jamk

TLJ-elinkaarimalli ja sen dokumentointi prosessiteollisuudessa

Tuomas Anttila

Opinnäytetyö, AMK
Toukokuu 2024
Sähkö- ja automaatiotekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Anttila, Tuomas

TLJ-elinkaarimalli ja sen dokumentointi prosessiteollisuudessa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2024, 47 sivua.

Sähkö- ja automaatiotekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tuotantolaitosten prosessit sisältävät riskejä, joiden pienentämiseksi pelkkä luontaisesti turvallinen suunnittelu ei ole riittävää. Tällöin on tarpeellista käyttää turva-automaatiojärjestelmiä, joiden suunnittelukäytänteitä ohjaa turva-automaation elinkaarimalli. Elinkaarimalli sisältää joukon menetelmiä ja käytänteitä, joita noudattamalla laitoksen turvallinen käyttö ja vaatimustenmukaisuus voidaan todentaa. Turvajärjestelmien suunnittelun ja käytön aikana syntyy mittava määrä dokumentteja, joiden hallinta on haasteellista mutta välttämätöntä. Toimeksiantaja PCS-Engineering Oy:llä havaittiin tarve elinkaarimallin mukaisen dokumentoinnin valmiuksien kehittämiselle.

Opinnäytetyö toteutettiin tutkimuksellisen kehittämistyön menetelmien mukaisesti ratkaisukeskeisesti. Tavoitteena oli havaita ne turvallisuuteen liittyvien järjestelmien suunnittelun osa-alueet, joiden dokumentointiin ei ollut valmistauduttu perusteellisesti. Samalla tuli selvittää, oliko tarvetta jatkokehittää jo olemassa olleita dokumenttipohjia. Tietoperustassa käsiteltiin toiminnallista turvallisuutta ja IEC 61508- ja IEC 61511-standardien vaatimuksia turvallisuuden eheyden ja elinkaaren vaiheiden dokumentoinnin suhteen.

Dokumentaation tilan ja turva-automaatioon liittyvien projektien vaateiden perusteella voitiin laatia dokumenttipaketti, joka antaa toimeksiantajalle paremmat valmiudet turva-automaatiojärjestelmien elinkaaren hallintaan. Tuotetuilla dokumenttipohjilla myös voidaan suorittaa myös prosessin riskianalyysi ja turvatoimintojen eheystasojen määritys.

Avainsanat (asiasanat)

Prosessiteollisuus, toiminnallinen turvallisuus, elinkaarimallit, dokumentointi

Muut tiedot (salassa pidettävät liitteet)

Liitteet 1-5 ovat salassa pidettäviä, ja niitä ei esitetä julkisessa työssä. Salassapidon peruste on Julkisuuslain 621/1999 24§, kohta 17 ja 20, yrityksen liike- tai ammattisalaisuus sekä kohta 20, teknologista taikka muuta kehittämistyötä ja niiden arviointia koskevat tiedot. Salassapitoaika on kaksikymmentä (20) vuotta, salassapito päättyy 30.5.2044.

jamk

Description

Anttila, Tuomas

Documenting the safety life cycle in process industries

Jyväskylä: JAMK University of Applied Sciences, May 2024, 47 pages.

Degree Programme in Electrical and automation engineering. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Industrial plant processes entail risks, for which simply designing inherently safe systems is not sufficient to reduce. Therefore, it is necessary to use safety automation systems, whose design practices are defined by the safety lifecycle model. The lifecycle model includes a set of methods and practices by which the safe operation and compliance of the plant can be verified. During the design and operation of safety instrumented systems, a considerable amount of documentation is created. Management of these documents is challenging but necessary. The client, PCS-Engineering Oy, identified the need to develop capabilities for documentation according to the safety life cycle model.

Thesis was carried out in accordance with the methods of research-based development while focusing on creating a solution. The objective was to identify areas of safety-related systems design where documentation had not been thoroughly prepared. Simultaneously, it was necessary to determine if there was a need to develop the existing document templates. The theoretical framework addressed functional safety and the requirements of the IEC 61508 and IEC 61511 standards regarding safety integrity and the documentation of life cycle phases.

Based on the state of the documentation and requirements of safety-related projects, a document package was created to provide the client with better readiness for managing the lifecycle of safety instrumented systems. Produced document templates can also be used to perform risk analysis of the process and to determine the required safety integrity levels of the safety instrumented functions.

Keywords/tags (subjects)

Process industry, functional safety, life cycle models, documentation

Miscellaneous (Confidential information)

Attachments 1-5 are confidential and are not presented in the public work. The basis for confidentiality is Act on the Openness on Government Activities 621/1999 sections 17 & 20 & 35. Confidentiality period is agreed to be twenty (20) years. Confidentiality ends at 30.5.2044.

Sisältö

Kuviot

Taulukot

1 Johdanto

1.1 Turvallisuus lähtökohtana

Onnettomuuksien välttämisen tulisi olla kaiken suunnittelun taustalla. Turvallisuuden merkitys teollisuussektorilla on erittäin suuri, sillä onnettomuuden tapahtuessa voidaan puhua merkittävistä haitoista niin ihmisisten terveydelle, materiaalille kuin ympäristölle. Riski onnettomuudelle on aina olemassa, mutta sitä voidaan pienentää monilla eri hallintatoimilla suunnitteluprosessin ja laitoksen käytön aikana. *Toiminnallinen turvallisuus* käsitteenä kuvaa toimintatapoja, joilla mainittua riskiä on mahdollista pienentää ja hallita. (Functional Safety Overview n.d.)

Iso-Britannian työsuojeluhallinto HSE:n tekemän tutkimuksen mukaan 44 % ohjausjärjestelmiin liittyvistä onnettomuuksista johtuu virheellisestä määrittelystä, 20 % käyttöönoton jälkeisistä muutoksista, ja 15 % vajavaisesta huollosta tai virheellisestä käytöstä. Määrittelyvaiheen yleisimpiä ongelmia olivat joko puutteellinen vaara-analyysi, tai jo ennalta havaittujen vikaantumistapahtumien vaikutusten virhearviointi. Onnettomuuksien juurisyynä ei siis useimmiten ole epämääräinen ja tunnistamaton poikkeama prosessissa, vaan suunnitteluprosessissa esiintyvät virheet, jotka ovat vältettävissä noudattamalla systemaattisesti hyviä käytänteitä koko suunnittelun elinkaaren ajan. (Out of control 2003, 31, 33.)

Toiminnallista turvallisuutta käsittelevät standardit, kuten IEC 61508 ja IEC 61511 ovat merkittävässä roolissa ohjatessaan prosessiteollisuuden suunnittelu- ja valmistuskäytänteitä turvalliseen suuntaan. Nämä standardit esittelevät turva-automaation elinkaarimallin, joka kattaa koko turvallistamisen konseptin vaiheet esisuunnittelusta turva-automaatiojärjestelmien ylläpitoon ja käytöstä poistamiseen asti.

1.2 Työn lähtökohdat

Opinnäytetyön tavoitteena oli tuottaa toimeksiantaja PCS-Engineering Oy:n käyttöön dokumenttipohjia turva-automaatiojärjestelmien elinkaaren hallintaa varten. Yrityksestä löytyi

osaamista turvallisuuteen liittyvien järjestelmien suunnitteluun ja toteutukseen, mutta koko elinkaaren vaiheet kokoava dokumenttipaketti havaittiin puuttuvan. Ennestään löytyviä dokumentteja ovat muun muassa laskenta- ja raporttipohjat turvatoimintojen verifiointiin, turva-automaatiojärjestelmään tehtäviin muutoksiin ja tehdastestiä varten.

Työssä perehdyttiin elinkaarimallin ja erityisesti sen noudattamisen todentamiseen dokumentaation avulla, eri lähestymistapoihin riskien ja vaarojen arviointiin, ja yleisesti toiminnalliseen turvallisuuteen sekä sen hallintaan prosessiteollisuudessa. Työ toteutettiin tutkimuksellisen kehittämistyön menetelmin. Työn toteuttamisen keskeisimmät kysymykset liittyivät elinkaarimallin vaiheiden sisältöön ja soveltamiseen:

- Mitä dokumentaation sisällöltä vaaditaan missäkin vaiheessa suunnitteluprosessia, jotta toiminnallisen turvallisuuden hallinta voidaan todentaa?
- Mitä dokumentteja toimeksiantajalla on jo ennestään käytössä, ja kuinka niitä tulisi kehittää?
- Mikä on toimeksiantajan kannalta otollisin menetelmä elinkaarimallin soveltamiseksi? Mitä menetelmää olisi soveliainta käyttää riskien arviointiin, entä turvatoimintojen eheystasojen määrittelyyn?

1.3 Aiheen rajaus

Aihe rajattiin IEC-standardien mukaiseen elinkaarimalliin ja toiminnalliseen turvallisuuden todentamiseen dokumentaation kautta. Rajauksen perusteena olivat toimeksiantajan pääasiallinen toimiala, sisältöön liittyvät toiveet sekä yrityksestä jo ennestään löytyvä kokemus IEC:n turvastandardien mukaisesta suunnittelusta turva-automaation osalta. Koneturvallisuutta koskevat standardit ja räjähdysvaarallisia tiloja koskevat ATEX-laitedirektiivit ovat myös tärkeitä laitosten turvallistamisen kannalta, mutta niiden osuus rajattiin työn ulkopuolelle. Työssä ei myöskään käsitelty sovellusohjelmien rakennetta, eikä turvatoimintoihin osallistuvien laitteiden malleja tai teknisiä ominaisuuksia spesifisti.

1.4 PCS-Engineering Oy

Työn toimeksiantaja PCS-Engineering Oy on Oulussa 2004 perustettu sähkö -automaatioalan palveluita tarjoava insinööritoimisto. Yrityksen toimipisteet sijaitsevat Kempeleessä, Jyväskylässä, Seinäjoella ja Rovaniemellä. Palvelut sisältävät niin projektinhoitopalvelut, suunnittelutyöt, asennusvalvonnan sekä laite- ja järjestelmätoimitukset käyttöönottoineen. Tärkeimpiä toimialoja ovat paperi- ja selluteollisuus sekä energia-, metalli- ja kaivosteollisuus. Yrityksellä on käytössä ISO 9001:2015 ja ISO 45001:208 -laatujärjestelmäsertifikaatteihin pohjautuva johtamisjärjestelmä. (PCS-Engineering Oy 2024.)

PCS-Engineering Oy:n liikevaihto 2022/12 tilikautena oli noin 5,9 miljoonaa euroa, josta liikevoittoa oli 874 000 €. Henkilöstömäärä yrityksessä on yli 55 henkilöä. Yritykselle on myös myönnetty vuodesta 2017 alkaen korkein AAA-luottoluokitus. (PCS-Engineering Oy 2024.)

2 Lainsäädäntö ja prosessiturvallisuus

Turvallisuus- ja kemikaaliviraston tuottaman, prosessiturvallisuutta käsittelevän oppaan mukaan useat lakisäädökset koskevat prosessiteollisuuden turva-automaatiojärjestelmiä. Näihin lukeutuvat erityisesti kemikaaliturvallisuuslaki, painelaitelaki sekä valtioneuvoston asetus vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista. (Turva-automaatio prosessiteollisuudessa 2021, 5-6.)

Kemikaaliturvallisuuslain § 10:n mukaan toiminnanharjoittajan on ryhdyttävä kaikkiin tarpeellisiin toimiin onnettomuuksien ehkäisemiseksi, sekä rajoitettava niiden seurauksia niin ihmisten terveydelle, ympäristölle ja omaisuudelle. Lisäksi toimintalaitoksiin tehtävät muutokset ovat tehtävä turvallisuutta vaarantamatta. Tuotantolaitoksen laitteiden on myös oltava siten suunniteltuja, mitoitettuja ja sijoitettua, että käytön tai ennakkoon havaitut poikkeustilanteet eivät aiheuta henkilö-, ympäristö-, tai omaisuusvahinkoja. Myös laitteiden sijoittelun on oltava sen mukainen, että niiden huoltaminen, tarkastukset ja käyttäminen ovat mahdollista. (Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta 2005/390 § 10, § 13).

Painelaitteita koskevassa lainsäädännössä määrätään, että turvallisten suunnittelu-, valmistus-, käyttö- ja tarkastusperiaatteiden lisäksi painelaitteessa on oltava riittävät laitteet ja laitejärjestelmät varmistamassa käyttöturvallisuutta. Ensimmäisessä määräaikaistarkistuksessa on tarkastettava suojaus- ja lukitustoiminnot suorittavan automaatiojärjestelmän asianmukaisuus. Muutostarkastus on tehtävä ennen uutta käyttöönottoa painelaitteelle, *jonka käyttöturvallisuuteen vaikuttavia laitteita tai laitejärjestelmiä on merkittävästi muutettu.* (Painelaitelaki 2016, § 5 & 55 & 61).

Miten toiminnanharjoittajat voivat todentaa, että suunniteltu turva-automaatiojärjestelmä täyttää muun muassa edellä mainitut vaatimukset? Tukesin mukaan tämä on todennettavissa siten, että suunnittelu on toteutettu standardissa IEC 61511-1 esiteltyä turva-automaatiojärjestelmän elinkaaren vaiheita, ja niihin sidottuja vaatimuksia noudattaen. (Turva-automaatio prosessiteollisuudessa 2021, 6.)

