	engl. *M out of N*, M alkiota N alkiosta
N	Resurssien tai osajärjestelmien lukumäärä
P	engl. *Probability or possibility of failing to avoid the hazardous event*, todennäköisyys välttää vaarallinen tapahtuma
PFD	engl. *Probability of Dangerous Failure on Demand*, vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä
PFD_{avg}	engl. *Probability of Dangerous Failure on Demand*, keskimääräi nen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä
PFD_{sys}	Järjestelmän vikaantumisen todennäköisyys
PFH	engl. *Probability of failure per hour*, vikaantumisen mahdollisuus tunnissa
SFF	engl. *Safe Failure Fraction*, turvallisten vikaantumisten osuus
SFS	ruots. *Finlands Standardiseringsförbund*, Suomen standarsoimis-liitto
TET	Turvallisuuden eheystaso
W	engl. *The demand rate (number of times per year that the hazardous situation would occur in the absence of the considered SIF)*, Kuinka monta kertaa vuodessa vaarallinen tapahtuma tapahtuisi ilman turvallisuusfunktiota

1. JOHDANTO

Ei ole olemassa sellaista tilannetta, jossa riskejä ei olisi. Tämä johtuu siitä, että yhdelläkään fyysisellä esineellä vikatiheys ei ole nolla, yksikään ihminen ei toimi virheettömästi ja mikään ohjelmisto ei voi ennustaa jokaista toiminnallista mahdollisuutta. [7, s.3]

Riskien arvioimista ja havainnollistamista varten on luotu turvallisuuden eheystasot (TET) yhdestä neljään. Standardissa IEC 61508 määritellään neljä turvallisuuden suorituskyvyn tasoa turvatoiminnalle. Turvallisuuden eheystasoista TET 1 on matalin eheystaso ja TET 4 on vaativin taso. Standardissa esitellään tarpeelliset vaatimukset kunkin turvallisuuden eheyden tason saavuttamiseksi. Vaatimukset tiukkenevat siirryttäessä korkeammalle turvallisuuden eheyden tasolle, jotta voitaisiin saavuttaa vaadittu vaarallisen vikaantumisen pienempi todennäköisyys. [5, s.16]

Turva-automaatiojärjestelmiä käytetään teollisuudessa useilla sovellusalueilla, kuten esimerkiksi prosessiteollisuudessa, voimalaitoksilla ja koneissa. Valmistajat ja käyttäjät vaativat yhä enemmän turvavaatimuksia ja -standardeja täyttäviä järjestelmiä. Standardin IEC 61508 luomisesta alkaen on ollut olemassa yleinen standardi, joka määrittelee vaatimukset turvallisuuteen liittyviin järjestelmiin, sekä sisältää myös ohjelmoitavat järjestelmät sekä verkot. Standardia on sovellettu viime vuosina suunniteltaessa, toteuttaessa, hyväksyessä sekä varmennettaessa turvallisuuteen liittyviä ohjelmoitavia järjestelmiä. [4]

Standardi IEC 61508 tarjoaa suosituksia ja käytäntöjä jokaiselle turvallisuuden eheystasolle. Nämä suositukset sisältävät sekä määrällisiä että laadullisia turvallisuusarviointitekniikoita. Määrälliset tekniikat kuten luotettavuuslohkokaaviot ja Markovin analyysi voivat mallintaa laitteiston satunnaisia vikoja ja tarkistaa, että vikojen todennäköisyys on TET-kohteelle hyväksyttävissä rajoissa. Laadulliset turvallisuusarviointitekniikat kuten esimerkiksi simulointi auttavat löytämään systemaattisia virheitä ohjelmistosta. [8, s.17]

Suunniteltaessa ja toteutettaessa turvatoimintoja sähköisellä, elektronisella tai ohjelmoitavalla tekniikalla, suositellaan noudattamaan kattostandardin sekä sovellusstandardien asettamia vaatimuksia. Standardien noudattamista ei vaadita, mutta se on erittäin suositeltavaa. Valmistajat voivat halutessaan valita muun menettelyn, joka täyttää säädösten asettamat vaatimukset. Standardien noudattaminen on kuitenkin hyvä tapa osoittaa järjestelmien soveltuvuus tehtäväänsä. [1, s.6]

Tässä kandidaatintyössä tutkitaan, mitä vaikututusta turvallisuuden eheystasolla on turva-automaatiosovelluksen arkkitehtuuriin. Kandidaatintyö muodostuu kahden tutkimuskysymyksen ympärille. Ensimmäinen tutkimuskysymys on seuraava: mikä on eheystaso? Tähän liittyen työssä esitellään muun muassa mitä eheystasolla tarkoitetaan sekä miten taso määritetään. Työn toinen tutkimuskysymys on seuraava: miten turva-automaation ratkaisuilla päästään vaadittavaan eheystasoon? Tutkimuskysymykseen liittyen työssä tarkastellaan esimerkiksi tilanteita eri eheystasoilta ja tutkitaan mitkä ratkaisut varmistavat sen, että arkkitehtuuri vastaa eheystason asettamia vaatimuksia. Tutkimusmenetelmänä kandidaatintyössä on kirjallisuusselvitys.

Tämä kandidaatintyö koostuu viidestä luvusta. Työn ensimmäinen luku on johdanto, jossa esitellään työn tutkimuskysymykset, sekä esitellään lukijalle suppeasti mitä kandidaatintyö tulee sisältämään.

Työn varsinainen käsittelyosa alkaa työn toisesta luvusta, jossa lukijalle esitellään toimintaympäristöä, eli lukija saa lyhyen katsauksen mitä turva-automaatiolla tarkoitetaan ja missä sitä voidaan esimerkiksi hyödyntää. Työn kolmannessa ja neljännessä luvussa keskitytään konkreettisemmin tarjoamaan vastauksia työn kahteen tutkimuskysymykseen. Ensimmäisenä mainitussa asiaa keskitytään tarkastelemaan pääosin työn ensimmäisen tutkimuskysymyksen näkökulmasta. Neljännessä luvussa asia painottuu turva-automaation rakenteeseen liittyvien ratkaisujen tarkasteluun sekä analysointiin. Työn viimeisessä luvussa eli yhteenveto -luvussa on tiivistetty esitys havainnoista, mitkä ilmenivät työn edetessä.

2. TOIMINTAYMPÄRISTÖ

2.1 Turva-automaation määrittely

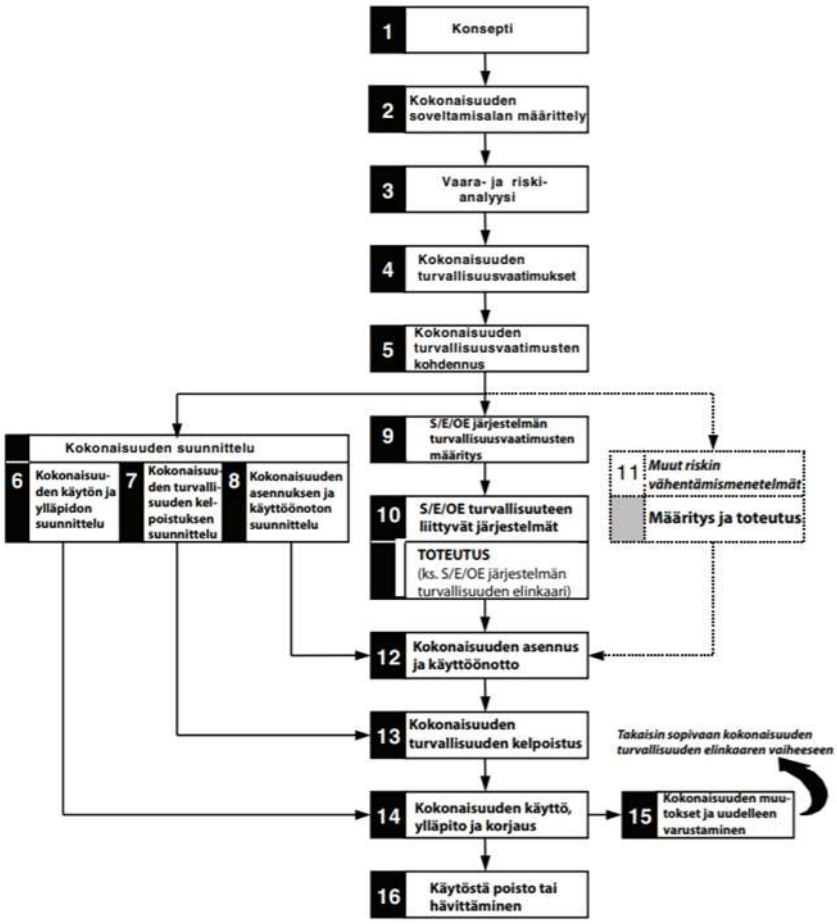
Turva-automaatiojärjestelmällä tarkoitetaan laitteesta tai prosessista erillistä järjestelmää, jonka päätehtävä on saattaa järjestelmä takaisin turvalliseen tilaan, jos laite on jo päätynyt vaaralliseen tilaan. Turva-automaation toisena tehtävänä on estää prosessia päätymään vaaralliseen tilaan. Sen on tarkoitus toimia tilanteissa, joissa käyttöautomaatiojärjestelmä tai muu varautuminen ei kykene saamaan häiriötä hallintaan. Järjestelmän käytöllä voidaan merkittävästi parantaa laitteiston tai prosessin turvallisuutta. Turva-automaatiojärjestelmän toimimattomuudesta saattaa seurauksena olla vakavia henkilö-, ympäristö- tai materiaalivahinkoja. [1, s.3] [3, s.197]

Mikä tahansa järjestelmä, jolla toteutetaan millä tahansa teknologialla turvatoimintoja, on turvallisuuteen liittyvä järjestelmä. Laitteiston ohjausjärjestelmä voi suorittaa turvatoimintoja joko itse tai turvallisuuteen liittyvä järjestelmä voi olla erillinen mistä tahansa laitteiston ohjausjärjestelmästä. Ensimmäisenä mainitussa tapauksessa laitteiston ohjausjärjestelmän voidaan katsoa olevan turvallisuuteen liittyvä järjestelmä. Turvallisuuden eheystason kasvaessa tasot edellyttävät yhä enemmän täsmällisyyttä turvallisuuteen liittyvän järjestelmän suunnittelussa. [5, s.10]

Turvallisuuskriittisten järjestelmien turva-automaation toteutuksessa tulee olla yksikäsitteisiä. Turvallisuuden automatisointiin liittyy tietokonelaitteita- ja ohjelmistoja, sähköisiä, elektronisia tai mekaanisia laitteita. Ohjelmisto tai laitteisto, jota käytetään turvallisuuden kannalta kriittisten järjestelmän toimintojen hallintaan, voi myös aiheuttaa vaaraa tai muiden komponenttien viallista toimintaa. Ohjelmistoa tai laitteistoa voidaan pitää turvallisena, jos tapaturman mahdollisuus on lähes mahdotonta tai erittäin epätodennäköistä. Turva-automaatiojärjestelmä sisältää sulautettuja ohjausjärjestelmiä. Turva-automaatio perustuu usein ohjelmistoihin, joiden avulla toteutetaan toimintoja turvallisuuden saavuttamiseksi. Ohjelmistokehitysprosessissa on oltava selkeä käsitys mitä ollaan toteuttamassa, jotta saadaan toteutettua laadukkaita sovelluksia, jotka voivat estää vakavan tapaturman havaitsemalla suoritusvirheet ja puuttumalla näihin tilanteen tarpeen mukaisesti [2]

2.2 Turva-automaatiojärjestelmän elinkaari

Turva-automaatiolaitteesta tai -järjestelmistä ei saa aiheutua vahinkoa missään elinkaaren vaiheessa. Täten turva-automaation toteuttamisen keskeisimpinä osa-alueina voidaan pitää toiminnallisen turvallisuuden järjestelmällistä hallintaa sekä elinkaariajattelun noudattamista. Turvallisuuden järjestelmällisen käsittelyn tueksi standardissa IEC 61508 on otettu käyttöön turvallisuuden elinkaarimalli, jossa projekti on jaettu vaiheisiin turvallisuuden eheyden tason määrittelystä aina järjestelmän poistoon saakka [1, s.7]. Suomen standardisoimisliiton [5, s. 16] mukaan: ”Standardissa IEC 61508 katetaan kaikki turvallisuuden elinkaaren toimenpiteet alustavasta konseptista vaara-analyysin, riskinarvioinnin, turvallisuusvaatimusten kehittämisen, määrittelyn, suunnittelun ja toteutuksen, käytön ja ylläpidon ja muutosten kautta lopulliseen käytöstä poistoon ja/tai hävittämiseen.”



Kuva 1. *Turvallisuuden elinkaarimalli [6, s.34]*

Turvallisuuden elinkaaren tavoitteena on käsitellä tapahtumien syitä. Tätä varten turvallisuustehtävissä työskentelevät insinöörit pyrkivät luomaan järjestelmän, joka auttaa vähentämään tai minimoimaan riskejä, täyttää asianmukaiset tekniset vaatimukset ja tukee henkilöstön osaamista. [9]

Suorituskyvyllä tarkoitetaan tasoja, joilla kuvataan keskimääräistä mahdollisuutta vaaralliseen vikaantumiseen yhden tunnin aikana. Suorituskyky *a* on alhaisin vaatimustaso ja suorituskyvyn taso *d* vaativin. Suorituskyky diagnostisen kattavuuden kanssa (ts. havaittujen vaarallisten vikojen määrä) ja keskimääräinen aika vaaralliseen vikaantumiseen ($MTTF_d$) määrittelevät systeemin arkkitehtuurin. Valittu suorituskyky vaikuttaa myös vaatimusten tiukkuuteen elinkaaren eri vaiheissa. Yleisesti ottaen nämä vaatimukset koskevat yleensä ohjelmistovikojen välttämistä elinkaaren aikana: vaatimusten määrittelyvaihe, suunnittelu, ohjelmointi- ja testausvaihe, integrointivaihe eli ohjelmistopohjaisen turvallisuuteen liittyvän ohjelmiston parametrisointi. Mitä korkeampi suorituskyvyn taso, sitä tehokkaammat mittaukset ovat pakollisia. [10]

Kansainvälinen standardi IEC 61508 ei ole sovelluskohtainen. Standardi tarjoaa vaatimuksia ja menettelytapoja, joita voidaan käyttää eri sovelluksissa. Standardin elinkaarimallia suositellaan soveltamaan, koska se tarjoaa kattavasti turvallisuusnäkökohtia. Standardien käyttö on suositeltavaa myös siksi, että ne ovat yleisesti tunnettuja ja niiden noudattamista arvostetaan. [11, s.313]

Aikaisemmat standardit ovat perustuneet määräämistoimenpiteisiin, joissa määritellään tilanteen vaatima suojaus. Uudemmat toiminnalliset standardit ovat sen sijaan suorittamiseen perustuvia. Tämä muutos on helpottanut insinöörien tehtävää turvallisuuden määrittelemisessä ja perustelussa. Tässä lähestymistavassa hyödynnetään metodisempaa, determinististä lähestymistapaa, joka tarjoaa mahdollisuuden räätälöidä spesifejä turvallisuustoimintoja sovelluksen mukaan. Se auttaa vähentämään kustannuksia, vähentää sovelluksien monimutkaisuutta, parantaa koneiden kestävyyttä ja auttaa saavuttamaan optimaalisen turvallisuustason jokaiselle määritetylle turvapiirille tai toiminnolle sijoitetun pääoman tuoton parantamiseksi. [9]

Turvallisuuden elinkaarimallin voidaan ajatella jakautuvan kahteen pääosuuteen [11, s.314]:

1. Ensimmäiseen osioon kuuluvat toiminnot, jotka liittyvät automaatioyksikön kehittämiseen. Kehitysvaiheeseen kuulu turvallisuuteen sekä turvatoimiin liittyvät toiminnot. Tämän lisäksi turvallisuusvaatimusten asettamat vaatimukset tulee ratkaista tässä vaiheessa.

2. Toiseen osioon kuuluu automaatiojärjestelmän käyttöön liittyvät toiminnot automaatiosysteemin käyttöiän aikana.

2.3 Käyttöautomaatio vs. turva-automaatio

Esimerkiksi prosessiteollisuuden turvastandardit vaativat, että laitoksen riskiä on vähennettävä siedettävälle tasolle, jonka määritellee prosessin omistaja. Ratkaisu tähän on toteuttaa suojausta useissa kerroksissa. Yleisesti kerrokset koostuvat käyttöautomaatiosta, operaattorin interventiosta, mekaanisesta apujärjestelmästä sekä turva-automaatiojärjestelmästä. [12, s.441]

Ensimmäinen kerros eli käyttöautomaatio ohjaa prosessia normaaliolosuhteissa. Jos prosessi poistuu stabiililta käyttöalueelta, operaattori tulee väliin. Jos operaattorikaan ei saa tilannetta hallintaan, turva-automaatiojärjestelmän on saatava prosessi turvalliseen tilaan, sillä muuten tapauksessa seuraa onnettomuus. [12, s.441]

Käyttöautomaatiojärjestelmä on automaatiojärjestelmä, jonka tarkoituksena on pyrkiä pitämään prosessia normaalilla toiminta-alueella. Käyttöautomaatiossa ei ole turvallisuuteen liittyviä järjestelmiä. Käyttöautomaatiolle ei ole määrätty turvallisuuden eheystasoa [1, s.15]. Käyttöautomaatio toteutetaan yleisimmin pneumaattisissa ohjauspiireissä, ohjelmoitavissa logiikkaohjaimissa, hajautetuissa ohjausjärjestelmissä, binäärilogiikkajärjestelmissä (esimerkiksi ON/OFF- rele) ja yksisilmukkaisissa ohjaimissa. Käyttöautomaation virhe sen suorittaessa normaaleita ohjausfunktioita on yksi yleisimmistä virhetilanteiden aiheuttajista.

Turva-automaatiojärjestelmällä tarkoitetaan turvallisuuteen liittyvää automaatiojärjestelmää, joka koostuu logiikkaosasta, mittausantureista, ohjattavista kohteista sekä näiden välisestä kaapeloinnista [1, s.15]. Turva-automaatiojärjestelmät toteutetaan useimmin käyttäen binäärilogiikkaa ja ohjelmoitavia elektronisia järjestelmiä [14, s.188]. Termi turva-automaatiojärjestelmä on mainittu standardissa IEC 61511 puhuttaessa turvallisuuteen liittyvästä järjestelmästä. Turva-automaatiojärjestelmälle määritetään aina eheystaso, jolla sen on kyettävä toimimaan [1, s.15]. Turva-automaatiojärjestelmän tarkoituksena on pienentää prosessista riskiä, jonka vuoksi prosessista voi tulla vaarallinen. Järjestelmä toteuttaa tämän vähentämällä epätoivottujen tapahtumien taajuutta. Eheystason suuruudella kuvataan, kuinka paljon riskiä turva-automaatiojärjestelmällä voidaan vähentää [15, s.2686]. Eheyden vaatimukset määritetään standardissa IEC 61508 tai IEC 61511, näistä sovelletaan tilanteeseen sopivampaa. [1, s.15]

Turva-automaatiojärjestelmä havaitsee vaaralliset olosuhteet ja tekee ohjaustoimenpiteen prosessin saamiseksi turvalliseen tilaan, estäen epätoivotun tapahtuman. Turva-

automaatiojärjestelmän luominen ja eheystason valinta tulisi perustua lakeihin, säädöksiin ja kansainvälisiin sekä kansallisiin standardeihin. Tehdäkseen parhaan päätöksen eheystasosta, suunnittelijan on tiedostettava ja arvioitava riskitekijät sekä mahdolliset seuraukset tapaturman sattuessa. Jos suunnittelija jättää toisen näistä seikoista huomioimatta, ovat tulokset todennäköisesti heikkoja. [15, s.2686]

Yhteisvikaantumisen sekä systemaattisten vikojen välttämiseksi käyttöautomaation ja turva-automaatiojärjestelmän tulee olla täysin erillisiä toisistaan. Nämä kaksi järjestelmää on suunniteltu ja toteutettu vastaamaan erilaisia riskinvähennysvaatimuksia. Pahimmassa tapauksessa ne voivat vikatilanteessa jopa häiritä toistensa toimintaa. Turva-automaatiojärjestelmän toiminnalle on tarjottava parhaat mahdolliset edellytykset toimia minimoimalla ulkoisten häiriöiden mahdollisuus. [13, s.135]