3 Vaatimuksenmukaisuus ja standardit

Tuotteiden ja palveluiden tekijöiden vastuualueelle kuuluu lakien, säädösten ja asetusten noudattaminen siten, että tuotteet ovat turvallisia käyttää. Näiden noudattamista kutsutaan vaatimuksenmukaisuudeksi, joka voidaan usein täyttää noudattamalla sopivaa standardia. Tietyissä tapauksissa vaatimuksenmukaisuutta voi olla arvioimassa kolmas osapuoli. Esimerkiksi prosessiteollisuudessatoiminnallista turvallisuutta ja vaatimusten noudattamista arvioidaan riippumattoman osapuolen toimesta. (Standardi, sertifikaatti ja CE-merkintä – tunne erot ja yhtäläisyydet, 2023; Painelaitteiden prosessiturvallisuuden todentaminen n.d.)

Standardit lisäävät myös tuotteiden tuotteiden ja palveluiden yhteensopivuutta ja laatua, ja niiden noudattamisen vaikutus yritysten toiminnalle on myönteinen niin kilpailukyvyn kuin tuottavuuden kannalta. Neimalan (2023) mukaan standardoinnilla on merkittävä rooli EU:n kilpailukyvyn ylläpidossa ja kasvattamisessa globaaleilla markkinoilla, ja hän mainitseekin standardisoinnin tehostamisen yhdeksi EU:n nykyisistä tavoitteista. Standardisoinnin arvoa tukee *The Influence of Standards on the Nordic Economies* (2018) -tutkimus, jonka mukaan 85 % vastanneista yrityksistä olivat yhtä mieltä, että standardien käyttö kasvattaa asiakkaiden luottamusta yrityksen

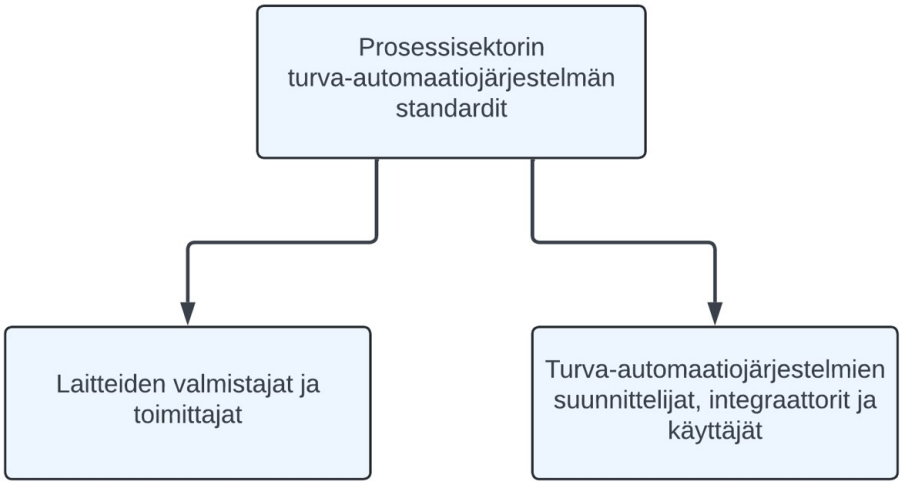
toimintaan. Tärkeimpiä syitä standardien implementoinnille olivat markkinoille pääsyn helpottaminen (34 %), tuotteen tai palvelun laadun kehittäminen (32 %) ja riskin pienentäminen (26 %).

Toiminnallista turvallisuutta käsitteleviä standardeja julkaisee useat eri organisaatiot. Kansainvälisistä organisaatioista ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) ovat julkaisseet niin yleisten suunnitteluperiaatteiden lisäksi toimiala- ja prosessikohtaisia standardeja, jotka käsittelevät esimerkiksi teollisuuspolttimien, raideliikenteen ja ajoneuvojen suunnitteluun liittyviä vaatimuksia.

3.1 IEC 61508

Standardisarja IEC 61508 on sähköisten, elektronisten tai ohjelmoitavien laitteiden toiminnallisen turvallisuuden elinkaareen keskittyvä julkaisu. Se käsittelee ensisijassa sähköisillä, elektronisilla tai ohjelmoitavilla turvallisuuteen liittyvillä järjestelmillä toteutettavien toimintojen vaatimuksia laitevalmistajien näkökulmasta. Standardin osia voidaan myös järjestelmien suunnittelijoiden toimesta, esimerkiksi jos sovellusalakohtaista standardia ei ole olemassa. Se soveltuu myös yleiseksi perustaksi turvallisuuden elinkaaren arvioinnille. (IEC-TR 61508-0, 22.)

IEC 61508:n osat 1-4 ovat perustavia turvallisuusjulkaisuja, joita IEC:n tekniset komiteat käyttävät pohjana valmistellessaan sovelluskohtaisia standardeja. Näitä ovat esimerkiksi prosessiteollisuussektoria käsittelevä IEC 61511, sekä ydinvoimaloiden instrumentointi- ja ohjausjärjestelmien vaatimuksia käsittelevä IEC 61513. Tärkeä huomio sovelluskohtaisista standardeista ja niiden soveltamisesta on se, että niiden myötä käyttäjien ei tarvitse enää ottaa erikseen huomioon IEC 61508 -standardijulkaisua. (IEC-TR 61508-0, 22.)



Kuvio 1: IEC 61511:n ja IEC 61508:n käyttäjät (SFS-EN 61511-1:2017, 12, muokattu)

3.2 IEC 61511

IEC 61511 -sarja käsittelee prosessiteollisuussektorin turva-automaatiojärjestelmiä, vaaran- ja riskinarviointia. Sarjassa esitellään kaksi tärkeää konseptia, turvallisuuden eheystasot (SIL) sekä turva-automaation turvallisuuden elinkaarimalli, joka käsittää vaiheet konseptista suunnitteluun ja käytöstä poistoon asti. IEC 61511-1 on ohjeellinen standardi, joka esittelee yleisiä vaatimuksia ja tavoitteita turva-automaatiojärjestelmän suunnitteluprosessin eri vaiheille. Myös aiheen termistö, sekä IEC 61511 ja IEC 61508 -standardien välinen suhde esitellään tässä osassa. (SFS-EN 61511-1:2017, 8)

IEC 61511-2 puolestaan tarjoaa ohjeita ja käytänteitä ensimmäisen osan soveltamiseen, sisältäen opastuksia ja käytännöllisiä esimerkkejä sisältäviä liitteitä. Esimerkiksi liitteessä F kuvataan esimerkkiprojekti, jossa esitellään turvallisuuden elinkaaren vaiheiden toteuttaminen ja dokumentaatio projektin kussakin vaiheessa. (SFS-EN-61511-2:2017, 114.)

IEC 61511-3 laatii ohjeita vaadittavan turvallisuuden eheyden tasojen määrittämiseen. Julkaisu opastaa riskin pienentämisen ja turvallisuuden eheyden yleisiin ohjeistuksiin ja käsitteisiin, sekä kuvaa esimerkein työvaiheiden toteuttamista. Liitteissä esitellään useita eri metodeja SIL-

tavoitetason määrittämiseen. Näitä ovat muun muassa tapahtumapuuanalyysi, suojauskerrosmatriisi sekä kalibroitu riskigraafi. (SFS-EN-61511-3:2017, 8.)

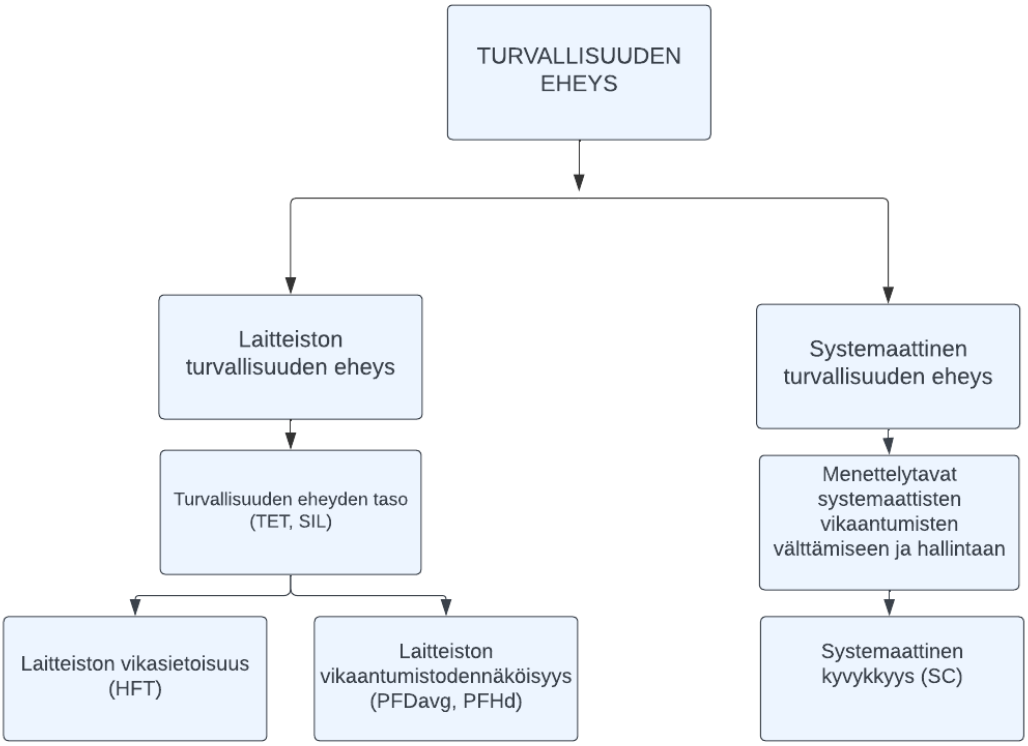
4 Toiminnallinen turvallisuus

Toiminnallisen turvallisuuden ymmärtämiseksi on ensin määriteltävä, mitä turvallisuus on. Standardi IEC 61508-0 määrittelee sen ”*Vapaudeksi sellaisen fyysisen vamman tai ihmisten terveyteen kohdistuvan vahingon riskistä joko suoraan tai epäsuoraan omaisuuteen tai ympäristöön kohdistuvan vahingon seurauksena, jota ei voida sietää.”*. Toiminnallisen turvallisuuden päätarkoituksena on siten suojella käyttäjiä laitteistojen aiheuttamilta vaaroilta. Järjestelmän kehittäjän on tunnistettava laitteiston ja niiden alajärjestelmien vaarat niille tarkoitetuissa ympäristöissä, ja otettava ne suunnittelussa huomioon. (IEC 61508-0:2011, 10)

Toiminnallisella turvallisuudella tavoitellaan turvallisuuden eheyttä, joka kuvaa turvatoiminnon todennäköisyyttä toteuttaa vaaditut turvatoiminnot kaikissa määritellyissä olosuhteissa, sille määritellyllä ajanjaksolla. Turvallisuuden eheys jakaantuu (ks. kuvio 2) kahteen elementtiin: Laitteiston eheyteen, joka liittyy laitteiston satunnaisiin vaarallisiin vikamuotoihin, sekä systemaattiseen turvallisuuden eheyteen. (SFS-EN 61508-5, 22)

> ***”Laitteiston turvallisuuden eheys****: Se osa turvallisuuden eheyttä, joka liittyy niihin laitteiston satunnaisiin vikaantumisiin, joilla on vaarallinen vikamuoto. Laitteiston määrätyn turvallisuuden eheyden tason saavuttaminen voidaan arvioida kohtuullisella tarkkuustasolla ja siten vaatimukset voidaan jakaa alajärjestelmien kesken käyttämällä vakiintuneita sääntöjä todennäköisyyksien yhdistämiseen ja yhteisvikaantumisten tarkasteluun. Laitteistolta vaadittavan turvallisuuden eheyden saavuttamiseksi voi olla tarpeen käyttää redundanttisia rakenteita.”* (SFS-EN 61508-5, 22)
>
> ***”Systemaattinen turvallisuuden eheys:*** *Se osa turvallisuuden eheyttä, joka liittyy niihin systemaattisiin vaarallisiin vikaantumisiin, joilla on vaarallinen vikamuoto. Vaikka eräiden systemaattisten vikaantumisten aiheuttama osuus vaikutuksesta voidaan arvioida, suunnitteluvirheistä ja yhteisvikaantumisista saadut tiedot osoittavat, että niiden jakautumaa voi olla vaikeaa ennakoida. Tällä on epävarmuutta lisäävä vaikutus vikaantumisten todennäköisyyden laskentaan tietyssä tilanteessa (esimerkiksi turva-automaatiojärjestelmän vikaantumisen*

todennäköisyys). Siksi tämän epävarmuuden minimoimiseksi on tehtävä päätös parhaiden tekniikoiden valinnasta...” (SFS-EN 61508-5, 22)