Usein tilanne on se, että käyttöautomaation vikaantumiset asettavat vaateen yhdelle tai useammalle turvallisuuteen liittyvälle järjestelmälle. Tällöin kaikki käyttöautomaatiojärjestelmän kohtuudella ennakoitavissa olevat vaaralliset vikaantumistavat tulee ottaa huomioon, kun määritetään vaatimuksia turva-automaatiojärjestelmälle. Tässä tilanteessa käyttöautomaatiolle esitettyä vikaantumistiheyttä on tuettava tiedoilla, jotka on hankittu jollakin standardissa IEC 61508 määritellyllä tavalla. Eräs vaihtoehto on käyttöautomaatiolla saatu käyttökokemus samantapaisessa sovelluksessa. Toinen vaihtoehtoja on esimerkiksi suorittaa luotettavuusanalyysi luotettavalla menetelmällä. Prosessin vaatiessa yhtä tai useampaa turvallisuuteen liittyvää järjestelmää on pidettävä huolta, että käyttöautomaatiojärjestelmä on riippumaton turva-automaatiojärjestelmästä ja muista riskinvähennysmenetelmistä. [6, s.58]

2.4 Turva-automaation sovelluskohteesta

Turva-automaatiota sovelletaan turvakriittisissä järjestelmissä. Turvallisuuskriittiseksi järjestelmäksi luokitellaan järjestelmä, joka voi vikaantuessaan aiheuttaa vahinkoa ihmisille, ympäristölle tai taloudellisesti. Jotkut virheet voivat suoraan aiheuttaa epätoivottuja seurauksia, kun taas toiset voivat kasvattaa tapaturman riskiä. Se, että määritelläänkö systeemi turvallisuuskriittiseksi, riippuu seurauksista, joita se voi vikaantuessaan aiheuttaa. Jos todetaan, että seuraukset joita järjestelmä voi vikaantuessaan aiheuttaa ovat sellaisia, joita ei voi hyväksyä, on kyseessä turvallisuuskriittinen järjestelmä. [16, s.1]

Turvallisuuteen liittyvät toiminnot, joita turvallisuuskriittisessä järjestelmässä toteutetaan, jakautuvat kahteen kategoriaan [16, s.2]:

Turvallisuuden valvontatoiminto (*safety control function*). Tämä toiminto on osa normaalia suoritusta. Tämä toiminto tapahtuu käyttöautomaatiotasolla ja voi olla esimerkiksi ilmoitus aikomuksesta siirtyä tilasta toiseen.

Turvallisuusfunktio (*safety protective function*). Tämä toiminto tapahtuu turva-automaatiosovelluksessa. Toiminnon suoritus ei siis ole osa normaalia suoritusta, vaan tapahtuu vain sellaisessa tilanteessa, joissa se on välttämätöntä. Käyttö on välttämätöntä tilanteessa, jossa prosessi on vaarassa edetä vaaralliseen tilaan.

Turvallisuuskriittisissä järjestelmissä on yleistä, että jotkin osuudet tai yksittäiset komponentit ovat erityisen tärkeitä laitteiston turvallisen toiminnan kannalta. Tällöin on kaksi mahdollisuutta varmistaa laitteiston korkea luotettavuus. Ensimmäinen vaihtoehto on käyttää korkean luotettavuuden omaavia komponentteja systeemin rakenteen kriittisissä paikoissa. Toisena vaihtoehtona on lisätä varmistavia komponentteja kriittisin paikkoihin. [17, s.930]

Turvallisuuskriittisten järjestelmien tapauksessa järjestelmän laatu on toisinaan jopa tärkeämpää tai vähintäänkin yhtä tärkeää kuin järjestelmän toiminnallisuus. Järjestelmän laadun tulee noudattaa oman sovellusalueensa standardeja ja ohjeistuksia. Ohjelmistot turvallisuuskriittisiin järjestelmiin toteutetaan seuraten spesifisiä, tarkasti määriteltyjä prosesseja, jotka ovat standardien ja ohjeistuksien mukaisia. Näissä määritellään vaiheet, joiden mukaan toimitaan tai vaatimukset mitkä järjestelmän on täytettävä. [18, s.35]

Ennen turvakriittisen järjestelmän käyttöönottoa se tulee hyväksyttää. Tätä pidetään jopa tärkeimpänä vaiheena turvakriittisen järjestelmän toteutuksessa, koska tällöin kehitysprojektista ulkopuoliset henkilöt tulevat suorittamaan testaukset ja arvioinnit järjestelmälle. Testaajat voivat olla esimerkiksi lupaviranomaisia, joilla on laaja tuntemus alan säädöksistä sekä mahdollisesti aiemmista vastaavanlaisista toteutuksista. Ulkopuolisen tarkastajan näkemys on tärkeää, koska he voivat esittää huomioita ja kysymyksiä järjestelmään liittyen ja havaita kohteita, joita olisi syytä vielä kehittää. [18, s.36]

3. EHEYSTASOT

3.1 Eheystasoista yleisesti

Turvallisuuden eheystaso on konsepti, joka esiteltiin standardin IEC 61508 kehitysvaiheessa. Turvallisuuden eheystaso asettaa järjestelmälle vaatimukset millä varmuudella sen on kyettävä toimimaan. [19]

Prosessin riskinalttius määrittelee, kuinka luotettavaa riskinvähennykseen käytettävän tekniikan on oltava. Turvallisuuden eheystaso on määritettävä erikseen jokaiselle erilliselle turvatoiminnolle. Turvallisuuden eheydellä tarkoitetaan sitä, että turvatoiminto hyväksyttävästi toteuttaa vaadittavat toiminnot määritellyissä olosuhteissa ja määritellyn ajan. Turvallisuuden eheystason kasvaessa kasvaa myös vaatimus sille, että kyseinen turvatoiminto toimii vaaratilanteessa oikein. Kattostandardissa IEC 61508 on annettu tekniikka- ja menetelmävaatimuksia, jotka ovat sitä vaativampia mitä korkeampi eheystaso on kyseessä. [20]

Turvallisuuden eheydellä on nelitasoinen asteikko, jossa TET 1 on vähimmäisturvallisuusvaatimus ja TET 4 on tiukin. Näitä tasoja käytetään määrittämään turvajärjestelmien suorittamien turvallisuustoimintojen luotettavuusvaatimukset. Turvakriittiselle järjestelmälle määritelty tavoite- eheystaso osoittaa kuinka merkittävät turvallisuusvaatimukset jokaisen turva-automaatiojärjestelmän osan on täytettävä. [19]

Laadullinen näkymä eheystasoista kehittyi hitaasti 90- luvulla kun eheystasot otettiin käyttöön useilla kemian ja petrokemian laitoksilla. Turvallisuusjärjestelmien vikaantumisesta aiheutuneet seuraukset jaettiin tällöin neljään eri tasoon, jotka on esitetty taulukossa 1. [20]

Taulukko 1. *Turvallisuuden eheystasojen kuvaus [20]*

TET	Tason kuvaus
4	Katastrofaalinen vaikutus yhteisöön
3	Vakavia vaikutus työntekijöihin ja yhteisöön
2	Suuria vahinkoja laitteistoon sekä tuotantoon. Työntekijän loukkaantuminen mahdollinen.
1	Pieniä vahinkoja laitteistoon sekä tuotantoon.

3.2 Turvallisuusuhkien määrittäminen

Ennen eheystasojen määrittelyä on selvitettävä, mitkä osuudet systeemistä, prosessista tai toiminnoista ovat potentiaalisia uhkia turvallisuudelle. HAZOP-menetelmä on yksi merkittävistä ja yleisesti käytetyistä analysointimenetelmistä uhkien tunnistamisessa. HAZOP lyhenne tulee englanninkielisestä nimityksestä: A HAZard and OPerability study.

HAZOP- tarkastelu eli poikkeamatarkastelu kehitettiin 1960-luvulla kemianteollisuuden yhdistyksen toimesta. Siitä lähtien menetelmää on sovellettu suunniteltaessa uusia prosesseja ja toimintoja. HAZOP on erinomainen työkalu turvallisuuden, terveyden ja ympäristövahinkojen tunnistamisessa. Tämän lisäksi sitä voidaan käyttää myös potentiaalisten käytettävyyden ongelmien havaitsemiseen. [21, s.1]

HAZOP-menetelmän perinteinen lähestymistapa ongelmaan on jäsennelty aivoriihi, joka toteutetaan ohjesanojen avulla. Aivoriihen toteuttajana toimii monialainen tiimi, joka toteuttaa sen poikkeamien syiden ja seurausten kirjaamiseksi. Oikein toteutettu analyysi varmistaa, että kaikki potentiaaliset poikkeamat suunnittelun todellisesta tarkoituksesta ja prosessin virheistä tulevat ilmi. Aivoriihi-istuntojen perusteella voidaan suunnitella korjaavia toimenpiteitä ei-toivottujen prosessin seurausten tai järjestelmäturvallisuuden eheystason parantamiseksi. On ensisijaisen tärkeää, että aivoriihi-istuntoja koskevat asiakirjat ja suunnitellun toiminnan dokumentaatiot ovat johdon ja viranomaisten tarkasteltavissa. [22, s.4150]

Tavanomainen HAZOP-tutkimus vie kuitenkin paljon aikaa ja aiheuttaa kustannuksia ja kärsii puutteellisuudesta. On huomattu, että HAZOP-tutkimus hyötyy huomattavasti teknologian viimeisten vuosikymmenien kehityksestä. Nykyisin analyysi perustuukin pääosin tietokoneella toteutettuihin simulointeihin ja malleihin. Yhdistelemällä useita malleja saavutetaan vaara-analyysin parempi johdonmukaisuus, kattavuus ja niin edelleen. Neljän viime vuosikymmenen aikana useat tutkimukset ovat keskittyneet parantamaan HAZOP-menetelmiä. Tehokkaan riskinanalyysin kehittämisessä on ollut selkeästi havaittavissa kaksi trendiä: HAZOP: n automatisointi kvalitatiivisten mallien avulla ja HAZOP, jonka tukena on kvantitatiivinen dynaaminen simulointi. [22, s.4151]

Esimerkkinä laajalti käytettävästä kvalitatiivisestä mallintamisesta voidaan pitää monitasoista virtausmallinnusta (MFM). Monitasoinen virtausmallinnus on hierarkkinen rakenteen mallintamismenetelmä, joka perustuu prosessin tavoitteeseen. Tämä lähestymistapa tarkastelee ongelmia materiaalivirtojen, energiavirtojen ja informaatiovirtojen kannalta tarkoituksena kuvata todellista järjestelmää. Käyttämällä joitain spesifejä graafisia

symboleita se kuvaa järjestelmän tavoitteet, toiminnot ja komponentit laitoksen tuotantoprosessin mallintamiseen. [23]