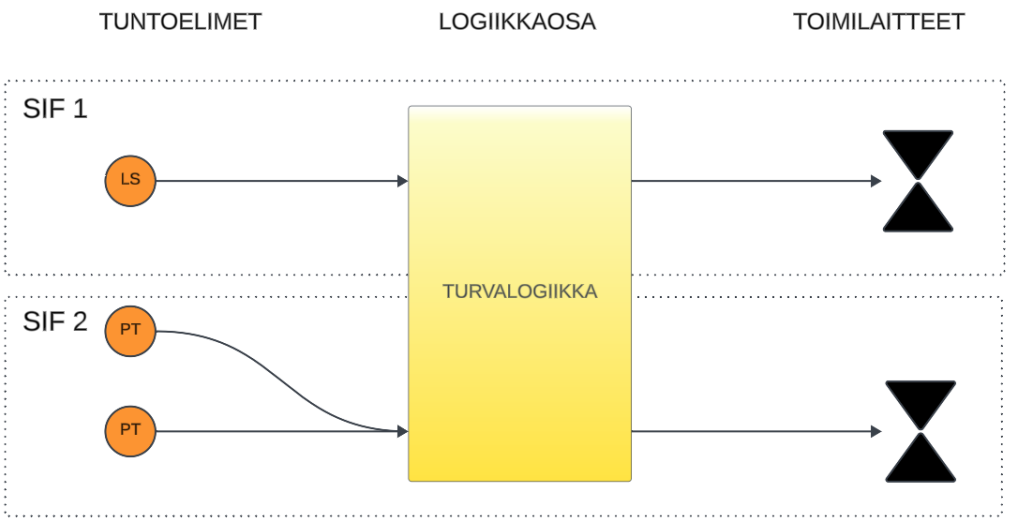
Kuvio 2: Turvallisuuden eheyden osa-alueet

5 Turvatoiminto

Normaalin ajon aikana perus- ja käyttöautomaatio (BPCS) ohjaa prosessia. Järjestelmässä toteutetaan lukitusten ja hälytysten kaltaisia varoittavia ja suojaavia toimenpiteitä, mutta varsinaiset turvatoiminnot suoritetaan erillisessä turva-automaatiojärjestelmässä (TAJ, SIS). Turva-automaation tehtävänä on suorittaa pelkästään turvatoimintoja, eikä se osallistu prosessin säätöön tai ohjaukseen. Perusautomaation ja TAJ:n kesken jaettujen kenttälaitteiden käyttöä ei olla kielletty, mutta usein se ei ole suositeltavaa. Skenaariossa on riski, että järjestelmien välille jaetun laitteen vaarallinen vikaantuminen aiheuttaa vaateen turvatoiminnolle, joka ei kuitenkaan enää kykene vastaamaan tapahtuneesta vikaantumisesta johtuen. (Control & Safety: Inegrate or Segregate 2019, 5.)

> *”Turva-automaatiojärjestelmä ei saa käyttää laitetta, jota käyttö- ja perusautomaatiojärjestelmä käyttää, jos laitteen vikaantuminen voi johtaa sekä turva-automaatiotoiminnon vaateeseen että turva-automaatiotoiminnon vaaralliseen vikaantumiseen, ellei ole suoritettu analyysia, joka vahvistaa kokonaisuuden riskin olevan hyväksyttävä.”* (SFS-EN 61511-1:2017, 63.)

Turva-automaatiojärjestelmä sisältää yhden tai useampia yksittäisiä turvatoimintoja (SIF, Safety Instrumented Function), joiden tehtävä on suojata niin laitteistoa kuin henkilöitä viemällä prosessi turvalliseen tilaan vaateen, eli vaarallisen tapahtuman ilmetessä. Turvatoiminnon kolme pääkomponenttia ovat tuntoelin, jonka tehtävänä on havaita vaarallinen tila, tuntoelimeltä saatua viestiä käsittelevä logiikkaosa ja toimilaite, joka toteuttaa määritetyt toiminnot prosessin ajamiseksi turvalliseen tilaan. Jokaisessa osassa voi olla yksi tai useampi laite. Tämä on havainnollistettu kuviossa kolme, jossa turvatoimintoon SIF 2 osallistuu kaksi tuntoelintä.



Kuvio 3: Turvatoiminnon komponentit

Turvatoiminnoilla pyritään pienentämään prosessin aiheuttamaa riskiä siedettävälle tasolle. Turvatoiminnon kyvykkyyden mitta on asteikolla 1-4 ilmaistava SIL-taso (Safety Integrity Level), eli turvallisuuden eheystaso (TET). Eheystaso muodostuu kolmesta osasta: Systemaattisesta kyvykkyydestä, turvatoiminnon arkkitehtuurin rajoitteista sekä sen

vikaantumistodennäköisyydestä, eli PFD_{avg}- tai PFH-arvosta, toimintatavasta riippuen. Myös riskinvähennyskerroin (RRF) voidaan laskea osaksi tätä kokonaisuutta, sillä turvatoiminnon PDFavg-arvon käänteisluvun tulee olla vähintään turvatoiminnolle määritetyn riskinvähennyskertoimen suuruinen. (SFS-EN 61511-2:2017, 27; The Three Barriers 2017.)

5.1 Toimintatavat

Turvatoiminnan käyttövaateen taajuutta kuvaava toimintatapa on keskeisessä osassa turvatoimintoa ja sen vaatimuksia määrittäessä. IEC:n standardeissa toimintatavat jaetaan kolmeen luokkaan (kts. taulukko 1). Merkittävä osa prosessiteollisuuden turvatoiminnoista on toteutettu harvojen vaateiden toimintatavalla, missä yksittäisen turvatoiminnon vaade esiintyy korkeintaan kerran vuodessa. Tällöin toimintojen vuosittainen testaus ja tarkastus on riittävää, ja turvatoiminnon vian havainnointi tarkastuksen yhteydessä on todennäköisempää kuin vian esiintyminen vaateen ilmetessä. Vastaavasti, mikäli vaateiden tiheys on suurempi kuin testausväli, vika esiintyy todennäköisemmin vaateen ilmetessä. (Generowicz 2022, 3.)

Harvojen vaateiden toimintatapa	Turvatoiminnon suorittamisen vaateen taajuus < 1 kerta/v
Tiheiden vaateiden toimintatapa	Turvatoiminnon suorittamisen vaateen taajuus > 1 kerta/v
Jatkuvien vaateiden toimintatapa	Turvatoiminnan suorittamisen vaade on jatkuvaa

Taulukko 1: Turvatoimintojen toimintatavat

PFD_{avg}-arvo (Probability of Failure on Demand average) kuvaa todennäköisyyttä turvatoiminnon vaaralliselle vikaantumiselle vaateen ilmetessä, kun turvatoiminnon vaade esiintyy kerran vuodessa tai harvemmin (kts. taulukko 2). Jatkuvien tai tiheiden vaateiden toimintatavalla SIL-tasoon vaikuttava parametri on PFH (Probablity of Dangerous Failure per hour), joka merkitsee vaarallisen vian ilmenemisen todennäköisyyttä tuntia kohden (kts. taulukko 3).

SIL	PFDavg	Vaadittu riskin pienennys
4	≥ 10^{-5} to < 10^{-4}	> 10 000 … ≤ 100 000
3	≥ 10^{-4} to < 10^{-3}	> 1 000 … ≤ 10 000
2	≥ 10^{-3} to < 10^{-2}	> 100 … ≤ 1 000
1	≥ 10-2 to < 10-1	> 10 … ≤ 100

Taulukko 2: PFD_{avg} raja-arvot (SFS-EN 61511-1:2017, 54, muokattu)

SIL	PFH (1/h)
4	≥ 10-9 to < 10-8
3	≥ 10-8 to < 10-7
2	≥ 10-7 to < 10-6
1	≥ 10-6 to < 10-5

Taulukko 3: PFH raja-arvot (SFS-EN 61511-1:2017, 55, muokattu)

5.2 Systemaattinen kyvykkyys

Turvatoimintoon osallistuvan laitteiston turvallisuuden eheys kattaa pääosin satunnaiset laitevikaantumiset tietyssä ympäristössä, eikä se paljasta kaikkia vikaantumiseen vaikuttavia tekijöitä. Virheet laitteen suunnitteluprosessissa voivat johtaa laitteen ja siten turvatoiminnon systemaattiseen vikaantumiseen, joka ei paljastu PFH- tai PFD-laskelmissa. (Creech 2014, 1)

Systemaattinen kyvykkyys (SC, systematic capability) on asteikolla SC 1…SC 4 esitetty *luottamuksen mitta* siitä, että laitteen systemaattinen turvallisuuden eheys täyttää turvatoiminnon eheystason suhteen määritellyt vaatimukset silloin, kun laiteen käytössä noudatetaan sen turvallisuuskäsikirjassa annettuja ohjeita. Käsite on johdettu standardeissa IEC 61508-2:2010 ja IEC 61508-3:2010 esitellyistä vaatimuksista systemaattisten vikojen välttämiseksi ja hallitsemiseksi. Julkaisuissa on kuvattu liki 400 erilaista toimenpidettä ja tekniikkaa laitteiston ja ohjelmiston suunnittelun ja koestamisen ohjenuoriksi. Taulukoissa on eritelty tärkeysasteet eri tekniikoille SIL-tason mukaisesti. Mitä perusteellisemmin laitevalmistaja on todennetusti tekniikoita noudattanut, sitä suurempi systemaattinen kyvykkyys mahdollista saavuttaa laitteistolle. Taulukko 4 on esimerkki, jossa esitellään ohjelmoitavan laitteiston

suunnitteluperiaatteiden suosituksia eri turvallisuuden eheyden tasoille. R tarkoittaa kohdan noudattamisen olevan suositeltavaa, HR puolestaan erittäin suositeltavaa. (Creech 2014, 1. The Three Barriers 2020, 6-7.)

Tekniikat/toimenpiteet*		**Viite**	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
1	Koodausstandardin käyttö virheiden todennäköisyyden pienentämiseksi	C.2.6.2	HR	HR	HR	HR
2	Dynaamisten olioiden välttäminen	C.2.6.3	R	HR	HR	HR
3a	Dynaamisten muuttujien välttäminen	C.2.6.3	–	R	HR	HR
3b	Dynaamisten muuttujien luomisen ajoaikainen tarkistus	C.2.6.4	–	R	HR	HR
4	Keskeytysten rajoitettu käyttö	C.2.6.5	R	R	HR	HR
5	Osoittimien rajoitettu käyttö	C.2.6.6	–	R	HR	HR
6	Rekursion rajoitettu käyttö	C.2.6.7	–	R	HR	HR
7	Ei ehdottomia hyppyjä korkeamman tason kielten ohjelmistoissa	C.2.6.2	R	HR	HR	HR
8	Ei automaattisia tyyppimuunnoksia	C.2.6.2	R	HR	HR	HR

Taulukko 4: Taulukko B.1: Suunnittelu- ja koodausstandardit (SFS-EN 61508-3, 100, muokattu)

5.3 Vikasietoisuus ja äänestyslogiikka

Turvatoiminnon eheystasoa rajoittaa myös arkkitehtuurin luomat rajoitteet. Laitteiston vikasietoisuus (hardware fault tolerance, HFT) kuvaa sitä määrää vikaantumisia jonka turvatoiminto sietää, vielä kyeten toimimaan. Siispä järjestelmä, jonka HFT=0, ei kestä yhtäkään vaarallista vikaantumista. Koko turvatoiminnon turvallisuuden eheyden taso on rajoitettava joko reitin 1H tai 2H mukaisesti (kts. taulukko 5, 6, 7). Reitti 1H perustuu laitteiston vikasietoisuuden ja turvallisten vikaantumisten osuuden konsepteihin, reitti 2H taas pohjautuu loppukäyttäjältä saatuihin tietoihin komponentin luotettavuudesta.

Reitti 1H jakautuu kahteen tyyppiin. Elementti tyyppiä A, jos sen osakomponenttien vikaantumismuodot ovat hyvin määriteltyjä, sen käyttäytyminen vikatilanteessa on täydellisesti määriteltävissä ja luotettavaa vikaantumistietoa on saatavilla. Mikäli laitteen vikaantumismuotoa tai käyttäytymistä vikatilanteessa ei voida täydellisesti määrittää, elementti on tyyppiä B. (IEC 61508-2, 42.)

Elementin turvallisten vikaantumisten osuus	Laitteiston vikasietoisuus		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4

Taulukko 5: Korkein SIL-taso tyypin A turvatoiminnalle (Reitti 1H) (SFS-EN 61508-2:2011, 46, muokattu)

Elementin turvallisten vikaantumisten osuus	Laitteiston vikasietoisuus		
	0	1	2
< 60 %	Ei sallittu	SIL 1	SIL 2
60 % - < 90 %	SIL 2	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4

Taulukko 6: Korkein SIL-taso tyypin B turvatoiminnalle (Reitti 1H) (SFS-EN 61508-2:2011, 48, muokattu)

Reitti 2H perustuu käyttäjiltä saatuihin tietoihin laitteiston luetettavuudesta. Näitä ovat käyttäjiltä saatu palaute elementeistä, joita on käytetty vastaavanlaisessa ympäristössä ja sovelluksessa. Lisäksi tietojen on perustuttava kansainvälisiin standardeihin ja oltava arvioituja palautteiden määrän suhteen. Standardissa IEC-61511 esitellyt vaatimukset laitteiston vikasietoisuudelle perustuvat suoraan reittiin 2H.