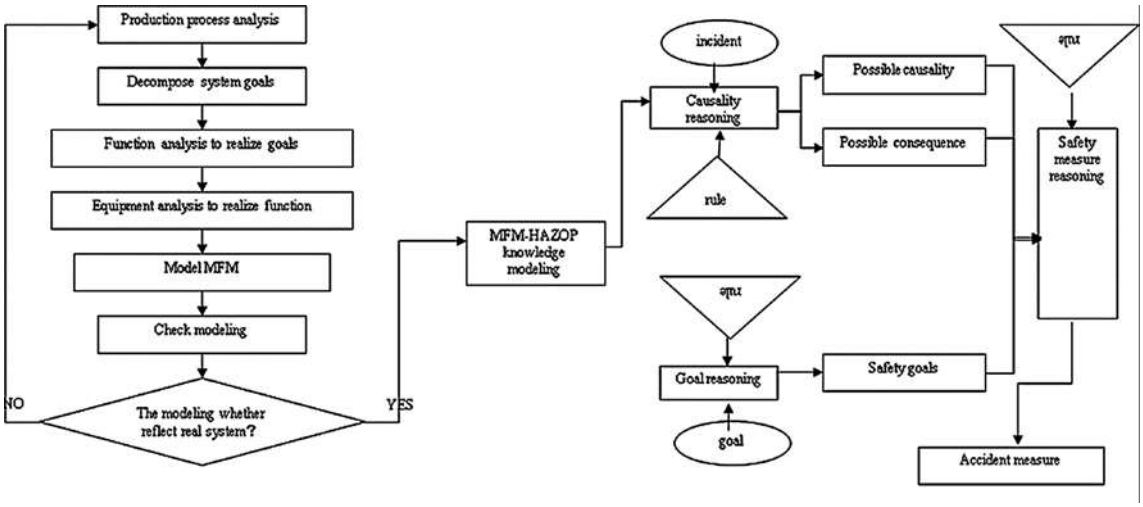
Monitasoinen virtausmalli on laitosmalli, joka voi toimia älykkään järjestelmän HAZOP-tarkastelun keskeisenä ytimenä. Se järjestelmäkuvaus, joka on yleisempi ja vähemmän riippuvainen tietyistä tilanteista tai tapahtumista verrattuna esimerkiksi vikapuihin. Järjestelmien tuntemuksen hankkiminen HAZOP-analyysin avulla vaatii merkittävästi vähemmän töitä kuin vikapuihin perustuvat menetelmät. [24]

Monitasoista virtausmallia luodessa toimitaan usein seuraavien periaatteiden mukaisesti [23]:

Ensimmäisen periaate on mallin luominen mallinnuskohteen tai järjestelmän päätavoitteista. Tämänlaisella ylhäältä alas-menettelyllä voidaan varmistaa, että määriteltävät toiminnot palvelevat järjestelmän päätavoitetta. Menettely soveltuu erityisesti mallintamisjärjestelmille, joissa fyysistä toteutusta ei tiedetä yksityiskohtaisesti tai sitä ei otettu huomioon suunnittelun alkuvaiheessa.

Toinen periaate on yhdistää funktiot tapahtumaan riittävän tarkasti systeemin todenmukaisissa komponenteissa. Nämä toiminnot kootaan sitten yhteen vastaamaan järjestelmän päätavoitteita. Tämä menettely on sopiva, kun välitavoitteet ovat tuntemattomia tai epämääräisesti määriteltyjä. Näin yhdistämällä laitteita prosessin avulla voidaan havaita tarvittavia ylemmän tason toimintoja järjestelmässä, joita ei voi liittää suoraan jo mallinnettuihin komponentteihin tai osajärjestelmiin. Useimmissa tapauksissa nämä kaksi yleistä periaatetta yhdistetään iteratiiviseksi menettelyksi.

HAZOP- menettelyitä käytetään tutkimaan poikkeamia normaalista. Monitasoisessa virtausmallissa funktioiden solmuissa arvojen normaaliarvoille asetetaan rajat ja jos jossakin solmuun vaikuttavassa komponentissa tapahtuu virhe, niin tämä näkyy solmun arvoissa poikkeamana. Näin ollen monitasoisesta virtausmallista voidaan siis toteuttaa HAZOP- tarkasteluun sopiva sovellus [23]. Kuvassa 2 on esiteltynä ohjekaavio MFM-HAZOP-mallin muodostamiseen.



***Kuva 2**. Kuinka muodostaa MFM-HAZOP-malli [23, s.581]*

3.3 Eheystason määrittäminen

Turvallisuuden eheystasot ovat tasoja, jotka perustuvat vikaantumisen todennäköisyyteen (PFD) tietylle turvallisuusinstrumentoidulle toiminnolle. Termillä PFD_{avg} kuvataan todennäköisyyden keskiarvoa sille, että turva-automaatiojärjestelmä ei onnistu estämään vaarallista tilaa. Vikaantumisen todennäköisyysluokat jaetaan neljään eri tasoon standardeissa IEC 61508 ja IEC 61511. [25, s.2]

IEC 61508 määrittelee kaksi tasoa turvallisuuteen liittyville järjestelmille. Toinen on alhaisen vaateen taso (Tyyppi A) ja toinen on suuren vaateen taso tai jatkuvan kysynnän taso (Tyyppi B). Alhaisen vaateen tasolla, joka on yleisesti käytetty mm. kemikaaliteollisuudessa, eheystaso asettaa vaatimukset sekä vikasietoisuudelle, että keskimääräiselle vaarallisen vikaantumisen todennäköisyydelle vaateen ilmetessä (PFD_{avg}) [34]. Taulukossa 2 on esitetty eheystasot määriteltyinä niiden alhaisten ja korkeiden vaatimusten avulla.

***Taulukko 2**. Eheystasot määriteltyinä niiden matalien ja korkeiden vaatimusten avulla [26, s.240].*

	Alhainen vaatimus (Tyyppi A)	Korkea vaatimus (Tyyppi B)
Eheystaso	Keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä (PFD_{avg})	Vikaantumisen todennäköisyys tunnissa (PFH)
1	$[10^{-2}, 10^{-1}]$	$[10^{-6}, 10^{-5}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-7}, 10^{-6}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-8}, 10^{-7}]$
4	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

Eheystaso on keskeinen suunnitteluparametri, joka määrittää riskinvähennyksen, johon turvallisuutta edistävän laitteiston on kyettävä. Ilman eheystason määrittämistä turva-automaatiojärjestelmää ei voida suunnitella oikein, koska muuten vain toiminta on määritelty, mutta potentiaaliset vikaantumiset ja niiden mahdollisesti aiheuttamat seuraukset eivät ole tarkasti tiedossa. Turva-automaatiojärjestelmän oikeaoppisessa suunnittelussa on määriteltävä, kuinka järjestelmä toimii sekä kuinka luotettavasti se pystyy toteuttamaan sille tarkoitetun tehtävänsä. Turvallisuuden eheystaso käsittelee näistä jälkimmäisenä mainittua. Eheystaso ilmoittaa pienimmän vaaditun todennäköisyyden, millä varmuudella järjestelmän on kyettävä suorittamaan onnistuneesti sille asetetut tehtävät. [25, s.2]

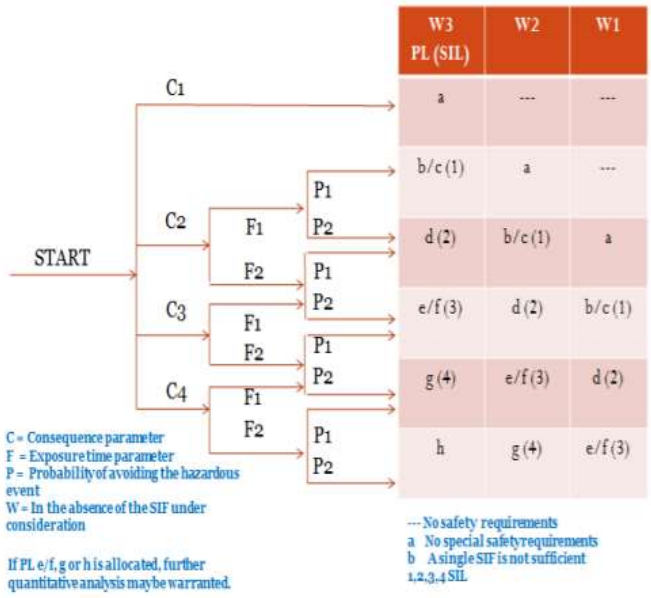
3.3.1 Riskikaaviomenetelmä

Eräs tapa määrittää eheystaso on riskikaaviomenetelmä (risk graph method). Riskikaaviomenetelmä on yleisesti käytetty menetelmä tarvittavan turvallisuuden eheystason määrityksessä. Riskikaaviossa tarkastellaan tapahtuman todennäköisyyttä, seurauksia, käyttöastetta ja todennäköisyyttä, että henkilöstö välttää vaarat. Nämä neljä parametria yhdistetään määrittämään riskien kokonaistaso. [27]

Vaarallisen tapahtuman taajuus koostuu kolmesta vaikuttavasta tekijästä: esiintymistiheydestä ja altistumisajasta, mahdollisuudesta välttää vaarallinen tapahtuma ja vaarallisen tapahtuman todennäköisyys ilman mitään turvallisuutta parantavaa järjestelmää. Näihin pohjautuen on luotu neljä riskiparametria: vaarallisen tapahtuman seuraukset tai vakavuus (C), vaarallisen alueen käyttöaste ja altistumisen taajuus (F), todennäköisyys välttää vaarallinen tapahtuma (P) ja kuinka monta kertaa vuodessa vaarallinen tapahtuma tapahtuisi ilman turvallisuusfunktiota (W). [27]

Suppiloriskikaaviomenetelmä (FRGM) tarjoaa kustannustehokkaan ja yksinkertaisen lähestymistavan turva-automaatiosysteemin suunnitteluun ja arviointiin. Kuvan 1 turvallisuuden elinkaarimallista FRGM keskittyy vaiheeseen 5, eli kokonaisuuden turvallisuusvaatimusten kohdennukseen. Sen sijaan, että käytäisiin kaikki turvallisuusfunktiot yksitellen läpi, kvalitatiivinen FRGM pyrkii tehokkaaseen analysointiin, joka etenee suppilomaisesti tai toimii tarkastelun ”ensimmäisenä vaiheena”. Jos arvioidut turvallisuuteen liittyvät järjestelmät saivat ensimmäisessä tarkastelussa korkeamman eheystasovaatimuksen kuin TET 2, on suoritettava kvantitatiivinen tai puolikvantitatiivinen tarkastelu (Layers of protection analysis (LOPA), vikapuuanalyysi) tuloksen varmistamiseksi. Toinen vaihtoehto on, että monialainen ryhmä toteaa perustellusti tuloksen olevan luotettava. [28, s.12105]

Kuvassa 3 on esiteltynä suppiloriskikaavion rakenne. Suppiloriskikaavion käyttäminen alkaa tarkasteltavan kohteen valinnasta, tämä tapahtuu kaavion kohdassa START. Kun kohde on valittu, arvioidaan parametri C eli vaarallisen tapahtuman seuraukset tai vakavuus. Tässä kuvitteellisessa esimerkkitapauksessa arvioidaan parametriksi C3, jonka jälkeen arvioidaan vaarallisen alueen käyttöastetta ja altistumisen taajuutta eli parametria F, arvioidaan sen olevan F1. Samalla tavoin arvioidaan myös todennäköisyys välttää vaarallinen tapahtuma eli parametri P ja kuinka tiheästi vaarallinen tapahtuma voisi esiintyä ilman turvallisuusfunktiota eli parametri W. Tässä tilanteessa arvioitiin edellä mainittujen parametrien arvoiksi P2 ja W3. Tämä tarkoittaa kaavion mukaan, että tilanteessamme turvallisuuden vaadittava eheystaso olisi TET3.



***Kuva 3**. Suppiloriskikaavio [28, s.12106]*

3.3.2 Vikapuuanalyysi

Suppiloriskikaavion lisäksi eheystason selvittämiseen on myös monia muitakin menetelmiä kuten esimerkiksi vikapuuanalyysi (Fault tree analysis, FTA) ja LOPA. Näistä ensimmäisenä mainittua käytetään usein kvantitatiivisena menetelmänä, koska se näyttää turva-automaatiojärjestelmän syy-seuraus suhteen. Teollisuudessa vikapuuanalyysi on yleisesti käytetty menetelmä järjestelmän turvallisuuden analysoimiseen. Vikapuuanalyysi ilmaisee selkeästi, miten laitevika, toimintavirheet ja ulkoiset tekijät johtavat järjestelmän toimintahäiriöihin. Vikapuuanalyysi perustuu valtaosin ammattilaisten alakohtaiseen tietämykseen ja arviointiprosessi on pääosin manuaalinen eikä automatisoitu. [29]

FTA on systemaattinen ja deduktiivinen prosessi, joka tutkii ja analysoi mahdollisia vikaantumisia ja niiden vaikutusta järjestelmän luotettavuuteen. Vikapuuanalyysi on ”ylhäältä-alas” etenevä lähestymistapa vikatilojen tunnistamiseen ja se toteutetaan käyttäen vikapuu symboleita. Analyysi alkaa siitä, että määritellään vaarallinen vikaantumistapaus. Tämän jälkeen tutkitaan kaikki mahdolliset tapahtumat, jotka voivat johtaa määritellyn vikaantumistapauksen toteutumiseen. Edellä mainitut tapaukset jaotellaan vielä ensisijaisiin tapauksiin, jotka voivat suoraan aiheuttaa määritellyn vikaantumistapauksen ja toissijaisiin tapauksiin, joiden aiheuttama ketjureaktio voi lopulta johtaa määriteltyyn vikaantumistapaukseen. Tämän jälkeen yksittäiset tapahtumasarjat yhdistetään käyttäen sopivia loogisia portteja ja näin saadut loogiset symbolit yhdistetään vielä tarpeiden mukaisesti. Kun kaikki tapahtumasarjat on määritelty ja yhdistetty asianmukaisesti, suoritetaan saadun loogisen mallin avulla tapahtuman todennäköisyyden arviointi. [29]

Suomen standardoimisliitto SFS: n ohjeissa on esitetty vikapuuanalyysin kaltaisista kvantitatiivisista menetelmistä seuraavia huomioita [30, s.42]: ” Menetelmä johtaa tavallisesti mataliin turvallisuuden eheyden tasoihin, koska riskimalli on erityisesti suunniteltu jokaiselle sovellukselle erikseen ja numeerisia arvoja käytetään kuvaamaan jokaista riskitekijää, kalibroiduissa riskigraafeissa käytettyjen numeeristen arvovälien asemesta. Kvantitatiivisissa menetelmissä kuitenkin tarvitaan erityisen riskimallin rakentamista jokaiselle vaaralliselle tapahtumalle. Mallintaminen edellyttää osaamista, työkaluja ja tietämystä sovelluksesta ja sen kehittäminen ja todentaminen voi viedä huomattavasti aikaa.”

3.3.3 Layers of Protection Analysis

Kolmas yleinen tapa määrittä eheystaso on jo aiemmin tässä työssä mainittu LOPA. Se on puolikvantitatiivinen riskinarvioimismenetelmä, joka perustuu suojaaviin kerroksiin, kuten suunniteltuihin turvaominaisuuksiin tai suojajärjestelmiin, joihin tyypillisesti liittyy erityisiä prosessin suunnittelun toteutuksia, prosessilaitteita, hallinnollisia menettelyitä ja käyttöautomaatiota. Nämä kerrokset tai järjestelmät suojaavat välittömiltä vaaroilta, joko automatisoidusti tai ihmisen toimesta. Se on menetelmä, jolla analysoidaan virheitä ja määritetään tarvitaanko turva-automaatiota, ja jos tarvitaan niin menetelmällä tutkitaan tarvittava eheystaso kullekin turva-automaatiojärjestelmälle [27]. Riskien arviointi LOPAlla tapahtuu seuraavasti [31, s.215]:

1. Tunnistetaan tarkasteltavat skenaariot, tähän voidaan käyttää esimerkiksi aiemmin työssä esiteltyä HAZOP- menetelmää. Tarkasteltavien skenaarioiden vaikutuskohde on myös arvioitava, että kohdistuuko vaikutus ihmisiin, ympäristöön,

omaisuuteen tai useampiin näistä. Myös vaikutuksen vakavuus arvioidaan tässä vaiheessa.

2. Listataan kunkin skenaarion aiheuttajat.
3. Arvioidaan aloittavien syiden esiintymistaajuus.
4. Listataan erilliset suojaustasot jokaiselle syy-seuraus parille
5. Määritellään vikaantumisen todennäköisyys jokaiselle itsenäiselle suojaustasolle.
6. Lasketaan tapahtumien esiintymistiheys jokaiselle syy-seurausparille kertomalla aloitustapahtuman taajuus PFD: llä kullekin sovellettavalle itsenäiselle suojakerrokselle.
7. Verrataan tapahtumien esiintymistiheyttä siedettävän riskin kriteereihin. Jos riskikriteerit eivät täyty, voidaan lisätä suojaustasoja, nostaa eheystasoa tai prosessi voidaan suunnitella uudelleen.

Kvalitatiivisella suppiloriskikaaviolla, puolikvantitatiivisella LOPAlla ja kvantitatiivisella vikapuuanalyysillä on jokaisella omat sovelluskohteensa, joissa niiden parhaat puolet nousevat esiin. Vikapuuanalyysi on hyvä työkalu vaativimpien prosessien eheystasojen tarkasteluun sen kvantitatiivisen lähestymistavan vuoksi. Analyysin suorittaminen vaatii kuitenkin paljon aikaa ja osaajia, joilla on syvä tuntemus alasta ja kokemusta vastaavista toteutuksista. LOPA tarjoaa vikapuuanalyysiä kevyemmän analysointiprosessin, mutta varsinkin alhaisen eheystason sovelluksissa senkin käyttäminen voi mennä tilanteeseen nähden liialliseksi tarkasteluksi.

Alhaisten eheystasojen kuten TET 1 ja TET 2 selvittämiseen tehokkain menetelmä on suppiloriskikaavio. Gabriel et al. esittävät artikkelissaan [27] tuloksia tutkimuksestaan, joissa vertailtiin LOPAn ja suppiloriskikaavion eroavaisuuksia. Tutkimuksen mukaan LOPAlla 10 000 turvallisuustoiminnon analysointiin kuluu aikaa 25 000 tuntia. Sen sijaan suppiloriskikaaviolla vastaava lukema on vain 3333 tuntia. Suppiloriskikaavion epätarkempi lähestymistapa ei aiheuta ongelmia, kun kyseessä on TET 0, TET 1 tai TET 2.

4. EHEYSTASON VAIKUTUS ARKKITEHTUURIIN

4.1 Arkkitehtuuriin vaikuttavia asioita

Turvallisuuden eheyden saavuttamiseksi on täytettävä neljä eheystasojen mukana muuttuvaa päävaatimusta, jotta saavutetaan vaadittu riskinvähennys prosesseissa turva-automaation avulla: Laitteiston turvallisuuden eheys (mitattuna epäonnistumisen todennäköisyytenä vaateen sattuessa), järjestelmän toiminta havaitessaan vian, arkkitehtuuriset rajoitukset ja systemaattisten vikojen hallinta. [38, s.2]

- Laitteiston turvallisuuden eheys tarkoittaa laitteiston kykyä hallita satunnaisia vaarallisia vikoja, tämä esitetään PFD arvona.
- Turva-automaatiojärjestelmän pitää pystyä turvalliseen toimintaan vian havaittuaan
- Kaikki rajoitukset valmiista järjestelmän arkkitehtuurista tulee arvioida ja näiden vaikutus turvallisuuden eheyteen tulee dokumentoida. Järjestelmän korkein mahdollinen eheystaso määritellään turvallisten vikaantumisten osuuden ja vikasietoisuuden avulla.
- Systemaattinen turvallisuuden eheys viittaa vikoihin, joita saattaa syntyä järjestelmän kehittämisprosessista, turvafunktion suunnittelusta ja toteutuksesta, mukaan lukien kaikki sen elinkaaren turvallisuuden hallinnan näkökohdat.