Turvallisuuden eheyden taso (SIL)	Pienin sallittu laitteiston vikasietoisuus (HFT)
1 (mikä tahansa toimintatapa)	0
2 (harvojen vaateiden toimintatapa)	0
2 (tiheiden vaateiden toimintatapa)	1
3 (mikä tahansa toimintatapa)	1
4 (mikä tahansa toimintatapa)	2

Taulukko 7: Pienin sallittu HFT SIL-tason mukaisesti (SFS-EN 61511-1:2017, 65, muokattu)

Kun turvatoiminnon vikasietoisuutta kasvatetaan lisäämällä siihen redundanttisia laitteita, esimerkiksi lisäämällä toinen tuntoelin, on suunnittelussa otettava huomioon elementtien keskinäinen äänestyslogiikka. Termi MooN (M out of N) kuvastaa monenko kanavan *M* pitää

äänestää kaikkien joukosta *N*, että trippitilanne, eli turvatoiminnon laukaisu tapahtuu. Periaatetta voidaan soveltaa niin mittalaitteille, logiikkaosalle kuin toimilaitteille. Teollisuudessa yleisimmin käytetyt äänestyslogiikat ovat 1oo1, 1oo2, 2oo2 ja 2oo3. Äänestyslogiikasta voidaan päätellä myös turvatoiminnon vikasietoisuus HFT, kun joukosta N vähennetään M (kts. kuvio 4). Äänestyslogiikalla on myös vaikutus turvatoiminnon vikaantumismuotoihin, jotka voidaan jakaa seuraaviin osuuksiin. (Marszal 2018.)

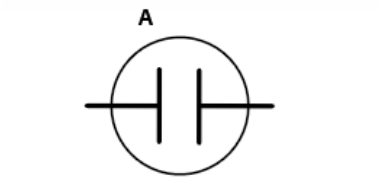
- Turvallinen vikaantuminen, jossa laukaisu tapahtuu ilman vaadetta. Vaaratilannetta ei ole tapahtunut, mutta turvatoiminto ajaa prosessin turvalliseen tilaan. Laukaisu oli turha ja aiheuttaa tuotannon menetyksiä.
- Vaarallinen vikaantuminen, jossa vika on piilevä ja estää turvatoiminnon toiminnan vaateen esiintyessä.

Table 1. Safety architectures versus hardware fault tolerance provided

Architecture	HFT
1oo1	0
1oo2	1
2oo2	0
1oo3	2
2oo3	1
3oo3	0

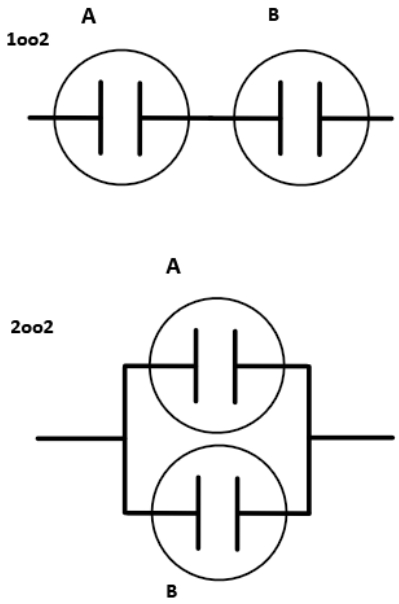
Kuvio 4: Äänestysarkkitehtuurin ja HFT:n suhde

1oo1 on yksikanavaisena kaikista yksinkertaisin toteutus, joka voidaan visualisoida yhdellä kytkimellä. (kts. kuvio 5). Ratkaisu on kustannustehokas ja helppo toteuttaa, ja sitä tulisi käyttää aina silloin kun tarvetta vikasietoisuudelle ei ole. Niin turvallisten kuin vaarallisten vikaantumisten todennäköisyys on tässä konfiguraatiossa täysin siinä käytettyjen laitteiden määrittämä. (Marszal 2018.)



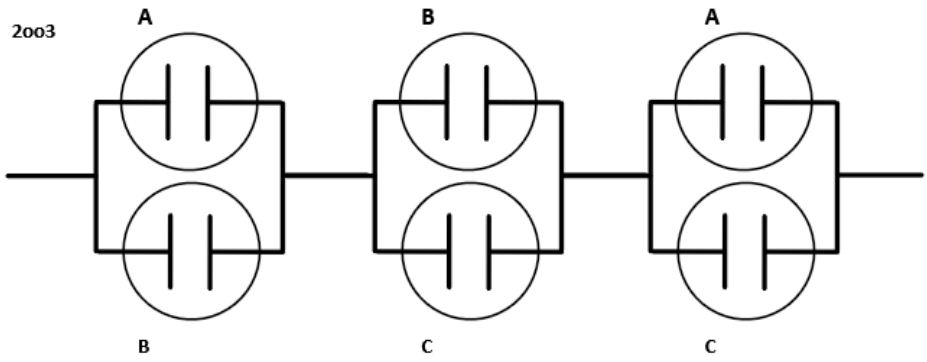
Kuvio 5: 1oo1 -äänestys (Marszal 2018, muokattu)

1oo2-äänestyslogiikassa hyödynnetään kahta redundanttista laitetta, joista kumman tahansa tekemä äänestys johtaa turvatoiminnon laukaisuun. Tämä rakenne sietää yhden vaarallisen vian redundanttisen kanavan ansiosta, ja täten pienentää PFD_{avg}-arvoa. Haittapuolena todennäköisyys turvalliseen vikaantumiseen ja siten turhaan laukaisuun, on kaksinkertainen 1oo1 -toteutukseen verrattuna. 2oo2-äänestyslogiikka käyttää myös kahta laitetta, mutta turvatoiminnon laukaisu tapahtuu vasta kun molemmat äänestävät sen puolesta. Turvallisten vikaantumisten osuus pienenee, mutta todennäköisyys vaaralliseen vikaantumiseen ei laske. (Marszal 2018.)



Kuvio 6: 1oo2- ja 2oo2 -äänestyslogiikat (Marszal 2018, muokattu)

2oo3-äänestyslogiikkassa laukaisu tapahtuu, kun kaksi kolmesta laitteesta äänestää. Ratkaisu on luonnollisesti kalliimpi toteuttaa, mutta se sietää yhden laitteen vikaantumisen millä tahansa muodolla (kts. kuvio 7). Marszalin (2018) mukaan 2oo3-konfiguraatiota käytetään usein kun turvatoiminnon eheysvaade on SIL 2 tai SIL 3, ja samalla halutaan minimoida turhat laukaisut. (Marszal 2018)



Kuvio 7: 2oo3-äänestyslogiikka (Marszal 2018, muokattu)

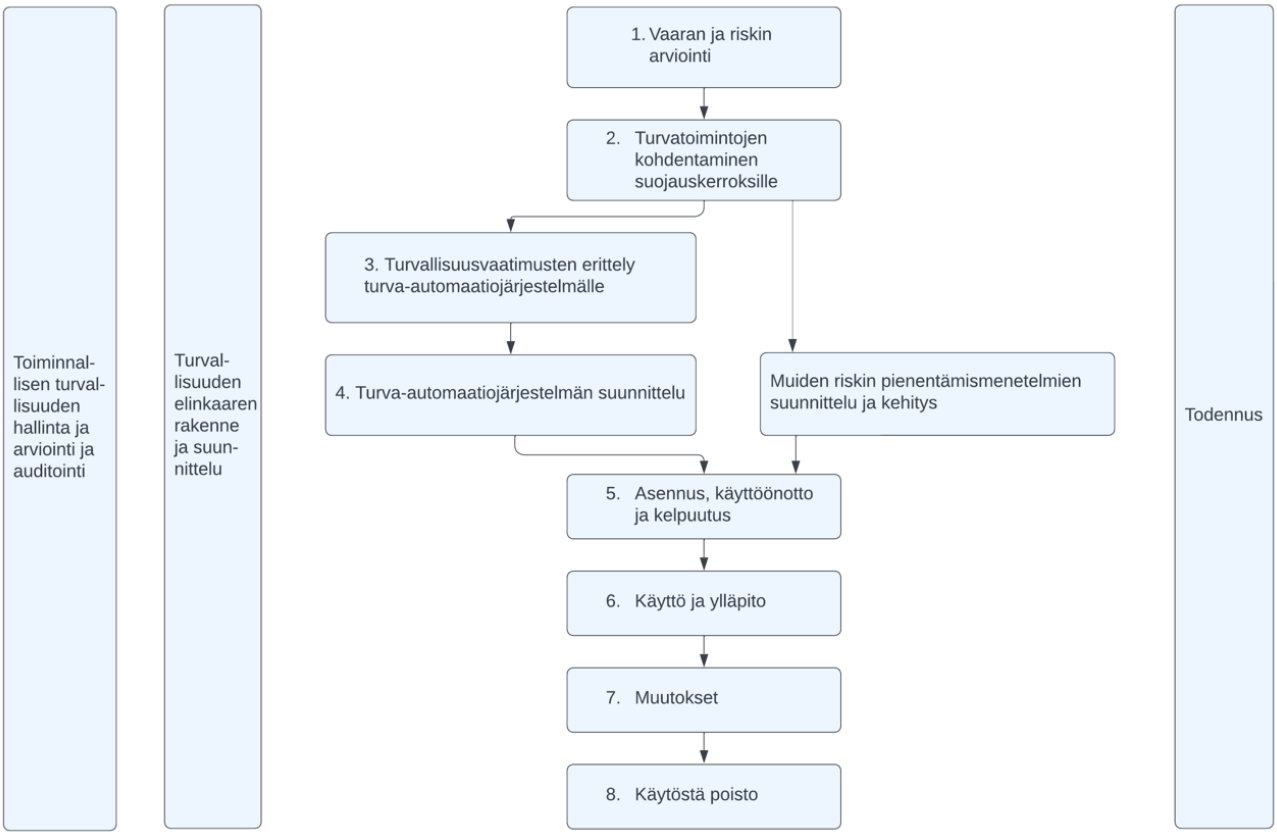
6 Turva-automaation elinkaari prosessiteollisuudessa

6.1 Elinkaarimalli ja turvallisuuden suunnittelu

IEC 61511 -standardijulkaisussa on esitetty konsepti turva-automaatiojärjestelmän elinkaaren hallintaan (kts. kuvio 8), joka sisältää vaiheet vaarojen tunnistamisesta turva-automaatiojärjestelmän suunnitteluun, toteutukseen ja lopulta käytöstä poistamiseen. Keswick (2024) toteaa, että standardien mukaisen elinkaarimallin esimerkkiesityksen noudattaminen ei ole aina paras ratkaisu, sillä malli on yleiskuvallinen. Toiminnanharjoittajien kannattaisi kehittää omat käytänteensä sen soveltamiseen. (Keswick 2024, 3.)

Elinkaaren vaiheelle on määritetty vaatimukset dokumentaation sisällön suhteen. Tämä sisältää muun muassa kirjaukset suunnittelun lähtötiedoista, turvatoimintojen suorituskyvyn vaatimuksista sekä järjestelmän testauskäytänteistä. Asianmukaisella raportoinnilla ja dokumenttihallinnalla

voidaan todentaa toiminnallisen turvallisuuden hallintaa arvioivalle osapuolelle, että laitteiston turvallisuuden eheys saavutetaan. Myös Keswick (2024) painottaa dokumentoinnin tärkeyttä, vaikkakin työprosessin laajuus sisältää haasteensa. Dokumenttien hallinta ja revisiointi on välttämätöntä suunnittelutyön seurattavuuden ja jäljitettävyyden vuoksi. (Chastain-Knight, Butz ja Donaldson n.d.)



Kuvio 8: Turva-automaatiojärjestelmän (SIS) turvallisuuden elinkaaren vaiheet (SFS-EN 61511-1:2017, 43) (muokattu)

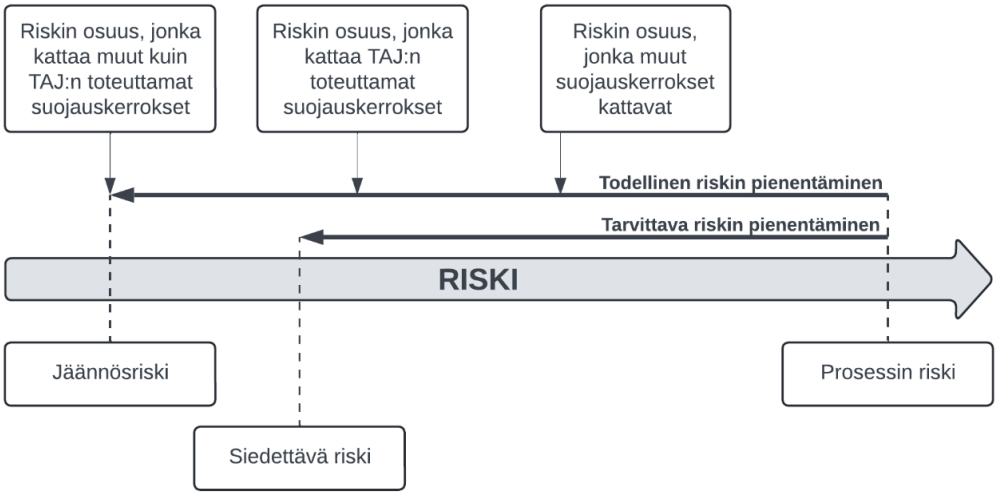
Elinkaaren vaiheet, menetelmät ja tuotokset on koottava turvallisuussuunnitelmaksi kutsuttuun dokumenttiin, joka toimii eräänlaisena yleiskuvana koko prosessista. Se elää ja päivittyy koko elinkaaren ajan muiden dokumenttien valmistuessa. Elinkaaren vaiheista vastuussa olevat henkilöt tai organisaatiot tulisi yksilöidä hallintasuunnitelmaan, ja heidän tulee olla selvillä omista vastuistaan projektissa. Organisaatioon kuuluvien henkilöiden pätevyyksiä sekä soveltuvuutta

tehtäviin tulee myös tarkastella ja dokumentoida. Tarkastelun näkökulmia ovat muun muassa prosessisovellukselle käypä osaaminen, asiantuntemus turvallisuussuunnittelusta tai viranomaisten sekä lainsäädännön vaatimusten tuntemus. (SFS-EN 61511.1:2017, 37-38.)