IEC 61508 määrittelee kaksi tasoa turvallisuuteen liittyville järjestelmille. Toinen on alhaisen vaateen taso (Tyyppi A) ja toinen on suuren vaateen taso tai jatkuvan kysynnän taso (Tyyppi B). Alhaisen vaateen tasolla, joka on yleisesti käytetty mm. kemikaaliteollisuudessa, eheystaso asettaa vaatimukset sekä vikasietoisuudelle, että keskimääräiselle vaarallisen vikaantumisen todennäköisyydelle vaateen ilmetessä (PFD_{avg}). Vikasietoisuus ilmaisee arkkitehtoniset rajoitteet, mikä tarkoittaa vaatimuksia riittävän vankan arkkitehtuurin saavuttamiseksi. [34]

Arkkitehtoniset rajoitteet estävät turvallisuuteen liittyvien järjestelmien suunnittelijoita ja järjestelmäintegraattoreita valitsemasta arkkitehtuuria pelkästään PFD-laskelmien perusteella, ja vaatimukset voidaan siksi nähdä rajoituksina vapaudelle valita laitteistoarkkitehtuuri. Turva-automaatiojärjestelmän jokaisen osan kohdalla arkkitehtoniset rajoitukset ilmaistaan vikasietoisuudella (Hardware fault tolerance, HFT), joka taas määritetään komponenttien tyypin (tyyppi A tai B), turvallisen vikaantumisen (Safe failure fraction,

SFF) ja määritetyn turvallisuuden eheystason mukaan. SFF on "turvallisten" vikojen osuus kaikista vioista, ja vikasietoisuus ilmaisee vikojen lukumäärän, jotka voidaan sietää ennen kuin turva-automaatiojärjestelmä ei pysty suorittamaan turvallisuusfunktiota. "Turvallinen" vika on joko vika, joka on suunniteltu turvalliseksi, tai vaarallinen vika, joka havaitaan ja korjataan välittömästi. [40]

Eheystason kasvattaminen aiheuttaa turva-automaatiojärjestelmässä lisää vaatimuksia turvallisuuden parantamiseksi. Eräitä yleisesti käytettyjä tekniikoita turvallisuuden ja luotettavuuden parantamiseen ovat redundanssi ja diversiteetti. Redundanssilla tarkoitetaan sitä, että järjestelmässä käytetään enemmän resursseja kuin suorittaminen minimissään vaatisi. Diversiteetti taas tarkoittaa sitä, että toteutuksessa saman asian toteuttamiseen käytetään kahta tai useampaa laitteistoa, joiden on tarkoitus suorittaa sama tehtävä, mutta systemaattisten virheiden vähentämiseksi ne on koottu eri komponenteista. Yleensä redundanssia ja diversiteettiä sovelletaankin samanaikaisesti. Tällöin kaksi tai useampi systeemiä, jotka on rakennettu käyttäen eri komponentteja, algoritmeja, elektroniikkaa, suunnittelumetodeja jne. suorittavat samaa tehtävää. Tämänkaltaisen toteutuksen avulla saadaan vähennettyä yhteisvikaantumisen mahdollisuutta ja systemaattisia vikoja, kuten suunnitteluvirheistä johtuvia vikoja. [32]

Turva-automaatiojärjestelmän arkkitehtuurissa tulee huomioida myös tilanne, jossa järjestelmä tai laite menettää käyttövoimansa. Järjestelmän tärkeät hälytykseen vaikuttavat tulot on syytä toteuttaa lepovirtaperiaatteen mukaisesti. Se on suunnitteluperiaate, jossa komponentin käyttövoiman menettäminen saa aikaan turvalliseen suuntaan vaikuttavan toiminnan [41, s.8]. Lepovirtaperiaatteen toiminta perustuu siihen, että järjestelmän ollessa turvallisessa tilassa, niin kaikki valvontapiirit ovat suljettuja. Jos jokin kytkimistä aukeaa, niin aiheutuu hälytys. Hälytys voi johtaa esimerkiksi järjestelmän alasajoon. [42, s.29]

4.1.1 Vikasietoisuus ja vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä

Toteuttamalla turva-automaatiolaitteisto soveltaen sekä redundanssia että diversiteettiä, saadaan nostettua järjestelmän turvallisten vikaantumisten osuutta, jolloin järjestelmä on vähemmän altis satunnaisille vaarallisille vikaantumisille [32]. Vikasietoisuus ilmaisee vikojen lukumäärän, jotka voidaan sietää ennen kuin turva-automaatiojärjestelmä ei pysty suorittamaan turvallisuusfunktiota [40]. Taulukossa 3 on esitetty, minkälaisia vaatimuksia eheystaso asettaa laitteiston vikasietoisuudelle.

Taulukko 3: Pienin sallittu laitteiston vikasietoisuus (HFT) turvallisuuden eheyden tason (TET) mukaisesti [33, s.65].

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

Vikasietoisuuden lisäksi turva-automaatiojärjestelmän tulee täyttää valitulle eheystasolle määritellyt keskimääräinen vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä (PFD_{avg}) sekä vikaantumisten todennäköisyys tunnissa (PFH), nämä ovat esiteltynä taulukossa 2.

Turva-automaatiojärjestelmän luotettavuuden arvo sarjaan kytketyille (1) ja rinnankytketyille (2) systeemeille voidaan laskea seuraavilla yhtälöillä [35]:

$$PFD_{SYS} = 1 - \prod_{i=1}^{N} PFD_i, \quad (1)$$

jossa

$\boldsymbol{PFD_{sys}}$ = Järjestelmän vikaantumisen todennäköisyys

$\boldsymbol{N}$ = Resurssien tai osajärjestelmien lukumäärä

$\boldsymbol{PFD_i}$ = erään i-elementin epäluotettavuus

$$PFD_{SYS} = \prod_{i=1}^{M} PFD_i, \quad (2)$$

jossa

$\boldsymbol{PFD_{sys}}$ = Järjestelmän vikaantumisen todennäköisyys

$\boldsymbol{M}$ = Resurssien tai osajärjestelmien lukumäärä

$\boldsymbol{PFD_i}$ = erään i-elementin epäluotettavuus

Jos järjestelmässä on sovellettu äänestysperiaatetta, niin tämänkin luotettavuuden laskemiseksi on oma kaavansa:

$$PDF_{sys} = 1 - \prod_{r=M}^{N} \binom{N}{r} (1 - PDF_i)^r (PFD_i)^{N-r}, \quad (3)$$

jossa

$\boldsymbol{PFD_{sys}}$ = Järjestelmän vikaantumisen todennäköisyys

$\boldsymbol{N}$ = Kokonaisresurssien lukumäärä

$\boldsymbol{M}$ = Minimissään vaadittavien resurssien lukumäärä

$\boldsymbol{PFD_i}$ = Todennäköisyys, erään resurssin vikaantumiselle

Jokaisessa kaavassa $\mathrm{PFD_i}$ edustaa vikaantumisen mahdollisuutta vaateen aikana i:nnessä turvafunktion osuudessa. Se voidaan laskea arkkitehtuurien 1oo1, 1oo2, 2oo2 jne. standardikaavoilla (Äänestysperiaatteeseen perustuvasta arkkitehtuurissa on kerrottu tarkemmin luvussa 4.2). Tässä työssä esitetty PFD: n laskentatapa perustuu luotettavuuslohkokaavioihin (Reliability block diagram, RBD) perustuvaan lähestymistapaan. RBD on graafinen esitys vaaditusta toiminnallisuudesta; se osoittaa myös loogisen yhteyden komponenttien välillä, joita tarvitaan tietyn järjestelmän toiminnon tai tehtävän suorittamiseen. Tästä syystä RBD muistuttaa turva-automaatiojärjestelmän fyysistä rakennetta, ja lohkojen sekvenssi voi olla samanlainen kuin komponentin aktivoinnin sekvenssi. Kuvassa 4 on esitetty eräs RBD. Järjestelmän epäluotettavuuden laskeminen voidaan laskea esimerkiksi seuraavasti [35]:

1) Määritellään turvafunktion looginen arkkitehtuuri

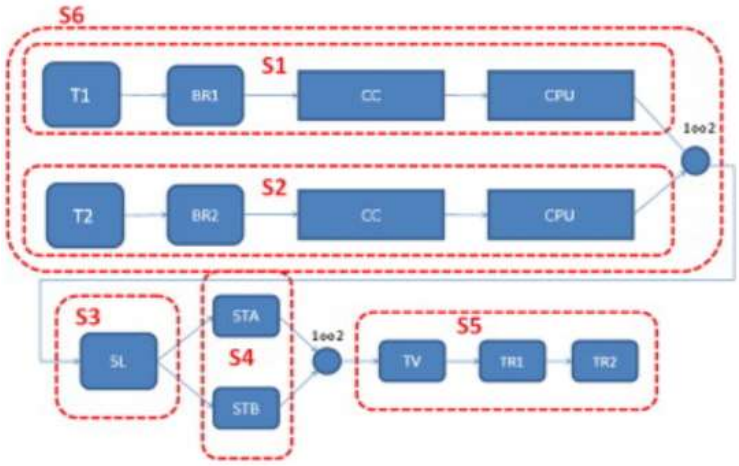
2) Määritellään toimiiko järjestelmä alhaisella vai korkealla vaateella

3) Tunnistetaan kaikki turvafunktion elementit

4) Lasketaan valitun vaateen mukaisesti PFD tai PFH arvot elementtitasolla ottaen huomioon valittu arkkitehtuuri ja hyödyntämällä arkkitehtuurille soveltuvaa standardikaavaa.

5) Ratkaistaan $PFD_{sys} (tai\ PFH_{sys})$ ottaen huomioon loogiset relaatiot elementtien välillä hyödyntäen kaavoja (1), (2), (3) tilanteen tarpeen mukaan.

6) Tarkistetaan taulukosta 2, mikä eheystaso tutkitulla arkkitehtuurilla on mahdollista saavuttaa.