6.2 Vaihe 1: Vaaran ja riskin arviointi

6.2.1 Riskien arviointi

Elinkaarimallin ensimmäisessä vaiheessa prosessille tehdään vaara-analyysi riskien, prosessipoikkeamien ja niiden seurausten tunnistamiseksi. Riskin suuruus määräytyy vaarallisen tapahtuman seurausten vakavuuden ja esiintymistaajuuden perusteella, ja sitä tulee pienentää vähintäänkin siedettävälle tasolle. Siedettävän riskin tasoa ei olla yleisesti määritetty, vaan se on prosessi-, yritys- ja toimialakohtainen. Hyväksytyn ja siedettävän riskin taso tulee olla määritetty riskimatriisissa. Yleisesti hyväksytty käytäntö on pienentää riskiä ALARP-periaatteen (As Low As Reasonably Practicable) mukaisesti niin matalalle tasolle, kuin se on kohtuullisesti mahdollista. Kuviossa 10 on esitetty prosessin riskin pienentämisen yleiset käsitteet, kun siihen liittyy käyttö- ja automaatiojärjestelmä, inhimilliset tekijät ja suojauskerrokset. (Turva-automaatio prosessiteollisuudessa 2021; SFS-EN 61511-3:2017, 98)



Kuvio 9: Riskin pientäminen, yleiset käsitteet (SFS-EN 61511-3:2017, 14, muokattu)

6.2.2 HAZOP (Hazard and Operability Study)

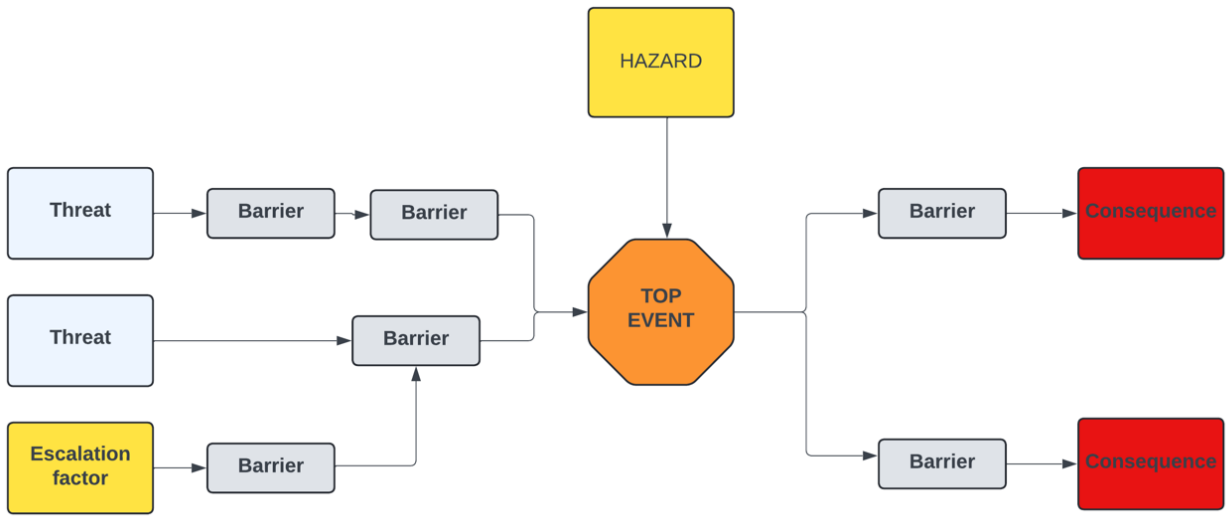
HAZOP eli poikkeamatarkastelu, on kvalitatiivinen menetelmä prosessihäiriöiden ja niihin liittyvien riskien arviointiin. Tarkastelua tehtäessä on henkilöillä oltava riittävät tiedot prosessin toiminnasta, laitteistosta sekä niihin liittyvistä vaaroista. Menetelmässä arvioidaan systemaattisesti järjestelmän tai prosessin solmukohdat monialaisen työryhmän toimesta. Menetelmä kannustaa aivoriihimäiseen tarkasteluun, jossa käytetään apuna ohjesanoja mahdollisten poikkeamatilanteiden etsintään. Merkittävät poikkeamat, kuten ei virtausta tai korkea paine, analysoidaan sen suhteen, voivatko ne aiheuttaa vaaraa turvallisuudelle, terveydelle tai ympäristölle. Poikkeaman juurisyiden selvittämisen jälkeen työryhmä arvioi poikkeaman seuraukset ottaen huomioon nykyiset suojauskerrokset, ja tarpeen tullen suosittelee toimenpiteitä riskin pienentämiseksi. (SFS-EN 61511-3:2017, 31; Crawley & Tyler 2015)

6.2.3 Solmukeanalyysi

Solmukeanalyysi (bowtie) on riskinarviointimenetelmä, jolla voidaan esittää monimutkaisiakin riskitilanteita visuaaliseen muotoon. Menetelmä havainnollistaa vaarallisten tapahtumien syiden

ja seurausten suhteen, mukaan lukien suojaavat ja lieventävät toimenpiteet. Kuviossa 10 esitetyn kaavion keskiössä on huipputapahtuma, eli potentiaalisesti vaarallinen tapahtuma. Huipputapahtumaan johtavat uhat ja juurisyyt on esitetty kaavion vasemmalla puolella. Uhilta suojaavat toimenpiteet on esitetty esteinä uhkien ja huipputapahtuman välissä.

Solmukkeen oikea puoli esittää huipputapahtuman seuraukset, ja siellä esitetyt esteet ovat luonteeltaan lieventäviä. Vaarallinen tapahtuman katsotaan jo tapahtuneen, joten esteillä pyritään hallitsemaan tilannetta ja estämään vakavia seurauksia. Minkä tahansa esteen toimintaan negatiivisesti vaikuttavaa tekijää voidaan kuvata eskalaatiokertoimella. Esimerkiksi mittalaite voi vikaantuessaan johtaa huipputapahtumaan, jolloin toinen mittaus toimii puolestaan vikaantumisen esteenä. (The Use of Bow Ties in Process Safety Auditing 2016, 2.)



Kuvio 10: Bowtie-kaavio (The Use of Bow Ties in Process Safety Auditing 2016, 2, muokattu.)

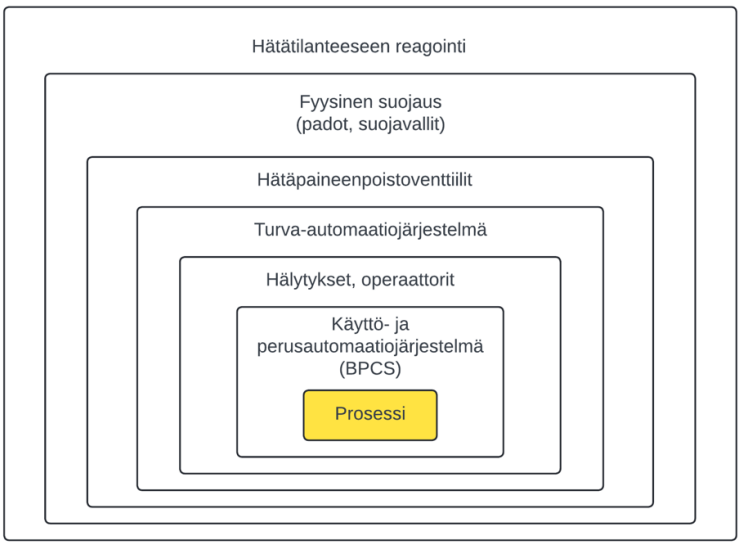
6.3 Vaihe 2: Turvallisuuden eheystason määritys

Riskianalyysin jälkeen on tarkasteltava tarkemmin skenaarioita, joiden hallitsemiseksi on todettu tarvittavan turva-automaatiota. SIL-määrittelyssä keskitytään turvatoimintojen eheystasovaatimusten määrittämiseen sen perusteella, kuinka paljon riskiä tarvitaan pienennettävän. Arviointi voidaan tehdä esimerkiksi kalibroidun riskigraafin, SIL-riskimatriisin tai

suojauskerrosanalyysin avulla. Menetelmän valintaan vaikuttavia tekijöitä ovat mm. sovelluksen monimutkaisuus ja siitä saatavilla olevat tiedot, tiimin tuntemus eri menetelmistä ja riskin luonne. SIL-määrittelyä ohjaa toimijan riskikriteerit, vaarallisten tapahtumien siedettävä taajuus ja ALARP-periaate. ALARP-periaatetta voidaan käyttää siedettävän riskitason määrittämisessä, mutta SIL-tason määritykseen sitä ei käytetä. (SIL Determination Techniques Report 2006.)

6.3.1 Suojauskerrosanalyysi

IEC 61511:3-standardissa esitelty suojauskerrosanalyysi (LOPA, Layers Of Protection Analysis) on menetelmä riskien kvantifioimiseksi ja suojakerrosten riippumattomuuden varmistamiseksi. Ns. sipulimallin mukaisesti (kts. kuvio 10) esitetyt suojauskerrokset ovat toisistaan riippumattomia järjestelmiä, laitteita tai toimintoja, joilla estetään tai lievennetään vaaraa. Suojauskerrosten riskinvähennystasoa analysoimalla voidaan selvittää, onko laitokseen tarpeellista hankkia turva-automaatiojärjestelmä riskin pienentämiseksi siedettävälle tasolle. Menetelmän lähtötietoina on esimerkiksi HAZOP-tarkastelun kautta saadut tiedot vaarojen alkusyistä. (Turva-automaatio prosessiteollisuudessa 2021.)



Kuvio 11: Suojauskerrokset (SFS-EN 61511-3:2017, 29) (muokattu)

LOPA-menetelmässä määritetään riskiarvioinnissa havaitun vaaratilanteen vakavuustaso, ja siihen johtaneen alkutapahtuman esiintymisen taajuus. Tämän jälkeen tunnistetaan nykyiset suojauskerrokset, ja määritetään jokaisen suojauskerroksen vikaantumistodennäköisyys PFD_{avg}. Kun alkutapahtuman todennäköisyys kerrotaan suojauskerrosten PFD_{avg}-arvolla, saadaan tulokseksi vaarallisen tapahtuman todennäköisyys vuotta kohden, kun kaikki suojauskerrokset on otettu huomioon. Mikäli todennäköisyys ylittää laitoksen riskikriteerit, turvatoiminto on tarpeellinen ja sen vaadittu riskinvähennyskerroin *RRF* on laskettavissa. Torres-Echeverria painostaa, että suojauskerrosten vikaantumistodennäköisyyttä kuvaavat numeraaliset arvot (kts. taulukko 8) ovat pohjimmiltaan olettamuksia ja tarkoituksellisesti konservatiivisia. (Torres-Echeverria 2014.)

Suojauskerros	**PFDavg**
Ohjauspiiri	1,0 × 10E-1
Ihmisen toiminta (ammattitaitoinen, stressittömänä)	1,0 × 10E-1 … 1,0 × 10E-2
Ihmisen toiminta (paineen alaisena)	0,5…1,0
Operaattorin reagointi hälytyksiin	1,0 × 10E-1
Painesäiliön luokitus sisäisistä ja ulkoisista painelähteistä johtuvaan suurimpaan vaatimustasoon	10E-4 tai parempi, jos painesäiliön eheyttä on ylläpidetty (tämä merkitsee, että korroosion merkitys on ymmärretty ja aikataulun mukaiset tarkastukset ja kunnossapito on tehty)

Taulukko 8: Tyypillisiä lieventävien ja estävien suojauskerrosten PFD_{avg}-arvoja (SFS-EN 61511-3:2017, 49, muokattu)

6.3.2 Kalibroitu riskigraafi

Kalibroitu riskigraafi on puolikvalitatiivinen menetelmä, jolla voidaan määrittää turvatoimintojen vaaditut SIL-tasot riskianalyysin ja prosessin ohjausjärjestelmän tietojen pohjalta. Se soveltuu eheyden tasojen vaatimuksen selvittämiseen niin henkilöriskien, kuin ympäristö- ja materiaalimenetysten suhteen. Tarkastelua tehtäessä ei oteta huomioon turva-automaatiotoimintoja, mutta muut suojauskerrokset lasketaan mukaan. Tarkastelussa käytetään vaaratilanteen seurauksia, alueen miehitysastetta ja toiminnon vaadetaajuutta kuvaavia parametrejä (kts. taulukko 9). (SFS-EN 61511-3:2017, 35)

Riskigraafimetodien eduiksi katsotaan helppokäyttöisyys ja yksinkertaisuus, siten niiden käyttäminen voi säästää aikaa ja resursseja etenkin siinä tapauksessa, jos turvatoimintoja on suuri määrä. Baybutt (2011) kritisoi menetelmästä puuttuvan mahdollisuus muiden vaikutustekijöiden huomioimiselle, lisäksi osa parametreista on epäselkeästi määritettyjä ja kattavuudeltaan suppeita, joka voi johtaa liian tiukkaan tai vastaavasti alimitoitettuun SIL-tason vaatimukseen. Myös parametrien kalibrointikriteerien subjektiivisuus voi aiheuttaa epäjärjestelmällisyyttä eri projektien välillä. (Torres-Echeverria 2014, 9.)

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

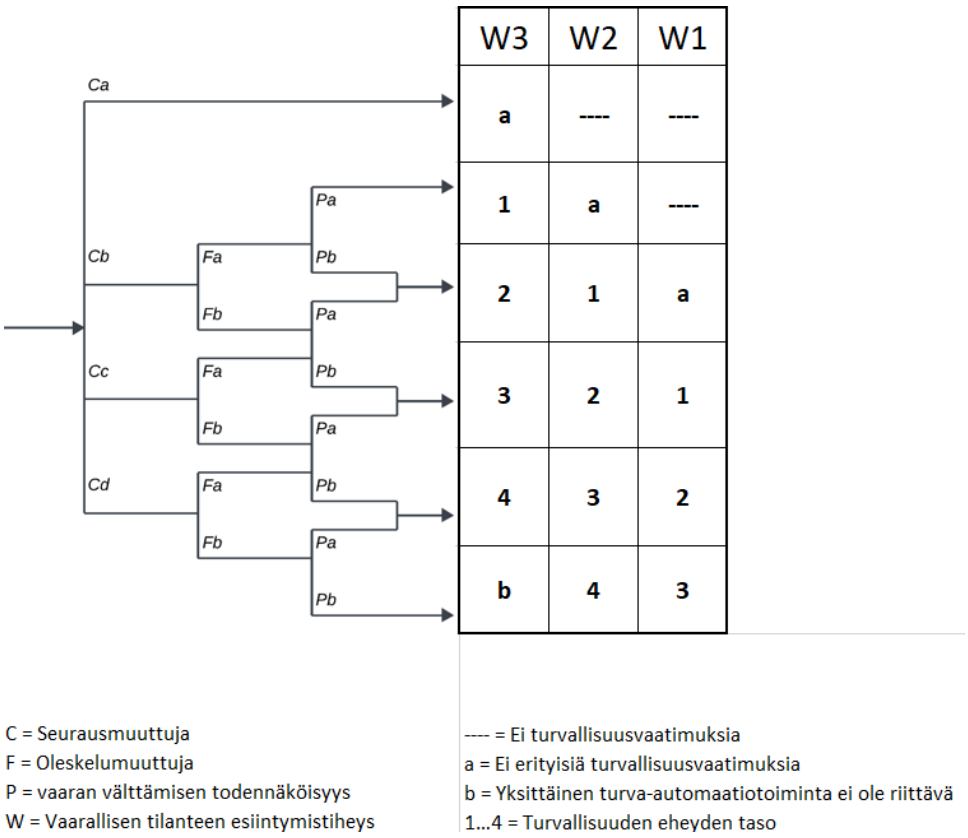
Taulukko 9: D.1 Prosessiteollisuuden riskigraafin parametrien kuvaukset (SFS-EN 61511-3:2017, 35, muokattu)

Kaikille neljälle parametrille asetetaan arvovälit laitoksen riskikriteereiden mukaisesti, ja niiden perusteet tulisi selvitä dokumentaatiosta. Standardissa IEC 61511 esiteltyä parametrien esimerkkikalibrointia (kts. taulukko 10) voidaan käyttää alustavana mallina, mutta sitä ei tulisi käyttää ilman laitoskohtaista arviointia. Kalibroinnin jälkeen tiimi voi määrittää turvatoiminnon

SIL-tason seuraamalla riskigraafia vasemmalta oikealle, parametrien arvojen mukaisesti. (kts. kuvio 12.)

Parametri		Luokitus	Kommentit
Seuraus C Kuolemantapausten lukumäärä	Ca	Vähäinen vamma	a) Luokitusjärjestelmä on kehitetty käsittelemään ihmisten vammautumisia tai kuolemantapauksia
Tämä voidaan laskea määrittämällä paikalla olevien ihmisten lukumäärä, kun vaaralle altistumisen alue on miehitetty ja kertomalla se yksilöidyn vaaran aiheuttamalla haavoittuvuudella. Haavoittuvuus määritetään sen vaaran luonteen perusteella, jota vastaan suojaudutaan. Seuraavia kertoimia voidaan käyttää: V = 0,01 Herkästi syttyvän tai myrkyllisen materiaalin vähäinen päästö V = 0,1 Herkästi syttyvän tai myrkyllisen materiaalin suuri päästö V = 0,5 Kuten edellä, mutta myös suuri syttymisen todennäköisyys tai erittäin myrkyllistä materiaalia V = 1 Repeämä tai räjähdys.	Cb Cc Cd	Vaihteluväli 0,01 - 0,1 Vaihteluväli > 0,01 - 1,0 Vaihteluväli > 1,0	b) Riskiparametrien CA, CB, CC ja CD tulkinnassa onnettomuuden seuraukset ja tavallinen parantumisprosessi tulisi ottaa huomioon.
Miehitys F Tämä lasketaan määrittämällä sen ajan suhteellinen pituus, jolloin altistumisalue vaaralle on miehitetty tavanomaisen työskentelyjakson aikana.	Fa Fb	Harvinainen–useammin toistuva altistuminen vaaravyöhykkeellä. Miehitysaste on alle 0,1. Toistuva–pysyvä-altistuminen vaaravyöhykkeellä	c) Katso edellä olevaa kommenttia a).

Taulukko 10: D.2 Esimerkki yleiskäyttöön tarkoitetun riskigraafin kalibroinnista, parametrit C ja F (SFS-EN 61511-3:2017, 39) (muokattu)



Kuvio 12: Riskigraafin yleinen kuvaus

6.4 Vaihe 3: Turvallisuusvaatimusten erittely

Riskianalyysin ja SIL-tason määritysten perusteella saatujen tietojen mukaan tuotetaan yksi elinkaaren avaindokumenteista: turva-automaation turvallisuusvaatimusten erittely (SRS, safety requirements specification). Tämän dokumentin täsmällisyys ja selkeys on ensiarvoisen tärkeää, viitaten jo aiemmin mainittuun HSE:n tutkimukseen, jonka mukaan 44 % automaatioon liittyvistä onnettomuuksista johtuu puutteellisesta määrittelystä. Myös Gandy (2016) toteaa, että vajavainen ja epäselvä määrittely johtaa korkeampaan riskiin, että turvajärjestelmä ei tavoita vaadittua eheystasoa.

SRS-dokumenttiin tulee kirjata kaikki vaatimukset siten, että turva-automaatiojärjestelmän suunnitteleminen on sen pohjalta mahdollista. Turvatoiminnoille spesifien vaatimusten lisäksi tulee soveltuvin osin kuvata yleisesti koko turva-automaatiojärjestelmän toimintaa ja vaatimuksia.

Yksittäisten turvatoimintojen vaatimuksiin liittyy mm. erittelyt tuloista ja lähdöistä, vaatimukset eheystasolle, toimintatavalle, yhteisvikaantumisten huomioimiselle, vasteajalle ja määräaikaistestausvälille. Näitä kohtia on esitetty standardissa yhteensä 29 kappaletta. (SFS-EN 61511-1:2017, 59-60)

SRS-dokumenttiin viitataan useassa elinkaaren vaiheessa, ja sitä tulisikin arvioida toiminnallisen turvallisuuden arvioinnin muodossa jo ennen seuraavaan vaiheeseen siirtymistä. Niin suunnittelu- kuin toteutusvaiheessa tehtyjä tuotoksia tulee verrata SRS-dokumentin vaatimuksiin. Tällä varmistetaan suunnittelutyössä noudatettavan vaatimuksia ja edistetään elinkaaren vaiheiden seurattavuutta. On siis tärkeää, että tuotokset ja SRS vastaavat toisiaan joka tilanteessa. Erityisesti käyttövaiheessa tehdyt muutokset tulee päivittää dokumentaatioon. (Heemels & Andre & Anton & Top 2021, 5-6)

6.5 Vaihe 4: Suunnittelu ja toteuttaminen

Suunnitteluvaiheessa tehdään laitevalinnat, ja kehitetään turva-automaatiojärjestelmän järjestelmäarkkitehtuuri tuntoelimiltä toimilaitteille. Detaljisuunnittelun aikana tuotetaan mm. piiri- ja johdotuskaaviot, I/O-määrittelyt, sovellusohjelmat ja käyttöliittymät. Vaiheen lopussa turva-automaatiojärjestelmälle tulee tehdä tehdashyväksyntä (FAT). Tehdashyväksyntätestissä suoritettavat toimenpiteet ja testikriteerit tulee määritellä testausprotokollat kuvaavaan suunnitelmaan. Loppudokumentaatiosta on käytävä ilmi, täyttyivätkö testauksen tavoitteet. Kokonaisuuteen sisältyy pöytäkirja suoritetuista testeistä, sen tuloksista ja niihin liittyvistä havainnoista. Testauksen aikana tehdyt muutokset, korjaukset ja niiden vaikutukset turva-automaatiojärjestelmän toimintaan on analysoitava. (Turva-automaatio prosessiteollisuudessa 2021; IEC-61511-1:2017, 79-80.)

Pelkästään SIL-sertifioitujen laitteiden ostaminen ei tarkoita, että turvatoiminto olisi vaatimusten mukainen. Verifioinnin tarkoituksena on todentaa, että turvatoiminto täyttää turvallisuusvaatimusten erittelyn mukaiset vaatimukset suorituskyvyn ja prosessin riskin pienentämisen suhteen. Tärkeä osa verifiointia on laskea turvatoiminnon PFD_{avg}- tai PFH-arvo, joka on turvatoimintoon osallistuvien komponenttien vikaantumistodennäköisyyksien summa:

$$PFDsif = \text{PFDtuntoelin} + \text{PFDlogiikka} + \text{PFDtoimilaite}$$

Laskelmat voidaan tehdä taulukkotyökaluilla laskentakaavoja käyttäen, mutta myös kaupallisia ohjelmistoja on saatavilla. Laskennassa käytetään laitevalmistajien ilmoittamia vikaantumistietoja, jotka on usein ilmoitettu laitteen SIL-sertifikaatissa. Mikäli äänestykseen osallistuu usea laite, myös äänestyslogiikka ja yhteisvikaantumiseen vaikuttava tekijä on otettava huomioon. Osa laskennassa käytettävistä parametreista on lueteltu alla. (Key Parameters n.d.)

1. Vikaantumistaajuus λ, sertifikaateissa vikaantumistaajuus ilmaistaan usein FIT-arvona (FIT = λ * 10^9)
2. SFF (Safe Failure Fraction) = Turvallisten vikaantumismuotojen osuus kaikista vikaantumismuodoista
3. MT (Mission Time) = Turvatoiminnon käyttöikä
4. TI (Test Interval) = Määräaikaiskoestusväli
5. C_{PT} (Proof Test Coverage) = Määräaikaiskoestuksen kattavuus
6. β-tekijä = yhteisvikaantumiseen vaikuttavan tekijän arviointi redundanttisissa arkkitehtuurimalleissa (1oo2, 2oo3 jne.)
7. MTTR (Mean Time to Restore) = keskimääräinen korjaukseen kuluva aika

(Key Parameters n.d.)

Laitteen kaikkia vaarallisia vikaantumismuotoja kuvaa parametri λD, joka koostuu havaitsemattomista (λDU), ja havaittavista (λDD) vikaantumismuodoista. Nämä vikaantumismuodot ovat erotettavissa turva-automaatiojärjestelmän itsediagnostiikalla. Mikäli diagnostiikkaa ei ole saatavilla, havaittavien vikaantumisten λDD osuus on 0 ja λDU = λD. (The Key Variables Needed for PFDavg Calculation, 2018)

Verifiointilaskennassa käytetään usein IEC 61508-6:ssa esitettyjä yksinkertaistettuja laskentakaavoja (kts. kaava 1). Tällöin laskennassa ei kuitenkaan oteta huomioon kaikkia tekijöitä, kuten määräaikaiskoestuksen kattavuutta, sekä koestuksiin ja korjauksiin kuluvaa aikaa. Kun nämä otetaan laskentaan mukaan kaavan 2 mukaisesti, voidaan saada realistisempia tuloksia turvatoiminnon suorituskyvystä. Kun PFD-arvo on laskettu, turvatoiminnon SIL-taso rajoitetaan arkkitehtuurin rajoitteiden ja laitteiston systemaattisen kyvykkyyden perusteella tasolle SIL 1…4. (Safety Instrumented Function Verification: The Three Barriers 2017, 9; Börcsök n.d.)

Kaava 1: $PFDavg = \lambda\mathrm{DU} * \frac{TI}{2}$

Kaava 2: $PFDavg = \lambda_{\mathrm{DD}} * \mathrm{MTR}_{\mathrm{dd}} + \left[C_{pt} * \lambda_{\mathrm{DU}} * \left(\frac{TI}{2} + MTR_{DU}\right)\right] + \left[(1 - C_{PT}) * \lambda_{\mathrm{DU}} * \frac{MT}{2}\right] - \frac{PTD}{TI}$

6.6 Vaihe 5: Asennus, testaaminen ja käyttöönotto

Turva-automaatiojärjestelmät tulee asentaa määritelmien ja piirustusten mukaisesti. Toimenpiteiden suunnitteludokumentaatioon sisällytetään vaadittavat asennustavat ja -menetelmät, toteutuksen aikataulu ja vastuussa olevat henkilöt. Asennuksen jälkeisen käyttöönoton aikana varmistetaan mm. instrumenttien kalibrointi ja konfigurointi, kenttälaitteiden toiminta, lähtöjen/tulojen oikeellisuus sekä väylien toiminta. Mikäli asennus ei vastaa alkuperäistä suunnitelmaa, on tärkeää päivittää muutosta koskeva dokumentaatio ”kuten rakennettu” -tilaan. Käyttöönottotoimenpiteet valmistelevat turva-automaatiojärjestelmän lopullista kelpuutusta varten. (IEC-61511-1:2017, 81-82.)