Kuva 4. Esimerkki luotettavuuslohkokaaviosta [35]

4.2 Äänestysperiaate

Laitteiden redundantteja rakenteita on kahden tyyppisiä, yksikanavainen äänestysrakenne ja monikanavainen äänestysrakenne, joka on jaettu yksittäisiin homogeenisiin rakenteisiin ja erilaisiin redundanssirakenteisiin. Erilaiset redundanssirakenteet voidaan valita teollisissa sovelluksissa, koska hyvin suunniteltuna ne voivat parantaa turva-automaatiojärjestelmän turvallisuutta ja toiminnan eheyttä vähentäen samalla yhteisvikaantumisen mahdollisuutta tai parantamalla diagnostista kattavuutta. [36]

MooN (M out of N) määritellään järjestelmäksi, joka koostuu N määrästä yksiköitä (esim. komponentteja, kanavia, jne.), järjestelmässä $M \leq N$ ja M määrä N määrästä yksiköitä riittää toiminnan aloittamisen. Toiminta turva-automaation tapauksessa tarkoittaa turvafunktion suorittamista, kuten esimerkiksi laitoksen alasajoa. Järjestelmä siis vaatii minimissään ennalta määritellyn määrän M yksiköitä ”äänestämään” turvallisuusfunktion suorittamisen puolesta, ennen kuin suoritus aloitetaan. MooN arkkitehtuuri on redundanttinen järjestelmä. [37]

Kuten työssä on jo aiemmin todettu, turvallisuuteen liittyvien järjestelmien tulee olla vikasietoisia, varsinkin vaarallisia vikaantumisia vastaan. Yksi käytetyimmistä tavoista tähän on soveltaa redundanssia rinnankytketyllä rakenteella. Täytyy kuitenkin muistaa, että jokainen järjestelmään lisätty komponentti tuo mukanaan uuden vikaantumisen mahdollisuuden. Tämä nostaa mahdollisuutta esimerkiksi turvatoiminnon (esim. alasajo) tarpeettomaan suorittamiseen, josta voi aiheuta käyttäjälle merkittäviä kustannuksia. Edellä mainittu on osoitus PFD: n ja turvatoimintojen väärien suoritusten välisestä risti-

riidasta. Äänestysperiaatteella toimivat järjestelmät tarjoavat hyvin mahdollisuuksia tämän ongelman ratkaisuun, niillä voidaan hakea sopiva kompromissi sovelluskohtaisesti vikasietoisuuden ja turvatoiminnon turhien suoritusten väliltä. [37]

4.3 Korkeimpien eheystasojen saavutettavuus

Korkeimmat turvallisuuden eheyden tasot TET 3 ja TET 4 asettavat turva-automaatiojärjestelmälle merkittäviä vaatimuksia tarvittavan riskinvähennyksen saavuttamiseksi. On suositeltavaa, että seuraavia vaatimuksia noudatetaan TET 3 ja TET 4 tasoilla toimivien laitteiden yksityiskohtaisessa suunnittelussa: Jäsennelty semiformaali tai formaali suunnittelu, sekä yksinkertaistamismenetelmät, tietokoneavusteisten suunnittelutyökalujen käyttö, defensiivinen ohjelmointi, modulaariset lähestymistavat, suunnittelun ja ohjelmoinnin ohjeistukset sekä jäsennelty ohjelmointi. [39]

Ohjelmistoarkkitehtuurin suunnittelussa semiformaalisten menetelmien käyttäminen on vahvasti suositeltua TET 3 tasosta alkaen. Myös alempia eheystasoja suunnitellessa sen käyttöä suositellaan. Formaaleita suunnittelu- ja tarkennusmenetelmiä suositellaan vahvasti käytettävän TET 4 tason sovelluksissa. Defensiivistä ohjelmointia suositellaan käytettävän turvallisuuden eheyden tasosta 3 alkaen. Defensiivisellä ohjelmoinnilla kehitetään ohjelmat, joiden tarkoituksena on havaita epänormaaleja virtauksia ja tiedonkäsittelyä suorituksen aikana. Havaitessaan jotain normaalista poikkeavaa, ohjelman tulee reagoida siihen ennalta määritetyllä tavalla. [39]

Korkeimpien eheystasojen suunnittelussa diversiteetin käyttö on koettu hyväksi keinoksi systemaattisten virheiden vähentämisessä. Esimerkki systemaattisesta virheestä on tilanne, jossa sama koodikappale antaa jokaisella suorituskerralla virheilmoituksen, vaikka olosuhteet olisivat muuttumattomat. Jos redundantit elementit on toteutettu diversiteetin vaadittua ohjeistusta noudattaen, niin diversiteetti estää systemaattisten vikojen vaikutuksen järjestelmän muihin kanaviin. Diversiteetti tulee toteuttaa aina niin, että suunnittelu, konfigurointi ja valmistus tapahtuu käyttäen eri komponentteja, suunnitteluprosesseja ja eri ryhmän toimesta. Tällä tavoin voidaan varmistaa, että kanavilla on riittävän erilaiset ominaisuudet, käyttäytyminen ja luotettavuus. Tämänlaista erilaistamisprosessia noudattaen on saavutettu merkittäviä parannuksia vaarallisten vikaantumisten havaitsemiseen. Turvallisten vikaantumisten osuus on saatu jopa 99.9 %, joka täyttää TET 3 ja TET 4 tasojen vaatimukset. [38, s.5]

Turvallisuuden eheyden tason 3 sovelluksissa turva-automaatiojärjestelmä on välttämätöntä toteuttaa suojattavasta prosessista fyysisesti erillisenä, tämän lisäksi turva-automaatiojärjestelmässä käytettävistä komponenteista tulee olla minimissään kahden vuoden käyttökokemukset vähintään kymmenestä eri relevantista sovelluksesta. Vaihtoehtoisesti käyttökokemukset voidaan korvata valtuutetun kolmannen osapuolen suorittamilla testauksilla ja testauksien perusteella todetulla hyväksynnällä. Sähköisen datan rajapinta tulee myös olla tarkasti määritelty. TET 4 sovelluksissa turva-automaatiojärjestelmä on välttämätöntä toteuttaa suojattavasta prosessista fyysisesti erillisenä. Tämän lisäksi turva-automaatiojärjestelmän sähköinen tietoliikenne ei saa olla mitenkään yhteydessä suojattavan prosessin tietoliikenteeseen tai toisinpäin. Tämä koskee myös turva-automaatiojärjestelmän redundanttisia osuuksia, nekin täytyy toteuttaa täysin toisistaan riippumattomina. TET 4 sovelluksissa on käytettävä komponentteja, joilla on sekä turvallisuuden eheystasolla 3 vaadittu käyttökokemus, että valtuutetun kolmannen osapuolen hyväksyntä. [7, s.6–7]

5. Yhteenveto

Tässä kandidaatintyössä käytiin turva-automaation esittelyn jälkeen läpi turvallisuuden eheyteen liittyviä asioita, sekä tarkasteltiin mitä vaikutuksia muuttuva turvallisuuden eheystaso aiheuttaa turva-automaatiosovellukseen. Kandidaatintyön pituus on rajallinen, mistä johtuen tämä työ ei ole kattava katsaus esiteltyihin asioihin, vaan pikemminkin yleiskatsaus asioihin, joita tulee ottaa huomioon turva-automaatiosovellusta toteutettaessa. Työhön valikoituneet asiat pohjautuvat työn ohjaajan ehdotuksiin sekä työn kirjoittajan omiin näkemyksiin.

Siitä huolimatta, että työ itsessään on suppea tuotos, niin eheystasoista tai turva-automaatiosta kiinnostunut lukija voi saada siitä hyviä ideoita ja näkemyksiä tiedon tarkempaa etsimistä varten. Työssä on pyritty käyttämään reilusti lähteitä, jotta työ perustuisi mahdollisimman paljon yleisiin havaintoihin, tuloksiin ja ohjeistuksiin. Tällä tavoin työssä on pyritty myös varmistamaan tietojen oikeellisuus ja yleinen hyväksyntä. Täten kirjoitetun sisältönsä lisäksi tämä kandidaatintyö tarjoaa lukijalleen myös johdatuksen useisiin alaan liittyvien artikkeleiden ja kirjallisuuden pariin.

Yhteenvetona työstä voidaan todeta, että turva-automaatiosovellusta suunniteltaessa riskinarviointi on tehtävä todella huolellisesti, jotta saadaan varmasti kaikki järjestelmän potentiaaliset uhkat selvitettyä. Vain huolellisesti suoritettu riskinarviointi antaa edellytykset onnistua eheystason määrityksessä ja tätä kautta myös tarpeen mukaisen turva-automaatiosovelluksen toteutuksessa. Eheystasoja selvitettäessä on syytä tilannekohtaisesti arvioida, lähteekö asiaa ratkaisemaan kvantitatiivisin metodein vai kvalitatiivisesti. Kvantitatiivisten menetelmien käyttöä on syytä harkita varsinkin, jos kyseessä on vaativan, oletettavasti korkean turvallisuuden eheyden tason prosessin suojaaminen.

Turva-automaatiosovelluksen arkkitehtuurin määrittämiseen ei ole olemassa yhtä oikeaa ohjeistusta, jonka mukaan rakenne tulisi valita. Arkkitehtuuriin on sen sijaan olemassa käyttökokemuksiin ja testauksiin perustuvia ratkaisumalleja, joiden noudattamista ja soveltamista suositellaan turva-automaatiosovellusta toteutettaessa. Standardissa IEC 61508 esitellään ohjelmistoarkkitehtuurin suunnitteluun tekniikoita ja toimenpiteitä, joita suositellaan/ei suositella käytettäväksi turva-automaatiosovelluksessa kullakin eheystasolla.

Kasvava eheystaso aiheuttaa muutoksia turva-automaatiosovelluksen vaatimuksiin, jotka turva-automaatiosovelluksen on kyettävä täyttämään. Nämä ovat tarkemmin esi-

teltynä luvussa 4, mutta laitteiston turvallisuuden eheys, järjestelmän toiminta havaitessaan vian, arkkitehtuuriset rajoitukset ja systemaattisten vikojen hallinta asettavat turva-automaatiojärjestelmälle vaatimukset, jotka on täytyttävä, jotta turva-automaatiosovelluksen voidaan katsoa vastaavan eheystasolle asetettuja vaatimuksia.

LÄHTEET

[1] Turva-automaatio prosessiteollisuudessa, Tukes, 2007, saatavissa: https://tukes.fi/documents/5470659/6409383/Turva-automaatio+prosessiturvallisuudessa/e159a62f-a1c2-4de9-a063-7050349d5081/Turva-automaatio+prosessiturvallisuudessa.pdf?version=1.0

[2] P.V. Srinivas Acharyulu, P.Seetharamaiah, A framework for safety automation of safety-critical systems operations, Elsevier Science & Technology, 2015, pp.133–142, saatavissa: https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0925753515000752?via%3Dihub#s0005

[3] N. Möller, S.O. Hansson, J-E. Holmberg, C. Rollenhagen, Handbook of Safety Principles, John Wiley & Sons, Incorporated, 2018, pp.196–234, saatavissa: https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=5216287#

[4] H. Gall, Functional Safety IEC 61508 / IEC 61511

The Impact to Certification and the User, IEEE, 2008, pp.1027–1031, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4493673

[5] IEC/TR 61508-0:fi Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0: Toiminnallinen turvallisuus ja IEC 61508, Suomen standardisoimisliitto, Helsinki, 2011.