Turvallisuuden kelpuutusta kutsutaan usein laitoshyväksyntätestiksi (SAT). Tarkoituksena on varmistaa, että turva-automaatiojärjestelmä toimii todellisessa ympäristössään kuten turvallisuusvaatimusten erittelyssä on määritetty. Kelpuutusprosessi kattaa koko järjestelmän toiminnan. Kaikki saatujen tulosten poikkeamat odotettuihin verrattuna tulee dokumentoida ja tarkastella tapauskohtaisesti. Poikkeamatilanteissa on päätettävä, onko toimenpiteenä palattava takaisin suunnittelun elinkaaren aikaisempaan osaan. Kelpuutusprosessin jälkeen kaikki testauksessa käytettävät ohitukset on poistettava, ja laitteisto palautetaan normaaliin tilaan. Kun kaikki toimenpiteet on suoritettu, laitos siirtyy elinkaaressaan käyttövaiheeseen. (IEC-61511-1:2017, 82-85.)

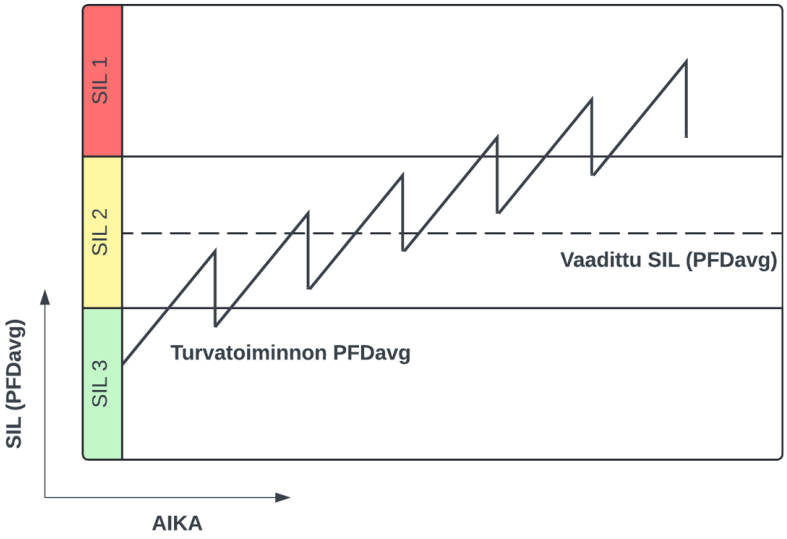
6.7 Vaihe 6: Käyttö ja ylläpito

Käyttövaiheessa operaattoreiden tulee olla perillä turva-automaatiojärjestelmän tehtävästä ja toimintaperiaatteista. Tämä sisältää operaattoreiden koulutuksen, jolla varmistetaan käyttäjien ymmärrys prosessin ja järjestelmien hallinnan suhteen. Kuten aikaisemmissakin elinkaaren

vaiheissa, myös käytön aikaiset poikkeamat järjestelmän todellisen ja odotetun käyttäytymisen välillä tulee analysoida. Lukitusten ohittaminen on aina valtuutettava ja dokumentoitava. (IEC-61511-1:2017, 86.)

Turvatoimintoja tulee koestaa määräaikaisesti järjestelmässä mahdollisesti piilevien havaitsemattomien vikojen paljastamiseksi. Testaus tulee suorittaa turvallisuusvaatimusten erittelyn mukaisesti turvatoiminnon jokaiselle komponentille. Komponenttien testausvälin ei tarvitse olla sama, sillä esimerkiksi laitevalmistajien ohjeistukset voivat vaikuttaa testausvälin määräytymiseen. Määräaikaistestausten lisäksi turva-automaatiojärjestelmä on tarkastettava jaksoittain silmämääräisesti kulumien, rikkoutumisten ja valtuuttamattomien muutosten varalta. (SFS EN-61511-1:2017, 89)

Middlerin (2019) mukaan on virheellistä olettaa, että määräaikaistestaus paljastaisi kaikki järjestelmässä piilevät viat. Mikäli näin olisi, turvatoiminnon ja laitteiston katsottaisi pysyvän aina uuden veroisena. Määräaikaistestauksen kattavuus (PTC, Proof Test Coverage) on välillä 0-100 % esitetty arvo, jolla kuvataan testausproseduurin kattavuutta koko turvatoiminnon osalta. Epätäydellisen kattavuuden seurauksena osa vioista jää aina paljastumatta, joten turvatoiminnon vikaantumistodennäköisyys kasvaa ajan funktiona (kts. kuvio 13). Mitä pienempi kattavuus, sitä nopeammin turvatoiminto saavuttaa rajan, jonka jälkeen sen eheystaso ei enää täytä asetettuja vaatimuksia. Tämän jälkeen komponentteja on uusittava. (Proof Testing: Overcoming Optimistic Design Assumptions 2019.)



Kuvio 13: PFDavg ajan funktiona (Middler 2019, muokattu)

6.8 Vaihe 7: Muutosten hallinta

Ennen kuin muutoksia turvajärjestelmään voidaan tehdä, tulee tekijällä olla selkeät menettelytavat muutosten hallintaan. Muutokset syytä suunnitella, katselmoida ja dokumentoida sekä niiden vaikutus turvajärjestelmään että turvallisuuden eheyteen tulee tarkastaa. Kaiken muutoksen kohteena olevan turvajärjestelmän dokumentaation tulee päivittyä. Käytännössä muutosta tehdessä voidaan joutua palaamaan elinkaaren vaiheissa taaksepäin aina riskiarviointiin asti. Muutosten dokumentoinnilla ylläpidetään seurattavuutta, ja osoitetaan toimintatapojen noudattavan systemaattista lähestymistapaa. (SFS-EN 61511-1:2017, 91; Should Functional Safety impact assessments be undertaken when changing a SIS? 2018.)

Pienetkin muutokset ja niiden vaikutukset toiminnalliseen turvallisuuteen tulisi aina arvioida asiantuntijoiden toimesta. Esimerkiksi käyttöliittymään tehtyjä muutoksia ei usein nähdä kriittisinä, mutta niiden mahdollinen vaikutus, esimerkiksi operaattorin vasteajan aleneminen hätätilanteessa, voi heikentää kyseistä suojauskerrosta. Tukesin mukaan muutokset on kirjattava ainakin alla luetelluissa tilanteissa. (Should Functional Safety impact assessments be undertaken when changing a SIS 2018; Turva-automaatio prosessiteollisuudessa 2021.)

- Turvatoiminnon muokkaaminen
- Laitteiden tai ohjelmistojen vaihtaminen tai muokkaaminen
- Prosessiparametrimuutokset (mitta-alueet, hälytys- ja lukitusrajat)
- Muutokset huolto- ja tarkastusväleihin
- Muutokset prosessin käyttöolosuhteissa
- Muu muutos, joka vaikuttaa laitoksen tekniseen dokumentaatioon

6.9 Vaihe 8: Käytöstä poistaminen

Turvatoiminnon käytöstä poistaminen tulee katselmoida ja toteuttaa suunnitellusti, sillä laitoksen toiminnallisen turvallisuuden eheys ei saa vaarantua missään tilanteessa. Käytöstä poistamiseen liittyvät toimenpiteet vertautuvat muutosten tekemiseen ja hallintaan, joten silloin voidaan soveltaa samoja metodeja. Toimenpiteet turvatoiminnon poistamiseksi voivat alkaa vasta, kun dokumentaatio on ajan tasalla ja toimenpide on valtuutettu. (SFS EN-61511-1:2017, 90-91)

7 Työn toteutus

7.1 Kehittämistyön aineisto

Opinnäytetyön lähtökohtana oli käytännön ongelma, jonka ratkaisemiseksi sovellettiin kehittämistyön menetelmiä, kuten toisilta oppimista ja havainnointia. Tietoperustan aineiston keruu aloitettiin noutamalla työhön liittyvät IEC-standardit SFS-Online-palvelusta. Aineistoa haettiin myös tieteellisiä artikkeleita sisältävistä tietokannoista, kuten IEEE Xploresta, josta löytyi hyvinkin sovelluskohtaisia julkaisuja. Verkkolähteistä erityisen hyödyllisiä olivat turvasertifikaatteja myöntävän Exidan julkaisemat oppaat, joiden sisältö oli avuksi oleellisten aihealueiden etsinnässä raskaista standardeista. Oppaiden ja luotettaviksi katsottavien blogitekstien ja muun materiaalin tarkastelu tarjosi perustan elinkaarimallin kokonaisuuden kuvaamiselle, sekä vaiheiden dokumentoinnin vaateiden erittelylle.

7.2 Aineiston luotettavuus ja työn eettisyys

Standardit IEC 61511 ja IEC 61508 tarjosivat luotettavan perustan työn toteuttamiselle, sillä julkaisut ovat olleet tarkan teknisen ja tieteellisen arvioinnin kohteena. Standardit toimivat koko

turvallisuuden elinkaarimallin perustana, ja niiden avulla suunnittelutyön vaatimuksenmukaisuus voidaan todentaa. Muuhun aineistoon sisältyi laaja joukko erilaisia verkkolähteitä, joiden luotettavuutta tuli arvioida. Arvioinnin kohteena olivat lähteen tuottajan organisaation tai kirjoittajan asiantuntemus, ajantasaisuus ja objektiivisuus. Vertaisarvioitujen ja kansainvälisten julkaisujen referoimista pyrittiin priorisoimaan.

Opinnäytetyössä noudatettiin JAMKin raportointiohjetta ja hyviä tieteellisiä käytäntöjä. Tämä tarkoittaa sitä, että raportointi on objektiivista ja lähdeviittaukset asianmukaisia. Standardijulkaisuiden kuvasisältöön viitatessa noudatettiin SFS-Onlinen ohjeistusta. Toimeksiantajan ja sen asiakkaiden sopimuksiin ja projekteihin liittyvät tiedot ovat salassa pidettäviä, joten arkaluontoista materiaalia ei tuoda työn yhteydessä esille. Opinnäytetyöhön ei ollut tarpeellista hakea tutkimuslupaa.

7.3 Työprosessi ja tulokset

Työn alussa toimeksiantajan TLJ-dokumentoinnin nyky- sekä tavoitetilasta tuli muodostaa käsitys. Tavoitetilan määrittämisen tukena olivat kerätty aineisto, projektien vaateet, olemassa olleet dokumenttipohjat ja yrityksen asiantuntijoiden kanssa käydyt keskustelut. Näiden havainnoinnin pohjalta voitiin määrittää elinkaarimallin vaiheiden mukaisesti TLJ-dokumenttipaketin rakenne (kts. taulukko 11). Lihavoidulla tekstillä merkatut dokumentit ovat opinnäytetyön tuloksia, jotka sisällytetään raportin liitteiksi. Muut taulukossa listatut pohjat ovat joko kehitteillä tai löytyivät jo toimeksiantajalta, jolloin ne voitiin sisällyttää osaksi dokumenttipakettia pienillä muokkauksilla. Kaikki dokumentit ovat salassa pidettäviä, joten liitteet on piilotettu työn julkisesta versiosta.

Projektin vaihe	Dokumentaatio
Vaihe 0: Esisuunnittelu	**Toiminnallisen turvallisuuden hallintasuunnitelma**
Vaihe 1: Riskien arviointi	**HAZOP**
Vaihe 2: Riskinvähennystoimenpiteiden kohdentaminen suojauskerroksille ja eheystaso	**SIL-määrittely**
Vaihe 3: Turvatoimintojen turvallisuusvaatimusten määrittely ja eheystason todennus	**Turva-automaatiojärjestelmän vaatimusmäärittely (SRS)**
Vaihe 4: Suunnittelu ja toteutus	SIL-verifiointilaskelmat SIS FAT -testausprotokollat ja -pöytäkirja
Vaihe 5: Asennus, käyttöönotto ja validointi	**Tarkastuspöytäkirja** SIS SAT -testausprotokollat ja -pöytäkirja
Vaihe 6: Käyttö ja ylläpito	Määräaikaiskoestusuunnitelma Kunnossapitosuunnitelma Tilapäinen lukituksen muutos
Vaihe 7: Muutosten hallinta	Turvatoiminnon muutoksen hallinta
Vaihe 8: Käytöstä poistaminen	Turvatoiminnon käytöstä poistaminen
Toiminnallisen turvallisuuden arviointi	Turva-automaatiojärjestelmän todennussuunnitelma

Taulukko 11: TLJ-elinkaarimallin dokumentaatio

Opinnäytetyöprosessin aikana toimeksiantajan asiakkaille toteutettiin useita projekteja, jotka liittyivät elinkaarimallin eri vaiheiden dokumentointiin ja ja toiminnallisen turvallisuuden todentamiseen. Projektien myötä oli luotava uudet dokumenttipohjat SIL-tarkastelua, turvallisuusvaatimusten määrittelyä ja turvatoimintojen tarkastusta varten. Työhön sisältyi myös turvatoimintojen verifiointilaskelmat ja arkkitehtuurianalyysit. Lisäksi oli päivitettävä ja revisioitava muuta suunnitteludokumentaatiota, kuten logiikkapiirikaavioita.

Dokumenteista saatu palaute oli tärkeää projektin etenemisen ja sisällön iteroimisen kannalta. Monipuolisissa turvallisuuteen liittyvien järjestelmien suunnittelutöissä toimineet henkilöt osasivat kohdistaa palautteen tehokkaasti. Aiheesta käydyt keskustelut herättivät hyviä ajatuksia dokumentaation sisällön sekä yleisesti toiminnallisen turvallisuuden hallinnan suhteen.

Dokumentaation ulkoasun ja sisällön selkeyden säilyttäminen oli tärkeä näkökulma kaikkien mielestä. Käytettävyyden edistämiseksi määrättyihin kohtiiin dokumentteja lisättiin kommentteja, jotka selittävät auki hankaliä termejä ja lyhenteitä. Sisällön laajuus antoi työprosessin aikana pohdittavaa; onko kaikkia mahdollisia standardien vaateita tarpeellista eritellä pohjiin? Esimerkiksi turvatoimintojen vaatimusten erittelyn osalta standardi IEC 61511 luettelee mittavan määrän dokumentoitavia kohtia, jotka eivät kuitenkaan ole aina relevantteja projektin kannalta. Ongelmaan etsittiin ratkaisua keskusteluissa, ja päädyttiin kehittämään suppeampi erittely kattavan vaihtoehdoksi.

Turva-automaatiojärjestelmän hallintasuunnitelmapohjaan koottiin elinkaaren kaikki vaiheet. Dokumenttiin voidaan kirjata ja seurata vaiheisiin kuuluvia aktiviteetteja, mikä auttaa kokonaisuuden etenemisen seurannassa. Vaiheen kohdalle merkataan siihen liittyvät dokumentit revisionumeroineen. Myös projektiorganisaation kuvaus ja osallistujien kompetenssien tarkastelu sisällytettiin osaksi hallintasuunnitelmaa.

Riskianalyysissä ja SIL-tarkastelussa käytettävien metodien valinnassa ei päädytty täysin kvantitatiivisiin menetelmiin tai LOPA:n käyttöön. Suojauskerroksille ja niiden riskinvähennyskyvylle on varsin hankala asettaa luotettavia numeraalisia arvoja, jos ei haluta tukeutua geneerisiin olettamuksiin suojauskerrosten suorituskyvystä. Riskien arviointia varten luotiin Excel-pohjainen HAZOP-dokumentti, johon yhdistettiin ALARP-periaatteen mukainen riskimatriisi. Riskimatriisia voidaan soveltaa kvantitatiivisesti, kvalitatiivisesti tai niiden yhdistelmällä, mikäli se nähdään soveltuvaksi projektin kannalta. SIL-tarkastelun metodiksi valikoitui kalibroitu riskigraafi. Näiden menetelmien yhdistelmillä on mahdollista selvittää tarve turvatoiminnolle, sen eheysvaade sekä jäännösriskin taso. Soveltaessa on tärkeää, että niin ALARP-matriisin kuin kalibroidun riskigraafin parametrit kalibroidaan laitoksen riskikriteerien mukaisesti.

Kun dokumenttipaketin sisältö on valmis, se jaetaan yrityksen sisäisen järjestelmän kautta asiantuntijoiden käytettäväksi. Paketti antaa valmiudet turva-automaatiojärjestelmän elinkaaren hallintaan, ja se koostuu työn aikana tuotetuista että vanhoista, mutta uudistetuista

dokumenttipohjista. Julkaisu tehdään sisäisen katselmoinnin jälkeen, joka on yksi osa tulosten arviointia.

8 Pohdinta

8.1 Saavutettiinko tavoitteet?

Työn päätavoitteena oli tuottaa toimeksiantaja PCS-Engineering Oy:lle dokumenttipohjia turva-automaation elinkaarimallin mukaisen suunnittelun tueksi. Työn tavoitteisiin päästiin osittain. Tuotettu dokumenttipaketti ei ole nykytilassaan täysin kattava, sillä kaikkia suunnittelu- ja käyttövaiheen raporttipohjia ei ehditty tekemään. Sisällössä voi esiintyä muitakin puutteita, jotka tullaan havaitsemaan käytön aikana. Voidaan kuitenkin uskoa, että dokumenttipaketti jo nykyisessä muodossaan mahdollistaa TLJ-projektin hallinnan osittain. Itselleni työprosessin läpikäynti antoi runsaasti ymmärrystä aiheesta ja resursseja tulevien projektien toteuttamiselle.

Toiminnallisen turvallisuuden kenttä on erittäin laaja, eikä vaatimuksenmukaisuuden todentamiseen ole yhtä oikeaa tapaa. Tämä aiheutti haasteensa työn aiheen rajaamisen suhteen. Esimerkiksi useat eri metodit riskien arviointiin osoittavat, että samaan lopputulokseen voidaan päästä monin eri keinoin. On siis tiimin päätettävissä, halutaanko analyysi toteuttaa poikkeamatarkastelulla, solmukeanalyysillä, tai jollain muulla menetelmällä. Menetelmien valinnasta kannattaa käydä keskustelua projektikohtaisesti ottaen huomioon kohteen tyyppi, sekä riskianalyysiin osallistuvan työryhmän aiemmat kokemukset ja havainnot eri menetelmistä. Yrityksessä oli eniten kokemusta HAZOP- ja riskigraafimetodien käyttämisestä, joten niiden sisällyttäminen dokumenttipohjiin oli luontevinta.

8.2 Suunnitelmat jatkokehittämiselle

Jatkokehittämisen suhteen on keskityttävä ensimmäiseksi puuttuvien dokumenttipohjien tuottamiseen. Lisäksi jokaisesta pohjasta olisi aiheellista muokata suomenkielisten rinnalle myös englanninkieliset versiot. Myös dokumenttien ulkoasua olisi paranneltava paikoitellen visuaalisesti laadukkaan ilmeen eteen. Riskiarvionnin osalta kvantifiointi kokonaan jätettiin pois nykyisestä

arviointipohjasta. Mikäli tarkemmalle riskianalyysille ja suojauskerrosten vaikutusten arvioimiselle nähdään tarvetta tulevaisuudessa, voidaan se sisällyttää osaksi dokumentaatiota. Siinä tapauksessa olisi paras tuottaa perusteellinen suojauskerrosanalyysipohja riskinarvioinnin ja eheysvaatimusten määrittämisen tueksi. SIL-verifiointilaskelmapohjan jatkokehittäminen on myös työlistalla. Dokumentaation ja toiminnallisen turvallisuuden hallinnan kehittämistyö tulee siis jatkumaan opinnäytetyöprosessin jälkeen.

Lähteet

Börcsök, J. N.d. Comparison of PFD calculation. Viitattu 12.5.2024. Engineering Institute of Technology. https://iceweb.eit.edu.au/sis/Hima/HIMA%20%20Comparison%20of%20PFD%20Calculation.pdf.

Chastain-Knight, D. & Butz, R. & Donaldson, W. N.d. Functional Safety Management Planning. Opas Exida.com -sivustolla. Viitattu 19.1.2024. https://www.exida.com/articles/Functional-Safety-Management-Planning.pdf.

Control & Safety: Inegrate or Segregate?. 2019. Yokogawa Corporation of America. Viitattu 3.4.2024. https://web-material3.yokogawa.com/2/28519/files/Control%20and%20Safety%20-%20Integrate%20or%20Segregate.pdf.

Crawley, F & Tyler, B. 2015. HAZOP: Guide to Best Practice. Elsevier Ltd. Viitattu 20.4.2024. https://hsseworld.com/wp-content/uploads/2021/01/HAZOP-GUIDE-TO-BEST-PRACTICE-IChemE-THIRD-EDITION.pdf.

Creech, G. 2014. IEC 61508 Systematic Capability. Institute of measurement and control. Viitattu 2.3.2024. https://journals.sagepub.com/doi/pdf/10.1177/0020294014528895.

Gandy, S. 2015. Safety Requirements Specifications (SRS): The Good and the Bad. Blogiteksti exida.com -sivustolla. Viitattu 10.2.2024. https://www.exida.com/blog/safety-requirements-specifications-srs-the-good-and-the-bad.

Heelems, L. & Fijan, A. & Prins, A. & Top, T. A Practical Approach to SRS – Safety Requirement Specification. 2021. NEN:n tuottama opas. Viitattu 25.3.2024. https://www.nen.nl/media/PDFjes/SIL_Platform_-_Brochure_Safety_Requirement_Specification_2021.pdf.

IEC/TR 61508-0. 2011, Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0: Toiminnallinen turvallisuus ja IEC 61508. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024. https://janet.finna.fi/.

Kelechava, B. 2017. ISO Type A-B-C Structure for Machinery Standards. Blogiteksti blog.ansi.org -sivustolla. Viitattu 20.2.2024. https://blog.ansi.org/2017/10/iso-type-abc-structure-machinery-standards-ansi-b11/

Keswick, J. 2024. Safety instrumented systems. E-kirja. Julkaistu eFunctionalSafety-sivustolla. Viitattu 18.3.2024. https://efunctionalsafety.com/new-safety-instrumented-system-ebook/.

Key Parameters. N.d. Blogi, safetyandsis.com. Viitattu 1.4.2024. https://safetyandsis.com/parameters/.

L 2005/390. Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta. Viitattu 18.3.2024. https://www.finlex.fi/fi/laki/ajantasa/2005/20050390.

L 2016/1144. Painelaitelaki. Viitattu 18.3.2024. https://www.finlex.fi/fi/laki/ajantasa/2016/20161144.

Marszal, E. 2018. Comparison of Voting Arrangements in SIS. Opas kenexis.com -sivustolla. Viitattu 12.4. 2024. https://www.kenexis.com/wp-content/uploads/2018/11/Comparison-of-2oo3-voting-and-2oo2-voting-1.pdf.

Middler, N. 2019. Proof Testing: Overcoming Optimistic Design Assumptions. LinkedIn-artikkeli. Viitattu 4.5.2024. https://www.linkedin.com/pulse/safety-instrumented-function-sif-proof-test-interval-amit-singh/.

Neimala, A. 2023. EU panostaa nyt standardointiin – tavoitteena vahvistaa kilpailukykyä, sisämarkkinoita ja vihreää siirtymää. Työ- ja elinkeinoministeriö. Viitattu 13.4.2024. https://valtioneuvosto.fi/-//1410877/eu-panostaa-nyt-standardointiin-tavoitteena-vahvistaa-kilpailukykya-sisamarkkinoita-ja-vihreaa-siirtymaa.

Painelaitteiden prosessiturvallisuuden todentaminen. N.d. Dekran kotisivusto. Viitattu 26.4.2024. https://www.dekra.fi/fi/turvallisuuteen-liittyvien-jarjestelmien-arvioinnit/.

PCS-Engineering Oy. 2024. Yrityksen kotisivut. Viitattu 28.3.2024. https://pcs-engineering.fi/.

Safety Instrumented Function Verification: The Three Barriers. 2017. Komiteamietintö. Viitattu 11.2.2024. https://www.exida.com/articles/Three-Barriers.pdf.

SFS-EN 61508-2. 2011, Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024. https://janet.finna.fi/.

SFS-EN 61508-6. 2011, Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024. https://janet.finna.fi/.

SFS-EN 61511-1:2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024 https://janet.finna.fi/.

SFS-EN 61511-2:2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 2: Ohjeita standardin IEC 61511-1:2016 soveltamiseen. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024. https://janet.finna.fi/.

SFS-EN 61511-3:2017. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 3: Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiseen. Suomen Standardoimisliitto SFS. Viitattu 15.3.2024. https://janet.finna.fi/.

SIL Determination Techniques Report. Macza, M. ACM Facility Safety. Viitattu 29.4.2024. https://iceweb.eit.edu.au/sis/ACMWhite-PaperSILDeterminationTechniquesReportA4.pdf.

Standardi, sertifikaatti ja CE-merkintä – tunne erot ja yhtäläisyydet. 2023. SFS Suomen standardit Ry. Viitattu 26.4.2024. https://sfs.fi/standardi-sertifikaatti-ja-ce-merkinta/.

The Influence of Standards on the Nordic Economies. 2018. Menon Economics. Viitattu 13.4.2024. https://sfs.fi/wp-content/uploads/2020/10/Nordic_market_study_-_influence_of_standards_FINAL.pdf.

The Key Variables Needed for PFDavg Calculation. 2018. Exida. Viitattu 30.4.2024. https://www.exida.com/Resources/Whitepapers/the-key-variables-needed-for-pfdavg-calculation.

The Use of Bow Ties in Process Safety Auditing. 2016. Institution of Chemical Engineers. Viitattu 4.5.2024. https://www.icheme.org/media/11749/hazards-26-paper-12-the-use-of-bowtie-analysis-in-process-safety-auditing.pdf.

Torres-Echeverria, A. 2014. On the Use of LOPA and Risk Graphs for SIL determination. Texas A&M University. Viitattu 20.4.2024. https://pscfiles.tamu.edu/symposia/2014/abstracts/095_Alejandro%20Torres%20Echevarria.pdf.

Turva-automaatio prosessiteollisuudessa. 2021. Tukesin opas turva-automaation elinkaaren hallintaan. Viitattu 15.1.2024. https://tukes.fi/turva-automaatio-prosessiteollisuudessa.

Liitteet

Liite 1. Turvallisuussuunnitelma

Liite 2. HAZOP

Liite 3. SIL-tarkastelu

Liite 4. Turvallisuusvaatimusten erittely (SRS)

Liite 5. SIF-testauspöytäkirjat