[6] SFS-EN 61508-1 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset, Suomen standardisoimisliitto, Helsinki, 2011.

[7] D.J. Smith, K. G. L. Simpson, The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance, Elsevier Science & Technology, 2016, saatavissa: https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=4625970#

[8] Z. E. Bhatti, P. S. Roop, R. Sinha, Unified Functional Safety Assessment of Industrial Automation Systems, IEEE, 2016, pp.17–26, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7569078

[9] G. Schuster, Improving Manufacturing Performance, Professional safety, 2012, saatavissa: https://search.proquest.com/openview/27a500174686204c49bb0fa6130e4d26/1?pq-origsite=gscholar&cbl=47267

[10] W. Kastner, T. Novak, Functional safety in building automation, IEEE, 2009, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5347168

[11] T. Novak, A. Treytl, Functional Safety and System Security in Automation Systems-A Life Cycle Model, IEEE, 2008, pp.311–318 saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4638412

[12] L. Ocheana, D. Popescu, G. Florea, Integrating versus Interfacing Safety and Security with Process Control System, IEEE, pp.441–447, 2013, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6569303

[13] T. Sangsuwan, T. Thepmanee, A. Julsereewong, Safety and Availability of Basic Process Control Using Foundation Fieldbus with Control in the Field – An Experimental Analysis, International Journal of Intelligent Engineering and Systems, pp.135–146, 2016, saatavissa: http://www.inass.org/2017/2017083115.pdf

[14] A. E. Summers, Safety Controls, Alarms, and Interlocks as IPLs, AIChE, pp.186–194, 2014, saatavissa: https://aiche.onlinelibrary.wiley.com/doi/epdf/10.1002/prs.11646

[15] L. Fang, Z. Wu, L. Wei, J. Liu, Design and Development of Safety Instrumented System, IEEE, pp.2685–2690, 2008, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4636627

[16] M. Rausand, Reliability of Safety-Critical Systems: Theory and Applications, Somerset: John Wiley & Sons, Incorporated, 2014, saatavissa: https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=1637653#

[17] X. Jia, L. Xing, G. Li, Copula-based reliability and safety analysis of safety-criticalsystems with dependent failures, Wiley Subscription Services, Inc, pp.928–938, 2018, saatavissa: https://onlinelibrary-wiley-com.libproxy.tuni.fi/doi/epdf/10.1002/qre.2301

[18] X. Ge, R.F. Paige, J.A McDermid, An Iterative Approach for Development of Safety-Critical Software and Safety Arguments, IEEE, pp.35–43, 2010, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5562808

[19] A. Gabriel, C. Ozansoy, J. Shi, Developments in SIL determination and calculation, Elsevier Science & Technology, pp.148–161, 2018, saatavissa: https://www.sciencedirect.com/science/article/pii/S0951832017311171?casa_token=heC0qoT-QKZAAAAAA:HT_tdc3xsdmXVJB8mzwHKF6FL0mqzzr7fQ3o6GKT3jRmG5KHttWx7ovZYTE1y2X2OyTmpAMbUw

[20] A.E. Summers, Techniques for assigning a target safety integrity level, Elsevier Science & Technology, pp.95–104, 1998, saatavissa: https://www.sciencedirect.com/science/article/pii/S001905789800010X?casa_token=bJFWrofPMUIAAAAA:eKaOsvujs-gOL-ZApTZIpPujx_ZuGIDgQaGj-6jO0vn-IhP5Np0iVyyeygkZcY9QPwmpUHJNe8Q

[21] F. Crawley, B. Tyler, HAZOP: Guide to Best Practice, Elsevier Science & Technology, 2015, saatavissa: https://books.google.fi/books?hl=en&lr=&id=XXjMBgAAQBAJ&oi=fnd&pg=PP1&dq=HAZOP&ots=9g-W0OyITw&sig=yx3K7de7t_xyCqZMsozev7WRHQI&redir_esc=y#v=onepage&q=HAZOP&f=false

[22] J. Wu, L. Zhang, J. Hu, M. Lind, X. Xhang, S. B. Jørgensen, G. Sin, N. Jensen, An Integrated Qualitative and Quantitative Modeling Framework for Computer-Assisted HAZOP Studies, AIChE, pp.4150–4173, 2014, saatavissa: https://aiche.onlinelibrary.wiley.com/doi/epdf/10.1002/aic.14593

[23] J. Wu, L. Zhang, W. Liang, J. Hu, Failure Mode Analysis Based on MFM-HAZOP Model of Gathering System, Springer London, 2013, saatavissa: https://link-springer-com.libproxy.tuni.fi/content/pdf/10.1007%2F978-1-4471-4993-4.pdf

[24] J. Hu, L. Zhang, Z. Cai, Y. Wang, An intelligent fault diagnosis system for process plant using a functional HAZOP and DBN integrated methodology, Elsevier Science & Technology, pp.119–135, 2015, saatavissa: https://www.sciencedirect.com/science/article/pii/S0952197615001323

[25] E.M. Marszal, E.W. Scharpf, Safety Integrity Level Selection, ISA – The Instrumentation, Systems, and Automation Society, 2002, saatavissa: https://downloads.oilprocessing.net/data/documents/Safety-Integrity-Level-Selection-Systematic-Methods-Including-Layer-of-Protection-Analysis.pdf

[26] M. Sallak, C. Simon, J-F. Aubry, A Fuzzy Probabilistic Approach for Determining

Safety Integrity Level, IEEE, pp.239–248, 2002, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4358822

[27] A. Gabriel, C. Ozansoy, J. Shi, Developments in SIL determination and calculation, Elsevier Science & Technology, pp.148–161, 2018, saatavissa: https://www.sciencedirect.com/science/article/pii/S0951832017311171?casa_token=heC0qoT-QKZAAAAAA:HT_tdc3xsdmXVJB8mzwHKF6FL0mqzzr7fQ3o6GKT3jRmG5KHttWx7ovZYTE1y2X2OyTmpAMbUw

[28] A. Gabriel, J. Shi, C.Ozansoy, A Proposed Alignment of the National Institute of-Standards and Technology Framework with the Funnel Risk Graph Method, IEEE, pp. 12103–12113, 2017, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7954946

[29] Y. Lee, J. Kim, J. Kim, I. Moon, A Verification of Fault Tree for Safety Integrity Level Evaluation, IEEE, s.5548–5551, saatavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5334238

[30] SFS-EN 61508-5 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tason määrittämiseksi, Suomen standardisoimisliitto, Helsinki, 2011.

[31] A.M. Dowell III, Layer of protection analysis and inherently safer processes, John Wiley & Sons, pp.214–220, saatavissa: https://aiche.onlinelibrary.wiley.com/doi/epdf/10.1002/prs.680180409

[32] L. Dong, H. Wang, J. Jiang, A. Xu, SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram, Elsevier Science & Technology, pp.170–187, 2017, saatavissa: https://www.sciencedirect.com/science/article/pii/S0951832016301880?casa_token=q_gsS0R9IdcAAAAA:e5KKl7BDyv6QDLk_scY8pMSVJbO4AuQ2lsLlLHMnGOwsfRBrS42skO7mY74Dqmive0zWmPdT3g

[33] Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset, SFS-EN 61511-1:2017, SFS, 2017.

[34] Y. Shu, J. Zhao, A simplified Markov-based approach for safety integrity level verification, Elsevier Science & Technology, pp.262–266, 2014, saatavissa: https://www.sciencedirect.com/science/article/pii/S0950423014000515?casa_token=PIMCAZWw_0wAAAAA:We-10X5NAylKofV2bX2FYkzoKdq7c8zvj19EDL3YiB0-0P9MlrzY9j2fmOapIDhscjlDeod3ZA

[35] M. Catelani, L. Ciani, V. Luongo, A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application, Elsevier Science & Technology, pp.1503–1507, 2011, saatavissa: https://www.sciencedirect.com/science/article/pii/S002627141100309X?casa_token=W8UsgPBAZXsAAAAA:LCE8V1E8MOVRuCNe2-sDFQJke_GrKADTPD4YG3QcdXJQrmboNAd4P3nmpPLCsBlTez9mDdOtzg

[36] J. Fu, H. Li, Y. Chi, J. Zhen, X. Xu, nSIL Evaluation and Sensitivity Study of Diverse Redundant Structure, Elsevier Science & Technology, 2021, saatavissa: https://www.sciencedirect.com/science/article/pii/S095183202100079X

[37] A.C. Torres-Echeverría, S. Martorell, H.A. Thompson, Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing, Elsevier Science & Technology, 2011, saatavissa: https://www.sciencedirect.com/science/article/pii/S0951832010002516?casa_token=JD1OoYEd8zkAAAAA:43-JsGR0gczmSa0PQl5_Y-oP2FtymB-gMPiicqSnG9nwRfyGXnoA_aOM_wNhZN5k-OmPq177xA

[38] E.C. Ramirez, Diverse redundancy used in SIS technology to achieve higher

safety integrity, ABB Inc, 2008, saatavissa: https://www.controlglobal.com/assets/assets/abb_wp_diverse_redundancy.pdf

[39] S. Andrulyte, J. Börcsök, Comparisation of the software requirements in safety related cases According to IEC 61508, University of Kassel, pp.232–239, saatavissa: http://www.wseas.us/e-library/conferences/2013/Budapest/CSECS/CSECS-33.pdf

[40] M.A Lundteigen, M. Rausand, Architectural constraints in IEC 61508: Do they have the intended effect?, Elsevier Science & Technology, 2009, saatavissa: https://www.sciencedirect.com/science/article/pii/S0951832008001774?casa_token=p4qSeyEXYC0AAAAA:4IrPzpwCcN8RHd7hzmp-NFOWTgLjLWD4Lg46TcWJJ7b6gZGCnixUnRHNLEkKlli-hu5W90bhb6Q

[41] Releiden käyttö rautatieturvalaitetekniikassa, Liikennevirasto, 2013, saatavissa: https://julkaisut.vayla.fi/pdf3/lop_2013-05_releiden_kaytto_web.pdf

[42] Varoituslaitosten tekniset toimitusehdot, Liikennevirasto, 2012, saatavissa: https://julkaisut.vayla.fi/pdf3/ohje_2012_varoituslaitosten_tekniset_web.pdf